UNIVERSIDAD POLITECNICA SALESIANA

FACULTAD DE INGENIERIA
SEDE QUITO – CAMPUS SUR

CARRERA DE INGENIERIA DE SISTEMAS
MENCION TELEMATICA

DISEÑO E IMPLEMENTACIÓN DE SEGURIDADES EN LA RED DE DATOS DE LA PLANTA CENTRAL DEL MINISTERIO DE EDUCACIÓN Y CULTURA DEL ECUADOR, APLICANDO LA METODOLOGÍA OSSTMM (OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL); Y, CREACIÓN DE POLÍTICAS DE SEGURIDAD MÍNIMAS PARA LAS SUBSECRETARÍAS, DIRECCIONES PROVINCIALES Y CANTONALES DE EDUCACIÓN.

TESIS PREVIA A LA OBTENCION DEL TITULO DE INGENIERO DE SISTEMAS

EDGAR FABRICIO ZAVALA VELA

DIRECTOR: ING. JOSE LUIS AGUAYO

QUITO, FEBRERO 2010

En el lomo texto vertical

DEDICATORIA

Todo el esfuerzo realizado en la elaboración del presente trabajo se lo dedico a la persona que me hace sentir la persona más feliz del mundo Kerlly Sánchez Garófalo, gracias por ser parte de mi vida.

AGRADECIMIENTO

A mi amada esposa ya que su apoyo ha sido fundamental en el desarrollo del presente trabajo, gracias Gordita.

A mi Madre quien me inspiro para alcanzar mis metas, por enseñarme que todo esfuerzo siempre tiene grandes recompensas.

A mi tutor que su tiempo y guía nos permitieron caminar en este largo proceso que dio como resultado el presente trabajo.

INDICE

CAPITULO 1

CONCEPTOS DE SEGURIDAD INFORMÁTICA Y POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

1.1 CONCEPTOS DE SEGURIDAD INFORMÁTICA

Cuando nos referimos a seguridad informática hay que estar muy claros que no es posible hablar de seguridad absoluta, ya que el elemento de riesgo está siempre presente, independiente de las medidas que se tomen en la organización; por lo que debemos hablar de niveles de seguridad el mismo que está asociado a la certeza, falta de riesgo o contingencia.

Por lo anteriormente mencionado entenderemos que la seguridad informática es un conjunto de técnicas encaminadas a obtener altos niveles de seguridad en los sistemas informáticos.

La **seguridad informática** consiste en asegurar que los recursos del sistema de información (material informático o programas) 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.[1]

Todos los sistemas computacionales, no importa cuán sofisticados sean sus sistemas de seguridad, están permanentemente expuestos a sufrir un error o una alteración maliciosa intencional. Como estos eventos es casi imposible evitarlos, el encargado de la informática siempre debe tener planes de contingencia para enfrentar tres tipos de instancias de alguna falla: La **Prevención** para minimizar la posibilidad de ocurrencia de alguna falla, la **Detección** oportuna cuando la falla haya ocurrido, y la **Corrección** para asegurar el más rápido regreso a la operación normal de los sistemas[2].

1.2 CUAL PUEDE SER EL VALOR DE LOS DATOS.

La intangibilidad de los datos hace que en la mayoría de las organizaciones no se le dé prioridad a la implementación de medidas de seguridad, ya que se considera como un gasto que no produce; este criterio ha hecho que no se tomen las debidas precauciones de seguridad lo que en muchos de los casos el no implementar sistemas de seguridad, ha conllevado a tener pérdidas superiores a los costos que implicaba el costo de la implementación.

Por otra parte hay que estar muy claros que toda organización depende de los datos que conforman la misma por lo que el valor de los datos es un factor fundamental para la continuidad de las actividades diarias, cabe indicar que el valor de los datos difiere dependiendo el servicio que brinda la misma.

---

1 Wikipedia, Seguridad Informática, http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

2 Oscar Andrés Schmitz, Conceptos básicos de Seguridad Informática, 09/06/2008, http://manuelgross.bligoo.com/content/view/207132/Conceptos-basicos-de-Seguridad-Informatica.html

Por lo anteriormente expuesto es importante establecer el valor de la información, una forma de ponerle valor a los datos puede ser considerar el costo hora de trabajo de los empleados por el número de horas que se tardaría en recuperar la infraestructura y sistemas que permitan a los funcionarios laborar con normalidad.

1.3 SEGURIDAD GLOBAL.

Como seguridad global comprenderemos la protección de todos los recursos de la Unidad de Tecnología Informática y Comunicaciones, cabe indicar que aunque por mas que se protejan los recursos y componentes que conforman la red de voz y datos, se debe tomar en cuenta el recurso humano que maneja los sistemas y la información, por lo que es fundamental socializar y concienciar al personal en seguir las normas de seguridad implementadas.

Los recursos que involucramos en la seguridad global son los siguientes:

- Control de Acceso al Data Center y a la UTIC
- Infraestructura de cableado estructurado
- Equipos Activos de Comunicación y Seguridad
- Servidores, Estaciones de trabajo, Computadoras portátiles y sistemas de información de la UTIC
- Funcionarios de la UTIC

1.4 IMPACTO EN LA ORGANIZACIÓN

Toda implementación dentro de la organización toma su resistencia por parte de los funcionarios ya que implica aprender o cumplir nuevos procesos que se deben realizar y más aun cuando estos son considerados complejos o que conllevan a realizar tareas extras.

Es este caso al implementar normas y políticas de seguridad informática los funcionarios deben definir claves con mayor complejidad por ejemplo: (que contengan al menos una mayúscula, una minúscula, un numero y mínimo 6

caracteres), esto es considerado por algunos funcionarios como burocracia y trabas para poder realizar el trabajo.

Por tal motivo es vital involucrar al personal en el proceso de implementación y siempre recalcar los beneficios de las seguridades implementadas una de ellas puede ser el establecer responsabilidades ante algún problema ocasionado dentro de la organización, entre otros beneficios.

1.5 QUE SON LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA

"Una política de seguridad informática es una 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."[3]

Las políticas de seguridad son las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños.

De acuerdo a los conceptos antes mencionados podemos decir que una política de seguridad informática requiere del compromiso de todos quienes conforman la organización, además que se describe la manera de gestionar nuestra infraestructura, aplicaciones y servicios los cuales deseamos proteger.

1.6 ELEMENTOS DE UNA POLÍTICA DE SEGURIDAD INFORMÁTICA

3 SECRETARIA DE LA FUNCION PUBLICA, *Manual de Seguridades en Redes*, 1.0, Argentina-1998, p. 16

Una política de seguridad informática permite definir decisiones que se toman en relación con la seguridad. Por tanto es recomendable que cada uno de los integrantes de la organización forme parte para lograr una visión conjunta de lo que se considera importante. Para lo cual las políticas de seguridad informática deben considerar los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica. Es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Invitación que debe concluir en una posición.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que cobija el alcance de la política.
- Definición de violaciones y de las consecuencias del no cumplimiento de la política.
- Responsabilidades de los usuarios con respecto a la información a la que ella tiene acceso.[4]

Estos elementos permitirán que las políticas de seguridad informática sean una guía para realizar los procesos, tareas y actividades que garanticen un nivel mínimo de seguridad. Además es muy importante indicar que el lenguaje utilizado debe ser explicito y simple el mismo que permita una comprensión clara para todos los funcionarios del Ministerio de Educación.

Por otro lado hay que considerar que las políticas de seguridad informática son un documento normativo de la organización, el mismo que debe seguir un proceso de actualización periódico sujeto a los cambios organizacionales relevantes: (aumento del recurso humano, infraestructura tecnológica, implementación de sistemas de información entre otros).

1.7 ALGUNOS PARÁMETROS PARA ESTABLECER POLÍTICAS DE SEGURIDAD

4 SECRETARIA DE LA FUNCION PUBLICA, *Manual de Seguridades en Redes*, 1.0, Argentina - 1998, p. 16

Para fortalecer nuestras políticas de seguridad informática mencionaremos aspectos generales recomendados.

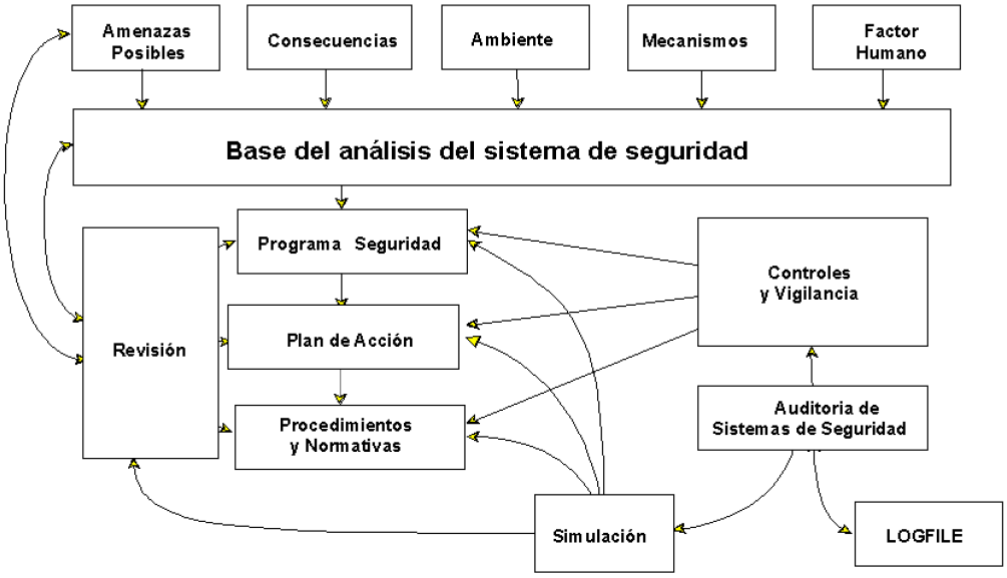
- Considere efectuar un ejercicio de análisis de riesgos informático, a través del cual valore sus activos, el cual le permitirá afinar las PSI de su organización.
- Involucre a las áreas propietarias de los recursos o servicios, pues ellos poseen la experiencia y son fuente principal para establecer el alcance y las definiciones de violaciones a la PSI.
- Comunique a todo el personal involucrado en el desarrollo de las PSI, los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.
- Recuerde que es necesario identificar quién tiene la autoridad para tomar decisiones, pues son ellos los responsables de salvaguardar los activos críticos de la funcionalidad de su área u organización.
- Desarrolle un proceso de monitoreo periódico de las directrices en el hacer de la organización, que permita una actualización oportuna de las mismas.[5]

Los parámetros anteriormente expuestos son fundamentales para la implementación de las políticas de seguridad informática ya que las autoridades juegan un papel fundamental en la toma la decisión y por supuesto el personal del ministerio en el desarrollo y aplicación de las mismas.

1.8 COMO REALIZAR EL ANÁLISIS PARA LLEVAR A CABO UN SISTEMA DE SEGURIDAD INFORMÁTICA

5 SECRETARIA DE LA FUNCION PUBLICA, *Manual de Seguridades en Redes*, 1.0, Argentina - 1998, p. 17

Diagrama para el análisis de un sistema de seguridad



Fuente: Secretaria de la Función Pública de Argentina, Seguridad en Redes, 1998

Tal como puede visualizarse, en el gráfico están plasmados todos los elementos que intervienen para el estudio de una política de seguridad.
Se comienza realizando una evaluación del **factor humano** interviniente - teniendo en cuenta que éste es el punto más vulnerable en toda la cadena de seguridad -, de los **mecanismos** con que se cuentan para llevar a cabo los procesos necesarios (mecanismos técnicos, físicos ó lógicos), luego, el **medio ambiente** en que se desempeña el sistema, las consecuencias que puede traer aparejado defectos en la seguridad (pérdidas físicas, pérdidas económicas, en la imagen de la organización, etc.), y cuáles son las **amenazas posibles**.
Una vez evaluado todo lo anterior, se origina un **programa de seguridad,** que involucra los pasos a tomar para poder asegurar el umbral de seguridad que se desea.
Luego, se pasa al **plan de acción**, que es cómo se va a llevar a cabo el programa de seguridad. Finalmente, se redactan los **procedimientos y normas** que permiten llegar a buen destino.
Con el propósito de asegurar el cumplimiento de todo lo anterior, se **realizan los controles y la vigilancia** que aseguran el fiel cumplimiento de los tres puntos antepuestos. Para asegurar un marco efectivo, se realizan auditorías a los controles y a los archivos **logísticos** que se generen en los procesos implementados (de nada vale tener archivos logísticos si nunca se los analizan o se los analizan cuando ya ha ocurrido un problema).
Con el objeto de confirmar el buen funcionamiento de lo creado, se procede a **simular** eventos que atenten contra la seguridad del

sistema. Como el proceso de seguridad es un proceso dinámico, es necesario realizar **revisiones** al programa de seguridad, al plan de acción y a los procedimientos y normas. Estas revisiones, tendrán efecto sobre los puntos tratados en el primer párrafo y, de esta manera, el proceso se vuelve a repetir.[6]

1.9 ¿POR QUÉ LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA GENERALMENTE NO CONSIGUEN IMPLANTARSE?

Actualmente en la mayoría de las organizaciones se realizan grandes esfuerzos para definir sus políticas y normas de seguridad, concretándolas en documentos que orienten las acciones de las mismas, con relativo éxito.

Lo difícil y el punto fundamental para implementar un sistema de seguridad informático es convencer a las autoridades de los problemas que acarrearíamos si no se implementa dicho sistema.

La falta de apoyo por parte de autoridades ha llevado a que muchas organizaciones, se encuentren expuestas a graves problemas de seguridad que, en la mayoría de los casos, lleva a comprometer su información.

En nuestro caso la Unidad de Tecnología Informática y Comunicaciones ha mantenido varias reuniones con las autoridades del Ministerio de Educación en las que se ha manifestado la necesidad de implementar PSI, estas reuniones han hecho posible que la UTIC elabore las PSI y sean remitidas a las autoridades para su revisión y aprobación. Cabe indicar que esta solicitud se ha enviado varias veces sin tener hasta el momento una respuesta favorable a nuestra solicitud.

6 SECRETARIA DE LA FUNCION PUBLICA, *Manual de Seguridades en Redes*, 1.0, Argentina - 1998, p. 17

1.10 LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA COMO BASE DE LA ADMINISTRACIÓN DE LA SEGURIDAD INTEGRAL.

> Las políticas de seguridad informática conforman el conjunto de lineamientos que una organización debe seguir para asegurar la confiabilidad de sus sistemas. En razón de lo anterior, son parte del engranaje del sistema de seguridad que la organización posee para salvaguardar sus activos. Las PSI constituyen las alarmas y compromisos compartidos en la organización, que le permiten actuar proactivamente ante situaciones que comprometan su integridad. Por tanto, deben constituir un proceso continuo y retroalimentado que observe la concientización, los métodos de acceso a la información, el monitoreo de cumplimiento y la renovación, aceptación de las directrices y estrategia de implantación, que lleven a una formulación de directivas institucionales que logren aceptación general.[7]

1.11 AMENAZAS Y RIESGOS PARA LA SEGURIDAD

La idea de realizar este tema es proteger toda la información que reposa en el Data Center del Ministerio de Educación del Ecuador apegados a la metodología abierta OSSTMM, con estos antecedentes se tomara como amenazas y riesgos las debilidades de las secciones correspondientes a Seguridad Física en cual se revisara los puntos de acceso, cobertura del sistema de monitoreo, respuestas de alarmas y revisión del entorno; Seguridad de la Información donde se busca proteger la integridad de la información y los controles de privacidad con los que cuenta; y la Seguridad en las Tecnologías de la Información donde se identificara la configuración de seguridad, revisión de los sistemas de protección contra intrusos, sondeo de red, identificación de servicios y sistemas, pruebas de control de acceso, descifrado de contraseñas y revisión de la política de seguridad.

Por lo anteriormente expuesto se considera una amenaza o riesgo toda persona que se dedique a delinquir ya sea de forma física o tecnológica, la infraestructura de servicios básicos instalada y los posibles desastres naturales de la región, además hay que tener presente que es fundamental

7 SECRETARIA DE LA FUNCION PUBLICA, *Manual de Seguridades en Redes*, 1.0, Argentina - 1998, p. 20

que el todo el personal de la organización sepa y cumpla las políticas de seguridad propuestas.

En general una amenaza o riego se puede ocasionar:

- Cuando se comenten errores por parte del recurso humano de la organización considerando de poco impacto y modificable
- Acceso indebido a los datos
- La utilización de medios de almacenamiento en equipos con información critica
- Modificar o copiar sin autorización aplicaciones o sistemas
- El Hacker el mayor riesgo existente, personaje que intenta acceder a los sistemas para demostrar que las medidas de seguridad implementadas por la organización objetivo son vulnerables.

En definitiva, toda amenaza que logre vulnerar nuestras medidas de seguridad puede llegar a afectar los datos, en las personas, en los programas, sistemas o aplicaciones, en los equipos y en la red.

1.12 DE QUIEN DEBEMOS PROTEGERNOS

La mayor parte de organizaciones identifican a las personas como posibles atacantes y tiene mucho sentido ya que todo ataque ya sea físico o lógico fue iniciado por una persona, pocas veces se considera una protección en caso de catástrofes naturales. A continuación se indicara algunos elementos que potencialmente pueden amenazar a nuestro sistema.

