ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL.

Facultad de Ingeniería en Electricidad y Computación

Maestría En Seguridad Informática Aplicada

"DESARROLLO E IMPLEMENTACIÓN DE UN ESQUEMA DE ASEGURAMIENTO INFORMÁTICO A LOS SERVIDORES DE PRODUCCIÓN CON SISTEMAS OPERATIVOS WINDOWS Y LINUX MINIMIZANDO EL ACCESO INTERNO Y EXTERNO NO AUTORIZADO"

TESIS DE GRADO

Previa a la obtención del Título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

FRANK EMERSON ORDOÑEZ CHÁVEZ

GUAYAQUIL – ECUADOR
AÑO: 2015

AGRADECIMIENTO

A Dios por darme vida haciendo posible lograr mis objetivos, a mis padres Lcdo. Alirio Ordóñez Bone y Sra. Martha Chávez Vizueta, por su ánimo y apoyo. A mis hermanos Ordóñez Chávez Leyton, Damaris, Jemima y Josías por todo el apoyo brindado y por incluirme siempre en sus oraciones.

A mi esposa Lcda. Daysi Buitrón Zambrano y a mis hijos Tahís y Emerson por al apoyo y comprensión que me brindaron en todo momento, por el tiempo que a ustedes pertenecía y que altruistamente me cedieron.

DEDICATORIA

Dedico este proyecto de tesis con mucho afecto a las personas que sirvieron de inspiración a mi persona por su ejemplo, lucha y persistencia, mi padre Alirio y madre Martha.

A personas muy importantes en mi vida, por su compresión, sacrificio y apoyo incondicional, mi esposa Daysi y mis hijos Tahís y Emerson.

A mis hermanos Leyton, Damaris, Jemima, Josías, que ante toda adversidad con preparación y dedicación se puede salir victorioso, incluyendo la pretensión de cinco sucres.

Frank Emerson Ordóñez Chávez.

TRIBUNAL DE SUSTENTACIÓN

_____

Mgs. Lenin Freire Cobo

DIRECTOR MSIA

_____

Mgs. Fabián Barbosa

DIRECTOR DE TESIS

_____

Mgs. Néstor Arreaga

MIEMBRO DEL TRIBUNAL

DECLARACIÓN EXPRESA.

La responsabilidad del contenido de esta tesis de grado, por los hechos, ideas y doctrinas expuesto en este proyecto, nos corresponden exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral.

(Reglamento de exámenes y título profesionales de la ESPOL).-

_____

Frank Ordóñez Chávez.

RESUMEN.

Se elaboró el presente proyecto de tesis con el objetivo de integrar los conocimientos adquiridos en la quinta promoción de la maestría en seguridad informática aplicada, desarrollando un esquema de aseguramiento informático a nivel de los sistemas operativos Windows server 2008 estándar y Linux red hat versión 5.5, los cuales son usados en los centros de procesamiento de la empresa de servicios postales nacionales, que por su lógica de negocio y actividad comercial, maneja, procesa y distribuye información sensible y a igual nivel confidencial, siendo necesario implementar esta medida de seguridad durante el procesamiento de la información.

En el capítulo 1 se tratará y revisará los antecedentes que son base para el desarrollo de este proyecto de tesis, se especificaran los objetivos generales, específicos, la descripción del problema y la solución propuesta.

En el capítulo 2 se revisara de forma general la historia de la seguridad informática, su definición y conceptos básicos, las principales amenazas de seguridad de los sistemas informáticos, las amenazas de seguridad de los

sistemas operativos y una explicación técnica de violación de acceso o acceso no autorizado.

En el capítulo 3 se exponen de forma general las actuales medidas de seguridad de los sistemas informáticos, en su ámbito lógico, físico, de comunicación y de aplicaciones. Adicionalmente se propone soluciones generales a las amenazas de estos sistemas.

En el capítulo 4 se desarrolla esta propuesta de solución mediante la revisión de los factores de riesgo, vulnerabilidades, análisis de requerimientos para crear un diseño base de protección, y así obtener un esquema de aseguramiento informático para los sistemas operativos Windows server 2008 estándar y Linux red hat versión 5.5.

En el capítulo 5 se realizara la implementación del esquema aseguramiento informático en los sistemas operativos Windows server 2008 estándar y Linux red hat versión 5.5 con la respectiva verificación. Se describirá la configuración básica en los servidores para el almacenamiento local de los log y también hacia un repositorio central. Adicionalmente se realizará un

análisis de resultados post implementación del aseguramiento que incluya las correcciones de las vulnerabilidades generales.

En el capítulo 6 se indicara las pautas para la implementación de una gestión de control a la implementación al esquema de aseguramiento informático a los sistemas operativos, se revisara un reporte post aseguramiento, se realizara una auditoria al aseguramiento realizado, se recomendará medidas contingentes y se dará sugerencias para la mejora continua al esquema de aseguramiento.

ÍNDICE GENERAL.

ABREVIATURAS Y SIMBOLOGÍA.

APPLIANCE	Equipos dedicados especializados para funciones específicas.
BIOS	Basic Input Output System.
CRACKERS	Personas que rompen algún sistema de seguridad.
DHCP	Protocolo de configuración dinámica de host.
DMZ	Zona desmilitarizada.
DNS	Sistema de nombres de dominio.
DVD	Digital Versatile Disc.
EEUU	Estados Unidos.
ESET	Compañía de seguridad informática.
ETHICAL HACKING	Metodología de análisis en diversas plataformas y aplicaciones con el objetivo de identificar y validar vulnerabilidades que las comprometan.
FILESYTEM	Sistema de archivos.
FIREWALL	Sistema que previene el uso y el acceso desautorizados a un ordenador.
FTP	File Transfer Protocol.
GUID	Globally unique identifier.
HOST	Se refiere a las computadoras conectadas a una red.
HTTP	Protocolo de transferencia de hipertextos.

IDS	Sistema de deteccion de intrusos.
IMAP	Internet Message Access Protocol.
IP	Acrónimo para Internet Protocol.
IPS	Sistema de prevención de intrusos
ISO	Organización Internacional de Normalización.
KVM	Keyboard, Video and Mouse.
LAN	Red de área local.
NASA	Administración Nacional de la Aeronáutica y del Espacio.
NAT	Network Address Translation.
NFS	Sistema de archivos de red.
NTFS	New Technology File System.
OSI	Open System Interconnection.
PC	Computadora personal.
POP3	Post Office Protocol.
SMTP	Simple Mail Transfer Protocol.
SOFTWARE	Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.
STAKEHOLDER	Se refiere a quienes son afectados o pueden ser afectados por las actividades de una empresa.
TCP/IP	Protocolo de Control de Transmisión/Protocolo de Internet

TELNET	Telecommunication Network, protocolo de red.
TI	Tecnologías de la Información.
TIC	Tecnologías de la Información y las Comunicación
TRUSTKEEPER	Software de evaluación de vulnerabilidades.
UDP	Protocolo de datagramas de usuario.
UID	Identificador de usuario.
UNIX	Es un sistema operativo, colección de programas que ejecuta otros programas en una computadora.
USB	Universal serial bus.
WAN	Red de área amplia.

ÍNDICE DE FIGURAS.

ÍNDICE DE TABLAS.

INTRODUCCIÓN.

El desarrollo tecnológico y sus avances para un mejor desempeño son notables en este último siglo, permitiendo a las personas y sociedades utilizarla en todos los ámbitos de su vida cotidiana. Actualmente los sistemas informáticos son implementados por empresas, industrias y gobiernos, siendo una base fundamental en sus actividades institucionales, tributarias, legales y de los procesos de comercialización de bienes y servicios que brindan.

En la mayoría de las entidades mencionadas, los datos junto con los sistemas de información, sean estos pequeños, medianos o grandes, son los activos esenciales e imprescindibles para la continuidad y permanencia de sus actividades de gestión o lucrativas en un país o mercado, según corresponda.

Los sistemas informáticos, por su propia naturaleza tienen un alto grado de vulnerabilidad siendo estos agravados por la inexistencia de políticas de seguridad o por la falta de la implementación de procedimientos que minimicen y corrijan estas vulnerabilidades, que al no ser tratadas de forma

preventiva, estas instituciones sufren o pueden sufrir ataques de virus, actividades de usuarios maliciosos, de crackers o hacker, accediendo de forma ilegal a información confidencial o sensible, pudiendo estas acciones ser perjudiciales para la entidad debido a la fuga, robo o venta de esta información, sin medir afectaciones intangibles como el deterioro de la imagen institucional, marca, prestigio y pérdida de mercado.

La tecnología también es usada para actividades ilícitas y el reciente informe sobre seguridad informática emitido por la empresa ESET Latinoamérica [1] indica que estas actividades indebidas están creciendo de forma exponencial con nuevos métodos y técnicas con el único objetivo de robar información, el activo más importante de un estado, empresa y persona.

CAPÍTULO 1.

GENERALIDADES.

1.1. ANTECEDENTES.

Priscila Balcázar [2] indicó: “Lo único seguro es que somos vulnerables”.

Una frase que expresa una gran verdad en cuanto a la seguridad a sistemas informáticos se refiere.

Actualmente, estado, gobierno, industria, empresas públicas y privadas ha incrementado el uso de las tecnologías de la información y comunicaciones (TIC), haciendo que la información y los recursos informáticos que la gobiernan tengan un rol importante en las actividades económicas, sociales y culturales, junto a este incremento es también cada vez mayor la cantidad de amenazas y

ataques que se producen a las aplicaciones y recursos informáticos como indica Symantec [3]

La empresa Mail Service Express con el objetivo de brindar un servicio ágil y eficiente invierte en la modernización de su plataforma tecnológica pasando de archivos planos en computadores con ninguna medida de seguridad, sin red en sus agencias y matriz a una infraestructura informática interconectada, actual y vanguardista. Es en este contexto que la información se convierte en un recurso crítico al que hay que salvaguardar. La seguridad informática se vuelve indispensable como forma de garantizar la integridad, disponibilidad y confidencialidad de la información.

Mail Service Express luego de haber adquirido e implementado su nueva plataforma no ha implantado en sus servidores del ambiente de producción ningún aseguramiento al sistema operativo, no ha desactivados los usuarios del sistema que vienen activos de forma nativa después de la instalación del mismo, no ha afinado los privilegios adecuados a los directorios importantes del sistema ni a los que usan las aplicaciones instaladas en los mismos. Es casi obligatoria para la organización la preparación técnica y metodológica para salvaguardar sus activos de información, ello involucra conocer y aplicar de forma apropiada estándares, normativas, metodologías, técnicas, herramientas, conceptos y

avances actuales en esta materia, para lograr el objetivo de seguridad.

Es necesario contar con talento humano profesional, adecuadamente instruido y actualizado, que puedan emplear de forma exitosa técnicas y conocimientos de seguridad informática para adaptarse ágilmente a los cambios tecnológicos y a las altas exigencias de un área que está en constante evolución y cambio.

1.2. OBJETIVO GENERAL.

Establecer un esquema de aseguramiento informático a los servidores de producción de la empresa Mail Service Express con el propósito de implantar medidas de seguridad recomendados en los servicios y sistemas de archivos de los sistemas operativos, incluyendo elementos de hardware.

1.3. OBJETIVOS ESPECÍFICOS.

Especificar directrices de seguridad en la administración de usuarios y grupos.

Implementar una política de seguridad de la información en la administración de usuarios

Establecer lineamientos de configuración y de seguridad recomendados en la administración del sistema operativo.

Definir esquemas de seguridad informática basadas en las mejores prácticas de TI con el objetivo de incrementar la seguridad física y lógica en las comunicaciones y aplicaciones.

1.4. DESCRIPCIÓN DEL PROBLEMA.

Actualmente la institución Mail Service Express brinda productos y servicios postales oportunos y eficientes a la ciudadanía ecuatoriana enmarcados en calidad y excelencia.

Para lograr esto, la empresa llevó a cabo un proceso de transformación mediante la renovación de imagen, reestructuración organizacional y modernización tecnológica implementando nuevos servicios los cuales son soportados por la nueva plataforma. Las aplicaciones informáticas y colaborativas de la institución están soportadas, en su mayoría, sobre servidores con sistemas operativos Linux y Windows, sin haberse implementado en ellos algún procedimiento de aseguramiento informático antes o durante la instalación, afinamiento y puesta en producción de estos equipos, adicionalmente no se ha realizado las correcciones correspondientes de las vulnerabilidades comunes de estos sistemas operativos, pudiendo ser usadas, aprovechadas y

explotadas por personal interno y externo para obtener acceso no autorizado a los servidores, servicios y aplicaciones de la institución. En este contexto se identifican los siguientes problemas en los sistemas operativos:

- No existe una adecuada administración de los usuarios y grupos del sistema que permitan diferenciar sus privilegios en los accesos a los recursos de la red.

- Falta de parametrización en las configuraciones de seguridad en la administración de los sistemas operativos.

- No existen registros de auditoría de las actividades realizadas en el sistema operativo.

- No existen medidas de seguridad en el acceso a los recursos compartidos de la red.

Todas estas omisiones y falencias en los servidores de producción deben ser corregidas para garantizar la integridad, confidencialidad y disponibilidad de la información. También se debe considerar que los servidores de producción están expuestos a recibir o ser objetivos de ataques informáticos usando las novedades descritas, los usuarios nativos de los sistemas los cuales no se han

deshabilitados o cambiado su clave, del uso indebido de servicios nativos innecesarios y recursos compartidos del sistema operativo en cuestión.

1.5. SOLUCIÓN PROPUESTA.

Dado que en la institución no existe un área de seguridad informática que defina y supervise la implementación de mejores prácticas u procedimientos de aseguramiento informático en la instalación o configuración de servidores, se presenta esta propuesta para la elaboración e implementación de un esquema de aseguramiento informático para los servidores salidos o salientes del ambiente de producción, con el objetivo de reducir las amenazas ocasionadas por la omisiones y la desatención de las falencias generales presentes en los sistemas operativos Windows y Linux.

Es obligatorio que los sistemas operativos Windows y Linux del ambiente de producción estén asegurado de múltiples (y hasta en muchas ocasiones desconocidas) amenazas informáticas y fin de garantizar la integridad total de los datos, la confidencialidad de los mismos para que la información sea accesible solo a las personas habilitadas y así los datos e información estén siempre disponibles y cuando lo necesiten los usuarios autorizados.

La creación e implementación de este esquema de aseguramiento para los servidores Windows y Linux del ambiente de producción, propone las siguientes medias para corregir las novedades existente mediante la:

- Definir una administración adecuada de usuarios y grupos del sistema operativo que permita asignar los privilegios precisos para el acceso de los recursos de red.
- Establecer una correcta parametrización de configuración de seguridad en la administración de los sistemas operativos.

- Habilitar, configurar y almacenar los registros de auditoría de las actividades realizadas en el sistema operativo.

- Precisar medidas de seguridad al compartir los recursos de red implementando una correcta gestión de acceso a los mismos.

Se busca que este esquema de aseguramiento informático establezca una base para el personal de TI de la institución y considere la importancia del aseguramiento informático en el ambiente de producción, concientizar sobre su valor para reducir drásticamente las falencias en este tema, el de resguardar los bienes y servicios que la institución brinda a la ciudadanía evitando accesos no autorizados y por ende afectaciones en la plataforma por alteraciones intencionadas o no intencionadas por parte de personal interno o externo. Igualmente inquiere formar parte en el proceso de diseño integral de aseguramiento, siendo tomado como base para ser aplicado no solo a nivel de servidores, sino también al hardware,

software, equipos activos, de red, comunicaciones, de almacenamiento primario y secundario, dispositivos de control y acceso. Mediante el uso de buenas prácticas de TI se busca incrementar la seguridad de los servidores Windows y Linux/Unix del ambiente de producción, protegiendo el activo más importante de la empresa que es la información ante accesos y uso por personal no autorizado.

CAPÍTULO 2

MARCO TEÓRICO

Los sistemas operativos deben ser protegidos teniendo en cuenta un enfoque multi-nivel que involucre controles humanos, físicos técnicos y administrativos que garanticen la mitigación de riesgos asociados a acceso no autorizados, amenazas de software malicioso y técnicas de hacking.

Como control mínimo, los servidores de la empresa Mail Service Express deben estar protegidos contra accesos no autorizados o al intentarlo sean detectados y desconectados del mismo.

Los estándares que se utilizan para la elaboración del esquema de aseguramiento informático es la norma ISO ISO/IEC 17799:2005 llamada hoy ISO/IEC 27002 basándonos en los siguientes dominios:

- Gestión de comunicaciones y operaciones (10), se incluye la supervisión (10.10) como objetivo de control y registros de auditoría (10.10.1), supervisión del uso del sistema (10.10.2), protección de la información de los registros (10.10.3), registros de administración y operación (10.10.4), registro de fallos (10.10.5) como controles.

- Control de acceso (11), el siguiente objetivo de control, requisitos de negocio para el control de acceso (1.1) con el control política de control de acceso (11.1.1). También el objetivo de control gestión de acceso de usuario (11.2) y los controles registro de usuario (11.2.1), gestión de privilegios (11.2.2), gestión de contraseñas de usuario (11.2.3), revisión de los derechos de acceso de usuario (11.2.4).