El mayor número de ataques a nuestro sistema definitivamente van a provenir de determinada persona la misma que si quebranta nuestro sistema de seguridad puede causar pérdidas incalculables.

Cuando se habla de personas se considera que todos pueden ser posibles atacantes: aquellos que fisgonean por la red de datos y no modifican o destruyen nada, y los que dañan o modifican en su favor u objetivo

propuesto. Estos dos tipos de personas pueden ser personal de la organización como personas ajenas a la organización.

Hay que tomar muy en cuenta que pocas veces se toman medidas de seguridad sobre ataques que provienen de la propia organización, sin considerar que nadie mejor que el personal de la organización conoce mejor los sistemas y sus debilidades. Por lo general sucede que por error, falta de comunicación o desconocimiento se cause un accidente y que produzca inconvenientes en los procesos de la organización esto pueden ser (funcionario de servicios generales que corte el suministro eléctrico, administrador de base de datos que digita un comando en una base diferente y cambia la información actual, etc.); en el primer caso el funcionario no tenía acceso físico a los equipos y ni siquiera supo las implicaciones que ocasiono el corte de energía.

A continuación detallamos los más interesantes atacantes en potencia:

Crackers
Los entornos de seguridad media son un objetivo típico de los intrusos, ya sea para fisgonear, para utilizarlas como enlace hacia otras redes o simplemente por diversión. De esta forma un atacante solo ha de utilizar un escáner de seguridad contra el dominio completo y luego atacar mediante un simple *exploit* los equipos que presentan vulnerabilidades.

Amenazas lógicas
Bajo la etiqueta de ‘amenazas lógicas’ se descubre todo tipo de programas que de una forma u otra pueden dañar al sistema, creado de forma intencionada para ello (*software* malicioso, también conocido como *malware*) o simplemente por error (*bugs* o agujeros).

Software incorrecto
Las amenazas más habituales a un sistema provienen de errores cometidos de forma involuntaria por los programadores de sistemas o de aplicaciones.
A estos errores de programación se les denomina *bugs*, y a los programas utilizados para aprovechar uno de estos fallos y atacar al sistema, *exploits*.

Herramientas de seguridad

Cualquier herramienta de seguridad representa un arma de doble filo: de la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o en la subred completa, un potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos. Herramientas como nessus, saint o satan pasan de ser útiles a ser peligrosas cuando las utilizan *crackers* que buscan información sobre las vulnerabilidades de un *host* o de una red completa.

Catástrofes
Las catástrofes (naturales o artificiales) son la amenaza menos probable contra los entornos habituales: simplemente por su ubicación geográfica, a nadie se le escapa que la probabilidad de sufrir un terremoto o una inundación que afecte a los sistemas informáticos. Sin embargo, el hecho de que las catástrofes sean amenazas poco probables no implica que contra ellas no se tomen unas medidas básicas, ya que si se produjeran generaran los mayores daños.[8]

1.13 QUE DEBEMOS PROTEGER

Algo que es indispensable para realizar un sistema de seguridad es identificar que debemos proteger para esto vamos a tomar la siguiente definición.

Los elementos de la organización que se va a proteger son : el hardware, el software y los datos.
Una vez identificado los elementos que se van a proteger detallaremos cada uno de estos:

El hardware, está considerado por todos los sistemas físicos del Data Center y de la Unidad de Tecnología Informática y Comunicaciones del Ministerio de Educación (Servidores, equipos activos de red, equipos de seguridad, equipos de comunicación, equipos de almacenamiento y respaldos, central telefónica, aires de precisión, sistema contra incendio estaciones de trabajo del personal de la UTIC).

8 BORGHELLO CRISTIAN, *Seguridad Informática sus Implicaciones e Implementación*, Argentina - 2001, p. 101

El Software son los elementos que permiten al hardware su operatividad (sistema operativo, sistemas de información y aplicaciones).

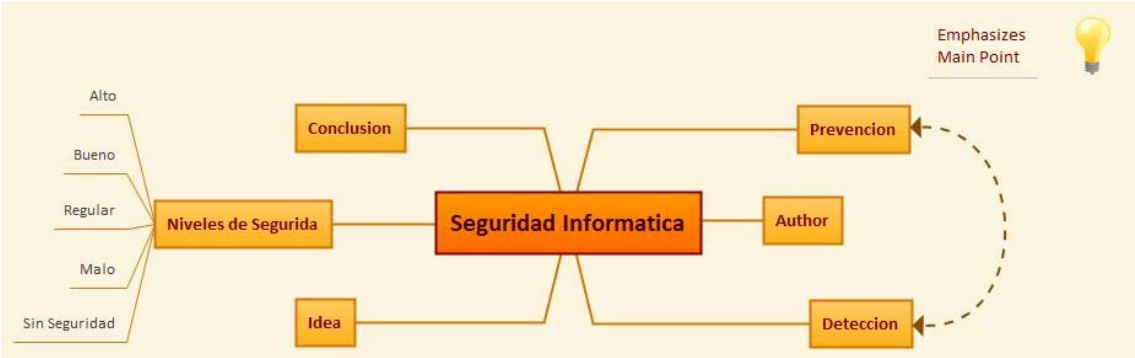
Los datos es toda la información lógica que maneja el software y el hardware (bases de datos, documentos, archivos, código fuente de los sistemas de información del Ministerio de Educación).

De los tres elementos citados el principal elemento a proteger son los datos, ya que este elemento si por alguna razón fue vulnerada, la recuperación del mismo depende de la fecha y hora del último backup con el que cuente la organización, esto no asegura que la recuperación sea del 100% ya que todo dependería de los niveles de seguridad implementados. Por otro lado la parte de hardware y software estos pueden ser reemplazados o reconfigurados según sea el caso. En estos dos casos el impacto hacia la organización se verá afectado en el tiempo que se tome en el reemplazo o la configuración de la parte afectada.

CAPITULO 2
ANÁLISIS DE LA SEGURIDAD INFORMÁTICA, NIVELES DE RIESGO DE LA INFORMACIÓN INVOLUCRADA, TIPOS DE ATAQUES Y VULNERABILIDADES

2.1 ANALISIS DE LA SEGURIDAD INFORMATICA

Una vez descrito varios conceptos de seguridad informática para su análisis se puede decir que para contar con seguridad informática se debe considerar estos tres elementos Prevención, Detección y Corrección; El primer elemento es fundamental ya que para prevenir nos obligamos a identificar todos los posibles huecos de seguridad o vulnerabilidades existentes en nuestra organización, y con este insumo implementar medidas de seguridad y/o políticas de seguridad que protejan nuestra organización, de las medidas adoptadas dependerá la certeza y el nivel de seguridad de la organización. La Detección es otro elemento fundamental pues como se menciono en conceptos anteriores no se puede hablar de seguridad total ya que cada día se descubren nuevas vulnerabilidades o programas maliciosos que pueden afectar la seguridad informática de nuestra organización, por lo que el monitoreo y pruebas de seguridad deben realizarse de forma constante, esto permitirá mejorar y comprobar las medidas adoptadas o perfeccionar las mismas según sea el caso; Por último la Corrección es el elemento el cual va a definir cuanto tiempo se tomara poner en operativo los sistemas de la organización cuando tengan un problema ya sea en la parte de infraestructura, sistemas o programas y datos almacenados.



2.2 SEGURIDAD FÍSICA

Para tener claro la parte de seguridad física se va a tomar conceptos que se consideran importantes:

2.2.1 CONCEPTO

"La seguridad física de los sistemas informáticos consiste en *la aplicación de barreras físicas y procedimientos de control como medidas de prevención y contramedidas contra las amenazas a los recursos y la información confidencial*. "[9]

De este concepto se consigue entender que las medidas de prevención que se adopten deben proteger desde un teclado en la parte de recurso hasta una cinta de backup en la parte de información de la organización.

Si bien se menciona en el capitulo anterior que una vulnerabilidad puede ser causada por alguna catástrofe natural por el momento no será prioridad este tipo amenaza, y más bien se dará lo siguiente:

Protección del *Hardware*

El *hardware* en casi todas las organizaciones es la parte más costosa de un sistema informático, por lo que proteger su integridad es la primera medida de seguridad que se toma.

Para esto se identificara varias amenazas, sus posibles efectos y algunas soluciones.

2.2.2 ACCESO FÍSICO

La posibilidad de acceder físicamente a la infraestructura de servidores hace inútil casi todas las medidas de seguridad que se haya aplicado sobre el sistema de informático (Firewall, IPS y ACL´s):

En todo caso lo primero es garantizar la seguridad global definida en el primer capítulo.

Prevención

Para prevenir un acceso físico no autorizado, podemos implementar soluciones para todos los gustos, y también de todos los precios: desde analizadores de retina hasta videocámaras, pasando por tarjetas inteligentes o control de las llaves que abren determinada puerta.

---

9 BORGHELLO CRISTIAN, *Seguridad Informática sus Implicaciones e Implementación*, Argentina - 2001, p. 17

En el caso del Ministerio de Educación el ingreso al Data Center se lo realiza a través de una puerta con llave hay 5 personas autorizadas a ingresar el jefe la UTIC y los funcionarios del Área de Redes, Infraestructura y Seguridades cuando alguien requiere entrar lo hace acompañado de uno de los funcionarios antes mencionados.

Detección

Cuando la prevención es difícil por cualquier motivo (técnico, económico, humano. . .) es deseable que un potencial ataque sea detectado cuanto antes, para minimizar así sus efectos. Aunque en la localización del problema, generalmente los accesos físicos no autorizados, intervienen medios técnicos, como cámaras de vigilancia de circuito cerrado o alarmas.

2.3 TIPOS DE DESASTRES

La información sobre desastres que pueden afectar a la organización hay por montones se va a tomar las que se considere más adecuadas a nuestro medio:

2.3.1 DESASTRES NATURALES

En este punto hay que estar consientes que todos están expuestos a algún desastre natural por lo cual se procede a ver lo que puede ocurrir.

Erupciones Volcánicas

Por la ubicación geográfica de nuestro país se está propenso a este tipo de desastre por lo cual hay que considerar implementar medidas que mitiguen el desastre.

Terremotos

Los terremotos es uno de los desastres naturales menos probables, por lo que no se suelen tomar medidas serias contra los movimientos sísmicos.

Pero si se desea prevenir se puede implementar fijaciones para los rack de servidores y comunicaciones así como los equipos activos de comunicación que no se encuentren empotrados.

> Tormentas eléctricas
> Generan subidas súbitas de tensión infinitamente superiores a las que pueda generar un problema en la red eléctrica, como se advierte a continuación. Si cae un rayo sobre la estructura metálica del edificio donde están situados los equipos es casi seguro que puede ir pensando en comprar otros nuevos; sin llegar a ser tan dramáticos, la caída de un rayo en un lugar cercano puede inducir un campo magnético lo suficientemente intenso como para destruir *hardware* incluso protegido contra voltajes elevados.[10]

Inundaciones y humedad

Este desastre es el más peligroso ya que con el alcantarillado deteriorado de la ciudad se está propenso a posibles inundaciones, por lo que se recomendaciones ubicar los Data Center en pisos elevados.

Con lo referente a la humedad hay que considerar que los servidores generan calor lo que implica que la temperatura suba, por lo que para controlar una temperatura adecuada se instalan aires acondicionados. Para evitar problemas con la humedad es necesario que cuando se instale un equipo de enfriamiento también controle la humedad.

2.3.2 DESASTRES DEL ENTORNO

Electricidad

> Quizás los problemas derivados del entorno de trabajo más frecuentes son los relacionados con el sistema eléctrico que alimenta los equipos; cortocircuitos, picos de tensión, cortes de flujo a diario amenazan la integridad tanto de nuestro *hardware* como de los datos que almacena o que circulan por él. El problema menos común en las instalaciones modernas son las subidas de tensión, conocidas como 'picos' porque generalmente duran muy poco: durante unas fracciones de segundo el voltaje que recibe un equipo sube hasta sobrepasar el límite aceptable que dicho equipo soporta. Lo normal es que estos picos apenas afecten al *hardware* o a los datos gracias a que en la mayoría de equipos hay instalados fusibles, elementos que se funden ante una subida de

10 BORGHELLO CRISTIAN, *Seguridad Informática sus Implicaciones e Implementación*, Argentina - 2001, p. 17

tensión y dejan de conducir la corriente, provocando que la máquina permanezca apagada. Disponga o no de fusibles el equipo a proteger (lo normal es que sí los tenga) una medida efectiva y barata es utilizar tomas de tierra para asegurar aún más la integridad; estos mecanismos evitan los problemas de sobretensión desviando el exceso de corriente hacia el suelo de una sala o edificio, o simplemente hacia cualquier lugar con voltaje nulo. Una toma de tierra sencilla puede consistir en un buen conductor conectado a los chasis de los equipos a proteger y a una barra maciza, también conductora, que se introduce lo más posible en el suelo; el coste de la instalación es pequeño, especialmente si lo comparamos con las pérdidas que supondría un incendio que afecte a todos o a una parte de los equipos.[11]

Ruido eléctrico

El ruido eléctrico suele ser generado por motores o por maquinaria pesada, pero también puede serlo por otros ordenadores o por multitud de aparatos, especialmente muchos de los instalados en los laboratorios de organizaciones de I+D, y se transmite a través del espacio o de líneas eléctricas cercanas a la instalación.
Para prevenir los problemas que el ruido eléctrico puede causar en los equipos lo más barato es intentar no situar *hardware* cercano a la maquinaria que puede causar dicho ruido; si no se tiene más remedio que hacerlo, se puede instalar filtros en las líneas de alimentación que llegan hasta los ordenadores. También es recomendable mantener alejados de los equipos dispositivos emisores de ondas, como teléfonos móviles, transmisores de radio o *walkie-talkies*; estos elementos puede incluso dañar permanentemente a nuestro *hardware* si tienen la suficiente potencia de transmisión, o influir directamente en elementos que pueden dañarlo como detectores de incendios o cierto tipo de alarmas.[12]

Incendios y humo

Aunque la causa de un fuego puede ser un desastre natural, lo habitual en muchos entornos es que el mayor peligro de incendio provenga de problemas eléctricos por la sobrecarga de la red debido al gran número de aparatos conectados al tendido. Un simple cortocircuito o un equipo que se calienta demasiado pueden convertirse en la causa directa de un incendio en el edificio, o al menos en la planta.[13]

---

11 BORGHELLO CRISTIAN, *Seguridad Informática sus Implicaciones e Implementación,* Argentina - 2001, p. 20

12 BORGHELLO CRISTIAN, *Seguridad Informática sus Implicaciones e Implementación,* Argentina - 2001, p. 22

13 Idem p.23

2.4 PROCEDIMIENTO DE CREACIÓN DE CUENTA DE USUARIO

Cuando un funcionario del Ministerio de Educación necesita una cuenta de usuario, debe llenar el formulario de solicitud:

ministerio de educación ECUADOR

Unidad de Tecnología Informática y Comunicaciones

Formulario de Solicitud

Información personal

Nombres: _____ C.I.: _____

Apellidos: _____ Fecha: _____

Dependencia: _____ No. Piso: _____

Servicios

Señale los servicios que desea solicitar.

Usuarios Internos	Describa su Solicitud
☐ Dirección de Correo Electrónico	
☐ Usuario y Contraseña de Domino	
☐ Red Wireless	
☐ Recursos Compartidos	
☐ Teléfono	
☐ Internet	

Aprobación

Firma Jefe Inmediato — Firma de Aprobación UTIC

Nombre: _____ Nombre: _____

Nota: Se dará atención a su requerimiento de acuerdo a la disponibilidad de los servicios siempre y cuando todos los campos solicitados de su información personal esten ingresados correctamente.

Información solo para personal de la UTIC

Pto. RED Datos: _____ Pto. de Voz: _____ IP: _____ Nombre PC: _____

Dirección: Av. Amazonas N34-451 entre Av. Atahualpa y Juan Pablo Sánz.
PBX 3961300 – 3961400 – 3961500

Cabe indicar que este formulario se envió por correo electrónico a todos los funcionarios del Ministerio de Educación por si lo requieren.

2.5 PROCEDIMIENTO DE BAJA DE CUENTA DE USUARIO

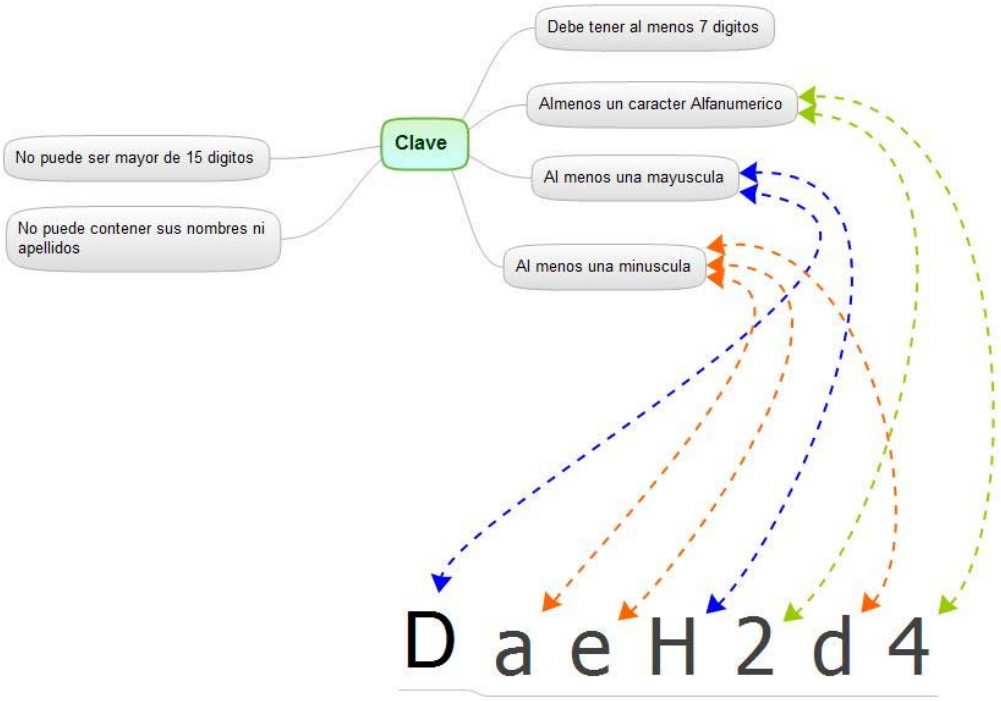
Para este procedimiento es indispensable contar con la coordinación de la Dirección Nacional de Recursos Humanos ya que cuando un funcionario deja de trabajar por un determinado tiempo (comisión de servicio, permiso personal, vacaciones, jubilación entre otros) se debe notificar a la Unidad de Tecnología Informática y Comunicaciones del particular para de acuerdo a la política de seguridad implementada se desactive o elimine el usuario asignado al funcionario.

Por ejemplo: Si el funcionario se jubila o renuncia el usuario puede ser eliminado pero si sale de vacaciones o comisión oficial se deshabilita y una vez que regresa se vuelve habilitar.

2.6 PROCEDIMIENTO PARA DETERMINAR UNA CLAVE SEGURA

Este procedimiento tuvo su resistencia y actualmente todavía hay usuarios que requieren asistencia cabe indicar que se socializo y se explico las normas que deben seguir, además se les entrego el siguiente documento:

- La clave no debe ser menor de 7 dígitos ni mayor de 15
- Debe contener al menos un carácter alfanumérico
- Debe contener al menos una mayúscula
- Debe contener al menos una minúscula
- La clave no puede ser sus nombres ni apellidos



2.7 PROCEDIMIENTOS DE VERIFICACIÓN DE ACCESOS

En este procedimiento hay que definir hasta donde se requiere realizar la auditoria de acceso, en la organización este proceso se lo realiza con la auditoria de active directory. En este punto es fundamental especificar en las políticas de seguridad se defina la persona responsable de revisar cada cierto tiempo los log y se hagan los reportes correspondientes de si existe alguna anomalía o todo está bien y eliminar o almacenar los log de acuerdo a la política implementada, esta medida es indispensable ya que los archivos log aumentan de tamaño considerablemente y pueden saturar el disco.

2.8 PROCEDIMIENTO PARA EL CHEQUEO DEL TRÁFICO DE LA RED

Este procedimiento es fundamental para verificar el rendimiento de la red y comprobar que el tráfico que mantiene la misma es normal. La política de seguridad debe contemplar chequeos permanentes del tráfico de la red y si es posible indicar los programas e intervalos que se han utilizado para dicha tarea.

En este caso se está utilizando el programa wireshark con los intervalos que posteriormente se van a indicar con detalle.

2.9 PROCEDIMIENTO PARA EL MONITOREO DE LOS VOLÚMENES DE CORREO

Este procedimiento también es muy necesario ya que permite conocer el volumen de tráfico de nuestra organización. Esto se lo puede realizar con programas o módulos del servidor de correo implementado el cual permita generar reportes del servidor para saber si está recibiendo spam o estamos generando spam**,** este monitoreo es preciso para evitar caer en listas negras como suele ocurrir si no se toman medidas. Como se muestra en los procedimientos anteriores la política de seguridad debe indicar el funcionario encargado del mantenimiento y del análisis de los datos generados, el mismo que tomara las medidas necesarias.

2.10 PROCEDIMIENTOS PARA EL MONITOREO DE CONEXIONES ACTIVAS

El objetivo de este procedimiento es identificar la inactividad de los usuarios ya sea por ausentarse del puesto de trabajo o algún otro motivo, para que la sesión se cierre, la política de seguridad debe definir el tiempo de inactividad para proceder al cierre de la sesión. Esto se aplica para usuarios de dominio como para todos los sistemas de información de la organización.

2.11 PROCEDIMIENTO DE MODIFICACIÓN DE ARCHIVOS

Este procedimiento sirve para detectar cualquier cambio o modificación no autorizada, lo cual permita asegurar la integridad de los datos como de los sistemas. Como casi todos los procedimientos se debe determinar el funcionario responsable de la revisión seguimiento y la toma de acciones.

2.12 PROCEDIMIENTOS PARA EL RESGUARDO DE COPIAS DE SEGURIDAD

Este procedimiento debe indicar claramente la frecuencia con que se van a sacar las copias de seguridad, dónde se deben guardar las copias de seguridad, la frecuencia en que se prueban las copias de seguridad y los pasos a seguir en caso de problemas. Como los procedimientos anteriores se debe definir el responsable o responsables.

2.13 PROCEDIMIENTOS PARA LA VERIFICACIÓN DE LAS MÁQUINAS DE LOS USUARIOS

Este procedimiento permitirá encontrar programas no autorizados instalados en los equipos informáticos de la organización. Esta medida evitara problemas con programas que pueden abrir huecos de seguridad, además que se evita tener software no licenciado. Explicar los métodos a utilizar para la verificación.

2.14 PROCEDIMIENTOS PARA EL MONITOREO DE LOS PUERTOS EN LA RED

Este procedimiento permite identificar que puertos están abiertos o filtrados dentro de la red. Se indicara la frecuencia del monitoreo y los programas y comandos que se han utilizado para dicha tarea.

En nuestro caso se está utilizando el programa nmap con los comandos que posteriormente se van a indicar con detalle.

2.15 PROCEDIMIENTOS DE CÓMO DIFUNDIR LAS NUEVAS NORMAS DE SEGURIDAD

Este tipo de procedimiento no siempre es tomado en cuenta. Sin embargo, en toda organización se debe describir la forma de socializar las nuevas normas de seguridad implementadas o modificadas según sea el caso. Esto evita que nadie pueda poner cómo excusa “que no conocía las modificaciones”.

2.16 PROCEDIMIENTOS PARA RECUPERAR INFORMACIÓN

Este procedimiento sirve para reconstruir todo el sistema o parte de él, a partir de las copias de seguridad. Se deben explicar todos los pasos a seguir para rearmar el sistema a partir de los back-up existentes, así como cada cuánto tiempo habría que llevarlos a cabo y quiénes son los responsables de dicha tarea.

2.17 CHECK-LISTS

- Algunos ejemplos de check-lists:
- Asegurar el entorno. ¿Qué es necesario proteger? ¿Cuáles son los riesgos?
- Determinar prioridades para la seguridad y el uso de los recursos.
- Crear planes avanzados sobre qué hacer en una emergencia.
- Trabajar para educar a los usuarios del sistema sobre las necesidades y las ventajas de la buena seguridad
- Estar atentos a los incidentes inusuales y comportamientos extraños.
- Asegurarse de que cada persona utilice su propia cuenta.
- ¿Están las copias de seguridad bien resguardadas?
- No almacenar las copias de seguridad en el mismo sitio donde se las realiza
- ¿Los permisos básicos son de sólo lectura?
- Si se realizan copias de seguridad de directorios/archivos críticos, usar chequeo de comparación para detectar modificaciones no autorizadas.
- Periódicamente rever todo los archivos de “booteo de los sistemas y los archivos de configuración para detectar modificaciones y/o cambios en ellos.
- Tener sensores de humo y fuego en el cuarto de computadoras.
- Tener medios de extinción de fuego adecuados en el cuarto de computadoras.
- Entrenar a los usuarios sobre qué hacer cuando se disparan las alarmas.
- Instalar y limpiar regularmente filtros de aire en el cuarto de computadoras.
- Instalar UPS, filtros de línea, protectores gaseosos al menos en el cuarto de computadoras.
- Tener planes de recuperación de desastres.

- Considerar usar fibras ópticas como medio de transporte de información en la red.[14]

2.18 PREVENCIÓN Y RESPUESTA

Para prevenir se ha considerado varias medidas que se detalla a continuación:

- Coloque access lists en los routers. Esto reducirá su exposición a ciertos ataques de negación de servicio
- Instale patches a su sistema operativo contra flooding de TCP SYN. Esta acción permitirá reducir sustancialmente su exposición a estos ataques aunque no pueda eliminar el riesgo en forma definitiva.
- Invalide cualquier servicio de red innecesario o no utilizado. Esto puede limitar la capacidad de un hacker de aprovecharse de esos servicios para ejecutar un ataque de negación de servicio. Por ejemplo: chargen, Echo, etc.
- Si su sistema operativo lo permite, implemente sistemas de cuotas. Por ejemplo, si su sistema operativo soporta “disk Quotas” impleméntelo para todos los logins. Si su sistema operativo soporta partición o volúmenes, separe lo crítico de lo que no lo es.
- Observe el funcionamiento del sistema y establezca valores base para la actividad ordinaria. Utilice estos valores para calibrar niveles inusuales de la actividad del disco, del uso de la CPU, o del tráfico de red.
- Incluya como parte de su rutina, el examen de su seguridad física. Considere, entre otras cosas, los servidores, routers, terminales desatendidas, ports de acceso de red y los gabinetes de cableado.
- Utilice Tripwire o una herramienta similar para detectar cambios en la información de configuración u otros archivos.
- Trate de utilizar configuraciones de red redundantes y fault-tolerant.[15]

2.19 E-MAIL BOMBING Y SPAMMING

14 SECRETARIA DE LA FUNCION PUBLICA, *Manual de Seguridades en Redes*, 1.0, Argentina - 1998, p. 39

15 SECRETARIA DE LA FUNCION PUBLICA, *Manual de Seguridades en Redes*, 1.0, Argentina - 1998, p. 44

Si la organización cuenta con un servidor de correo para evitar inconvenientes en la utilización del servicio se debe tener presente los posibles problemas que pueden afectar al servicio.

El e-mail bombing consiste en enviar muchas veces un mensaje idéntico a una misma dirección, saturando el mailbox del destinatario.

El spamming, que es una variante del e-mail bombing, se refiere a enviar el email a centenares o millares de usuarios e, inclusive, a listas de interés.

Los usuarios que cuentan con correo electrónico son vulnerables a los ataques antes mencionados por lo que para prevenir hay que definir políticas de uso, además el administrador de servicios debe monitorear constantemente el rendimiento de nuestro servidor ya que cualquier anomalía podría ser indicio de algún ataque los cual puede ser comprobado en los log del sistema.

Nadie está libre de ataques de spam por lo que para evitar nuestro servidor lo mejor es poner un anti spam.

2.20 SEGURIDAD EN WWW

Como un sistema de seguridad informático puede proteger el servidor de Web de la institución. La protección WWW es un dolor de cabeza si no se tiene la idea de cómo proteger por lo cual indicaremos algunos problemas y vulnerabilidades detectados.

> "Atacar el sistema operativo vía WWW implica generalmente "trampear" un cgi script o lograr que el webserver haga algo que no fue pensado que haga, como por ejemplo dar al hacker acceso al shell del host, que ese hacker ejecute comandos arbitrarios en él , o le provea información útil para lograr esos objetivos.
> Es obvio que los datos provistos a cualquier cgi script vía un form deben ser probados para su validez por una razón u otra, y una de esas razones indudablemente es la seguridad."

Como experiencia en el Ministerio de Educación se recibe un sistema web el cual contenía una función que generaba una vulnerabilidad lo cual boto por el piso toda la seguridad física firewall e IPS montados en la organización y encontrar el hueco de seguridad se toma varios días por lo que todo sistema

web antes que se suba a la red, debe pasar por un chequeo minucioso de la programación implementada.

Además se recomienda no ejecutar los aplicativos como root, se debe crear un usuario x con este usuario se establece la conexión y ahí tomar atributos de root.

Los servicios WWW son los más atacados y los que pueden decir mucho de la seguridad de la organización.

CAPITULO 3
DISEÑO E IMPLEMENTACION DEL SISTEMA DE SEGURIDAD INFORMATICA

3.1. IMPLEMENTACAION DEL SISTEMA DE SEGURIDAD INFORMATICA EN EL MINISTERIO DE EDUCACION

Para realizar la implementación del Sistema de Seguridad Informática es necesario contar con todos los datos de la organización referente a infraestructura tecnológica, servicios y aplicaciones; Es fundamental que el personal brinde todas las facilidades para realizar pruebas las que permitan identificar el estado de los equipos y aplicaciones.

La metodología implementada es OSSTMM la cual permite realizar el testeo de seguridad de acuerdo a la realidad y necesidad de cualquier organización, en nuestro caso en el Ministerio de Educación se aplicara las secciones de Seguridad de la Información, Seguridad en las Tecnologías de Internet y Seguridad Física.

Para esto es de vital importancia las políticas de seguridad con respecto al objetivo que se quiere lograr, las políticas por lo general no son complejas pero involucra a todos los funcionarios de la organización.

3.2. ANALISIS DE SEGURIDAD

En el proceso del análisis de seguridad correspondiente se evaluara las siguientes áreas.

3.2.1. VISIBILIDAD

> La visibilidad es lo que puede verse, registrar, o monitorear en el nivel de seguridad con o sin la ayuda de dispositivos electrónicos. Esto incluye, pero no se limita a, ondas de radio, luz por encima del espectro visible, dispositivos de comunicación como teléfonos, GSM, email y paquetes de red como TCP/IP.[16]

3.2.2. ACCESO

> El acceso es el punto de entrada al nivel de seguridad. Un punto de acceso no requiere ser una barrera física.
> Esto puede incluir, pero no se limita a, una página web, una ventana, una conexión de red, ondas de radio, o cualquier cosa cuya ubicación soporte la definición de casi-público o donde un computador interactúa con otro por medio de una red. Limitar el acceso significa negar todo excepto lo que este expresamente permitido financieramente y por buenas prácticas.[17]

3.2.3. CONFIANZA

> La confianza es una ruta especializada en relación con el nivel de seguridad. La confianza incluye la clase y cantidad de autenticación, no-repudio, control de acceso, contabilización, confidencialidad e integridad entre dos o más factores dentro del nivel de seguridad.[18]

3.2.4. AUTENTICACION

---

[16] PETE HERZOG, Manual de la Metodología Abierta de Testeo de Seguridad, 2.1, 2003, p. 22
[17] Idem., p. 22
[18] Idem., p. 22

"La autenticación es la medida por la cual cada interacción en el proceso está privilegiada."[19]

3.2.5. CONFIDENCIALIDAD

"La confidencialidad es la certeza que únicamente los sistemas o partes involucradas en la comunicación de un proceso tengan acceso a la información privilegiada del mismo."[20]

3.2.6. PRIVACIDAD

"La privacidad implica que el proceso es conocido únicamente por los sistemas o partes involucradas."[21]

3.2.7. AUTORIZACION

"La autorización es la certeza que el proceso tiene una razón o justificación de negocios y es administrado responsablemente dando acceso permitido a los sistemas."[22]

3.2.8. INTEGRIDAD

"La integridad es la certeza que el proceso tiene finalidad y que no puede ser cambiado, continuado, redirigido o reversado sin el conocimiento de los sistemas o partes involucradas."[23]

3.2.9. ALARMA

"La alarma es la notificación apropiada y precisa de las actividades que violan o intentan violar cualquiera de las dimensiones de la seguridad. En la

[19] Idem., p. 22
[20] Idem., p. 22
[21] PETE HERZOG, Manual de la Metodología Abierta de Testeo de Seguridad, 2.1, 2003, p. 22
[22] Idem., p. 22
[23] Idem., p. 22

mayoría de violaciones de seguridad, la alarma es el único proceso que genera reacción."[24]

3.3. EVALUACION DE RIESGO

Una vez que todos los datos sean recopilados, esta información permitirá realizar una evaluación por medio de pruebas. El riesgo siempre está presente en todo proceso de seguridad por lo que para minimizar cualquier estado de riesgo en el ambiente se tendrá presente lo siguiente:

3.3.1. SEGURIDAD

Todos los tests deben ejecutarse con la precaución necesaria para evitar problemas que impliquen parar las actividades de la organización.

3.3.2. PRIVACIDAD

Todos los análisis deben ejecutarse manteniendo la ética y el entendimiento de la privacidad.

3.3.3. PRACTICIDAD

"Todos los tests deben ser diseñados buscando la mínima complejidad, la máxima viabilidad y una profunda claridad."[25]

3.3.4. USABILIDAD

"Todos los tests deben permanecer dentro del marco de seguridad útil. Es decir, lo más seguro es lo menos bienvenido y perdonable. Los tests dentro de este manual son desarrollados para encontrar un nivel de seguridad útil (también conocido como seguridad práctica)."[26]

---

[24] Idem., p. 22
[25] PETE HERZOG, Manual de la Metodología Abierta de Testeo de Seguridad, 2.1, 2003, p. 26
[26] Idem., p. 26

3.4. SEGURIDAD DE LA INFORMACION

En lo concerniente a la seguridad de la Información los datos recolectados permitirán medir la presencia del Ministerio de Educación en Internet, la justificación de las aplicaciones y servicios implementados, un perfil de la UTIC y de los funcionarios y el perfil de las tecnologías de la organización.