- El objetivo de control que indica el control de acceso al sistema operativo (11.5), que incluye los controles, procedimientos seguros de inicio de sesión (11.5.1), identificación y autenticación de usuario (11.5.2), sistema de gestión de contraseñas (11.5.3), uso de los recursos del sistema (11.5.4), desconexión automática de sesión (11.5.5), limitación del tiempo de conexión (11.5.6), aislamiento de sistemas sensibles (11.6.2)

2.1. HISTORIA.

Las organizaciones y empresas en general, son reactivas en vez de proactivas frente a incidentes o problemas tecnológicos, luego de ocurrido graves problemas de seguridad en la información ahí consideran la necesidad de implementar medias para evitar se repitan, otras en ocasiones no le dan mucha importancia, y así inicia la década de los 80 donde los sistemas informáticos tuvieron la necesidad de ser interconectados para agilizar el procesamiento y distribución de la información, presentándose una desventaja, la complejidad de administrar sistemas distribuidos de computadoras comparado con un único mainframe, debido a ello, se exteriorizaron varios incidentes que afectaron a estos sistemas, entre muchos uno de los más renombrados fue la vulneración y acceso a los sistemas de la NASA, el pentágono, la Universidad de Berkeley, Stanford, Princeton y la red de defensa de los EEUU; afectados por el primer gusano informático creado por Robert Tappan Morris, en primera instancia para demostrar las vulnerabilidades del trabajo de su padre Robert Thomas Morris experto en UNIX y empleado ingeniero en Bell Laboratories. El programa de bajo nivel se aprovechó de los fallos de seguridad se los sistemas operativos Unix realizando dos tareas, enviarse a otras máquinas y duplicarse en la maquina infectada, sin extender la historia, este gusano afecto y colapso al 10% del internet en 1988 estimando perdidas de cientos de millones de dólares.

Estos equipos computacionales no contaron con medidas de protección informática como en el día de hoy se realizaría a un servidor de un ambiente de producción, siendo fácilmente extraíble o copiable información, software, cintas y hasta discos confidenciales de las empresas, muchos de los cuales no dejaron rastros de estas acciones.

Mediante la aparición y el consecuente uso de la tecnología que ahora soportan grandes sistemas de información, también se ha incurrido y se incide en una práctica ilícita llamada fraude, que ocasionó y ocasiona pérdidas económicas para personas, empresas grandes o pequeñas así también como entidades estatales y de gobiernos, lo que causa graves efectos secundarios como el deterioro de la imagen corporativa, daño de la reputación en mercados y desprestigio a servicios profesionales.

Por estos acontecimientos y para no exponer o perder el control de sus sistemas informáticos, los gobiernos, en conjunto con iniciativas de empresas privadas, iniciaron la revisión de sus plataformas tecnológicas registrando todos los puntos “ciegos” o vulnerables, con el objetivo de encontrar la forma de solventar, corregir, reducir y evitar estas intrusiones o “accesos” no autorizados.

Creadas, normalizadas e implementadas las normas, buenas prácticas de protección y sistemas de gestión de seguridad de la

información, surgió otra práctica nociva dentro de las organizaciones, el sabotaje.

Un empleado descontento, un colega con rivalidad, la competencia que paga a un recurso interno por realizar una acción indebida, alguien que está a punto de perder su puesto de trabajo por recorte de personal, debido a esto, una persona dentro de una entidad que no posea los controles y la supervisión diaria necesaria, puede fácilmente realizar acciones u omisiones para lograr compartir, alterar, borrar, indisponer o destruir datos, archivos, bases de datos, respaldos, sistemas de almacenamientos, sistemas de comunicación, servidores y hasta centros de datos.

Para minimizar los posibles riesgos descritos anteriormente se incurre a la renovación de la tecnología y la implementación de actuales medidas de seguridad en ambientes de producción lo que genera costos de inversión elevados dando oportunidad a la aparición de un nuevo escenario, cómputo en la nube.

Este nuevo concepto de computación lo que busca es reducir estos riesgos y costos así como también el de traspasar la responsabilidad de mantenimientos, estimación de crecimiento de recursos como también la seguridad de la misma, siendo esta última una de las más importantes debido a la integración de muchas “herramientas” para la conformación de la nube.

2.2. CONCEPTOS BÁSICOS.

Seguridad significa proteger recursos valiosos, que pertenecen a un legítimo propietario, de los posibles peligros y ataques perpetrados por agentes no autorizados. **La seguridad informática** se ocupa de proteger los recursos de un sistema informático, información, servicios, arquitecturas.

Debemos conocer previamente las características de lo que vamos a proteger para iniciar el análisis de seguridad informática, de forma puntal, la información.

Sistema Operativo es un conjunto de programas que gestionan el hardware y los recursos de un computador mediante la interacción de rutinas de control, lenguajes y programas de aplicación, creando una interfaz de comunicación entre humano y maquina con la cual un usuario pueda dar instrucciones, sentencias u órdenes a dicho equipo.

Servidor es un hardware o equipo informático que brinda servicios en una red, proveyendo información a otros equipos o componentes de una red interna/externa, la cual es recibida, analizada y procesada por aplicaciones (software) para un uso final respectivo.

En comparación con los recursos de un PC y laptop, un servidor es un equipo de mayores prestaciones e inclusive dimensiones físicas.

2.3. DEFINICIÓN DE SEGURIDAD INFORMÁTICA.

SEGURIDAD INFORMÁTICA.

Se puede definir a la seguridad informática como la disciplina que vela por mantener el cumplimiento de los siguientes principios:

Integridad,

Disponibilidad y

Confidencialidad,

En sus aspectos fundamentales, así como el control y autenticidad de la información manejada por computadores, siendo esta la base de protección contra el comportamiento inesperado.

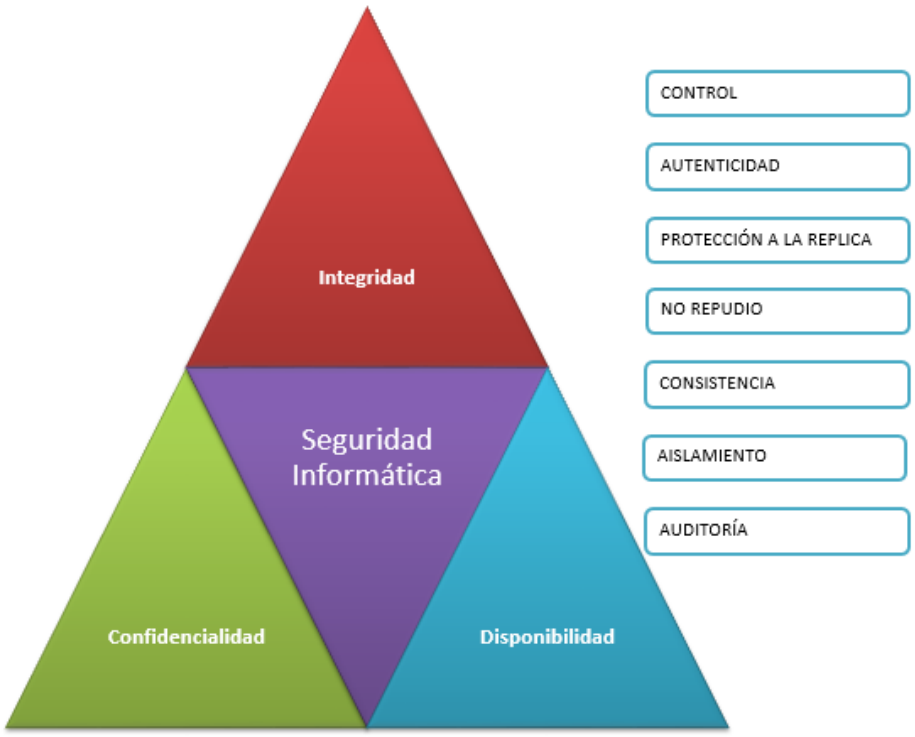


Figura 2.1 Seguridad de la Información norma ISO/IEC 27000.

En cambio la seguridad de la información se logra implementando un adecuado conjunto de controles incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware.

Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos. Esto se debiera realizar en conjunción con otros procesos de gestión del negocio.

Existe información con carácter público y privada, la pública es accedida por cualquier persona como por ejemplo: Los datos de censos nacionales, elecciones presidenciales.

En cambio la información privada debe ser accedida por personas autorizadas como por ejemplo: Doctores hacia antecedentes médicos, militares a información clasificada.

En ambos escenarios nuestro accionar debe estar dirigido para preservar la misma clasificándola bajo los criterios de criticidad, por su valor y si es sensitiva.

Integridad: Se requiere que la información no haya sido modificada o alterada (de manera malintencionada) por entidades o personas

no autorizadas durante la transmisión de la misma o en el propio equipo donde se encuentra. La modificación incluye cualquier operación posible sobre la misma como borrado, copia, escritura, creación, etc. La integridad de los datos asegura que los datos recibidos no han sido modificados, se puede caracterizar como la escritura no autorizada de la información.

Disponibilidad, es la capacidad de la información o los recursos informáticos del sistema estén accesibles en todo momento por las personas u entidades autorizadas, implica que se mantenga correctamente almacenada e incluye el correcto funcionamiento de hardware y software evitando la denegación de servicio (bloqueos o pérdidas debido a ataques, malas gestiones)

La confidencialidad es la garantía de que la información no será revelada por individuos, programas o procesos no autorizados, se incluyen todas la faces que definen desde cuales y en qué grado son confidenciales determinados datos, hasta cómo debe ser tratada la información, con qué mecanismos, qué criterios, qué personas, qué procedimientos.

Existe información que es privada y no se requiere compartir con entidades no Requiere que la información sea accesible únicamente

por las entidades autorizadas, autorizadas ejemplo, número de tarjetas de crédito, historial clínico, secretos de estado, industriales

Existen varias técnicas para conseguir confidencialidad, una de ellas es el cifrado y también existen multitud de ataques para romperla privacidad, especialmente la de los datos. La mayoría de estos ataques se basan en interceptar la información que se envía por la red o la intrusión directa en los sistemas donde se almacena la información.

Control, es la acción que nos permite asegurar el cuándo y cómo permitir el acceso a los usuarios e entidades autorizadas a la información.

También se refiere a que el acceso a los recursos de los sistemas sea restringido mediante la implementación de mecanismos automáticos, manuales o la combinación de estos, para que solo puedan acceder a los recursos entidades autorizadas, evitando así la manipulación de la información. La técnica más común para el control de acceso es la utilización de contraseñas.

Autenticidad es la que nos permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución, también nos permite asegurar el origen de la información, validando el emisor para evitar suplantación de identidades.

ASPECTOS ADICIONALES.

Protección a la réplica, es mediante la cual aseguramos que una transacción solo se realizara una sola vez, evitando mecanismo de grabación con la intención de copiar y así aparentar múltiples peticiones del mismo remitente.

El no repudio es mediante con la cual se evita que cualquier persona o entidad que envía o reciba información alegue o indique, ante un tercero, que no la envió o recibió.

Consistencia, se debe poder asegurar que el o los sistemas se comporten como se diseñó ante los usuarios correspondientes.

Aislamiento, este aspecto está relacionado con la confidencialidad ya que permite regular el acceso a los sistemas informáticos y por ende a la información, impidiendo que personas o entidades no autorizadas los usen.

Auditoria, es lo que nos permite determinar qué acciones o procesos se llevan o llevaron a cabo en los sistemas, esto incluye el cuándo y quién los realiza o realizo.

2.4. AMENAZAS DE SEGURIDAD A LOS SISTEMAS INFORMÁTICOS.

Definimos **amenaza** como:

Eventos que pueden desencadenar un incidente en la organización produciendo daños materiales o pérdidas inmateriales en sus activos.

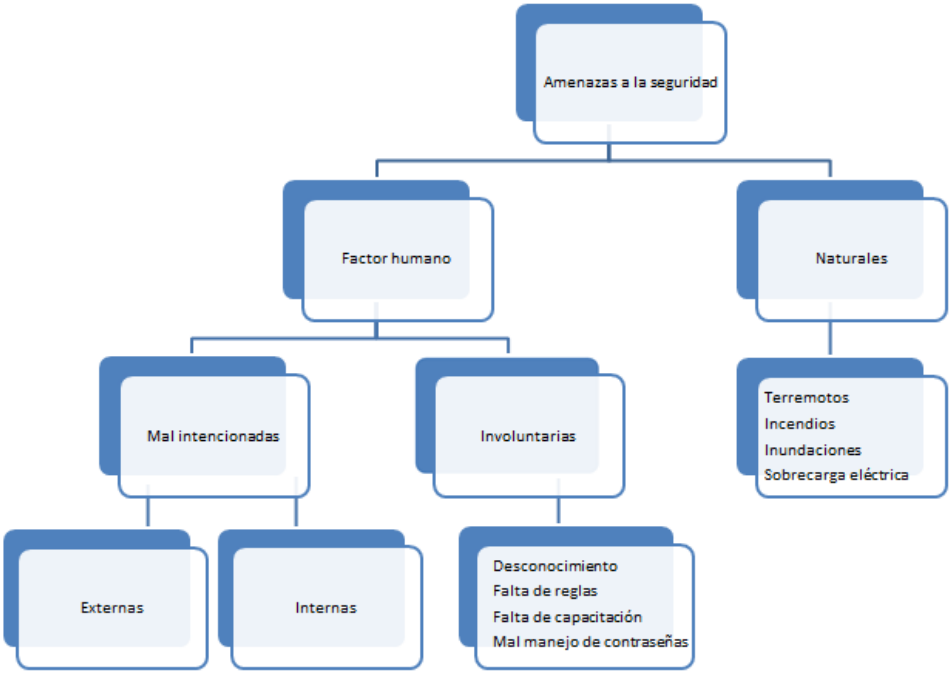


Figura 2.2 Amenazas a la seguridad.

Una amenaza o ataque se puede definir como una acción o un acontecimiento que puede atentar contra la seguridad, o como la violación en potencia de la seguridad de un sistema. También se pueden definir como cualquier acción que suponga una violación de la seguridad de los sistemas. Los sistemas informáticos están expuestos a tres tipos básicos de amenazas:

- Intencionadas,
- Involuntarias y no intencionadas,
- Naturales o de fuerza mayor.

Intencionadas: Generalmente se producen por usuarios no autorizados externos o internos al sistema clasificándolos según sus intenciones entre curiosos y maliciosos.

Los usuarios clasificados como curiosos pretenderán acceder a los sistemas por simple fisgoneo, diversión y por saber si pueden hacerlos, estos normalmente no tienen objetivos concretos y simplemente revisan la información sin interés específico.

Los usuarios clasificados como maliciosos pretenden acceder a los sistemas con intenciones nocivas. Estas intenciones pueden ir desde el robo de información con fines de lucro, se incluye la destrucción o modificación de información.

Involuntarias y no intencionadas: Son el resultado de acciones de usuarios inhábiles que ya sea por negligencia o descuido borran información, crean agujeros de seguridad, no actualizan apropiadamente el software que administran o facilitan sus contraseñas personales.

También está comprometido en estas amenazas el personal asignado al procesamiento de datos e información que al no seguir los procedimientos de seguridad establecidos facilitan el acceso a información clasificada, pudiendo inclusive crear agujeros en la seguridad con pequeños programas pudiendo llegar a afectar a la aplicación global o aplicaciones institucionales.

Se debe considerar a los virus informáticos también como amenazas, que aunque son creados por el hombre, estos una vez puestos en funcionamiento en cualquier sistema informático son autónomos, nocivos siendo totalmente evitables siguiendo procedimientos básicos de seguridad acompañado con la implementación de un sistema antivirus confiable.

Naturales o de fuerza mayor:

Son todos aquellos desastres imaginables tanto naturales (terremotos, tornados, incendios, inundaciones, erupciones, etc.) como por fallos de los equipos (sobrecarga, cortocircuito, fallo de hardware, cortes del sistema eléctrico, etc.).

Amenazas, factores externos: Son todos los virus informático, troyanos, spam, ataques de denegación de servicios por parte de

una organización criminal o activista, disturbios, conflictos sociales, intrusos en la red, robos, y estafas.

Amenazas, factores internos: Aquí se agrupan las acciones resultantes de empleados descuidados o con formación inapropiada, disgustados. También se incluyen los errores en el uso de las herramientas, recursos y procedimientos establecidos en los sistemas informáticos.

Es necesario también realizar una valoración de las amenazas, determinándose la misma por dos formas:

Frecuencia de ocurrencia.

Degradación causada.

Ambas estiman la exposición efectiva o cuan vulnerable es un activo a una amenaza de forma parcial o total, cualitativa o cuantitativamente.

Frecuencia de ocurrencia.

Es determinar, o estimar de alguna forma cada qué tiempo, periódico o no, se efectiviza una o varias amenazas, la periodicidad resultante pone en vista aquella degradación, pudiendo presentarse dos comportamientos comunes:

- Amenazas de terribles consecuencias al efectivizarse pero con bajo índice de ocurrencia, ó
- Amenazas de muy bajas consecuencias pero con un alto índice de ocurrencias o con la frecuencia suficiente para acumular efectos dañinos.