3.4.1. ESTRUCTURA DEL DIRECTORIO Y CONFIGURACION DEL SERVIDOR WEB

El sitio web y el administrador de contenidos se encuentra desarrollado en **HTML**, con paginas activas **PHP** y motor de base de datos **SQL Server 2005**

El sitio web y el administrador de contenidos pueden funcionar tanto en sistemas operativos **Linux** como en **Windows,** siempre y cuando tengan instalados el software base mencionado en el párrafo anterior.

Estructura de Archivos:

_funciones	Contiene las librerías javascript y las librerías PHP para el funcionamiento del sistema administrador de contenidos.
_upload	En esta carpeta se cargan todos los archivos que se suben desde el sistema administrador de contenidos, por lo tanto es importante que esta carpeta tenga **permisos de escritura** en el hosting contratado.
Flash	Contiene todos los archivos de animación flash que

	requiere el sitio web.
Graficos	Contiene todos los gráficos e imágenes del sistema administrador de contenidos.
Images	Contiene todos los gráficos e imágenes del sitio web.
Mantenimiento	Contiene todas las páginas PHP del sistema administrador de contenidos.
Pages	Contiene todas las páginas PHP del sitio web.
Scripts	Contiene las librerías javascript necesarias para el funcionamiento del sitio web.
CSS	Contiene las página de style.

Fuente: Unidad de Tecnología del Ministerio de Educación, Formulario de Solicitud, 2009

Configuración**:**

Para la configuración del sitio web y el sistema administrador de contenidos debemos editar las siguientes variables que se encuentran en el archivo **parametros.hp** en la carpeta _**funciones:**

aplServer	Nombre del Host (servidor) donde se encuentra

	levantada la base de datos.
aplUser	Nombre del usuario que tiene acceso a la base de datos.
aplDataBase	Nombre de la base de datos.
aplPassword	Clave del usuario que tiene acceso a la base de datos.
aplAplicationURL	Dominio (dirección URL) del sitio web, incluido **http://**
aplUploadPathArch	Path o ruta del directorio _**upload** dentro del hosting contratado.

Fuente: Unidad de Tecnología del Ministerio de Educación, Formulario de Solicitud, 2009

3.4.2. BASE DE DATOS WHOIS REGISTRADOS POR EL MINISTERIO DE EDUCACION

Los Dominios registrados en NIC.EC por el Ministerio de Educación son los que detallo a continuación:

Dominio: www.educacion.gov.ec

Registrante:

Ministerio de Educacion y Cultura

Paul Andrade C. paul_ac02@hotmail.com

Telf:5932-3961434

Fax:5934-3961434

San Salvador E6-49 y Eloy Alfaro

Quito, Pichincha,
Ecuador

Contacto Administrativo:
Ministerio de Educación y Cultura
Paúl Andrade Cuvi paul_ac02@hotmail.com
Telf: 5392-3961434
Fax:5392-3961434
San Salvador E6-49 y Eloy Alfaro
Quito, Pichincha,
Ecuador

Contacto Técnico:
Ministerio de Educación y Cultura
Lorena Montalvo lorenamontalvo@gmail.com
Telf: 5392-3961433
Fax: 5392-3961434
San Salvador E6-49 y Eloy Alfaro
Quito, Pichincha,
Ecuador

Contacto de Facturación:
Ministerio de Educación y Cultura
Paúl Andrade Cuvi paul_ac02@hotmail.com
Telf:5392-3961434
Fax:5392-3961434
San Salvador E6-49 y Eloy Alfaro
Quito, Pichincha,
Ecuador

Fecha de expiración del dominio: 22-Noviembre-2010

Fecha de creación del dominio: 22-Noviembre-1999

Fecha de última modificación del registro: 23-Noviembre-2009

Nombres de Servidores DNS listados en orden:

pichincha.andinanet.net 200.107.10.62
tungurahua.andinanet.net 200.107.60.58

Dominio www.educarecuador.ec

Registrante:

Ministerio de Educación y Cultura
Paúl Andrade Cuvi paul_ac02@hotmail.com
Telf:5392-3961434
Fax:5392-3961434
San Salvador E649 y Eloy Alfaro
Quito, Pichincha,
Ecuador

Contacto Administrativo:

Ministerio de Educación y Cultura
Paúl Andrade Cuvi paul_ac02@hotmail.com
Telf: 5392-3961434
Fax:5392-3961434
San Salvador E6-49 y Eloy Alfaro
Quito, Pichincha,
Ecuador

Contacto Técnico:

Ministerio de Educación y Cultura
Lorena Montalvo lorenamontalvo@gmail.com
Telf: 5932-3961433
Fax: 5932-3961434
San Salvador E649 y Eloy Alfaro
Quito, Pichincha,
Ecuador

Contacto de Facturación:

Ministerio de Educación y Cultura
Paúl Andrade Cuvi paul_ac02@hotmail.com
Telf:5392-3961434
Fax:5392-3961434
San Salvador E649 y Eloy Alfaro

Quito, Pichincha,
Ecuador
Fecha de expiración del dominio: 01-Junio-2012
Fecha de creación del dominio: 01-Junio-2006
Fecha de última modificación del registro: 08-Junio-2009
Nombres de dominios DNS listados en orden:
pichincha.andinanet.net 200.107.10.62
tungurahua.andinanet.net 200.107.60.58

Dominio www.dineib.gov.ec
Registrante:
Direccion Nacional de Educacion Intercultural Bilingue
Paul Andrade paul.andrade@educacion.gov.ec
Telf:593-23961439
Fax:-
Amazonas Y Juan Pablo Sanz
Quito, Pichincha,
Ecuador
Contacto Administrativo:
Direccion Nacional de Educacion Intercultural Bilingue
Paul Andrade paul.andrade@educacion.gov.ec
Telf: 02-3961439
Fax:-
Amazonas Y Juan Pablo Sanz
Quito, Pichincha,
Ecuador

Contacto Técnico:
Direccion Nacional de Educacion Intercultural Bilingue
Paul Andrade paul.andrade@educacion.gov.ec
Telf: 02-3961439
Fax: -
Amazonas Y Juan Pablo Sanz
Quito, Pichincha,

Ecuador

Contacto de Facturación:

Direccion Nacional de Educación Intercultural Bilingue

Paul Andrade paul.andrade@educacion.gov.ec

Telf:02-3961439

Fax:-

Amazonas Y Juan Pablo Sanz

Quito, Pichincha,

Ecuador

Fecha de expiración del dominio: 12-Marzo-2011

Fecha de creación del dominio: 12-Marzo-2009

Fecha de última modificación del registro: 13-Marzo-2009

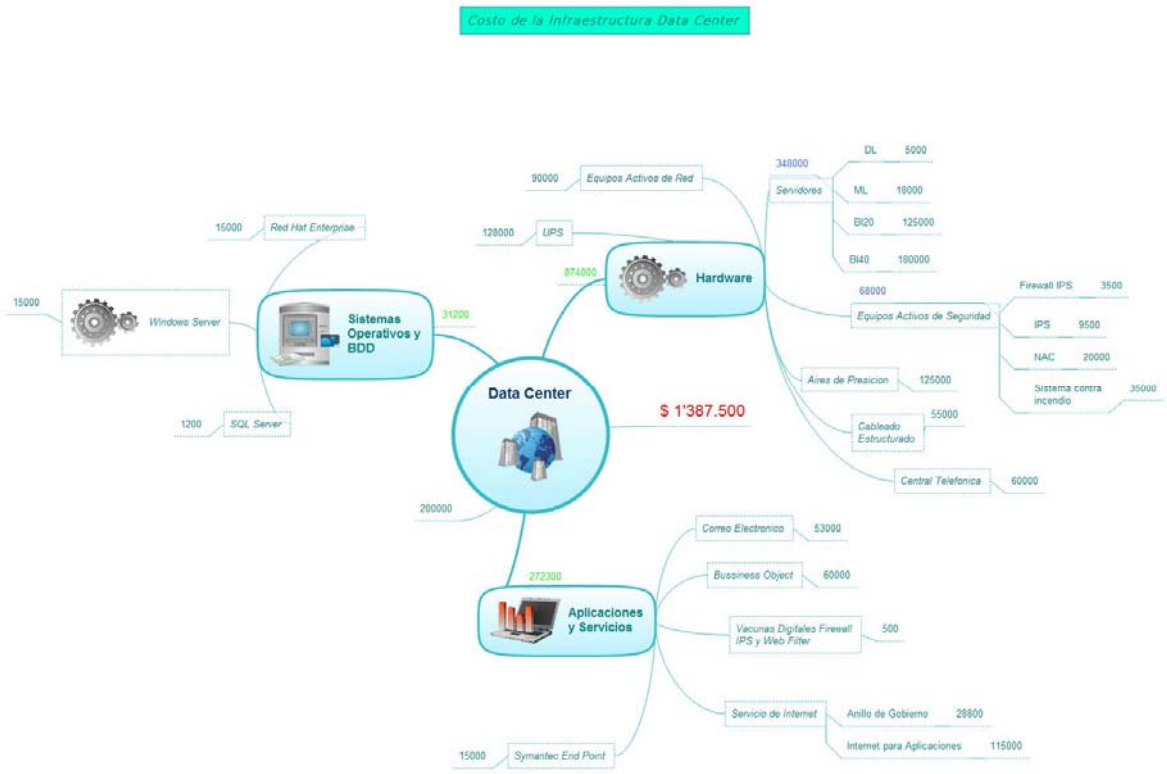
Nombres de Servidores DNS listados en orden:

pichincha.andinanet.net 200.107.10.62

tungurahua.andinanet.net 200.107.60.58

3.4.3. COSTO DE LA INFRAESTRUCTURA TECNOLÓGICA, SISTEMA OPERATIVO, SERVICIOS, APLICACIONES Y HARDWARE DEL DATA CENTER DEL MINISTERIO DE EDUCACIÓN.

El costo total de la Infraestructura tecnológica aproximadamente es de 1’387.500 dólares como se detalla en el siguiente grafico.

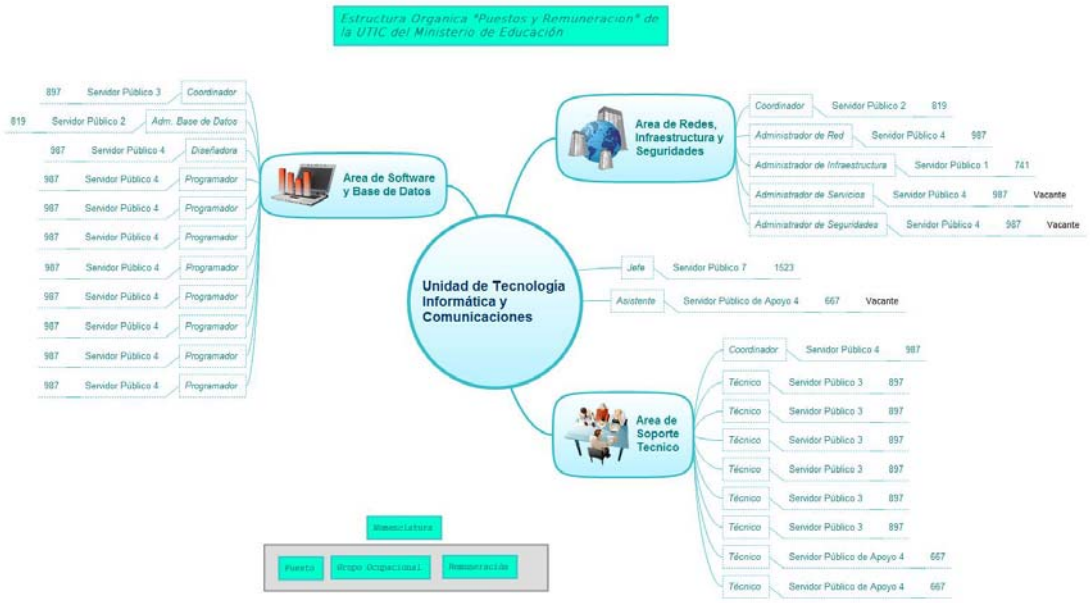


Fuente: Fabricio Zavala Vela

Cabe indicar que los tópicos de servicios de internet, vacunas digitales, Windows Server y SQL Server son costos anuales.

3.4.4. COSTO DEL SOPORTE Y GESTIÓN DE LA INFRAESTRUCTURA BASADO EN REQUERIMIENTOS SALARIALES DE LOS PROFESIONALES DE LA UNIDAD DE TECNOLOGÍA INFORMÁTICA Y COMUNICACIONES, PUESTOS DE TRABAJO, CANTIDAD DE PERSONAL.

El costo mensual de las remuneraciones a los funcionarios de la Unidad de Tecnología Informática y Comunicaciones asciende a 23490 dólares. El grafico siguiente detalla el puesto la denominación y el sueldo.



Fuente: Fabricio Zavala Vela

3.4.5. PRODUCTOS Y SERVICIOS PUBLICADOS ELECTRÓNICAMENTE

La página WEB da servicios mediante el Sistema de información del Ministerio de Educación (SIME) el cual actualmente cuenta con los siguientes módulos:

a) El de Recursos Humanos que integra la Personal con el concurso de Meritos y Oposicion orientado a todos los profesionales que quieran ingresar a Esta Cartera de Estado, el de Autoridades que permite participar a los docentes en los cargos de autoridades, además Jubilación

b) SIPROFE este modulo permite que los docentes del magisterio tengan una formación continua mediante seminarios y conferencias que se imparte a nivel nacional

c) AMIE este modulo se pone al aire 2 veces por cada régimen escolar el cual permite ingresar toda la información con respecto a la alumnos de todas las instituciones educativas del país.

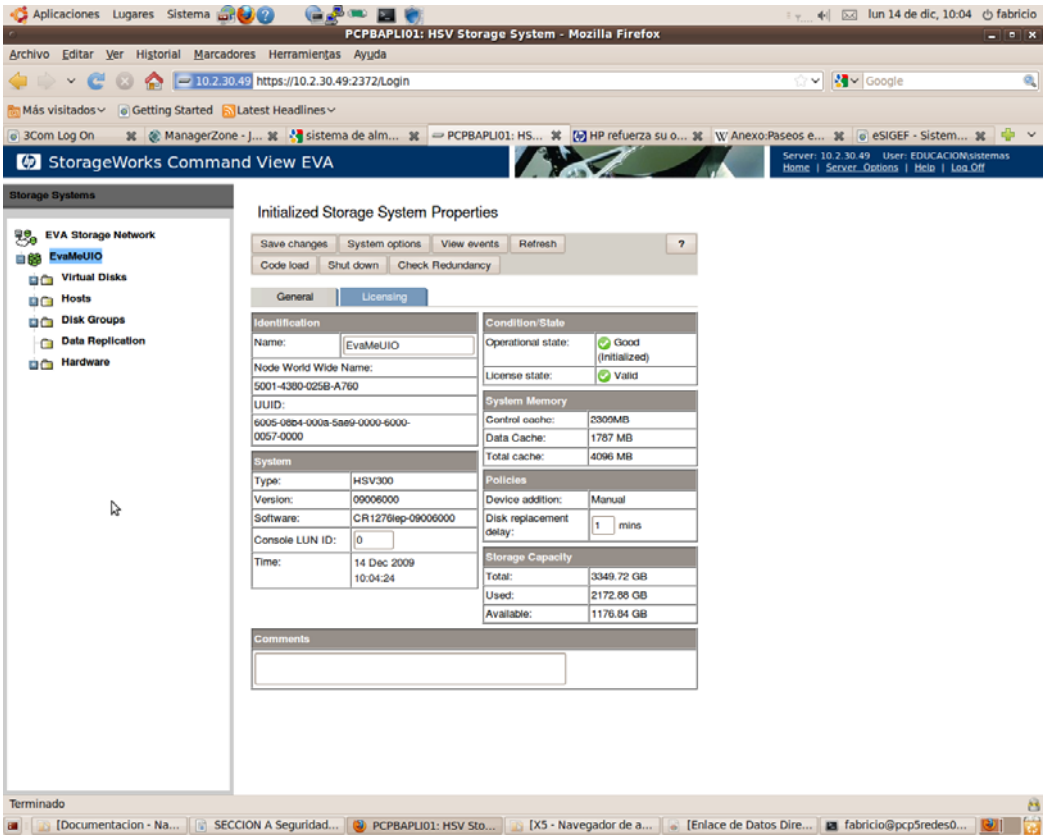
Fuente: Fabricio Zavala Vela

3.4.6. IDENTIFICAR EL TIPO DE TAMAÑO DE LA BASE DE DATOS Y SU CONFIGURACIÓN PARA EL ALMACENAMIENTO DE LOS DATOS

El Ministerio de Educación cuenta con dos sistemas de almacenamiento estos sistemas son administrador y configurados vía web. A continuación detallamos la configuración de cada uno de los sistemas de almacenamiento.