Degradación.

La degradación mide el daño causado por un incidente en el supuesto que ocurriera. La degradación se suele caracterizar como una fracción del valor del activo y así aparecen expresiones como que un activo se ha visto "totalmente degradado", o "degradado en una pequeña fracción".

Cuando las amenazas no son intencionales, probablemente baste conocer la fracción físicamente perjudicada de un activo para calcular la pérdida proporcional de valor que se pierde. Pero cuando la amenaza es intencional, no se puede pensar en proporcionalidad alguna pues el atacante puede causar muchísimo daño de forma selectiva.

2.5. AMENAZAS DE SEGURIDAD A LOS SISTEMAS OPERATIVOS.

Personas.

Debemos estar conscientes que la mayoría de los ataques a nuestros sistemas son provenientes de personas que intencionada o inintencionadamente pueden llegarnos a causar pérdidas considerables, estas personas se ingenian en obtener acceso a nuestros sistemas desde la forma más básica para luego mediante diferentes técnicas incrementar el privilegio hasta el máximo permitido, aprovechando los agujeros en software que en esencia son ineficientes validaciones en su código, las vulnerabilidades o riesgos existentes tanto como en las aplicaciones y productos comerciales, sistemas operativos y plataforma tecnología en general.

Se debe mencionar también que existen administradores de sistemas que no velan por mejorar, incrementar o robustecer la seguridad de la plataforma tecnológica que gestionan y por ende a los sistemas operativos, mínimamente preocupados por esto, también son víctimas de otras personas que usando ingeniería social puede llegar a obtener el acceso deseado.

A la amenaza por personas podemos clasificarlas en dos grupos, pasiva y activa, se incluye a curiosos, empleados, ex empleados, crackers, terroristas e intrusos remunerados.

Nos referimos a pasivas por aquellas personas que acceden al sistema operativo de un servidor o computador sin autorización vulnerando sus seguridades pero sin realizar modificaciones, alteraciones o destrucción del mismo, su fin es de curiosidad, alcanzar acceso como reto o diversión.

Decimos que es activo cuando el fin de la intrusión, a diferencia del pasivo, es destruir, dañar, alterar o modificar a su favor.

Ex empleados, empleados, administradores y usuarios finales, personas que tuvieron y tienen acceso a los sistemas, son por las cuales debemos implementar políticas de acceso, control y supervisión para reducir el acceso no autorizado y alteraciones a los sistemas operativos de los ambientes de producción.

Un ineficiente o inexistente control de acceso.

Un sistema operativo, cualquiera que sea su distribución requiere siempre se realice una parametrización básica de usuario y clave, en muchos casos, por desconocimiento, exceso de confianza o comodidad, usuarios e inclusive administradores de sistemas omiten esta configuración en los sistemas operativos, olvidando que este control brinda la capacidad de identificación para distinguir de quien ingresa a los sistemas informáticos, a sus servicios, aplicaciones y archivos de forma autorizada de los que no,.

Si no se realiza una correcta habilitación, configuración y de ser posible la implementación de un servicio como un directorio activo o ldap que soporte la administración de usuarios y sus claves, se tendrá como resultado graves problemas de seguimiento o auditoria, inconvenientes de habilitación y restricción de accesos a directorios, recursos compartidos, información sensible y publica.

También existe un escenario opuesto al mencionado, es cuando ya existe una aceptable administración de usuarios y claves para el ingreso a los sistemas operativos y por ende a las aplicaciones e información institucional. Un usuario puede a llegar a tener distintas claves dependiendo a cuantos servidores requiera o deba ingresar, presentándose la dificultad de que pueda olvidar varias de estas, haciéndolo recurrir a cambiar las mismas con palabras de fácil deducción o a escribir estas claves en lugares físicos o lógicos de fácil acceso.

Debido a esto, muchos administradores de sistemas han optado por la homogenización y sincronización de la clave de los usuarios, brindándole a estos, acceso a toda la plataforma tecnológica. Esta “sincronización” puede ser manual, automática o mixta dependiendo de cuan interrelacionados estén los componentes de la plataforma informática, esta práctica se la puede considerar altamente arriesgada ya que una vez que la clave de un usuario, mayor aun si es de un administrador, es comprometida, quien la posee pude

fácilmente ingresar a cualquier servidor, aplicación, información y realizar cambios no autorizados sin generar sospechas.

Algo que siempre se tiene que tener implementado en un control de acceso, en especial en los sistemas operativos, es la caducidad de la clave de los usuarios, definiendo un periodo máximo de vigencia y uno mínimo para realizar el cambio.

Una mala administración.

Los sistemas operativos no solamente están expuestos a irrupciones externas sino también interna, esta última, nace de los propios integrantes de una organización, colaboradores, empleados y personas de confianza que por negligencia, apatía, ignorancia u otra mala práctica, alteran, sustituyen o borran información sensible creando indisponibilidad de la información.

La administración a los sistemas operativos debe ser eficaz y permanente, con el objetivo de supervisar todos los usuarios que ingresan al mismo para hacer uso de las aplicaciones y servicios que estos alojan y que están autorizados a acceder. Esta administración debe incluir también la implementación de controles que prevenga y notifique mediante alertas sean estas sonoras, visuales o de texto como mail, ante modificaciones, ediciones, alteraciones (o intentos de estos) de privilegios, permisos o roles establecidos, de ser necesario y para garantizar un efectivo control, es recomendable

hacer uso software, hardware o combinación de estas que impidan modificaciones sin la autorización correspondiente.

Se debe complementar la gestión, administración y uso de los servidores, por ende a los sistemas operativos, mediante un programa de concientización describiendo en un documento firmado las responsabilidades y compromisos que asume cada usuario al solicitar acceso sean estos mínimos, medios o totales.

Ineficiente control de los protocolos y puertos de comunicación.

Debido a la falta de control en los protocolos de comunicación, existen ambientes productivos, redes y servidores, que al no poseer controles en los 65535 puertos de comunicación existentes en un sistema operativo, personas no autorizadas pueden hacer uso de los mismos para acceder y tomar el control sin autorización de los sistemas informáticos, servicios y aplicaciones de una institución, pudiendo causar graves daños y pérdidas.

Si los errores están directamente en los protocolos o relacionados a estos, sin importar el sistema operativo, todo lo que se componga de un protocolo en particular puede verse afectado. La creación y posterior desarrollo de los protocolos de comunicación en los años 70, no necesariamente incluían aspectos relacionados a la seguridad.

Figura 2.3 Comparativa entre el modelo OSI y la TCP/IP.

Debido a que existen muchos protocolos, también existen muchas posibilidades de detectar y encontrar fallos en estos, si estos son por diseño puede que su corrección sea difícil o imposible de implementarse, siendo necesario implementar distintos niveles de seguridad para solventarlos como cifrado o algoritmos de criptografía, siendo recomendable su reemplazo por uno más seguro. Recordemos que varios de los virus actuales se introducen a los sistemas por protocolos no monitoreados o supervisados (http, imaps, imap, pop3s, pop3, smtp), por ello, se debe supervisar la comunicación en una red (lan o wan) que hacen uso de los puertos TCP/IP y UDP hacia los sistemas operativos del ambiente de

producción, pudiéndose implementar un dispositivo de control de puertos que permitan filtrar, clasificar o restringir el acceso. Un firewall, ayuda a mejorar la administración de los puertos, permite prevenir intromisiones, virus, escaneos, inclusive monitorear las conexiones que se intentan realizar a un computador o servidor de nuestra red, permitiéndonos obtener datos importantes como IP implicadas, permisos, servicios solicitados, fecha.

Puede también realizarse acciones como bloqueos a conexiones ya establecidas o por establecerse, dar avisos u alertas al administrador de nuevas conexiones o intentos de estas.

Errores de configuración.

La configuración de un sistema operativo es también un punto bastante descuidado a la hora de la preparación de un servidor o computador. Por muy seguro que sea este, una deficiente parametrización, configuración y afinamiento, puede tornarlo vulnerable, maleable e inseguro.

Se debe considerar consolas de administración, paneles de administración web, credenciales de acceso por defecto que al no ser modificadas o desactivadas podrían ser usadas, teniendo en cuenta que también existen sitios en internet que brinda información de estas credenciales tanto para sistemas operativos, equipos activos y aplicaciones o software.

Existen aplicaciones que requieren configuraciones y permisos específicos en el sistema operativo local para poder ser instaladas y ser funcionales, por este caso, administradores de sistemas con el objetivo de no incrementar sus actividades laborales dejan a potestad del implementador o proveedor externo la configuración del sistema operativo del servidor, sin considerar ninguna medida de seguridad o en su defecto reduciendo las mismas con tal de que su aplicación no presente problemas y cumplir con los tiempos de atención programados de instalación.

Por muy segura que se una aplicación y esté sobre un sistema operativo aparentemente estable, sin las configuraciones adecuadas en ambos puede generar una falsa sensación de seguridad.

Este tipo de prácticas se las debe evitar y reducir al mínimo (como excepciones) ya que aunque se implementen demás herramientas de protección existirá esta brecha de seguridad la cual puede volverse grave en un ambiente empresarial.

Herramientas de análisis en seguridad informática.

Parece irónico, existen profesionales de sistemas y seguridad informática que hacen uso de herramientas gratuitas existentes en internet, las cuales sirven para realizar análisis de seguridad a una plataforma tecnológica con el objetivo de encontrar y corregir vulnerabilidades/fallos, estas mismas herramientas pueden ser

usadas por **crackers** que en muchas de sus ocasiones no buscan aportar en las soluciones de problemas (que detectaren) en los sistemas operativos, plataformas y sistemas tecnológicos, sino más bien, aprovecharse de la información que les brindan estas aplicaciones (software) luego de un escaneo/análisis que realizaren a una red particular para consecuentemente cometer actos ilícitos

Puede indicarse que las herramientas de análisis de seguridad informática, son armas de doble filo, que en manos de profesionales responsables pueden y son usadas para mejorar o incrementar las seguridades de un sistema operativo, aplicación o software.

Puertas traseras y bombas lógicas.

Las puertas traseras, que en si son métodos alternativos a los normales de autenticación, han sido puntos de discusiones entre clientes, usuarios finales y los fabricantes de los sistemas operativos dominantes en la actualidad. Recordando que los sistemas operativos, en esencia es un software, muchos “desarrolladores” con el fin de garantizar el acceso a este software crean “atajos” temporales durante el desarrollo del sistema operativo (software) y una vez que se obtiene la versión final o definitiva, olvidan retirar este atajo o lo mantienen para futura actividades de revisión, mantenimiento o actualización, por lo cual se crea un brecha de

seguridad que pueden ser descubiertas por atacantes y obtiene acceso a los datos y manipular los mismos a su conveniencia.

Las bombas lógicas son instrucciones pasivas que son parte del código de algún software, que hasta ahí no realizan actividad alguna. Para ser activadas es necesario se cumpla una o más condiciones ya establecidas previamente, que pueden ser la ausencia o presencia de algún fichero, alguna ejecución mediante un usuario especifico u una fecha específica. Muchas de estas son creadas este tipo de amenaza puede tener consecuencias fatales si no se detectaren y trataren a tiempo, estas bombas lógicas pueden estar presentes desde simples instrucciones de consola, trigger o disparador de base de datos, gusanos y virus informáticos.

2.6. VIOLACIÓN, ACCESO NO AUTORIZADO.

El acceso no autorizado (informático) consiste en ingresar a sistemas de tratamiento de información infringiendo las formas regulares establecidas en una institución o ley local o nacional vigente, esto quiere decir que de forma indebida se obtiene acceso a un sistema informático con un fin, pudiendo ser por satisfacción intelectual al poder descifrar códigos, usuarios y clave, por encontrar vulnerabilidades en la plataforma tecnológica de una empresa o gobierno, o por encargo siendo una actividad remunerada con fines

de espionaje, intercepción, sabotaje, fraude, manipulación, terroristas, delictivas e ilícitas.

Obtenido el acceso, se convierte en un delito informático (violación), que puede tener connotaciones legales y jurídicas según su gravedad y efectos.

CAPÍTULO 3

MEDIDAS DE SEGURIDAD.

Para tener la capacidad de asegurar un sistema informático o tecnológico, implica tener un vasto conocimiento de cómo es su funcionamiento, incluyendo las redes, los sistemas operativos, sistemas de almacenamientos, aplicaciones y servicios, teniendo en claro que no necesariamente debemos ser expertos en todos y cada uno de los temas implicados, sino más bien tener un entendimiento amplio de esta para ensanchar o mejorar nuestra visión de la infraestructura que queremos proteger. Con estos conocimientos ya podríamos implementar medidas, planes y soluciones de seguridad.

Ninguna medida de seguridad es completamente segura e infalible, existirá fallas lógicas en programas, agujeros o vulnerabilidades que inclusive son

desconocidos para los administradores o responsables de sistemas, debido a esto es necesario una constante evaluación, revisión y mejoras a las medidas de seguridad, con el objetivo principal de mejorarla y actualizarla conforme se realizan los avances tecnológicos, se descubren nuevas fallas o vulnerabilidades, se liberan nuevas versiones de herramientas/software y aplicaciones.

Como su nombre lo indica, las medidas de seguridad son eso, medidas, que deberán ser complementadas con inducción, capacitación, implementaciones de normas y reglas a todo el personal institucional, inclúyase también al personal externo y proveedores, estos últimos deberán tener claro mediante documentación cuáles son sus responsabilidades y obligaciones para no afectar la integridad de los sistemas informáticos de la empresa en la cual colaboran.

3.1. SOLUCIONES BÁSICAS A LA SEGURIDAD DE LOS SISTEMAS.

Las soluciones que describiremos a continuación tienen como objetivo proteger un único activo, la información.

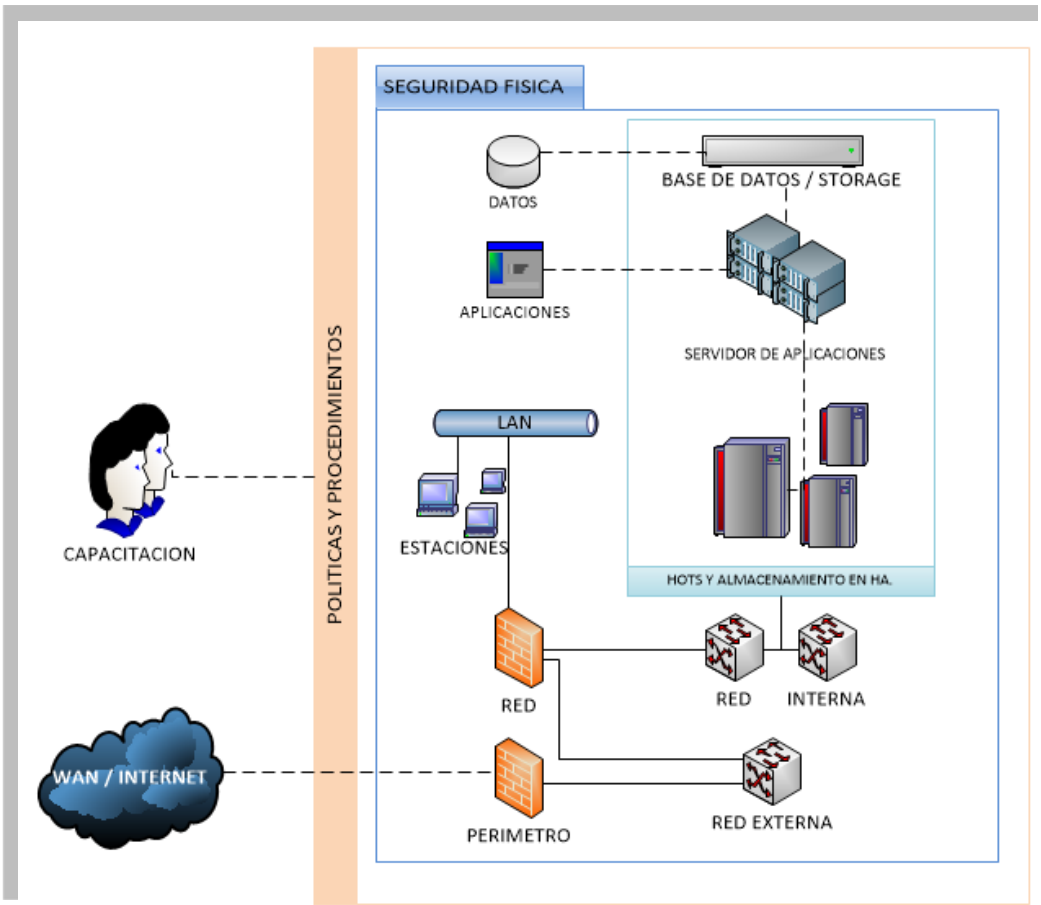


Figura 3.1 Enfoque de protección desde la visión de plataforma.

En la figura 4, se puede observar los principales componentes que interactúan en una plataforma tecnológica, que se comprende por los sistemas de almacenamiento de datos, aplicaciones, servidores, red interna y red perimetral. Se añade también medias adicionales

como la implementación de políticas y procedimientos más la capacitación e inducción de las mismas para su uso efectivo.

Lo descrito en la Fig. 4 se puede resumir bajo el siguiente enfoque en capas, destinado para incrementar la seguridad de una plataforma tecnológica en una empresa.

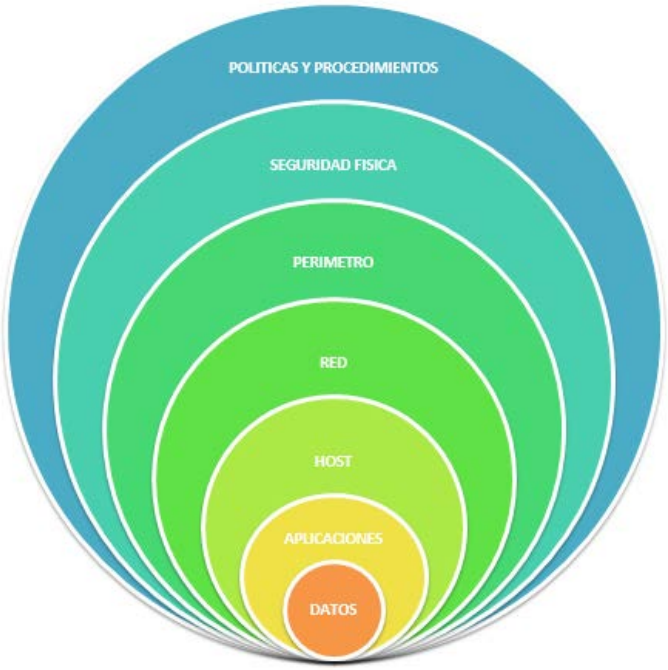


Figura 3.2. Enfoque de protección por capas.

3.2. SEGURIDAD FÍSICA.

Consiste en implementar “defensas” palpables soportadas mediante el uso de mecanismos de control, ello dentro y fuera del área de servidores, de almacenamiento y procesamiento de datos llamado comúnmente centro de cómputo, con el objetivo de impedir que

personas no autorizadas puedan acceder a los dispositivos de red que contienen o permitan acceder a información sensible pudiéndolos manipular a su conveniencia o placer.

La seguridad física debe ser una mediad preventiva y nunca deberá ser relegada o desatendida ya que tal acción pudiere general graves problemas a la disponibilidad, integridad y confidencialidad de la información, e inclusive le permite al atacante acceder a los siguientes niveles o capas. Ejemplo: Utilizar un USB “infectado” en un equipo terminal fuera del centro de cómputo, o, usar este mismo dispositivo en un servidor dentro de centro de cómputo, lo que puede provocar una afectación grave a los sistemas de la institución.

La seguridad física también debe incluir protecciones contra desastres naturales como tormentas eléctricas, inundaciones, terremotos, otros como incendios, sabotaje y amenazas ocasionadas por el hombre como los disturbios, cortes del suministro eléctrico normal.

La seguridad física deberá contemplar un área adecuada para el centro de cómputo, muy bien iluminada, con piso de placas extraíbles, con temperatura controlada de precisión, filtros de protección a emisiones electromagnéticas y un único punto de acceso (puerta reforzada) para el personal autorizado y/o administrador(es) con control de acceso mediante sistemas biométricos.

3.3. RED. SEGURIDAD DE LAS COMUNICACIONES

Busca controlar los accesos a la red interna y los componentes activos que la conforman, asegurándola con controles y correctas medias de seguridad para evitar intrusiones y acceso no autorizados. Para ello habitualmente se usa un firewall, se suele reforzar esta medida de seguridad con el acompañamiento de sistemas IPS e IDS, refuerzos aplicables para detectar, analizar y bloquear acciones que pudieren generar interrupciones a los sistemas. El objetivo de la seguridad de las comunicaciones es proteger la integridad y privacidad de los datos, los cuales, son transmitidos por la red, para esto se pueden usar mecanismos de llave pública y privada, firmas digitales y también el uso de protocolos seguros.

PERÍMETRO.

Es la implementación de un zona desmilitarizada, que permite tener un grado se seguridad entre las conexiones de la red externa e interna hacia la DMZ, y no permita conexiones desde la DMZ hacia la red interna. Su aplicación está orientada a controlar e inclusive evitar conexiones de posibles atacantes mediante puertos tcp y UDP, permitiendo exponer dispositivos/servidores que brinden servicios públicos mediante internet.

HOST.

En este nivel o capa, es donde por lo general es donde se trata las vulnerabilidades del sistema operativo, permitiéndonos implementar service packs para tratar u corregir las amenazas, de no tratarse, los atacantes pueden aprovecharse de estos agujeros de seguridad haciendo uso de distintas formas de ataques con fines nocivos para cualquier institución.

También la seguridad a nivel de host busca evitar fallas que pudieren generar pérdidas, robo o corrupción de datos

3.4. SEGURIDAD DE LAS APLICACIONES.

En esta capa se busca evitar que atacantes o usuarios puedan aprovecharse de vulnerabilidades, accesos o fallas en aplicaciones/software aplicativo para realizar ataques a nuestro sistema. Las actividades para reducir estos riesgos deberían enfocarse en el tratamiento del acceso no autorizado a los archivos y binarios de las aplicaciones alojadas en un sistema operativo con función de servidor, a los puertos del mismo y a los servicios expuestos en el servidor con el objetivo de evitar la explotación u aprovechamiento que tienen las mismas aplicaciones sean propias o de terceros.

3.5. SEGURIDAD LÓGICA.

Si fallaren las medidas anteriormente descritas, personal no autorizado puede llegar a tener acceso a datos o información de carácter confidencial existiendo el riesgo de intercepción, alteración, cambio, eliminación parcial o total de la información.

Por esto es importante incluir medidas del uso correcto de la información, su distribución y las responsabilidades de los usuarios en el tratamiento de la misma. Entre las medidas podemos destacar:

- Un estricto método de identificación y autenticación.
- Controles y autorizaciones para la instalación, actualización y eliminación de software en la institución.
- Implementación de copias y backups de seguridad.
- Uso de firewall para la red interna y uno distinto para la red externa.
- Monitoreo de las actividades en los equipos y servidores de la institución, registrando desde la forma más básica las actividades de logging y el historial de actividades.
- Cifrado de datos, carpetas y discos.
- Encriptación de archivos por recepción y transmisión.
- Restricciones a los servicios, ubicación y horario.
- Limites en la interfaz para usuarios finales.

Es importante también definir las funciones y responsabilidades de los usuarios a la hora de usar los sistemas institucionales, mediante la implementación de medidas administrativas publicando políticas de seguridad para el uso de los sistemas de información, describiendo las medidas legales que pueden tomarse ante las infracciones que cometieren los usuarios.

3.6. SOLUCIONES A AMENAZAS DE LOS SISTEMAS INFORMÁTICOS.

Cualquier medida de seguridad debe ser implementada en el mismo grado de importancia en todos los niveles o partes que conforman la plataforma tecnológica en una institución, o en su defecto atender las áreas menos protegidas robusteciéndolas hasta alcanzar homogeneidad en este sentido. Si la seguridad (informática) no es uniforme en todos los aspectos, nuestro nivel de seguridad es igual al punto más débil existente.

Es de vital importancia incluir la participación activa de los usuarios de la institución mediante la capacitación sobre temas de ingeniería social, sus consecuencias y del cómo evitar caer o ser víctimas de estas prácticas cuyo fin es el suplantar su identidad para obtener acceso a nuestros sistemas informáticos, lo que puede llegar a tener afectaciones negativas a nivel de negocio, imagen y económico.

En ocasiones será necesario acudir a la asesoría externa para captar u adquirir nuevos conocimientos y experiencias en el tratamiento, la

mitigación de riesgos y amenazas que pueden presentarse en nuestra plataforma tecnológica. La realización de auditorías periódicas es una ayuda importante para saber el estado actual de nuestros sistemas.

Para toda amenaza o riesgo existe una contramedida que puede implementarse para evitar o minimizar efectos dañinos o nocivos, podemos mencionar:

MEDIDAS PARA AMENAZAS EXTERNAS.

Siempre existirán personas o grupos de personas que por intereses personales están dispuestos, ya sea por reto o recompensa, violentar las seguridades de una plataforma tecnológica, ingresando en ellas obteniendo la información deseada o realizando las actividades que tiene por objetivo, pudiendo ser desde la observación, copia, alteración, eliminación de información y destrucción de sistemas.

No podemos evitar totalmente este tipo de actividades, pero si reducirla de forma considerable e inclusive dificultando la realización de las mismas llevando a cabo un programa o plan de actualización de todos los programas y sistemas de nuestra plataforma a sus últimas versiones, incluyendo los parches, solución de bug y corrección de vulnerabilidades.

También es importante la implementación de hardware (firewall) y software (IPS, IDS) dedicado, destinado a controlar el tráfico externo.

MEDIDAS PARA AMENAZAS INTERNAS.

Ya sea de formas intencionadas o no, para evitar amenazas internas es aconsejable implementar estrictos controles de uso de los sistemas que van desde la política de contraseñas, su uso, renovación y bloqueo hasta el cifrado de los datos.

Al igual que las medidas externas, es recomendable la implementación de hardware (firewall) y software (IPS, IDS) dedicado, destinado a controlar el tráfico interno.

CAPÍTULO 4

ANÁLISIS Y DISEÑO DEL ESQUEMA DE ASEGURAMIENTO INFORMÁTICO.

Realizaremos la revisión de los riegos presente en los sistemas operativos que este esquema de aseguramiento atenderá, realizando un análisis de los riesgos y las vulnerabilidades presentes tanto en Windows server 2008 R2 y RedHat Linux 5.5.

4.1. VULNERABILIDADES Y FACTORES DE RIESGO.

Actualmente los sistemas operativos son los encargados de procesar, almacenar y distribuir la información de una institución o empresa, convirtiéndose en unos de los pilares de las áreas de

tecnología, ya que su uso es aplicado desde equipos de oficina hasta los componentes que conforman el centro de datos, procesamiento y almacenamiento, entre ellos podemos encontrar, computadores, servidores, unidades de almacenamiento, equipos activos, hardware de alta disponibilidad y equipos dedicados.

Por el perfeccionamiento del hardware informático, la incorporación de nuevas funcionalidades y la inclusión de un mayor alcance en sus capacidades, los sistemas operativos han tenido que evolucionar en sus características y prestaciones para soportar y funcionar correctamente, llegando a un punto en que los sistema operativos incluso son compatibles con una gran parte del hardware disponible en el mercado actual.

Un sistema operativo al tener mayores funcionalidades, intrínsecamente tiene más vectores o aristas para una posible falla y así también para un ataque, debido a las vulnerabilidades que de forma involuntaria están presentes en su diseño y construcción.

Existen varios sistemas operativos dependiendo de la funcionalidad que se le dé, se puede usar Windows o un Unix/Linux. Del primero tenemos vigente actualmente Windows 7, 8, 8.1, 10, los cuales son orientados a actividades de escritorio, para servidores tenemos Windows Server 2003, 2008, 2012.

De UNIX tenemos muchas variaciones de la cual mencionaremos las versiones más reconocidas para servidores que son HP-UX, IBM AIX, Solaris, Red Hat, Centos, BSD.

Los factores de riesgos que trataremos referenciaran únicamente a Windows Server 2008 y Linux Red Hat 5.5, los factores de riesgo son todas aquellas características que puede producir un aumento en la probabilidad de que una amenaza pueda ocasionar un mal funcionamiento, indisponibilidad o daños al sistema operativo, entre ellos tenemos:

- Única partición para la instalación del sistema operativo.
- Todos los servicios del sistema operativo instalados innecesariamente.
- Instalación de actualizaciones del sistema operativo sin revisión técnica previa.
- Inexistente configuración de los parámetros mínimos de seguridad.
- Realizar instalación por defecto del sistema operativo.
- Falta de mecanismos de control de acceso a objetos del sistema.
- Ineficiente gestión y administración de cuentas normales y especiales, que incluya creación, edición, bloqueo, eliminación, cuentas sin contraseña, predeterminadas y de invitados.

- Falta de control y supervisión en los procesos de arranque del sistema operativo.
- Una inadecuada o inexistente implementación de cifrado de datos.
- Mala administración y uso del acceso remoto.
- Falta de mitigación, infección y control de virus.

4.2. ANÁLISIS DE VULNERABILIDAD.

Acorde al sistema operativo implementado en el servidor, este pude ser Windows server o Red Hat, se detectará las vulnerabilidades y riesgos que serán tratados y cubiertos en el esquema de aseguramiento informático.

En la gráfica a continuación, se ilustra y explica la secuencia desde la detección de la vulnerabilidad hasta la implementación de su contramedida con el objetivo de reducir la amenaza, exposición y riesgo.

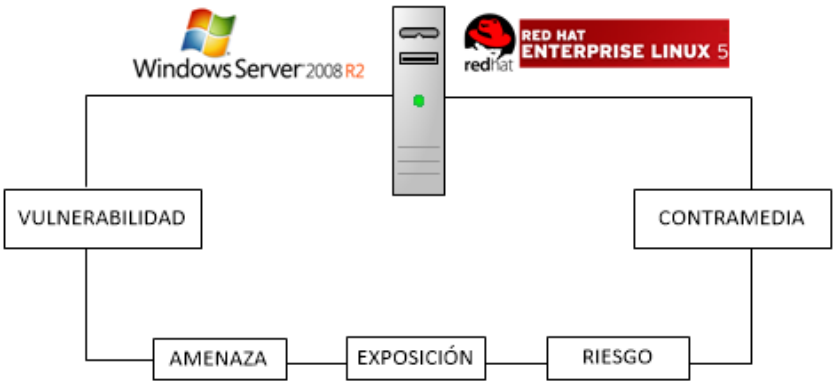
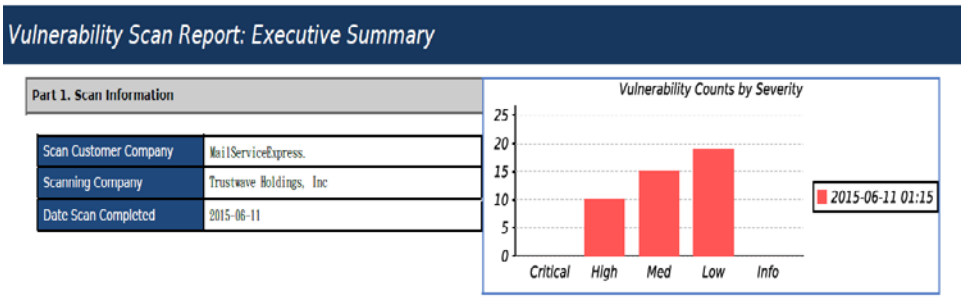


Figura 4.1 Ciclo de análisis de riesgos y vulnerabilidades.

En la revisión realizada mediante software TRUSTKEEPER tanto para Windows y Linux, más las recomendaciones y normas del ISO 27001, en los sistemas operativos de los servidores de producción se obtuvieron en el resultado vulnerabilidades que detallamos a continuación:

EN LINUX.



#	IP Address	Vulnerabilities Noted	Severity	CVSS Score	Compliance Status
1	172.18.91.21	User Mountable NFS Shares, CVE-1999-0170 CVE-1999-0211 CVE-1999-0554	High	10.00	PCI 11.2.1 relevant
2	172.18.91.21	statd RPC Service, CVE-2004-1014 CVE-2000-0666 CVE-2000-0800 CVE-1999-0493 CVE-1999-0019 CVE-1999-0018	High	10.00	PCI 11.2.1 relevant
3	172.18.91.21	OpenSSH Wildcards on AcceptEnv Vulnerability, CVE-2014-2532	Medium	5.80	PCI 11.2.1 relevant
4	172.18.91.21	OpenSSH SSHFP DNS resource record look up bypass in the client, CVE-2014-2653	Medium	5.80	PCI 11.2.1 relevant
5	172.18.91.21	OpenSSH socket exhaustion denial of service, CVE-2010-5107	Medium	5.00	Not PCI 11.2.1 relevant
6	172.18.91.21	System Responds to SYN+FIN TCP Packets	Low	0.00	Not PCI 11.2.1 relevant

Figura 4.2 Resultado de primer análisis de vulnerabilidad.

Sin protección de contraseña del sistema operativo.

Sin protección de contraseña de arranque del sistema operativo.

Está habilitada la inicialización del sistema operativo desde la unidad óptica.

Esta activada las unidades USB.

Existen varias cuentas con privilegios root. (GUID=0, UID=0)

Están activas todas las cuentas del sistema operativo, como por ejemplo gopher, games, Uucp, News, Nobody, man, ftp, daemon, bin, lp.

No hay restricciones de uso para el comando su y sudo.

No existe una clasificación de los grupos de usuarios del sistema.

No se ha configurado adecuadamente las variables de entorno de inicialización de cada usuario.

No se ha implementado un banners que sirva de advertencia al ingreso del sistema.

No sé a realizado las configuraciones respectivas para evitar el reinicio del sistema operativo de forma involuntaria.

No se ha implementado una política de seguridad de manejo de contraseñas de los usuarios.

El sistema operativo no tiene implementado las últimas actualizaciones de seguridad ni existe una apolítica de actualización.