3.4.6.1. SISTEMA DE ALMACENAMIENTO EVA(ENTERPRISE VIRTUAL ARRAY)

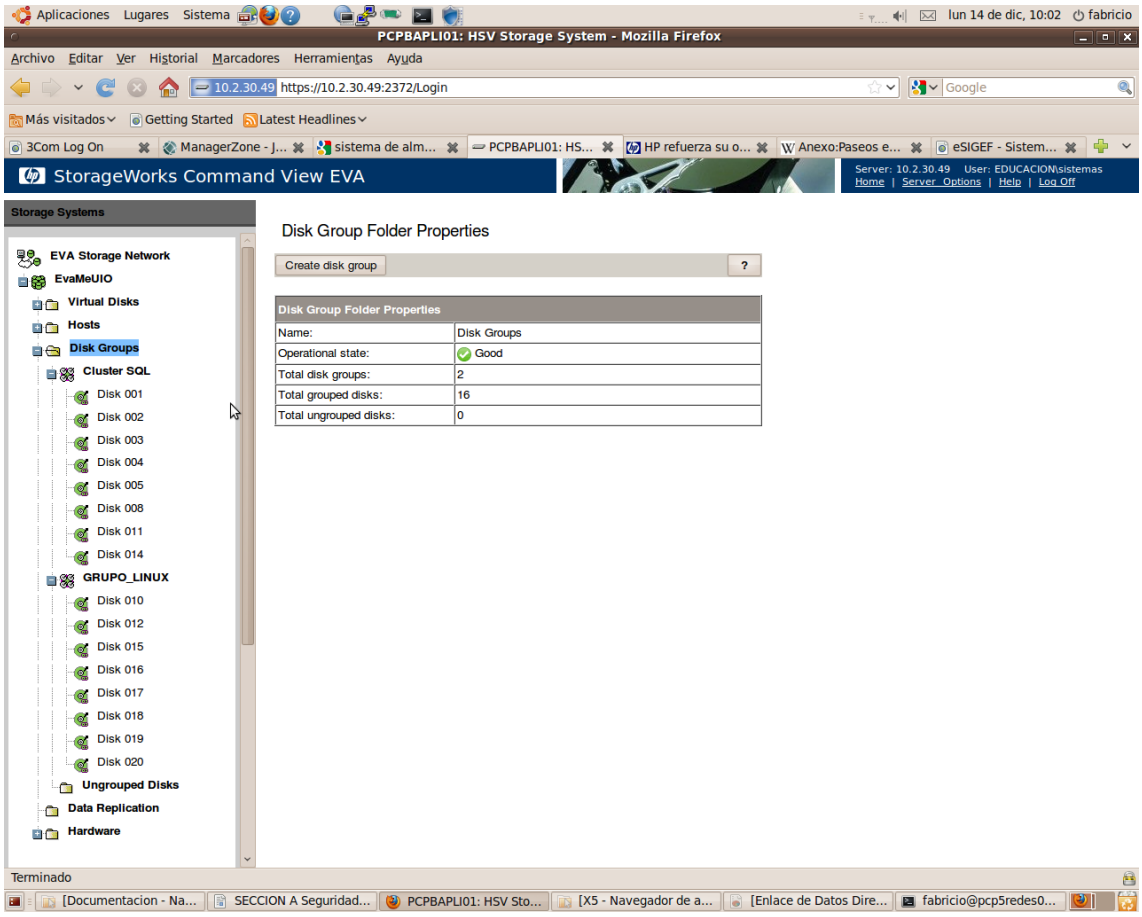
Capacidad de almacenamiento actual 4 Teras distribuidos en dos Enclosure con 8 discos de 279.39 GB cada uno.



sistema de almacenamiento EVA tiene la siguiente configuración:

Grupo de Discos

Dos grupos de disco: Cluster SQL y GRUPO_LINUX con 8 discos cada uno



Discos Virtuales

En el grupo Cluster SQL tenemos los siguientes discos virtuales:

1. Quorum_Cluster_WEB (50 GB, Raid 1)
2. BO_REPOSITORIO_DATA (120 GB, Raid 5)
3. BO_SQL_DATA (120 GB, Raid 5)
4. BO_SQL_LOGS (80 GB, Raid 5)
5. CL2DATA (270 GB, Raid 5)
6. CL2LOG (100 GB, Raid 5)
7. CL2MSDTC (16 GB, Raid 5)
8. CL2QUORUM (10GB, Raid 5)
9. CL3DATA (270 GB, Raid 5)

10. CL3LOG (100GB, Raid 5)

11. CL3MSDTC (16GB, Raid 5)

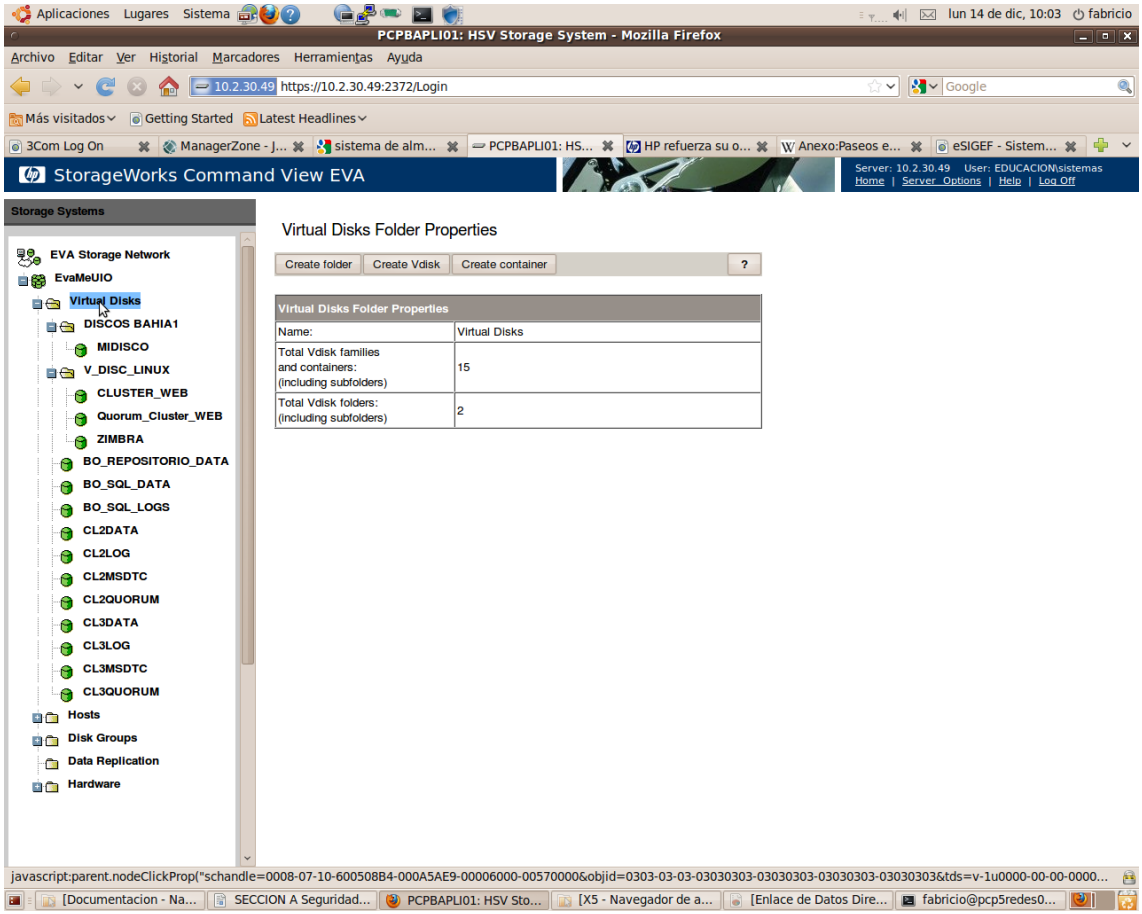
12. CL3QUORUM (10GB, Raid 5)

En el grupo GRUPO_LINUX tenemos los siguientes discos virtuales:

1. MIDISCO (5 GB, Raid 5)

2. CLUSTER_WEB (150 GB, Raid 1)

3. ZIMBRA (300 GB, Raid 5)



3.4.6.2. SISTEMA DE ALMACENAMIENTO SAN (STORAGE AREA NETWORK)

Capacidad de almacenamiento 1 Tera distribuidos en 10 discos de 160 GB cada uno, los mismos que tienen la siguiente configuración:

Vista Física

Se crearon los siguientes array:

1. Array A integrado de dos discos de 146GB de la cual se crearon las siguientes unidades lógicas:

   Unidad lógica 1 (1023 MB, RAID 1+0)

   Unidad lógica 2 (1023 MB, RAID 1+0)

   Unidad lógica 3 (1023 MB, RAID 1+0)

   Unidad lógica 6 (1023 MB, RAID 0)

   Espacio no utilizado 137020 MB

2. Array B integrado de tres discos de 146GB de la cual se crearon las siguientes unidades lógicas:

   Unidad lógica 4 (10239 MB, RAID 5)

   Unidad lógica 5 (269787 MB, RAID 5)

3. Array C integrado con dos discos de 146GB de la cual se crearon las siguientes unidades lógicas:

   Unidad lógica 8 (49999 MB, RAID 1+0)

   Unidad lógica 9 (90011 MB, RAID 1+0)

4. Array D integrado con tres discos de 146GB de la cual se crearon las siguientes unidades lógicas:

   Unidad lógica 10 (420041 MB, RAID 0)

3.4.7. IDENTIFICAR LOS TIPOS DE COOKIES

Los tipos de cookies identificados son los de sección y permanentes los mismos que están configurados con la administración de cookies con los siguientes parámetros.

Internet Explorer 7.0

Configuración para la zona de Internet **Alta**

Cookies de origen **Aceptar**

Cookies de Terceros **Aceptar**

3.4.8. IDENTIFICAR LAS FECHAS DE EXPIRACIÓN DE LAS COOKIES

Los cookie están configurados para que expiren en 2 días en el servidor proxy de nuestra institución.

3.4.9. RECOPILAR DIRECCIONES DE EMAIL DE LA ORGANIZACIÓN DE PERSONAS CLAVES.

Nombre	**Cargo**	**Dirección E-mail**
Raúl Vallejo	Ministro de Educación	raul.vallejo@educacion.gov.ec
Gloria Vidal	Viceministra de Educacion	Gloria.vidal@eduacion.gov.ec
Verónica Falconi	Subsecretaria Administrativa y Financiera	Veronica.falconi@educacion.gov.ec
Eduardo Chiliquinga	Secretario Particular del señor Ministro	Eduardo.chiliquinga@educacion.gov.ec

Pablo Cevallos	Subsecretario de Calidad	Pablo.cevalloseducacion.gov.ec
Verónica Benavides	Subsecretaria de Planeamiento	Verónica.falconi@educacion.gov.ec
Wankar Kowi	Subsecretario de Interculturalidad Bilingüe	Wankar.kowi@educacion.gov.ec
Jose Cevallos	Director de Recursos Humanos	Jose.cevallos@educacion.gov.ec
Danny Endara	Director Administrativo	Danny.endara@educacion.gov.ec
Mayra Polo	Directora Financiera	Mayra.polo@educacion.gov.ec
Teodoro Barros	Director Nacional de Educación	Teodoro.barros@educacion.gov.ec
Paul Andrade	Jefe de la Unidad de Tecnología Informática y Comunicaciones	Paul.andrade@educacion.gov.ec

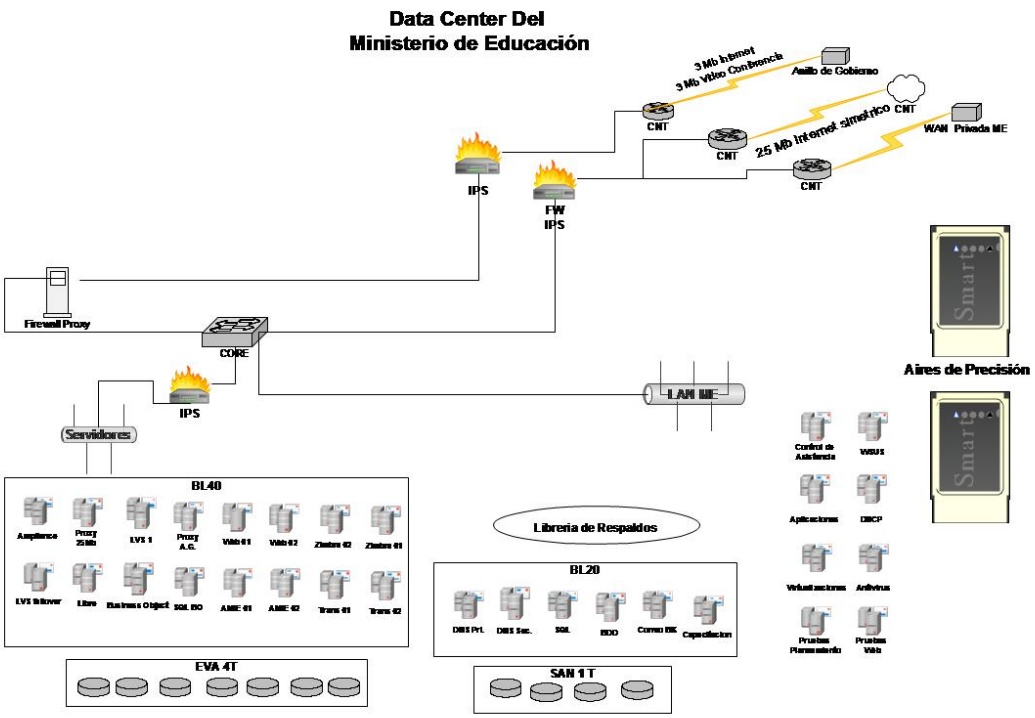
3.5. SEGURIDAD EN LAS TECNOLOGIAS DE INTERNET

En esta sección identificaremos todos los recursos tecnológicos del Data Center y de la UTIC del Ministerio de Educación; problemas de enrutamiento; nombres de dominio; nombres de los servidores; direcciones IP; mapa de red; puertos abiertos, cerrados y filtrados; direcciones IP de los sistemas activos; nivel de parchado de los servicios; sistema operativo utilizados; nivel de parcheado; aplicaciones o servicios por vulnerabilidad;

las vulnerabilidades de las aplicaciones; equipos activos y propiedades implementadas; paquetes que deben entrar a la red; información de las características implementadas en el firewall; protocolos con acceso dentro de la red; protocolos que han entrado a la red; sistemas vulnerables a ataques de descifrado de contraseñas.

3.5.1. IDENTIFICAR LA INFRAESTRUCTURA TECNOLÓGICA DEL DATA CENTER Y DE LA UTIC DEL MINISTERIO DE EDUCACIÓN

En el Data Center del Ministerio de Educación cuenta con los equipos identificados en la diagrama siguiente.



Fuente: Fabricio Zavala Vela

Servidores

- 16 Blade BL46
- 6 Blade Bl20

- 7 ML
- 1 DL

Equipos Activos de Seguridad

- Un Firewall IPS
- Un IPS TP50 de un segmentos
- Un IPS TP200E de dos segmentos

Equipos Activos de Red

- Un 7700 Core
- Dos 5500 Servidores
- Un 4500 Servidores

Aires de Precisión

- Dos aires de precisión

3.5.2. PLATAFORMA DE EQUIPOS INFORMATICOS DE LA UTIC

Jefe de la Unidad

- Una10 estación de trabajo

Area de Soporte Tecnico y Mantenimiento

- 9 estaciones de trabajo
- 1 lapto

Area de Sofware y Base de Datos

- 11 estaciones de trabajo
- 1 lapto

Area de Redes, Infraestructura y Seguridades

- 6 estaciones de trabajo
- 3 laptos

3.5.3. INFRAESTRUCTURA DE LA RED LAN DEL MINISTERIO DE EDUCACIÓN

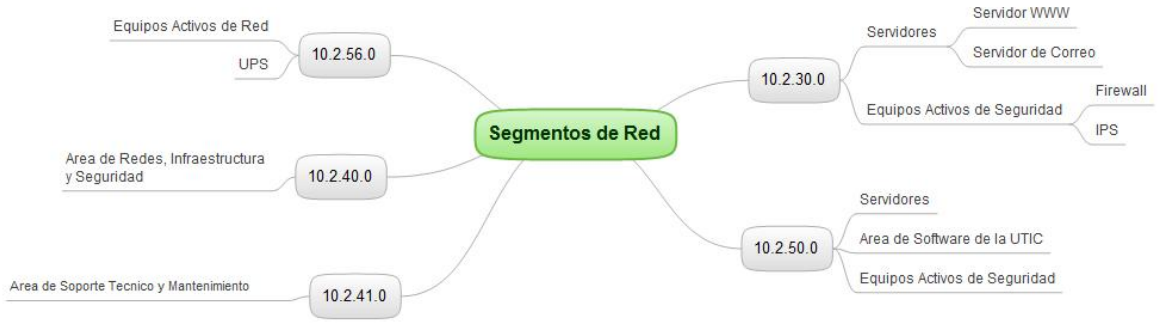
Los equipos activos de red son:

- Un switch 7700
- 10 switch 5500
- 11 switch 4500
- 6 switch 4200

3.5.4. IDENTIFICAR LOS SEGMENTOS DE RED QUE UTILIZAN LOS EQUIPOS DEL DATA CENTER Y LA UTIC DEL MINISTERIO DE EDUCACIÓN.

El Data Center y la UTIC trabajan con 5 segmentos de red con la siguiente distribución:

- En el segmento 10.2.30.0/24 tienen servidores y equipos activos de seguridad
- En el Segmento 10.2.50.0/24 tienen servidores; equipo activo de seguridad; estaciones de trabajo del Área de software y Base de Datos; y la estación de trabajo del jefe de la UTIC
- En el segmento 10.2.56.0/24 tienen equipos activos de red y los UPS
- En el segmento 10.2.40.0/24 tienen los equipos del Área de Redes, Infraestructura y Seguridades
- En el segmento 10.2.41.0/24 tienen los equipos del Área de Soporte Técnico y Mantenimiento al Usuario.



Fuente: Fabricio Zavala Vela

3.5.5. IDENTIFICAR TODOS LOS PUNTOS CONECTADOS EN CADA SEGMENTO

Para esto vamos a utilizar herramienta nmap y además identificar la latencia de los host que se encuentran conectados en cada segmento.

3.5.5.1. SEGMENTO 10.2.30.0/24

En este segmento tenemos servidores y equipos de seguridad firewall e IPS.

```
root@pcp5redes03:/# nmap -sP 10.2.30.0/24
Starting Nmap 5.00 ( http://nmap.org ) at 2010-01-13 11:06 ECT
Host 10.2.30.0 is up (0.29s latency).
Host 10.2.30.1 is up (0.11s latency).
Host pcpbutic01.educacion.gov.ec (10.2.30.10) is up (0.00071s latency).
Host 10.2.30.11 is up (0.00071s latency).
Host 10.2.30.12 is up (0.00090s latency).
Host pcpbutic17.educacion.gov.ec (10.2.30.13) is up (0.00072s latency).
Host 10.2.30.14 is up (0.00083s latency).
Host pcpbutic05.educacion.gov.ec (10.2.30.15) is up (0.0010s latency).
Host 10.2.30.16 is up (0.00088s latency).
Host 10.2.30.17 is up (0.00091s latency).
Host pcpbutic009.educacion.gov.ec (10.2.30.18) is up (0.0010s latency).
Host pcpbutic0010.educacion.gov.ec (10.2.30.19) is up (0.00099s latency).
Host pcpbutic20.educacion.gov.ec (10.2.30.20) is up (0.0011s latency).
Host 10.2.30.21 is up (0.0011s latency).
```

Host pcpbcobi09.educacion.gov.ec (10.2.30.22) is up (0.0014s latency).
Host 10.2.30.23 is up (0.0012s latency).
Host 10.2.30.24 is up (0.0011s latency).
Host 10.2.30.25 is up (0.0013s latency).
Host 10.2.30.26 is up (0.00080s latency).
Host 10.2.30.27 is up (0.00047s latency).
Host 10.2.30.29 is up (0.0053s latency).
Host 10.2.30.30 is up (0.039s latency).
Host pcpbutic01.educacion.gov.ec (10.2.30.31) is up (0.038s latency).
Host dmp4capacit.educacion.gov.ec (10.2.30.32) is up (0.037s latency).
Host pcpbapli01.educacion.gov.ec (10.2.30.49) is up (0.00015s latency).
Host 10.2.30.50 is up (0.00051s latency).
Host pcpbblad01.educacion.gov.ec (10.2.30.51) is up (0.00051s latency).
Host 10.2.30.60 is up (0.00063s latency).
Host pcpbblad02.educacion.gov.ec (10.2.30.61) is up (0.00016s latency).
Host 10.2.30.70 is up (0.00051s latency).
Host sqlserver2005.educacion.gov.ec (10.2.30.74) is up (0.00017s latency).
Host basededatos.educacion.gov.ec (10.2.30.75) is up (0.00031s latency).
Host mail1.educacion.gov.ec (10.2.30.77) is up (0.00020s latency).
Host 10.2.30.80 is up (0.00068s latency).
Host 10.2.30.90 is up (0.00062s latency).
Host documentos.educacion.gov.ec (10.2.30.99) is up (0.00034s latency).
Host 10.2.30.100 is up (0.00066s latency).
Host call.educacion.gov.ec (10.2.30.113) is up (0.00017s latency).
Host 10.2.30.114 is up (0.00013s latency).
Host www.educacion.gov.ec (10.2.30.115) is up (0.00014s latency).
Host dib03serv03.educacion.gov.ec (10.2.30.116) is up (0.0024s latency).
Host 10.2.30.118 is up (0.00015s latency).
Host mail.educacion.gov.ec (10.2.30.119) is up (0.00014s latency).
Host pcpbserv14.educacion.gov.ec (10.2.30.120) is up (0.00019s latency).
Host (10.2.30.121) is up (0.00019s latency).
Host 10.2.30.126 is up (0.00015s latency).
Host 10.2.30.135 is up (0.00012s latency).
Host 10.2.30.140 is up (0.00016s latency).
Host virtualxpub9pac (10.2.30.141) is up (0.00042s latency).
Host dwh.educacion.gov.ec (10.2.30.190) is up (0.00014s latency).
Host meblad12bo2.educacion.gov.ec (10.2.30.191) is up (0.00014s latency).

Host meblad13nd1amie.educacion.gov.ec (10.2.30.200) is up (0.00012s latency).

Host meblad14nd2amie.educacion.gov.ec (10.2.30.201) is up (0.00013s latency).

Host meclusteramie.educacion.gov.ec (10.2.30.202) is up (0.00013s latency).

Host meservsqlamie.educacion.gov.ec (10.2.30.203) is up (0.00015s latency).

Host meblad15nd1tran.educacion.gov.ec (10.2.30.210) is up (0.00012s latency).

Host meblad16nd2tran.educacion.gov.ec (10.2.30.211) is up (0.00013s latency).

Host meclustertrans.educacion.gov.ec (10.2.30.212) is up (0.00013s latency).

Host 10.2.30.222 is up (0.00027s latency).

Host 10.2.30.224 is up (0.00015s latency).

3.5.5.2. SEGMENTO 10.2.50.0/24

En este segmento tenemos servidores; equipos de seguridad firewall e IPS; los equipos de estaciones de trabajo del área de software y base de datos; y la estación de trabajo del jefe de la UTIC.

root@pcp5redes03:/# nmap -sP 10.2.50.0/24

Starting Nmap 5.00 (http://nmap.org) at 2010-01-13 11:11 ECT

Host 10.2.50.0 is up (0.15s latency).

Host 10.2.50.1 is up (0.024s latency).

Host paul_virtualpc.educacion.gov.ec (10.2.50.13) is up (0.0033s latency).

Host mepcutic008.educacion.gov.ec (10.2.50.17) is up (0.00024s latency).

Host mepcpbutic013.educacion.gov.ec (10.2.50.22) is up (0.00016s latency).

Host 10.2.50.23 is up (0.00015s latency).

Host pcpbuticjj.educacion.gov.ec (10.2.50.27) is up (0.00012s latency).

Host servayuda.educacion.gov.ec (10.2.50.28) is up (0.00034s latency).

Host 10.2.50.36 is up (0.00020s latency).

Host pcpbutic22-virtual.educacion.gov.ec (10.2.50.37) is up (0.00042s latency).

Host serv_antivirus.educacion.gov.ec (10.2.50.66) is up (0.00023s latency).

Host mepcserv_wsus.educacion.gov.ec (10.2.50.67) is up (0.00028s latency).

Host 10.2.50.81 is up (0.00023s latency).

Host ministro.educacion.gov.ec (10.2.50.82) is up (0.074s latency).

Host 10.2.50.84 is up (0.058s latency).

Host mepcutic005.educacion.gov.ec (10.2.50.100) is up (0.00013s latency).

Host mecpcutic030.educacion.gov.ec (10.2.50.116) is up (0.00011s latency).

Host mesfielmagister.educacion.gov.ec (10.2.50.117) is up (0.00017s latency).

Host mepcutic033.educacion.gov.ec (10.2.50.118) is up (0.00038s latency).

Host pcpbutic01.educacion.gov.ec (10.2.50.119) is up (0.0014s latency).

Host callcenter07.educacion.gov.ec (10.2.50.120) is up (0.00048s latency).

Host mepcutic014.educacion.gov.ec (10.2.50.123) is up (0.00010s latency).

Host 10.2.50.124 is up (0.00017s latency).

Host mepcservtarific.educacion.gov.ec (10.2.50.135) is up (0.00017s latency).

Host 10.2.50.147 is up (0.0019s latency).

Host 10.2.50.160 is up (0.00010s latency).

Host pcpbserv02.educacion.gov.ec (10.2.50.187) is up (0.00017s latency).

Host svctag-7z3t0f1.educacion.gov.ec (10.2.50.188) is up (0.00013s latency).

Host educaci-86f9ccd.educacion.gov.ec (10.2.50.197) is up (0.00018s latency).

3.5.5.3. SEGMENTO 10.2.56.0/24

En este segmento se obtienen equipos activos de red y UPS.

Starting Nmap 5.00 (http://nmap.org) at 2010-01-13 11:13 ECT

Host 10.2.56.0 is up (0.0018s latency).

Host 10.2.56.1 is up (0.037s latency).

Host 10.2.56.5 is up (0.0015s latency).

Host 10.2.56.6 is up (0.0037s latency).

Host 10.2.56.7 is up (0.0014s latency).

Host 10.2.56.11 is up (0.12s latency).

Host 10.2.56.12 is up (0.0017s latency).

Host 10.2.56.13 is up (0.038s latency).

Host 10.2.56.22 is up (0.0013s latency).

Host 10.2.56.24 is up (0.0020s latency).

Host 10.2.56.33 is up (0.0027s latency).

Host 10.2.56.34 is up (0.0013s latency).
Host 10.2.56.35 is up (0.032s latency).
Host 10.2.56.50 is up (0.033s latency).
Host 10.2.56.51 is up (0.17s latency).
Host 10.2.56.55 is up (0.0026s latency).
Host 10.2.56.56 is up (0.0014s latency).
Host 10.2.56.57 is up (0.00034s latency).
Host 10.2.56.66 is up (0.0032s latency).
Host 10.2.56.67 is up (0.061s latency).
Host 10.2.56.70 is up (0.030s latency).
Host 10.2.56.77 is up (0.12s latency).
Host 10.2.56.78 is up (0.0019s latency).
Host 10.2.56.79 is up (0.0019s latency).
Host scan.tippingpoint.local (10.2.56.80) is up (0.00013s latency).
Host 10.2.56.81 is up (0.00084s latency).
Host 10.2.56.99 is up (0.013s latency).
Host 10.2.56.100 is up (0.0039s latency).
Host 10.2.56.101 is up (0.0038s latency).
Host 10.2.56.102 is up (0.0036s latency).
Host 10.2.56.111 is up (0.0018s latency).
Host 10.2.56.112 is up (0.0036s latency).
Host 10.2.56.113 is up (0.0018s latency).
Host 10.2.56.114 is up (0.030s latency).
Host 10.2.56.115 is up (0.023s latency).
Host 10.2.56.116 is up (0.0018s latency).

3.5.5.4. SEGMENTO 10.2.41.0/24

En este segmento se tiene estaciones de trabajo del área de soporte técnico y mantenimiento.

root@pcp5redes03:/# nmap -sP 10.2.41.0/24

Host 10.2.41.0 is up (0.089s latency).

Host 10.2.41.1 is up (0.016s latency).
Host dmp3cuse01.educacion.gov.ec (10.2.41.10) is up (0.00s latency).
Host hp16080324341 (10.2.41.11) is up (0.00s latency).

Host dmp2bain03.educacion.gov.ec (10.2.41.51) is up (0.00s latency).
Host your-9c69ce59aa (10.2.41.54) is up (0.00s latency).
Host dmp2fdei01.educacion.gov.ec (10.2.41.55) is up (0.00s latency).
Host mepcrrhh030.educacion.gov.ec (10.2.41.58) is up (0.047s latency).
Host hp15237323173.educacion.gov.ec (10.2.41.64) is up (0.00s latency).
Host 10.2.41.75 is up (0.00s latency).

3.5.5.5. SEGMENTO 10.2.40.0/24

En este segmento se tiene estaciones de trabajo del área de Redes, Infraestructura y Seguridades.

root@pcp5redes03:/# nmap -sP 10.2.40.0/24
Host 10.2.40.0 is up (0.089s latency).
Host 10.2.40.1 is up (0.016s latency).
Host dmp3cuse01.educacion.gov.ec (10.2.40.11) is up (0.00s latency).
Host hp16080324341 (10.2.40.12) is up (0.00s latency).
Host dmp2bain03.educacion.gov.ec (10.2.40.13) is up (0.00s latency).
Host your-9c69ce59aa (10.2.40.14) is up (0.00s latency).
Host dmp2fdei01.educacion.gov.ec (10.2.40.16) is up (0.00s latency).
Host mepcrrhh030.educacion.gov.ec (10.2.40.17) is up (0.047s latency).
Host hp15237323173.educacion.gov.ec (10.2.40.18) is up (0.00s latency).
En este segmento tenemos respuesta de 9 hosts arriba que posteriormente identificaremos y analizaremos a detalle.

3.5.6. CONSULTAR LOS SERVIDORES DNS PRIMARIO Y SECUNDARIO DEL ISP

; <<>> DiG 9.6.1-P2 <<>> -x 200.107.10.46
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39628
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION: ;46.10.107.200.in-addr.arpa. IN PTR

;; ANSWER SECTION: 46.10.107.200.in-addr.arpa. 75909 IN PTR pichincha.andinanet.net.

;; AUTHORITY SECTION:
10.107.200.in-addr.arpa. 25101 IN NS tungurahua.andinanet.net.
10.107.200.in-addr.arpa. 25101 IN NS pichincha.andinanet.net.

;; ADDITIONAL SECTION:
pichincha.andinanet.net. 29231 IN A 200.107.10.46
tungurahua.andinanet.net. 29231 IN A 200.107.60.46

;; Query time: 3 msec
;; SERVER: 10.2.30.51#53(10.2.30.51)
;; WHEN: Sun Feb 7 18:33:52 2010
;; MSG SIZE rcvd: 152

root@pcp5redes03:/# dig -x 200.107.60.46

; <<>> DiG 9.6.1-P2 <<>> -x 200.107.60.46
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3135
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;46.60.107.200.in-addr.arpa. IN PTR

;; ANSWER SECTION:
46.60.107.200.in-addr.arpa. 3669 IN PTR tungurahua.andinanet.net.

;; AUTHORITY SECTION:
60.107.200.in-addr.arpa. 27198 IN NS pichincha.andinanet.net.
60.107.200.in-addr.arpa. 27198 IN NS tungurahua.andinanet.net.

;; ADDITIONAL SECTION:
pichincha.andinanet.net. 29222 IN A 200.107.10.46
tungurahua.andinanet.net. 29222 IN A 200.107.60.46

;; Query time: 2 msec
;; SERVER: 10.2.30.51#53(10.2.30.51)
;; WHEN: Sun Feb 7 18:34:01 2010
;; MSG SIZE rcvd: 152

3.5.7. MONITOREO DE PAQUETES BROADCAST DE LA RED

Con la Herramienta wireshark identifico tráfico broadcast de varios equipos activos de red que se muestra en la siguiente tabla

Origen		Destino	Secuencia paquete por segundo	Protocolo	Equipo	Detalle
Direccion IP	**MAC**	**Direccion IP**				
10.2.56.67		Broadcast	1 s/p	ARP	Switch de Borde Piso 6	Actualiza las tablas ARP del Switch por la peticion de spanning-tree
10.2.56.5		Broadcast	1 s/p	ARP	Switch Data Center	Actualiza las tablas ARP del Switch por la peticion de spanning-tree
10.2.56.116		Broadcast	1 s/p	ARP	Switch Piso 11	Actualiza las tablas ARP del Switch por la peticion de spanning-tree
10.2.56.111		Broadcast	1 s/p	ARP	Switch de Distribución Piso 11	Actualiza las tablas ARP del Switch por la peticion de spanning-tree
10.2.56.11		Broadcast	1 s/p	ARP	Switch de Distribución Piso 1	Actualiza las tablas ARP del Switch por la peticion de spanning-tree
10.2.56.55		Broadcast	1 s/p	ARP	Switch de Distribucion Piso 5	Actualiza las tablas ARP del Switch por la peticion de spanning-tree
10.2.56.56		Broadcast	1 s/p	ARP	Switch de Borde Piso 5	Actualiza las tablas ARP del Switch por la peticion de spanning-tree
10.2.56.24		Broadcast	35 s/p	ARP	Switch de Borde Lobby	Actualiza las tablas ARP del Switch por la peticion de spanning-tree
10.2.56.67		Broadcast		ARP	Switch de Borde Piso 6	Actualiza las tablas ARP del Switch por la peticion de

						spanning-tree

Fuente: Fabricio Zavala Vela

Los servicios SPT no están levantados en los equipos activos de red por lo que se realiza una revisión de la configuración de todos los equipos activos de red.