Existen servicios innecesarios que están activados, telnet, ftp, nfs.

No se tiene una configuración segura del servicio ssh.

No hay una configuración adecuada de almacenamiento de logs.

No hay una configuración adecuada de auditoría de eventos del sistema operativo.

No se ha establecido permisos octales seguros a directorios y archivos del sistema operativo.

EN WINDOWS.

Sin protección de contraseña del sistema operativo.

Recursos compartidos sin restricciones de acceso, abiertos para todos.

Puertos USB habilitados.

Sin servipack y parches de seguridad implementados.

Excesivos números de usuarios en el grupo de administradores del equipo.

La cuenta a*dministrador* mantiene el nombre por defecto.

La cuenta *invitado*, está activa.

No existen políticas de seguridad aplicadas para las contraseñas.

No existen políticas de auditoría aplicadas al sistema operativo.

No existe un ANUNCIO o ADVERTENCIA al ingreso del sistema operativo.

No se ha restringido permisos a directorios y archivos del sistema operativo.

Una gran cantidad de servicios del sistema están habilitados de forma innecesaria, entre ellos fax, ftp, telnet, computer browser, dhcp server, dns server, dfs namespace, internet connection sharing, iis admin service, iSCSI Initiator Service, offline files, Virtual Disk, Volume shadow, WinHttp Web proxy Auto Discovery Service, Word Wide Web Publishing Service, Application host helper service.

Sin protección de un sistema antivirus.

4.3. ANÁLISIS DE REQUERIMIENTOS.

Una vez identificadas las vulnerabilidades, se registrarán las contramedidas en el esquema de aseguramiento informático que tiene el objetivo de corregir las mismas mediante la implementación de mecanismos manuales o automáticos para reducir drásticamente los riegos y posibles amenazas que estos puedan producir en los sistemas operativos Linux y Windows.

Se busca:

Determinar una secuencia de pasos estableciendo una base de configuración para el sistema operativo Windows.

Determinar una secuencia de pasos estableciendo una base de configuración para el sistema operativo Linux.

Crear un esquema de aseguramiento para los sistemas operativos Windows y Linux que incluya configuraciones especiales cubriendo la mayoría de las vulnerabilidades identificadas, que pueda ser entendible para los administradores de sistemas y analistas de la institución.

Registrar estas secuencias de pasos y esquema de aseguramiento mediante la creación de plantillas de aseguramiento para la plataforma Windows y Linux respectivamente.

4.4. DISEÑO BASE DE PROCEDIMIENTO DE ASEGURAMIENTO INFORMÁTICO.

La base para la realización de un procedimiento se compone de 4 fases esenciales que las describiremos de forma general a continuación.

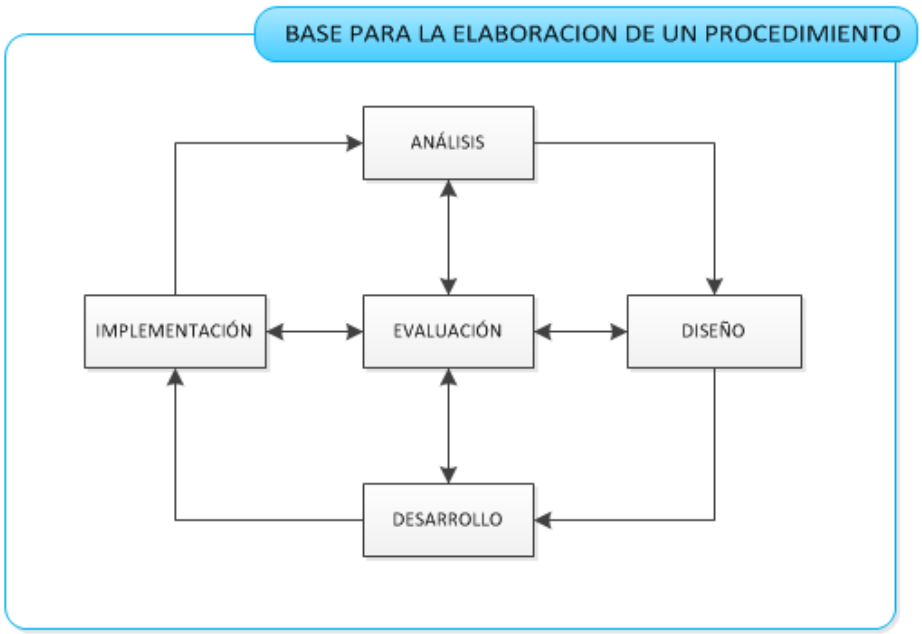


Figura 4.3 Base para el diseño de un procedimiento.

El análisis lo hemos realizado mediante la revisión y descripción de los problemas se seguridad que tiene la institución Mail Service Express en sus servidores de producción los cuales tienen instalado el sistema operativo Windows server 2008 R2 y Red Hat 5.5.

Continuaremos con el diseño base del procedimiento de aseguramiento informático tanto para Windows y Linux, buscando

sea totalmente entendible para el personal del departamento de sistemas con el objetivo de adoptarlo como requisito obligatorio de seguridad al momento de preparar un servidor y también para la revisión y corrección de los que actualmente se encuentran en producción.

DISEÑO.

Este diseño tendrá la siguiente estructura.

- **Portada**

  En la misma se incluirá

- **Encabezado.**

  Incluirá el logotipo de la empresa.

  La cabecera especificara que se trata de un procedimiento.

  Revisión del procedimiento con la fecha respectiva.

  Inicio de aplicación del procedimiento.

- **Título del procedimiento**

  El cual debe incluir codificación de identificación, siglas, abreviaturas, dígitos de referencias.

- **Índice.**

  Donde se describirá de forma puntual el contenido del procedimiento, indicando con un par de dígitos la ubicación del tema.

- **Casillas.**

  Se incluirá en el procedimiento una casilla para la inclusión de los siguientes datos.

  - El nombre y apellido de la o las persona que realizaron la revisión del procedimiento de aseguramiento.
  - Día, mes y año de la revisión.
  - Rubrica, firma o sello de la o las personas que revisaron el procedimiento.
  - Cargo, Nombre, apellido y firma de la persona que aprobó el procedimiento.
  - Día, mes y año de la aprobación del procedimiento.

- **Pie de Página.**

  Numero de página y total de páginas.

  La información descrita de las casillas.

- **Objetivo**

  Describiremos el propósito a alcanzar mediante las actividades del documento.

- **Ámbito de aplicación.**

  Especificaremos para que plataforma o sistema operativo en específico se implementara este procedimiento.

- **Referencias**

  Se incluirán todos los documentos, anexos y recomendaciones que complementes este procedimiento.

- **Vigencia**

  Si indica la fecha inicial en la cual el estándar inicia estar vigente. EN caso de ser derogado se especificara la fecha de retiro.

- **Responsabilidades**

  Se especifica las áreas o cargos que deberán aplicar, cumplir y vigilar su cumplimiento.

- **Cuerpo del procedimiento.**

  Se describe las actividades, pasos o etapas a realizarse, esta pueden ser de forma secuencial o independiente. Se registrara las actividades aplicadas, las excepciones y sus sustentos, entre otros.

- **Revisiones**

  Se registrará las versiones de este procedimiento, sea por revisiones, mejoras o inclusión de nuevos pasos/etapas del procedimiento.

- **Recomendaciones**

  Puntos que pueden ser incluidos en el aseguramiento para mejorar y afinar el mismo.

4.5. ELABORACIÓN DE PROCEDIMIENTO DE ASEGURAMIENTO DE SISTEMA OPERATIVO LINUX.

Se creó el esquema de aseguramiento informativo para el sistema operativo Linux con el nombre “Anexo 1- Aseguramiento Linux base de tesis”, en el cual se describe las acciones a realizarse de forma detallada donde se incluye la gestión de grupos y usuarios, la configuración de privilegios, de seguridad, de variables, de contraseñas, de servicios del sistema operativo, de auditoría, permisos de directorios, entre otros.

4.6. ELABORACIÓN DE PROCEDIMIENTO DE ASEGURAMIENTO DE SISTEMA OPERATIVO WINDOWS.

Se creó el esquema de aseguramiento informativo para el sistema operativo Windows con el nombre “Anexo 2 - Aseguramiento Windows, base de tesis”, en el cual se describe las acciones a realizarse de forma detallada donde se incluye la gestión de grupos y usuarios, la configuración de privilegios, de seguridad, de variables, de contraseñas, se servicios del sistema operativo, de auditoría, permisos de directorios, entre otros.

4.7. PROCEDIMIENTO DE IMPLEMENTACIÓN Y CONFIGURACIÓN DE CENTRAL DE RECOLECCIÓN DE LOGS.

Todos los sistemas operativos e inclusive aplicaciones, crean y guardan registros de actividades que llamamos logs, termino anglosajón para referirnos a los registros o eventos suscitados en un intervalo de tiempo, siendo estos de vital importancia para análisis y seguimientos de seguridad posteriores, pudiendo determinar ingreso de usuarios, actividades como reinicio de servicios, cambio en configuraciones, errores en servicios y aplicaciones.

En actualidad existen muchas soluciones en el mercado que brindan funcionalidades de repositorio de logs, algunos incluyen sistemas avanzados de alertas, filtrados, monitoreo y clasificaciones de eventos, estos en su gran mayoría son privativos con costos considerables de licenciamientos, entre ellos tenemos ArcSight de HP, PRTG, 3CDDaemon, Kiwisyslog, entre otros.

Para la configuración de una central de almacenamiento de logs para la empresa Mail Service Express usaremos el software Datagram SyslogServer y Datagram SyslogAgent en su versión de 64 bit, también está disponible en 32 bits.

Se preparará un server para instalar este software con el objetivo de almacenar los logs de los servidores de producción, estableciendo a este como el repositorio central y como mediad contingente ante

posible eliminaciones de estos registros en los servidores principales.

Describiremos básicamente las actividades que se deben realizar para crear y configurar una central de log en la cual podamos recibir los registros y eventos de los sistemas operativos Windows y RedHat. También la herramienta soporta la recepción de registros desde equipos activos como firewall, router, impresoras, equipos activos y base de datos.

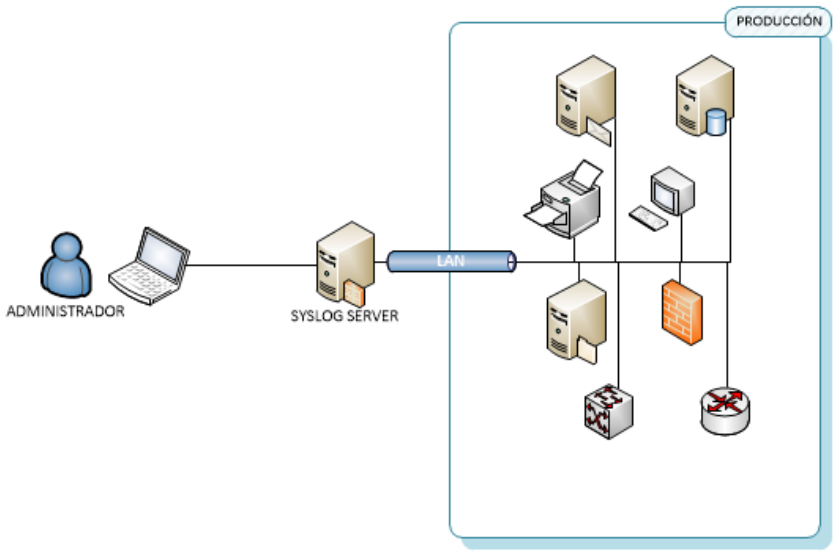


Figura 4.4 Representación de SyslogServer para almacenamiento.

ACTIVIDADES.

Cargaremos los siguientes instaladores en los servidores

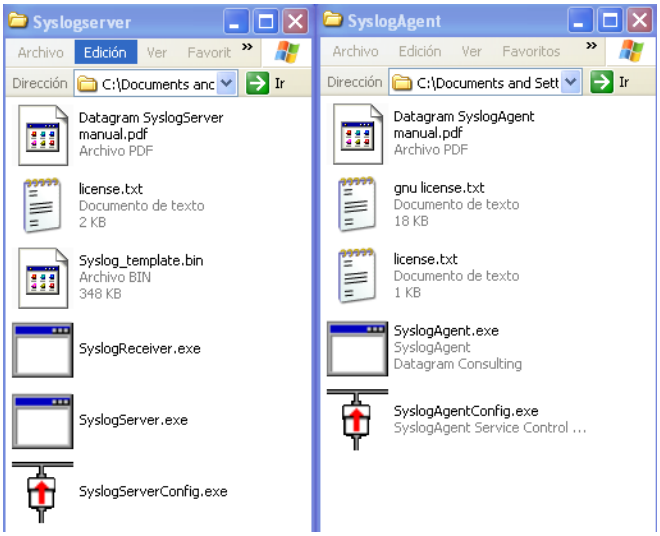


Figura 4.5 Software para creación de ServerLog.

- Confirmar que este realizado el aseguramiento informático al sistema operativo.
- Verificar que exista comunicación por el puerto UDP 514 en el cual se envía esta información entre servidores origen y destino.
- Instalar en el servidor el software Datagram SyslogServer que funcionará como repositorio de los registros. Esta aplicación es gratuita para almacenar los logs de hasta 50 direcciones ip distinta y Mail Service Express hará uso de 32. La instalación es sencilla, ejecutamos SyslogServer.exe y aparecerá la siguiente ventana

Figura 4.6 Instalación de SyslogServer.

Luego ejecutamos SyslogServerConfig.exe instalamos el servicio e inicializamos el mismo.

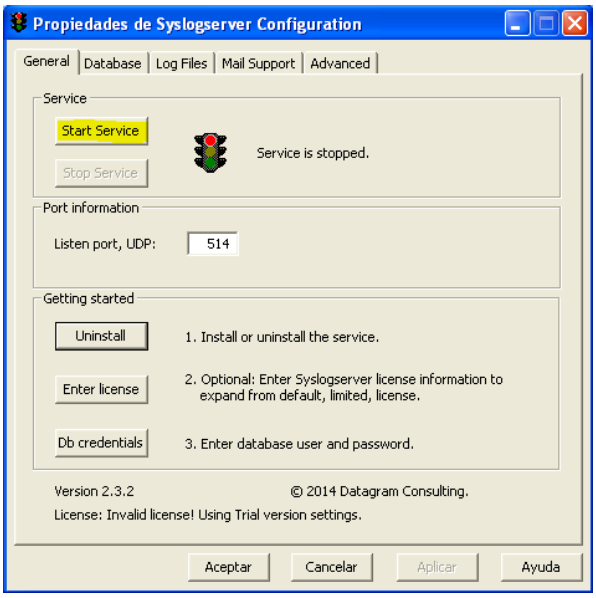


Figura 4.7 Inicializando de SyslogServer.

El software permite la personalización de los siguientes parámetros:

Puerto UDP para recepción de logs.

Directorio para almacenar los registros o logs.

Configuración de alertas mail por niveles de criticidad y personalización de repetición de las mismas.

Una vez instalado podemos configurar este servicio a nivel de sistema operativo para que se inicie de forma automática luego de cada reinicio del servidor.

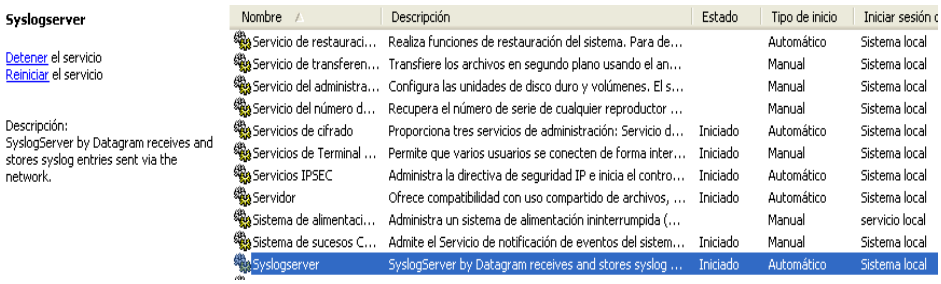


Figura 4.8 Automatización de servicio SyslogServer.

Con las acciones realizadas tenemos listo un servidor para receptar los logs de los servidores de producción.

En lo servidores Windows se procederá a instalar SyslogAgent.exe, aparecerá la ventana.

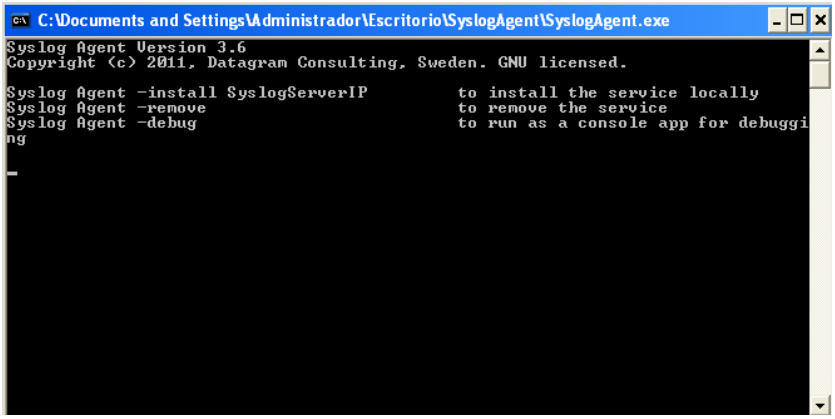


Figura 4.9 Instalación de servicio SyslogAgente.