3.5.8. REALIZAR ESCANEOS TCP SYN PARA TODOS LOS SERVIDORES DE LA RED

Se realizan escaneos a todos los servidores de la organización se detalla el escaneo de un servidor el resto de resultados se encuentran en el anexo A

root@pcp5redes03:/home/fabricio# nmap -sS 10.2.30.74
Starting Nmap 5.00 (http://nmap.org) at 2010-02-07 16:13 ECT
Interesting ports on sqlserver2005.educacion.gov.ec (10.2.30.74):
Not shown: 988 closed ports
PORT STATE SERVICE
80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1025/tcp open NFS-or-IIS
1065/tcp open unknown
1073/tcp open unknown
1433/tcp open ms-sql-s
2301/tcp open compaqdiag
2381/tcp open unknown
2382/tcp open unknown
3389/tcp open ms-term-serv

Nmap done: 1 IP address (1 host up) scanned in 1.65 seconds

3.5.9. REALIZAR ESCANEOS UDP PARA TODOS LOS SERVIDORES DE LA RED

Los resultados se encuentran consolidados en el anexo A

3.5.10. REALIZAR ESCANEOS PARA IDENTIFICAR IP, SISTEMA OPERATIVO.

El comando –O nos permitirá identificar el sistema operativo del equipo escaneado. Un ejemplo los resultados de los equipos se encuentran en el anexo A.

root@pcp5redes03:/home/fabricio# nmap -v -sS -O 10.2.30.51

Starting Nmap 5.00 (http://nmap.org) at 2010-02-07 16:32 ECT
NSE: Loaded 0 scripts for scanning.
Initiating Ping Scan at 16:32
Scanning 10.2.30.51 [4 ports]
Completed Ping Scan at 16:32, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:32
Completed Parallel DNS resolution of 1 host. at 16:32, 0.00s elapsed
Initiating SYN Stealth Scan at 16:32
Scanning pcpbblad01.educacion.gov.ec (10.2.30.51) [1000 ports]
Discovered open port 53/tcp on 10.2.30.51
Discovered open port 3389/tcp on 10.2.30.51
Discovered open port 135/tcp on 10.2.30.51
Discovered open port 139/tcp on 10.2.30.51
Discovered open port 445/tcp on 10.2.30.51
Discovered open port 80/tcp on 10.2.30.51
Discovered open port 2381/tcp on 10.2.30.51
Discovered open port 464/tcp on 10.2.30.51
Discovered open port 1063/tcp on 10.2.30.51
Discovered open port 636/tcp on 10.2.30.51
Discovered open port 1027/tcp on 10.2.30.51
Discovered open port 2301/tcp on 10.2.30.51
Discovered open port 3268/tcp on 10.2.30.51
Discovered open port 593/tcp on 10.2.30.51

Discovered open port 1070/tcp on 10.2.30.51
Discovered open port 5555/tcp on 10.2.30.51
Discovered open port 1054/tcp on 10.2.30.51
Discovered open port 1075/tcp on 10.2.30.51
Discovered open port 1026/tcp on 10.2.30.51
Discovered open port 88/tcp on 10.2.30.51
Discovered open port 389/tcp on 10.2.30.51
Discovered open port 3269/tcp on 10.2.30.51
Completed SYN Stealth Scan at 16:32, 1.16s elapsed (1000 total ports)

Initiating OS detection (try #1) against pcpbblad01.educacion.gov.ec (10.2.30.51)
Host pcpbblad01.educacion.gov.ec (10.2.30.51) is up (0.00042s latency).
Interesting ports on pcpbblad01.educacion.gov.ec (10.2.30.51):
Not shown: 978 closed ports
PORT STATE SERVICE
53/tcp open domain
80/tcp open http
88/tcp open kerberos-sec
135/tcp open msrpc
139/tcp open netbios-ssn
389/tcp open ldap
445/tcp open microsoft-ds
464/tcp open kpasswd5
593/tcp open http-rpc-epmap
636/tcp open ldapssl
1026/tcp open LSA-or-nterm
1027/tcp open IIS
1054/tcp open unknown
1063/tcp open unknown
1070/tcp open unknown
1075/tcp open unknown
2301/tcp open compaqdiag
2381/tcp open unknown
3268/tcp open globalcatLDAP
3269/tcp open globalcatLDAPssl
3389/tcp open ms-term-serv

5555/tcp open freeciv
Device type: general purpose
Running: Microsoft Windows 2003
OS details: Microsoft Windows Server 2003 SP1 or SP2
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: /usr/share/nmap
OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.54 seconds
Raw packets sent: 1101 (49.134KB) | Rcvd: 1017 (41.310KB)

3.5.11. SIMULAR MULTIPLES EQUIPOS ATACANTES A LOS SERVIDORES WEB y CORREO ELECTRONICO

Escaneo servidor WWWW

root@pcp5redes03:/home/fabricio# nmap -sF www.educacion.gov.ec

Starting Nmap 5.00 (http://nmap.org) at 2010-02-05 08:50 ECT
Interesting ports on www.cluster.educacion.gov.ec (10.2.30.115):
Not shown: 997 closed ports
PORT STATE SERVICE
22/tcp open|filtered ssh
111/tcp open|filtered rpcbind
901/tcp open|filtered samba-swat

Nmap done: 1 IP address (1 host up) scanned in 1.47 seconds
root@pcp5redes03:/home/fabricio# nmap -sX www.educacion.gov.ec

Starting Nmap 5.00 (http://nmap.org) at 2010-02-05 08:51 ECT
Interesting ports on educarecuador.cluster.educacion.gov.ec (10.2.30.115):
Not shown: 997 closed ports
PORT STATE SERVICE

22/tcp open|filtered ssh
111/tcp open|filtered rpcbind
901/tcp open|filtered samba-swat

Nmap done: 1 IP address (1 host up) scanned in 1.37 seconds
root@pcp5redes03:/home/fabricio# nmap -sN www.educacion.gov.ec

Starting Nmap 5.00 (http://nmap.org) at 2010-02-05 08:51 ECT
Interesting ports on desarrollo.cluster.educacion.gov.ec (10.2.30.115):
Not shown: 997 closed ports
PORT STATE SERVICE
22/tcp open|filtered ssh
111/tcp open|filtered rpcbind
901/tcp open|filtered samba-swat

Escaneo Servidor de Correo

root@pcp5redes03:/home/fabricio# nmap -sF mail.educacion.gov.ec
Starting Nmap 5.00 (http://nmap.org) at 2010-02-05 08:53 ECT
Interesting ports on mail.educacion.gov.ec (10.2.30.119):
Not shown: 985 closed ports
PORT STATE SERVICE
22/tcp open|filtered ssh
25/tcp open|filtered smtp
80/tcp open|filtered http
110/tcp open|filtered pop3
111/tcp open|filtered rpcbind
143/tcp open|filtered imap
389/tcp open|filtered ldap
465/tcp open|filtered smtps
993/tcp open|filtered imaps
995/tcp open|filtered pop3s
5222/tcp open|filtered unknown
5269/tcp open|filtered unknown
7025/tcp open|filtered unknown
7777/tcp open|filtered unknown
11111/tcp open|filtered unknown

```
Nmap done: 1 IP address (1 host up) scanned in 1.37 seconds
root@pcp5redes03:/home/fabricio# nmap -sX mail.educacion.gov.ec

Starting Nmap 5.00 ( http://nmap.org ) at 2010-02-05 08:53 ECT
Interesting ports on mail.educacion.gov.ec (10.2.30.119):
Not shown: 985 closed ports
PORT STATE SERVICE
22/tcp open|filtered ssh
25/tcp open|filtered smtp
80/tcp open|filtered http
110/tcp open|filtered pop3
111/tcp open|filtered rpcbind
143/tcp open|filtered imap
389/tcp open|filtered ldap
465/tcp open|filtered smtps
993/tcp open|filtered imaps
995/tcp open|filtered pop3s
5222/tcp open|filtered unknown
5269/tcp open|filtered unknown
7025/tcp open|filtered unknown
7777/tcp open|filtered unknown
11111/tcp open|filtered unknown
Nmap done: 1 IP address (1 host up) scanned in 1.37 seconds
root@pcp5redes03:/home/fabricio# nmap -sN mail.educacion.gov.ec

Starting Nmap 5.00 ( http://nmap.org ) at 2010-02-05 08:53 ECT
Interesting ports on mail.educacion.gov.ec (10.2.30.119):
Not shown: 985 closed ports
PORT STATE SERVICE
22/tcp open|filtered ssh
25/tcp open|filtered smtp
80/tcp open|filtered http
110/tcp open|filtered pop3
111/tcp open|filtered rpcbind
143/tcp open|filtered imap
389/tcp open|filtered ldap
465/tcp open|filtered smtps
```

993/tcp open|filtered imaps
995/tcp open|filtered pop3s
5222/tcp open|filtered unknown
5269/tcp open|filtered unknown
7025/tcp open|filtered unknown
7777/tcp open|filtered unknown
11111/tcp open|filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 1.48 seconds

3.5.12. IDENTIFICAR LA REGLAS DEL FIREWALL IMPLEMENTADAS

3.5.13. IDENTIFICAR LOS SERVIDORES VIRTUALES “NAT” CONFIGURADOS

3.6. A PLANTILLA DE PERFIL DE RED

3.7. LISTA DE SERVIDORES

3.8. PLANTILLA DE DATOS DE SERVIDORES

3.9. SEGURIDAD FÍSICA

Este es un método para evaluar la seguridad física de una organización y sus bienes, verificando las medidas de seguridad de su perímetro físico.

3.9.1. IDENTIFICACIÓN DE PUNTOS DE ACCESO

Para ingresar al edificio del ME existen los siguientes accesos

- El acceso principal por la avenida Amazonas en cual esta resguardado por dos guardias de seguridad en la puerta de acceso que dirige a la gente hasta una isla de información donde se registra el ingreso y se asigna una identificación del piso que va a visitar a cambio de un documento personal.
- El acceso secundario por la avenida Juan Pablo Sanz exclusivamente para funcionarios del Ministerio de Educación, resguardado por dos personas de seguridad
- El acceso vehicular por la avenida Juan Pablo Sanz para vehículos de los funcionarios y oficiales del Ministerio

3.9.2. SEGURIDAD POR PISOS

Los pisos estratégicos que cuentan con seguridad son los siguientes:

- El Lobby cuenta con una persona de seguridad ya que existe las ventanillas que se atiende al público y la biblioteca Pablo Palacios
- EL piso 12 cuenta con una persona de seguridad que resguarda el ingreso de las personas al Despacho Ministerial y Subsecretaria de Educación
- El piso 13 cuenta con una persona de seguridad que resguarda el ingreso de las personas a la Subsecretaria de Planificación, Planeamiento. Desarrollo Institucional, y Interculturalidad
- Parqueadero E1 y E2 cuenta con una persona de seguridad que vigila cualquier anomalía en la parte del parqueadero

3.9.3. SISTEMAS DE MONITOREO

Se encuentra instalado un circuito cerrado de televisión que está en proceso de capacitación y traspaso al personal de seguridad

3.10. PROPUESTA DE POLITICA DE SEGURIDAD PARA EL USO DE LOS RECURSOS INFORMATICOS DEL MINISTERIO DE EDUCACION

Versión 1.0.0.

ARTÍCULO 1. NORMAS Y RESTRICCIONES PARA EL USO DE COMPUTADORES E INFRAESTRUCTURA DE COMUNICACIONES

1.1 NORMAS PARA EL USO DE COMPUTADORES:

Los usuarios del Ministerio de Educación deberán cumplir las siguientes normas para el manejo de los computadores:

a) Los recursos de computación se deben usar exclusivamente en el desarrollo de las funciones y actividades laborales vinculadas a esta Cartera de Estado.

b) La Unidad de Tecnología Informática y Comunicaciones, conjuntamente con la Unidad de Activos fijos y Donaciones, hará la entrega oficial del equipo informático en correcto funcionamiento, con el respectivo software instalado, de acuerdo con las actividades que se realicen en el mismo con los respectivos documentos.

c) Únicamente el personal autorizado de la Unidad de Tecnología Informática y Comunicaciones, puede llevar a cabo cualquier tipo de mantenimiento, tanto del hardware como del software, instalación de aplicaciones y configuración de acceso a la red.

d) Todos los equipos de computación que utilicen la red de datos, deberán estar integrados al dominio de la institución, contar con antivirus con definiciones actualizadas.

e) Queda prohibida la instalación de cualquier tipo de software en los equipos informáticos del Ministerio de Educación que no haya sido debidamente revisado y/o autorizado por la Unidad de Tecnología Informática y Comunicaciones.

f) El usuario debe reportar cualquier tipo de anomalía o daño detectado en el equipo informático a la Unidad de Tecnología Informática y Comunicaciones.

g) El usuario es el único responsable del uso que se dé al equipo informático bajo su cargo

No se permite a los usuarios:

a) Retirar computadores o sus accesorios del edificio del Ministerio de Educación

b) Fumar, comer o ingerir bebidas mientras se esté usando el computador.

c) Pegar calcomanías propagandas imantadas o cualquier tipo de adornos en los equipos.

1.2 NORMAS PARA EL USO DE LA INFRAESTRUCTURA FÍSICA DE COMUNICACIONES.

1. El diseño, la administración y el mantenimiento de las redes del Ministerio de Educación son responsabilidad del área de Gestión de Redes de la Unidad de Tecnología Informática y Comunicaciones.

2. La construcción de redes de cableado será dirigida por la Unidad de Tecnología Informática y Comunicaciones, de acuerdo a estándares internacionales.

3. No está permitido intervenir las redes de cableado, instalando cables no suministrados por la Unidad de Tecnología Informática y Comunicaciones, cortando o empalmando cables, desprendiendo etiquetas de tomas, puertas o ductos, golpeando o forzando tubos y/o canaletas.

4. Tampoco está permitida la instalación de cables, derivaciones a través de conectores en “T” o cualquier tipo de derivación de voz o datos por parte de los usuarios, salvo previa autorización de la UTIC.

5. Por ningún motivo se permite el acceso a los ductos de comunicaciones a personal no autorizado.

6. Los ductos ubicados en la parte noroeste del edición son exclusivamente para los equipos de comunicación de la red de datos del ME

7. Las oficinas que dan acceso a los ductos ubicados en la parte noroeste de los pisos: 1, 3, 5, 6, 7, 9 y 11; deben permanecer accesibles a los funcionarios del Área de Redes, Infraestructura y Seguridades de la UTIC.

8. Es responsabilidad del ARIS la seguridad física de los equipos activos ubicados en los ductos del edificio.

ARTÍCULO 2. NORMAS SOBRE EL USO DE LA RED INTERNA E INTERNET

Los funcionarios del Ministerio de Educación deben cumplir las siguientes normas para el uso de la red interna e internet:

- A cada funcionario se le asignara un usuario de red el mismo que tiene el carácter de personal e intransferible, el estándar para la creación del usuario es: nombre el símbolo punto y apellido. Ejemplo fabricio.zavala

- Para la creación del usuario de red el funcionario debe llenar el Formulario de Solicitud

- Todo usuario de la red institucional, gozará de absoluta privacidad sobre su información, o la información que provenga de sus acciones, salvo en casos, en que se vea involucrado en actos ilícitos o contraproducentes para la seguridad de la red institucional.

- Respetar la privacidad de otros usuarios. No está permitido obtener copias intencionales de archivos, códigos, contraseñas o información ajena; ni suplantar a otra persona en una conexión que no le pertenece o enviar información a nombre de otra persona sin consentimiento del titular de la cuenta.

- Los usuarios tendrán el acceso a Internet e intranet, siempre y cuando se cumplan los requisitos mínimos de seguridad (sistema operativo y antivirus actualizado).

- Los Funcionarios que trabajen con sistemas de información, se les asignará un usuario para el sistema con los accesos requeridos según las tareas que debe realizar.

- Las contraseñas utilizadas por los funcionarios deben cumplir las siguientes características:

    - Debe contener mínimo 7 caracteres y máximo 15
    - Debe contener al menos un mayúscula
    - Debe contener al menos una minúscula
    - Debe contener un carácter alfanumérico

  Ejemplo: Sidf34Fk

- Se debe evitar el guardar o escribir las contraseñas en cualquier papel o superficie o dejar constancia de ellas, a menos que ésta sea guardada en un lugar seguro.

- Cualquier usuario que encuentre un hueco o falla de seguridad en los sistemas informáticos de la institución, está obligado a reportarlo a la UTIC.

- Se realizará un respaldo periódico de la información de los servicios de mayor importancia o críticos, la cual deberá ser guardado y evitar su utilización a menos que sea estrictamente necesaria.

- Respetar la protección legal otorgada a programas, textos, artículos y bases de datos según legislación internacional sobre propiedad intelectual y las normas pertinentes de nuestro país.

- Respetar la integridad de los sistemas de computación. Esto significa que ningún usuario podrá adelantar acciones orientadas a infiltrarse, dañar o atacar la seguridad informática del Ministerio de Educación a través de medio físico o electrónico alguno.

- El acceso a la configuración del sistema operativo de los servidores, es únicamente permitido al usuario administrador.

- Los administradores de servicios, tendrán acceso único a los módulos de configuración de las respectivas aplicaciones que tienen bajo su responsabilidad.

- No obtener ni suministrar información sin la debida autorización.

- Las claves de acceso y contraseñas tienen carácter de confidenciales e intransferibles, quedando estrictamente prohibida su divulgación o préstamo.

- Los usuarios están en la obligación de cambiar sus claves y contraseñas periódicamente (cada 3 meses).

- No se permite el uso de Internet en el edificio de la Planta Central del ME a través del sistema telefónico.

- No está permitido acceder a Internet con fines diferentes a los propios de las actividades laborales. Esto significa no hacer uso del internet para realizar ataques desde o hacia el Ministerio de Educación, no acceder a lugares riesgosos entiéndase pornografía, paginas de crackers, hackers.

- Se prohíbe el uso de Internet y del servicio de Correo Electrónico con fines obscenos, de esparcimiento o contenidos que no tenga que ver con temas laborales.