Luego ejecutaremos SyslogAgentConfig.exe, instalaremos e inicializamos el servicio.

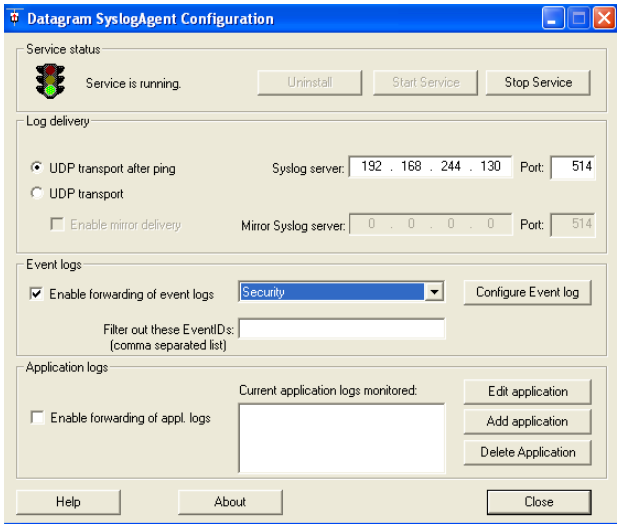


Figura 4.10 Configuración de servicio SyslogAgente.

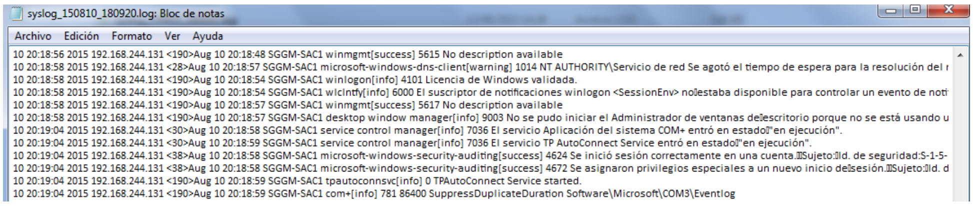
Aquí configuramos la ip donde enviaremos los logs y los tipos de eventos de las lista de despliegue.

En lo servidores Linux no es necesario instalar ningún agente o software, con la correcta configuración del servicio syslog durante el aseguramiento informático del sistema operativo se deberá indicar la ip donde se enviaran los registros.

```
#kern.*                                         /dev/console
*.info;mail.none;authpriv.none;cron.none        /var/log/messages
*.info;mail.none;authpriv.none;cron.none        @192.168.244.130
authpriv.*                                      /var/log/secure
authpriv.*                                      @192.168.244.130
#mail.*                                         -/var/log/maillog
#cron.*                                         /var/log/cron
*.emerg                                         *
#uucp,news.crit                                 /var/log/spooler
local7.*                                        /var/log/boot.log
local7.*                                        @192.168.244.130
auth,info.*                                      /var/log/messages
kern.*                                           /var/log/kern.log
kern.*                                           @192.168.244.130
daemon.*                                        /var/log/daemon.log
daemon.*                                         @192.168.244.130
syslog.*                                        /var/log/syslog
syslog.*                                        @192.168.244.130
lpr,news,uucp,local0,local1,
local2,local3,local4,local5,local6.*            /var/log/unused.log
local2,local3,local4,local5,local6.*            @192.168.244.130
```

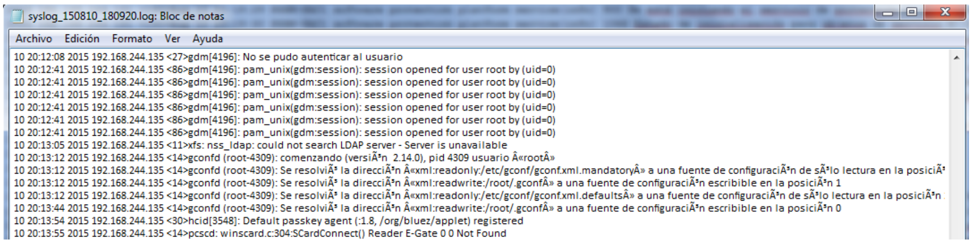
Figura 4.11 Configuración de Syslog en Linux.

Una vez concluidas las configuraciones indicadas receptaremos los logs de los sistemas operativos en el cual se instaló el agente en Windows y donde se indicó la dirección ip destino en Linux.



```
syslog_150810_180920.log: Bloc de notas
Archivo  Edición  Formato  Ver  Ayuda
10 20:18:56 2015 192.168.244.131 <190>Aug 10 20:18:48 SGGM-SAC1 winmgmt[success] 5615 No description available
10 20:18:58 2015 192.168.244.131 <28>Aug 10 20:18:57 SGGM-SAC1 microsoft-windows-dns-client[warning] 1014 NT AUTHORITY\Servicio de red Se agotó el tiempo de espera para la resolución del r
10 20:18:58 2015 192.168.244.131 <190>Aug 10 20:18:54 SGGM-SAC1 winlogon[info] 4101 Licencia de Windows validada.
10 20:18:58 2015 192.168.244.131 <190>Aug 10 20:18:54 SGGM-SAC1 wlclntfy[info] 6000 El suscriptor de notificaciones winlogon <SessionEnv> no estaba disponible para controlar un evento de noti
10 20:18:58 2015 192.168.244.131 <190>Aug 10 20:18:57 SGGM-SAC1 winmgmt[success] 5617 No description available
10 20:18:58 2015 192.168.244.131 <190>Aug 10 20:18:57 SGGM-SAC1 desktop window manager[info] 9003 No se pudo iniciar el Administrador de ventanas de escritorio porque no se está usando u
10 20:19:04 2015 192.168.244.131 <30>Aug 10 20:18:58 SGGM-SAC1 service control manager[info] 7036 El servicio Aplicación del sistema COM+ entró en estado "en ejecución".
10 20:19:04 2015 192.168.244.131 <30>Aug 10 20:18:59 SGGM-SAC1 service control manager[info] 7036 El servicio TP AutoConnect Service entró en estado "en ejecución".
10 20:19:04 2015 192.168.244.131 <38>Aug 10 20:18:58 SGGM-SAC1 microsoft-windows-security-auditing[success] 4624 Se inició sesión correctamente en una cuenta. Sujeto: Id. de seguridad:S-1-5-
10 20:19:04 2015 192.168.244.131 <38>Aug 10 20:18:58 SGGM-SAC1 microsoft-windows-security-auditing[success] 4672 Se asignaron privilegios especiales a un nuevo inicio de sesión. Sujeto: Id. d
10 20:19:04 2015 192.168.244.131 <190>Aug 10 20:18:59 SGGM-SAC1 tpautoconnsvc[info] 0 TPAutoConnect Service started.
10 20:19:04 2015 192.168.244.131 <190>Aug 10 20:18:59 SGGM-SAC1 com+[info] 781 86400 SuppressDuplicateDuration Software\Microsoft\COM3\Eventlog
```

Figura 4.12 Log recibido desde sistema operativo Windows.



```
syslog_150810_180920.log: Bloc de notas
Archivo  Edición  Formato  Ver  Ayuda
10 20:12:08 2015 192.168.244.135 <27>gdm[4196]: No se pudo autenticar al usuario
10 20:12:41 2015 192.168.244.135 <86>gdm[4196]: pam_unix(gdm:session): session opened for user root by (uid=0)
10 20:12:41 2015 192.168.244.135 <86>gdm[4196]: pam_unix(gdm:session): session opened for user root by (uid=0)
10 20:12:41 2015 192.168.244.135 <86>gdm[4196]: pam_unix(gdm:session): session opened for user root by (uid=0)
10 20:12:41 2015 192.168.244.135 <86>gdm[4196]: pam_unix(gdm:session): session opened for user root by (uid=0)
10 20:12:41 2015 192.168.244.135 <86>gdm[4196]: pam_unix(gdm:session): session opened for user root by (uid=0)
10 20:12:41 2015 192.168.244.135 <86>gdm[4196]: pam_unix(gdm:session): session opened for user root by (uid=0)
10 20:13:05 2015 192.168.244.135 <11>xfs: nss_ldap: could not search LDAP server - Server is unavailable
10 20:13:12 2015 192.168.244.135 <14>gconfd (root-4309): comenzando (versiÃ³n 2.14.0), pid 4309 usuario Â«rootÂ»
10 20:13:12 2015 192.168.244.135 <14>gconfd (root-4309): Se resolviÃ³ la direcciÃ³n Â«xml:readonly:/etc/gconf/gconf.xml.mandatoryÂ» a una fuente de configuraciÃ³n de sÃ³lo lectura en la posiciÃ³
10 20:13:12 2015 192.168.244.135 <14>gconfd (root-4309): Se resolviÃ³ la direcciÃ³n Â«xml:readwrite:/root/.gconfÂ» a una fuente de configuraciÃ³n escribible en la posiciÃ³n 1
10 20:13:12 2015 192.168.244.135 <14>gconfd (root-4309): Se resolviÃ³ la direcciÃ³n Â«xml:readonly:/etc/gconf/gconf.xml.defaultsÂ» a una fuente de configuraciÃ³n de sÃ³lo lectura en la posiciÃ³n
10 20:13:44 2015 192.168.244.135 <14>gconfd (root-4309): Se resolviÃ³ la direcciÃ³n Â«xml:readwrite:/root/.gconfÂ» a una fuente de configuraciÃ³n escribible en la posiciÃ³n 0
10 20:13:54 2015 192.168.244.135 <30>hcid[3548]: Default passkey agent (:1.8, /org/bluez/applet) registered
10 20:13:55 2015 192.168.244.135 <14>pcscd: winscard.c:304:SCardConnect() Reader E-Gate 0 0 Not Found
```

Figura 4.13 Log recibido desde sistema operativo Linux.

El archivo de log de esta configuración esta agregado como anexo para constatar la recepción de los log.

CAPÍTULO 5

IMPLEMENTACIÓN.

A continuación se detallan las actividades por la aplicación del esquema de aseguramiento el cual fue elaborado para RedHat 5.5 y Windows 2008 R2. Iniciaremos con el esquema de aseguramiento del S.O Linux, RedHat.

5.1. IMPLEMENTACIÓN DE ASEGURAMIENTO DE SISTEMA OPERATIVO LINUX.

USUARIOS POR DEFECTO.

Las siguientes cuentas son creadas durante la instalación del sistema operativo, estas no deberán tener ningún Shell asignado, limitando el acceso al sistema operativo. Para configuración se debe editar el archivo ***"etc/passwd"***

Tabla 1. Usuarios por defecto sin shell.

avahi	/sbin/nologin
dbus	/sbin/nologin
ftp	/sbin/nologin
gdm	/sbin/nologin
haldaemon	/sbin/nologin
mailnull	/sbin/nologin
nfsnobody	/sbin/nologin
nobody	/sbin/nologin
nscd	/sbin/nologin
ntp	/sbin/nologin

pcap	/sbin/nologin
rpc	/sbin/nologin
rpcuser	/sbin/nologin
Rpm	/sbin/nologin
sabayon	/sbin/nologin
smmsp	/sbin/nologin
sshd	/sbin/nologin
Vcsa	/sbin/nologin
xfs	/sbin/nologin

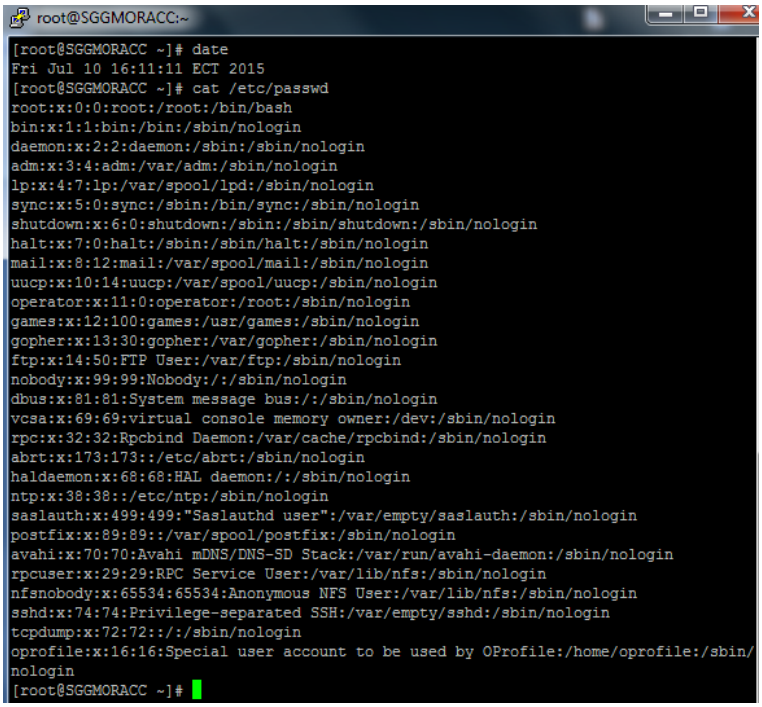


Figura 5.1 Limitación de acceso a usuarios por defecto colocando

USUARIOS DESACTIVADOS

Se desactivan los siguientes usuarios.

Tabla 2. Usuarios desactivados.

Usuarios Deshabilitados
Bin
Daemon
ftp
Games
Gopher
Lp
Mail
Man
News
Nobody
Uucp

Se confirma mediante la revisión del archivo "***/etc/shadow"***, visualizar el * en el parámetro donde corresponde el clave.

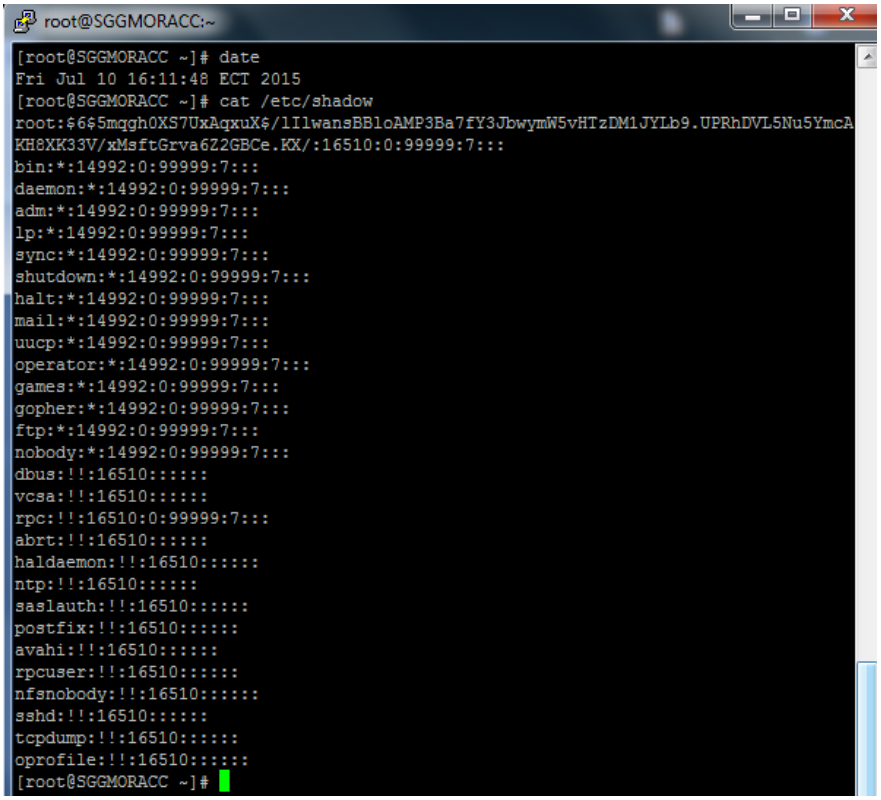


Figura 5.2 Cuentas de usuarios deshabilitadas.

LIMITACIÓN DE COMANDO SU

Solo los administradores pueden usar el comando “su”, para lograr esto se agrega la siguiente línea ***auth required pam_wheel.so use_uid group= TI_UNIX_ADMIN*** en el archivo “***/etc/pam.d/su”***

Se especifica que grupo únicamente tendrá acceso a este privilegio.

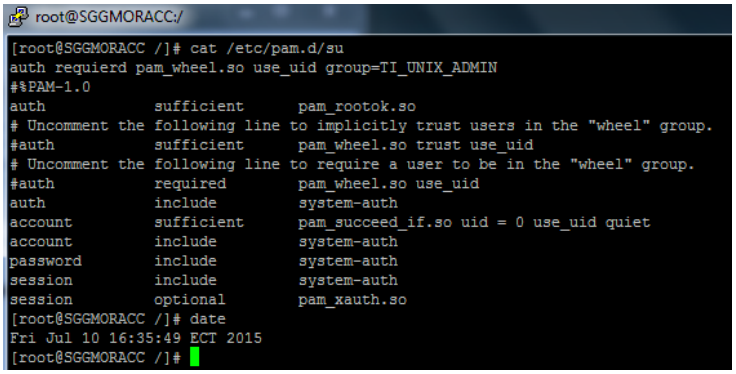


Figura 5.3 Configuración de grupo con privilegio su.

PARAMETRIZANDO DEL COMANDO SUDO

Se configura el archivo ***“/etc/sudoers”*** solo debe estar la siguiente línea: %TI_UNIX_ADMIN ALL=(ALL) ALL

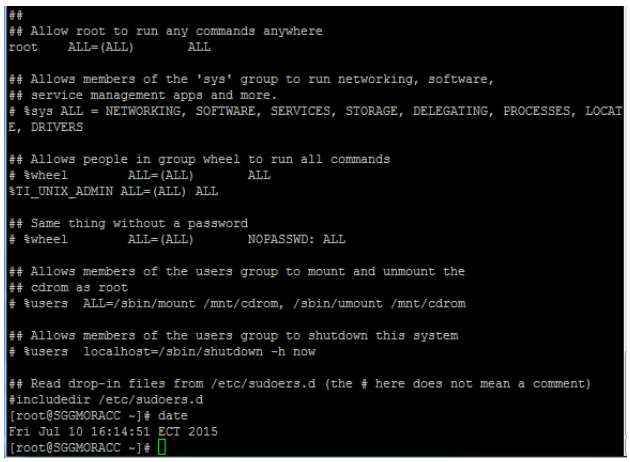


Figura 5.4 Configuración de sudo para grupo de usuarios.

Esto permitirá realizar seguimientos por temas de auditoría. La información será complementada con la revisión de los logs de "***/var/logs/messages"*** por autenticación, y de comandos en "***/var/log/secure"***

GESTIÓN DE GRUPOS.

Editamos el archivo "***/etc/groups"*** donde establecemos los valores adecuados para la administración de los grupos en el sistema operativo.

Tabla 3. Gestión de grupos

Grupo	GID	Miembros	Miembros
adm	4	root, adm, daemon	Gestión de informes de accounting.
avahi	70	ninguno	Grupo por default
bin	1	root, bin, daemon	Privilegio para comando s y aplicaciones del S.O
daemon	2	root, bin, daemon	Privilegio para comando s y aplicaciones del S.O
dbus	81	ninguno	Grupo por default
dip	40	ninguno	Grupo por default
disk	6	root	Grupo por default
floppy	19	ninguno	Grupo por default
ftp	50	ninguno	Grupo por default
games	20	ninguno	Grupo por default
gopher	30	ninguno	Grupo por default
TI_UNIX_USER	11	usuarios generales	Grupo para usuarios estándar
haldaemon	68	ninguno	Grupo por default
lock	54	ninguno	Grupo por default
lp	7	daemon, lp	Grupo por default
mail	12	ninguno	Grupo por default
mailnull	47	ninguno	Grupo por default
man	15	ninguno	Grupo por default
news	13	ninguno	Grupo por default
nfsnobody	65534	ninguno	Grupo por default
nobody	99	ninguno	Grupo por default
nscd	28	ninguno	Grupo por default
ntp	38	ninguno	Grupo por default
pcap	77	ninguno	Grupo por default
root	0	root	Usuario de máximo privilegio del S.O
rpc	32	ninguno	Grupo por default
rpcuser	29	ninguno	Grupo por default

rpm	37	ninguno	Grupo por default
slocate	21	ninguno	Grupo por default
smmsp	51	ninguno	Grupo por default
sshd	74	ninguno	Grupo por default
sys	3	root, bin, adm	Privilegio para comando s y aplicaciones del S.O
TI_UNIX_ADMIN	N	administradores	Administradores del sistema operativo
tty	5	ninguno	Grupo por default
users	100	ninguno	Grupo por default
utempter	35	ninguno	Grupo por default
utmp	22	ninguno	Grupo por default
wheel	10	root	Grupo con privilegios de administración en el sistema operativo
xfs	43	ninguno	Grupo por default

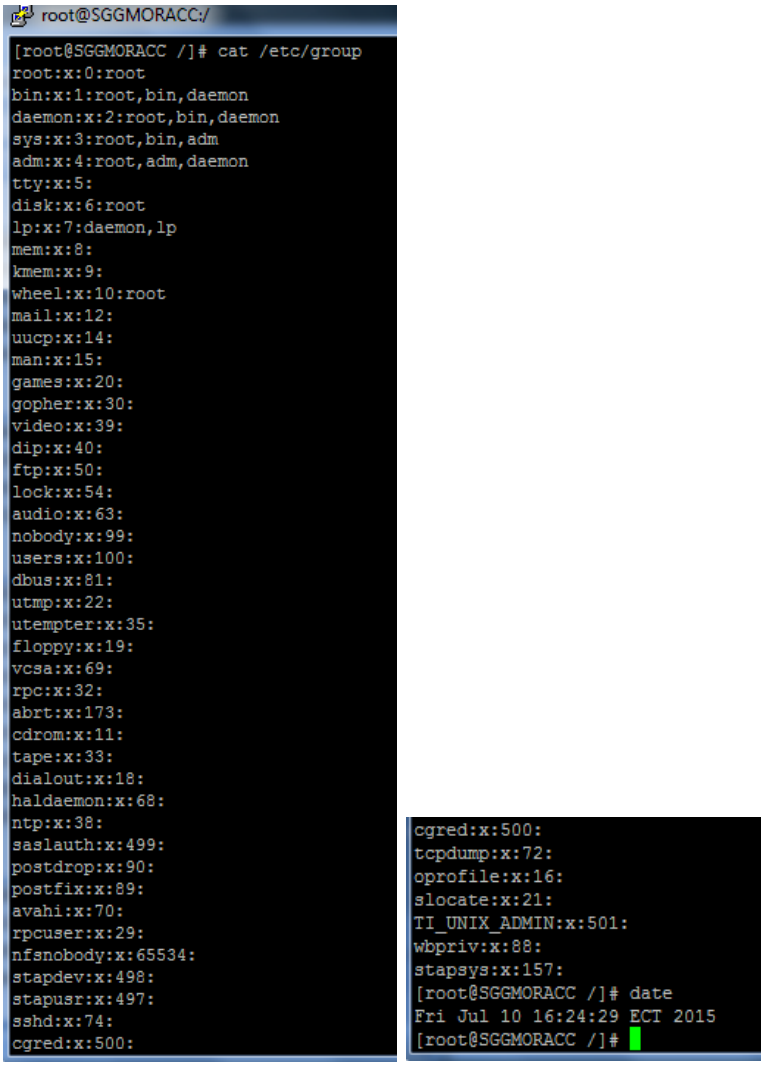


Figura 5.5 Configuración de los grupos con sus usuarios.

CONFIGURACIÓN DE SEGURIDAD EN EL SISTEMA OPERATIVO.

Para incrementar la seguridad y protección a los sistemas de archivos y filesystem críticos del sistema operativo realizamos las siguientes configuraciones.

ALERTA DE BIENVENIDA.

Se deberá agregar a los archivos “/etc/issue.ssh” y “/etc/issue.net” el siguiente fragmento de texto:

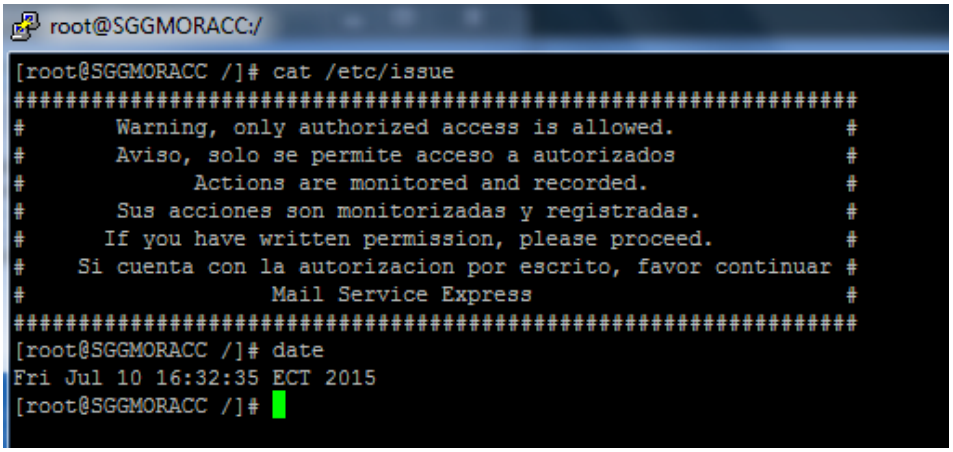


Figura 5.6 Configuración de banners.

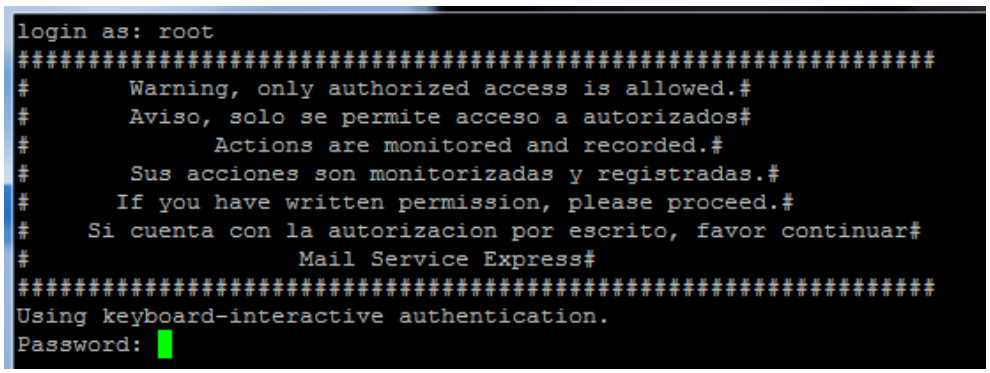


Figura 5.7 Verificación de alerta configurada.

Nota. Han existido casos llevados juicio que obtuvieron sentencia de inocencia debido a la falta de advertencia o en su defecto se dio la bienvenida al ingresar a los sistemas informáticos, aunque se realizaran actividades ilícitas luego del ingreso no autorizado.

CONFIGURACION DE VARIABLES.

Se deberá configurar el archivo ***"/etc/profile/"*** en el cual se encuentran los parámetros del sistema, así mismo a los archivos .profile, .login, .bashrc de cada usuario habilitado del sistema operativo, con los siguientes parámetros.

TMOUT, *export TMOUT=600*.

Para cierre automática ante inactividad

UMASK, Umask 057

Permisos por defecto cuando algún usuario crear archivos/directorios

Trap, 1, 2,3

Evita desconexiones involuntarias del comando de menú.

Path, Privilegios de ejecución de comandos, variables acorde al rol

Root. "/usr/bin" y "/usr/sbin" sin directorio corriente (.)

Otros, "/bin", "/usr/bin" con directorio corriente (.).

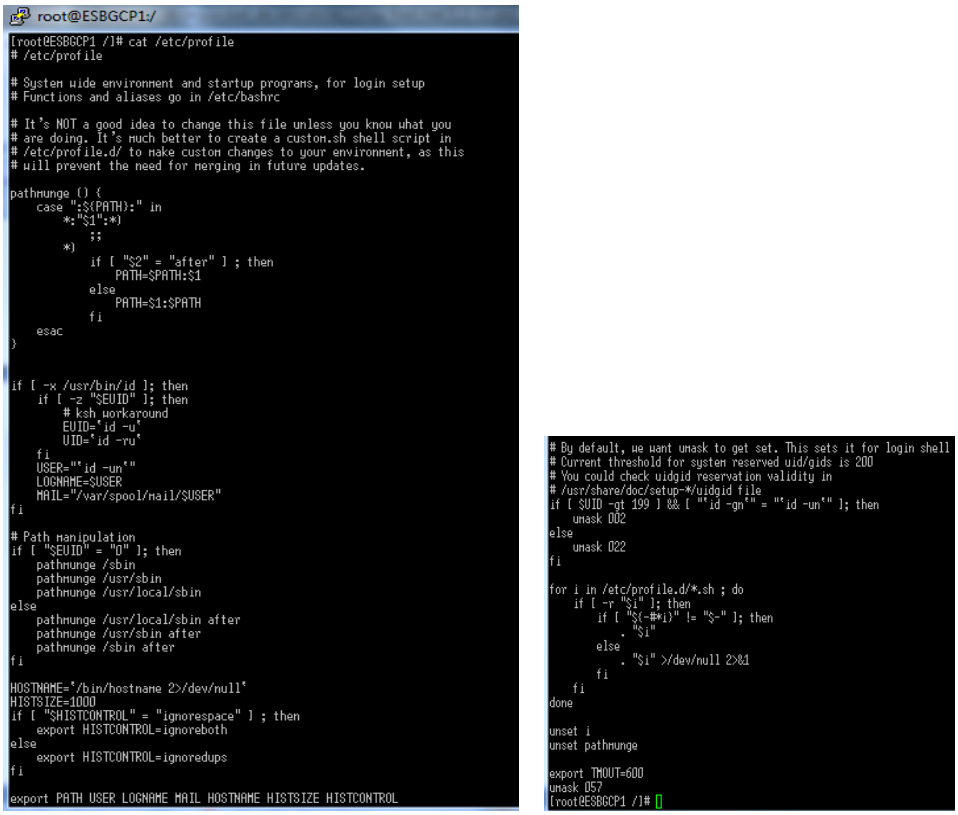


Figura 5.8 Configuración de variable de seguridad.

PARAMETRIZACIÓN DE SELINUX.

Se debe tener activo el SELinux.

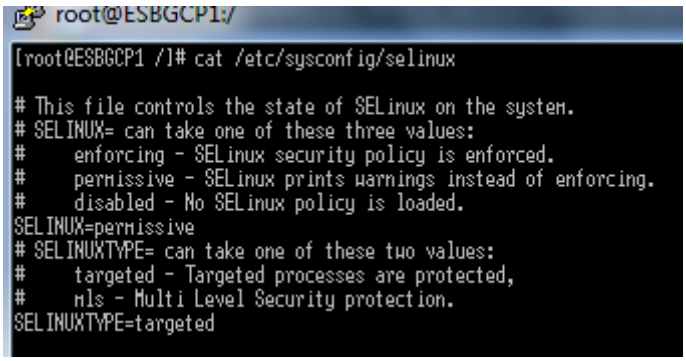


Figura 5.9 Configuración de SELinux de seguridad.

PARAMETRIZACION DE INITTAB.

Para evitar reinicios por algún usuario sin que este se identifique se agrega la siguiente línea

 # Trap CTRL-ALT-DELETE

#ca::ctrlaltdel:/sbin/shutdown -t3 -r now

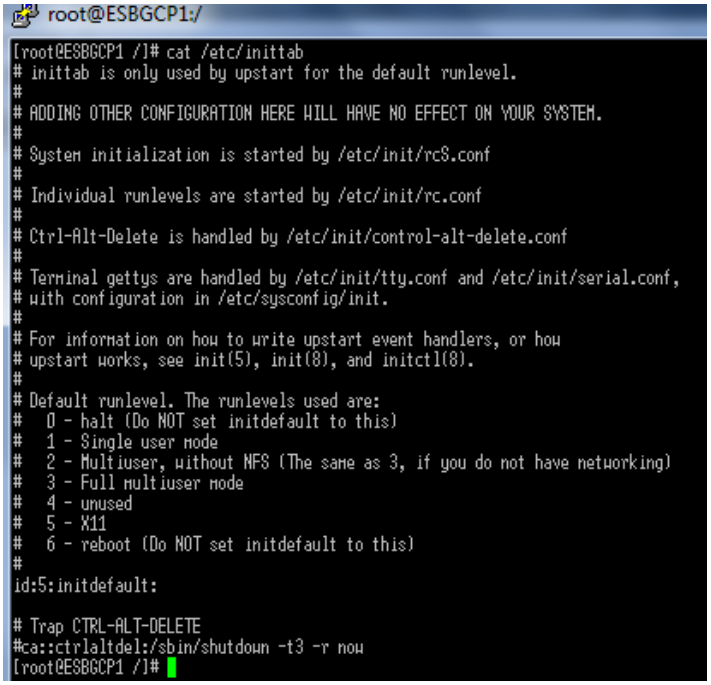


Figura 5.10 Configuración para evitar reinicios no autorizados.

Para aplicar los cambios se ejecutó el comando “init q”

PARAMETRIZACIÓN DE POLÍTICA DE CONTRASEÑAS.

Modificamos el archivo ***/etc/login.defs*** aplicando los siguientes valores.

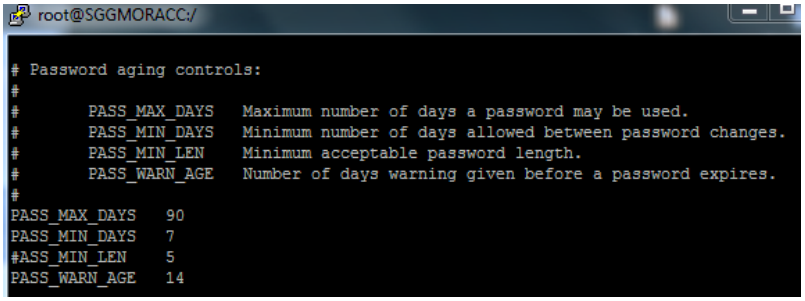


Figura 5.11 Configuración de parámetros contraseñas.