- Se prohíbe de forma terminante el acceso y difusión de contenidos de carácter discriminatorio de cualquier tipo, pornografía infantil, sexista, de apología del terrorismo, religiosa, de incitación a la violencia o atentatorio contra la moral y los derechos humanos.

- La creación de nuevas redes o reconfiguración de las existentes, solo podrá ser realizada por personal autorizado por la Unidad de Tecnología Informática y Comunicaciones del ME.

- Los usuarios de la red institucional, serán capacitados en cuestiones de seguridad de la información, según sea el área operativa y en función de las actividades que se desarrollan.

- Se registrará y archivará toda actividad, procedente del uso de las aplicaciones, sistemas de información y uso de la red, mediante archivos de Log o bitácoras de sistemas.

- Las configuraciones y puesta en marcha de servicios, son normadas por la UTIC

- La UTIC, es la responsable de mantener en óptimo funcionamiento los servicios, coordinando esfuerzos con proveedores y contratistas

- El personal responsable de los servicios, llevará archivos de registro de fallas de los sistemas, revisara, estos archivos de forma frecuente y en especial después de ocurrida una falla.

- Se debe efectuar una auditoria de seguridad a los sistemas de acceso a la red, semestral, enmarcada en pruebas de acceso tanto internas como externas, desarrolladas por personal técnico especializado o en su defecto personal capacitado en el área.

ARTÍCULO 3. NORMAS SOBRE EL USO DE CORREO ELECTRÓNICO INSTITUCIONAL

El Ministerio de Educación, asignará una cuenta de correo electrónico a todos sus funcionarios y al personal que lo requiera en direcciones provinciales, comisiones, subsecretarias regionales, proyectos y programas institucionales que requieran manejar correo oficial. Dicha cuenta es personal e intransferible.

Cuando un funcionario salga de vacaciones, comisión o sea suspendido en sus funciones, la Dirección de Recursos Humanos deberá informar oportunamente los cambios a la Unidad de Tecnología Informática y Comunicaciones para proceder a la depuración correspondiente (activar, desactivar o eliminar) el usuario asignado al funcionario.

En el uso del correo electrónico no está permitido:

Atentar contra la integridad del Ministerio de Educación.

- Se prohíbe el uso de Correo Electrónico con fines obscenos, religioso, de esparcimiento o contenidos que no tenga que ver con temas laborales.

- Divulgar información que incite a la discriminación o la violencia.

- Actuar en perjuicio de los derechos a la intimidad, al honor, a la propia imagen en contra de la dignidad de las personas.

- Enviar contenidos con fines publicitarios y comerciales de bienes y servicios en beneficio propio, de familiares o de terceros, salvo en los casos en los cuales la Unidad de Tecnología Informática y Comunicaciones o una instancia superior lo autorice expresamente.

- Enviar correo tipo SPAM, es decir “correo basura”, relacionado con falsos virus, con publicidad de empresas, cadenas de mensajes, etc.

- Usar la cuenta de correo electrónico de otro usuario o entregar a un tercero la contraseña propia y falsificar mensajes de correo electrónico.

- Leer, borrar, copiar o modificar mensajes de correo electrónico de otras personas, sin su autorización.

- Enviar mensajes de correo electrónico, alterando la dirección electrónica del remitente para suplantar a terceros; identificarse como una persona ficticia o simplemente no identificarse.

- Iniciar o continuar cadenas de mensajes pues éstas tienden a congestionar innecesariamente la red.

- Usar el servidor de correos como medio para archivar los mensajes, los cuales se recomienda borrar una vez leídos. Si hay necesidad de conservarlos, los mensajes se deberán grabar en un sitio destinado para su almacenamiento; esto también se aplica a los correos enviados y a la papelera de reciclaje. Así mismo, cuando las unidades requieran compartir un archivo, se sugiere hacerlo utilizando las herramientas pertinentes, en vez de enviarlo por correo.

- El uso del correo electrónico institucional está destinado para toda aquella labor que se lleve a cabo para la institución.

- No se usaran correos libres personales para enviar o recibir información concerniente al Ministerio de educación. Ningún correo personal dará el carácter de oficial a la información institucional.

- En caso de detectar una saturación o ataque a un buzón ya sea por spam o virus, el Administrador de Red con el Administrador de Seguridad están facultados para depurar y borrar dichos correos.

- El Ministerio de Educación, no asume responsabilidad alguna por los contenidos emitidos a través del correo electrónico o por el uso ilegal y mal intencionado por parte de los usuarios.

Data Center.-

- Toda visita al Data Center (sala de servidores) deberá ser registrada mediante el formulario de accesos a las salas de procesamiento crítico, para posteriores análisis del mismo.

- La sala o cuarto de servidores, deberá estar separada de las oficinas administrativas de la unidad de informática o cualquier otra unidad, departamento o sala de recepción del personal, mediante una división en la unidad de informática, recubierta de material aislante o protegido contra el fuego, Esta sala deberá ser utilizada únicamente para los servidores y/o dispositivos a fines.

- La división de servicios generales del ME, deberá garantizar el suministro de energía eléctrica a través de un circuito exclusivo para los equipos de cómputo, o en su defecto el circuito que se utilice no debe tener conectados equipos que demandan grandes cantidades de energía.

- El Data Center debe contar con una adecuada instalación eléctrica, y provista del suministro de energía mediante una estación de alimentación ininterrumpida o UPS para poder proteger la información.

ARTÍCULO 4. SANCIONES

La violación de cualquiera de estas normas podrá causar al usuario la cancelación de la cuenta de correo electrónico, la suspensión indefinida de todos los servicios de la red e internet y demás sanciones contempladas en los Reglamentos Internos del Ministerio de Educación.

CAPITULO 4

CONCLUSIONES Y RECOMENDACIONES

4.1. INTRODUCCIÓN

En el proceso de elaboración de esta tesis se tuvo grandes enigmas respecto a la seguridad ya que si aseguramos puertos y servicios el problema era el trafico solucionamos el problema y encontramos la autenticación como saber que el usuario que se logea es el usuario que dice ser y así si tapamos un hueco encontrábamos otro. Esto conllevo a asegurar que para mantener un nivel alto de seguridad hay que estar constantemente investigando nuevas herramientas de seguridad y cruzar los resultados con otras, además un elemento fundamental son las políticas de seguridad planteadas las mismas que se deben cumplir a cabalidad sin excepción alguna.

4.2. CONCLUSIONES GENERALES

Se alcanzo el objetivo de Implementar un Sistema de Seguridad Informática para la Planta Central del ME, el cual permita proteger, gestionar y administrar de forma adecuada la información, proporcionando confidencialidad, integridad, rendimiento y disponibilidad a la misma.

Se planteo las políticas de seguridad para el Ministerio de Educación necesarios para cubrir vulnerabilidades internas de la organización.

Para que la seguridad informática sea todo un éxito todos los que forman parte de la organización deben conocer y cumplir las políticas implementadas ya que solo basta uno que no cumpla para que las seguridad quede vulnerable

4.3. CONCLUSIONES ESPECÍFICAS

El contar con equipos activos de seguridad no garantiza que nuestra organización esté libre de vulnerabilidades por los que estar en constante investigación es importante para adelantar y poder proteger de nuevos ataques o vulnerabilidades explotadas.

Se obtuvo un listado completo de puertos y servicios con su versión de cada uno de los servidores lo cual permitió tomar medidas en algunos casos de eliminar el servicio y en otros parchar el servicio

Existe herramientas de software libre que permiten realizar monitoreo de la seguridades y buscar vulnerabilidades de los equipos. Estas herramientas también son utilizadas por personas que tratan de causar daños a la organización por lo que conocerlas y aplicarlas permitirán proteger nuestra infraestructura.

4.4. RECOMENDACIONES

Los funcionarios que administran los equipos activos de seguridad del ME, deben tomar los cursos necesarios que permita dominar la gestión de los equipos implementados.

Los funcionarios de la UTIC deben capacitarse el idioma ingles ya que en la actualidad la mayoría de herramientas e información de seguridad está en ingles.

Integrar a la mayor parte de dependencias para fortalecer las políticas de seguridad implementadas o están por implementarse.

Los funcionarios deber recibir una remuneración acorde a sus responsabilidades.

La continuidad del personal es fundamental para el desarrollo del Ministerio por lo que la estabilidad es fundamental para los procesos a corto y largo plazo.

Se debe realizar dos veces al año un análisis de tráfico de red, servicios y protocolos utilizados en la red

Cada dos años se debe contratar una empresa especializada que realice una auditoría de seguridad informática en el ME

Las copias de seguridad deben ser guardadas semanalmente en una caja de seguridad fuera del edificio del ME

Las conexiones a los servidores vía SSH no se debe realizar como root debe crearse un usuario de conexión y una vez ingresado darse privilegios

No permitir excepción alguna en las políticas de seguridad implementadas

Todos los equipos activos de red deben contar con seguridad física para evitar un mal manejo

GLOSARIO

Acnowledgement (ACK) (acuse de recibo) Un tipo de mensaje que se envía para indicar que un bloque de datos ha llegado a su destino sin errores.

ARP: Address resolution protocol. Protocolo utilizado en las redes de difusión para resolver la dirección de IP en base a la dirección de trama de capa 2.

Backbone Nivel más alto en una red jerárquica. Se garantiza que las redes aisladas (stub) y de tránsito (transit) conectadas al mismo eje central están interconectadas.

BOOTP Protocolo de bajo nivel para la asignación de direcciones IP a maquinas simples desde un servidor en una red física.

CGI. (Common Gateway Interface). Una interfaz escrita en un lenguaje de programación (perl, c, c++,visual basic, etc) y posteriormente ejecutada o interpretada por una computadora servidor para contestar a pedidos del usuario desde una computadora con una aplicación cliente; casi siempre desde el World Wide Web. Esta interfaz permite obtener los resultados pedidos, como los que resultan al consultar una base de datos.

Cookie. Procedimiento ejecutado por el servidor que consiste en guardar información acerca del cliente para sus posterior recuperación En la práctica la información es proporcionada desde el visualizador al servidor del Word Wide Web vía una forma o un método interactivo que puede ser recuperado nuevamente cuando se acede al servidor en el futuro. Es utilizado por ejemplo para el registro a un servicio.

Cracker (intruso) Un "cracker" es una persona que intenta acceder a un sistema informático sin autorización. Estas personas tienen a menudo malas

intenciones, en contraste con los "hackers", y suelen disponer de muchos medios para introducirse en un sistema.

DNS (Domain Name Service) Base de Datos distribuida que mapea nombres de sistemas con direcciones IP y viceversa.

Dominio. Conjunto de computadoras que comparten una característica común, como el estar en el mismo país, en la misma organización o en el mismo departamento. Cada dominio es administrado un servidor de dominios.

Intranet. Una red privada dentro de una compañía u organización que utiliza el mismo software que se encuentra en Internet, pero que es solo para uso interno.

IP address (Dirección IP) Dirección de 32 bits definida por el Protocolo Internet en STD 5, RFC 791. Se representa usualmente mediante notación decimal separada por puntos.

Local Area Network (LAN) (Red de Area Local) Red de datos para dar servicio a un área geográfica pequeña, un edificio por ejemplo, por lo cual mejorar los protocolos de señal de la red para llegar a velocidades de transmisión de hasta 100 Mbps (100 millones de bits por segundo).

Navegador: Aplicado normalmente a programas usados para conectarse al servicio WWW.

Nodo: Por definición punto donde convergen más de dos líneas. A veces se refiere a una única máquina en Internet. Normalmente se refiere a un punto de confluencia en una red.

Packet internet Groper (PING) (Búsqueda de Direcciones de Internet) Programa que se utiliza para comprobar si un destino está disponible.

POP. Protocolo de Oficina de Correos (Post Office Protocol) Programa cliente que se comunica con el servidor, identifica la presencia de nuevos mensajes, solicita la entre de los mismos y utiliza al servidor como oficina despachadora de correo electrónico cuando el usuario envía una carta.

Protocolo Descripción formal de formatos de mensaje y de reglas que dos Computadores deben seguir para intercambiar dichos mensajes.

Proxy Una substitución de direcciones, usado para limitar la información de direcciones disponibles externamente.

Proxy Server: Un server que se sitúa entre la aplicación cliente, como por ejemplo un web browser, y un server real. Intercepta todos los requerimientos al server real para ver si las puede resolver el, si no, envía el requerimiento al server real. Los proxy servers tienen dos propósitos principales:
Mejorar la performance: Los proxy server mejoran la perfomance de un grupo de usuarios, ya que guardan los resultados de los requerimientos de los mismo una determinada cantidad de tiempo..

PSI
Política de Seguridad Informática

RARP: Reverse Address Resolution Protocol. Protocolo de Resolución de Dirección de Retorno. Protocolo de bajo nivel para la asignación de direcciones IP a maquinas simples desde un servidor en una red física.

Request For Comments (RFC) (Petición de comentarios) Serie de documentos
iniciada en 1969 que describe el conjunto de protocolos de Internet. No todos los rfcs (en realidad muy pocos de ellos) describen estándares de Internet pero todos los estándares Internet están escritos en forma de rfcs. La serie de documentos RFC es inusual en cuanto los protocolos que

describen son emitidos por la comunidad Internet que desarrolla e investiga, en contraste con los protocolos revisados y estandarizados formalmente que son promovidos por organizaciones como la ITU.

Router (direccionador) Dispositivo que distribuye tráfico entre redes. La decisión sobre a dónde enviar se realiza en base a información de nivel de red y tablas de
direccionamiento. El router se necesita cuando las dos redes utilizan la misma capa de transporte y tienen diferentes capas de red. Por ejemplo, para una conexión entre una red local ethernet y una red pública X.25, se necesitaría un router para convertir las tramas ethernet a la forma que exige la red X.25.

SIME
Sistema de Información del Ministerio de Educación

S-HTTP: Secure HTTP. HTTP seguro. Protocolo HTTP mejorado con funciones de seguridad con clave simétrica.

SMTP: Simple Mail Transfer Protocol. Protocolo de Transferencia Simple de correo. Es el protocolo usado para transportar el correo a través de Internet.

SSL: Secure Sockets Layer. Capa de Socket Segura. Protocolo que ofrece funciones de seguridad a nivel de la capa de transporte para TCP.

Switching Hub: También llamado port-switching hub o simplemente switch es un tipo especial de hub que envía los paquetes al port apropiado basado en la dirección del paquete. Los hubs convencionales simplemente difunden cada paquete a cada port. Como los switching hubs envían cada paquete solo a los ports requeridos, proveen mucha mejor perfomance. Muchos switching hubs soportan además load balancín, de esta manera los ports son reasignados dinámicamente a diferentes segmentos de LAN basados en el tráfico. Además, varios modelos soportan ethernet a 10 Mbps. y Fast Ethernet (100 Mbps), esto permite al administrador establecer un canal

dedicado de Fast ethernet a dispositivos como por ejemplo servers. **NOTA** Nótese la implicancia en seguridad que tiene usar switching hubs, un sniffer colocado en un port solo vería las tramas dirigidas a ese port, con lo cual no podría inspeccionar tramas que no le correspondan. Por ende, es esencial utilizar switches en vez de hubs comunes.

TCP: Transmisión Control Protocol. Protocolo de control de Transmisión. Uno de los protocolos más usados en Internet. Es un protocolo de capa de transporte.

TCP/IP (Transmisión Control Protocol/Internet Protocol) Arquitectura de red desarrollada por la "Defense Advanced Research Projects Agency" en USA, es el conjunto de protocolos básicos de Internet o de una Intranet.

Trojan Horse (Caballo de troya) programa informático que lleva en su interior la lógica necesaria para que el creador del programa pueda acceder al interior del sistema que lo procesa.

UDP. Protocolo de Datagramas de usuario (User Datagram Protocol). Protocolo que no pide confirmación de la validez de los paquetes enviados por la computadora emisora.
Este protocolo es actualmente usado para la transmisión de sonido y vídeo a través de Internet. El UDP está diseñado para satisfacer necesidades concretas de ancho de banda, como no reenvía los datos perdidos, es ideal para el tráfico de voz digitalizada, pues un paquete perdido no afecta la calidad del sonido.

URL. Localizador Uniforme de recursos (Uniform Resorce Locator). Sistema de direccionamiento estándar para archivos y funciones de Internet, especialmente en el Word Wide Web. El url está conformado por el servicio (p. e. http://) más el nombre de la computadora (p. e. www.sfp.gov.ar) más el directorio y el archivo referido.

UTIC

Unidad de Tecnología Informática y Comunicaciones del Ministerio de Educación

WWW, WEB o W3: World Wide Web. Estrictamente que la WEB es la parte de Internet a la que accedemos a través del protocolo HTTP y en consecuencia gracias a Browsers normalmente gráficos como Netscape.

BIBLIOGRAFIA

- Libros

RUIZ, Víctor, Seguridad de Redes, Ediciones Anaya Multimedia
España-Madrid

- Manuales

BORGHELLO, Cristian, Seguridad Informatica sus Implicanciase Implementación
Buenos Aires- Argentina 2001

HERZOG, Peter, Manual de la Tecnología Abierta de Testeo de Seguridad
Buenos Aires- Argentina 2003

MONROY, Daniel, Análisis Inicial de la Atomía de un Ataque a un Sistema Informático
México 2009

SUBSECRETARIA, de la Función Pública, Manual de Seguridad en Redes
Buenos Aires -Argentina 1998

ANEXO A