Modificamos el archivo ***/etc/pam.d/system-auth*** aplicando los siguientes valores.

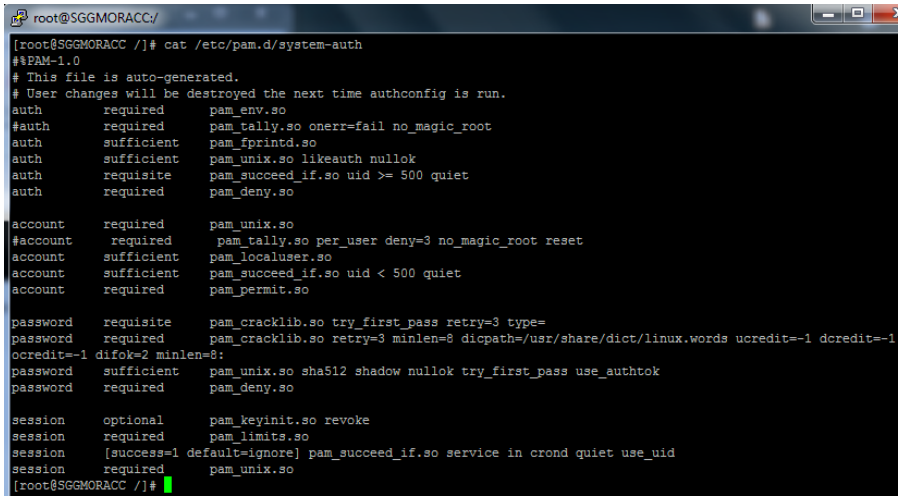


Figura 5.12 Configuración de directiva de contraseñas.

CONFIGURACIÓN DE RELACIÓN DE CONFIANZA.

No debe existir el archivo /etc/hosts.equiv.

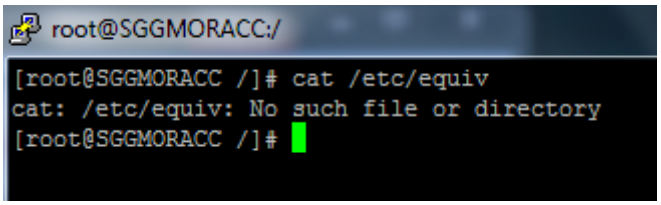


Figura 5.13 Verificación de inexistencia de archivo

ACTUALIZACIONES.

El sistema operativo cuenta con las actualizaciones de seguridad hasta el 10/07/2015.

Figura 5.14 Verificación de actualizaciones de seguridad.

CONFIGURACIONES DE SERVICIOS DEL SISTEMA OPERATIVO.

Están activos solo los servicios del sistema especificado en el esquema de aseguramiento.

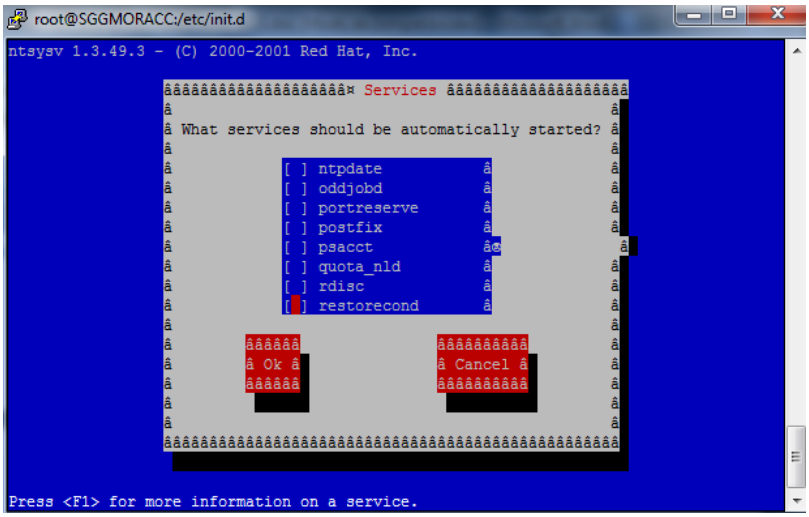
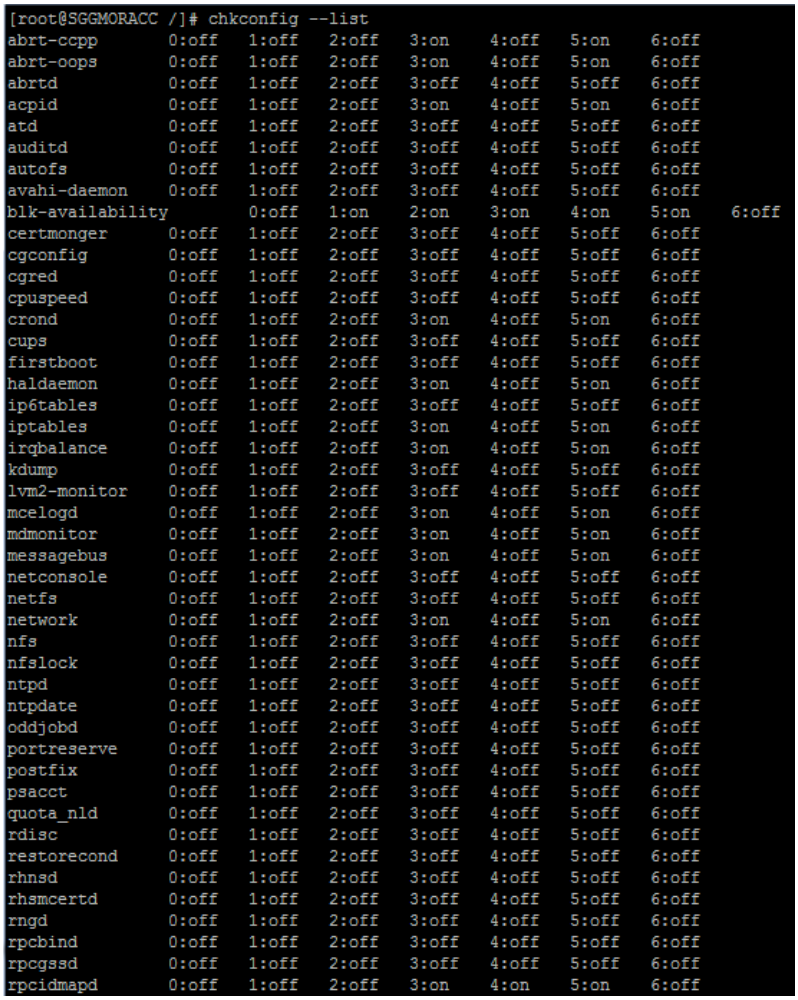


Figura 5.15 Configuración de servicios del sistema operativo.

Nota: se puede verificar cuales servicio inician automáticamente con el sistema operativo con el comando chkconfig --list



```
[root@SGGMORACC /]# chkconfig --list
abrt-ccpp       0:off   1:off   2:off   3:on    4:off   5:on    6:off
abrt-oops       0:off   1:off   2:off   3:on    4:off   5:on    6:off
abrtd           0:off   1:off   2:off   3:off   4:off   5:off   6:off
acpid           0:off   1:off   2:off   3:on    4:off   5:on    6:off
atd             0:off   1:off   2:off   3:off   4:off   5:off   6:off
auditd          0:off   1:off   2:off   3:off   4:off   5:off   6:off
autofs          0:off   1:off   2:off   3:off   4:off   5:off   6:off
avahi-daemon    0:off   1:off   2:off   3:off   4:off   5:off   6:off
blk-availability        0:off   1:on    2:on    3:on    4:on    5:on    6:off
certmonger      0:off   1:off   2:off   3:off   4:off   5:off   6:off
cgconfig        0:off   1:off   2:off   3:off   4:off   5:off   6:off
cgred           0:off   1:off   2:off   3:off   4:off   5:off   6:off
cpuspeed        0:off   1:off   2:off   3:off   4:off   5:off   6:off
crond           0:off   1:off   2:off   3:on    4:off   5:on    6:off
cups            0:off   1:off   2:off   3:off   4:off   5:off   6:off
firstboot       0:off   1:off   2:off   3:off   4:off   5:off   6:off
haldaemon       0:off   1:off   2:off   3:on    4:off   5:on    6:off
ip6tables       0:off   1:off   2:off   3:off   4:off   5:off   6:off
iptables        0:off   1:off   2:off   3:on    4:off   5:on    6:off
irqbalance      0:off   1:off   2:off   3:on    4:off   5:on    6:off
kdump           0:off   1:off   2:off   3:off   4:off   5:off   6:off
lvm2-monitor    0:off   1:off   2:off   3:off   4:off   5:off   6:off
mcelogd         0:off   1:off   2:off   3:on    4:off   5:on    6:off
mdmonitor       0:off   1:off   2:off   3:on    4:off   5:on    6:off
messagebus      0:off   1:off   2:off   3:on    4:off   5:on    6:off
netconsole      0:off   1:off   2:off   3:off   4:off   5:off   6:off
netfs           0:off   1:off   2:off   3:off   4:off   5:off   6:off
network         0:off   1:off   2:off   3:on    4:off   5:on    6:off
nfs             0:off   1:off   2:off   3:off   4:off   5:off   6:off
nfslock         0:off   1:off   2:off   3:off   4:off   5:off   6:off
ntpd            0:off   1:off   2:off   3:off   4:off   5:off   6:off
ntpdate         0:off   1:off   2:off   3:off   4:off   5:off   6:off
oddjobd         0:off   1:off   2:off   3:off   4:off   5:off   6:off
portreserve     0:off   1:off   2:off   3:off   4:off   5:off   6:off
postfix         0:off   1:off   2:off   3:off   4:off   5:off   6:off
psacct          0:off   1:off   2:off   3:off   4:off   5:off   6:off
quota_nld       0:off   1:off   2:off   3:off   4:off   5:off   6:off
rdisc           0:off   1:off   2:off   3:off   4:off   5:off   6:off
restorecond     0:off   1:off   2:off   3:off   4:off   5:off   6:off
rhnsd           0:off   1:off   2:off   3:off   4:off   5:off   6:off
rhsmcertd       0:off   1:off   2:off   3:off   4:off   5:off   6:off
rngd            0:off   1:off   2:off   3:off   4:off   5:off   6:off
rpcbind         0:off   1:off   2:off   3:off   4:off   5:off   6:off
rpcgssd         0:off   1:off   2:off   3:off   4:off   5:off   6:off
rpcidmapd       0:off   1:off   2:off   3:on    4:on    5:on    6:off
```

Figura 5.16 Verificación de servicios que se inician automáticamente.

CONFIGURACIÓN TELNET.

Está desactivado el servicio de telnet.

CONFIGURACIÓN SSH.

La configuración está realizada como indica el esquema de aseguramiento.

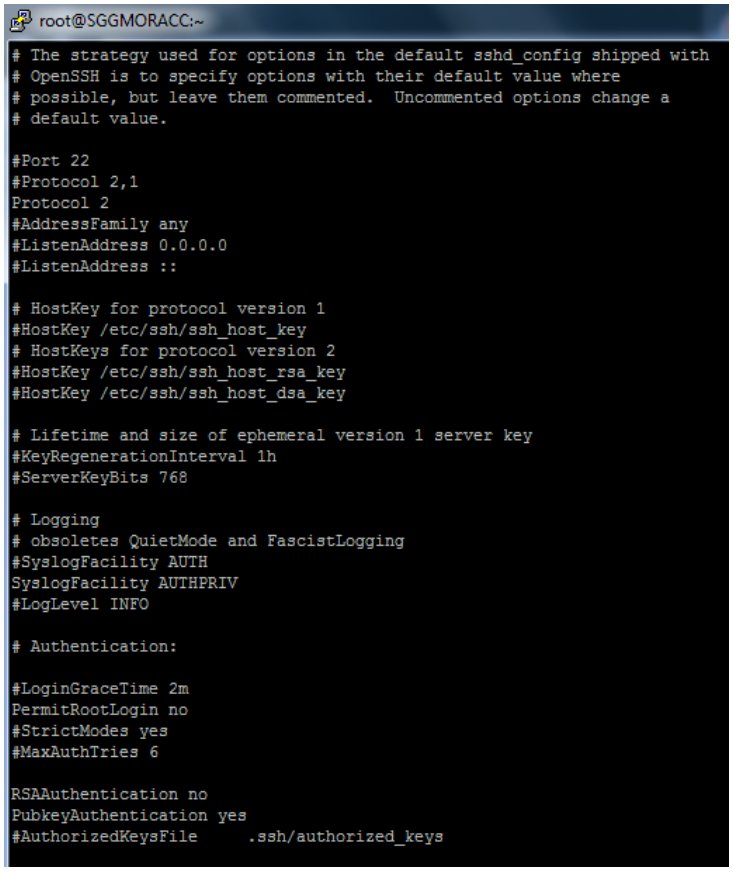


Figura 5.17 Configuración del servicio ssh.

CONFIGURACIÓN FTP.

La configuración FTP esta desactivada.

CONFIGURACIÓN DE TAREAS CRONT Y ALT.

La configuración está realizada acorde al esquema de aseguramiento, adjunto evidencia

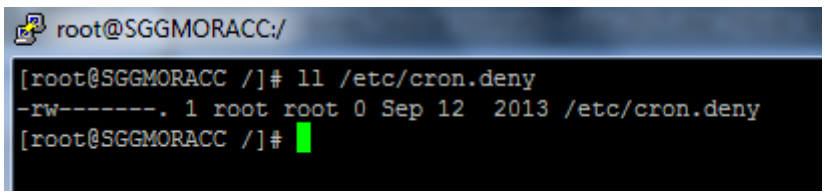


Figura 5.18 Configuración de cront y alt.

CONFIGURACIÓN DE AUDITORÍA DE EVENTOS.

La configuración fue realizada como especifica el esquema de aseguramiento.

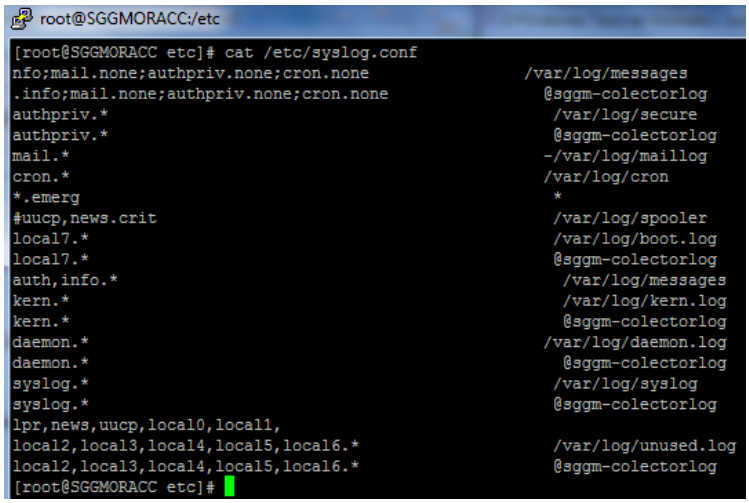
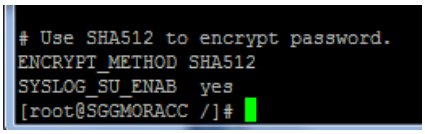


Figura 5.19 Configuración de parámetros para la auditoria de eventos.

CONFIGURACIÓN DE AUDITORÍA DE SUDO Y SU.

La configuración fue realizada como especifica el esquema de aseguramiento.



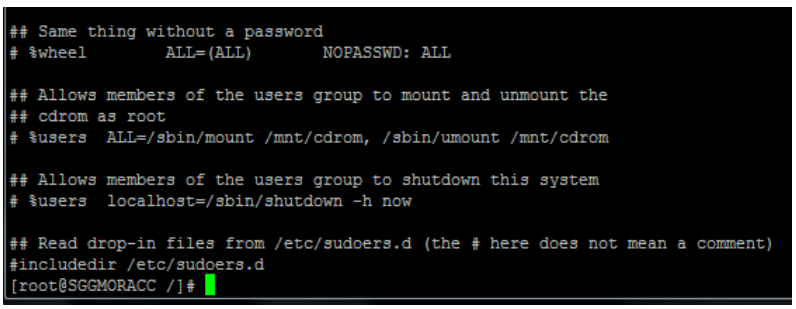


Figura 5.20 Configuración de auditoría para sudo y su.

CONFIGURACIÓN DE ROTACIÓN Y RETENCIÓN DE LOG.

La configuración fue realizada como especifica el esquema de aseguramiento.

```
[root@SGGMORACC /]# cat /etc/logrotate.conf
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 12

# create new (empty) log files after rotating old ones
create

# use date as a suffix of the rotated file
dateext

# uncomment this if you want your log files compressed
compress
```

Figura 5.21 Configuración de rotación de log.

PERMISOS EN DIRECTORIOS.

La configuración fue realizada como especifica el esquema de aseguramiento

```
root@SGGMORACC:/
[root@SGGMORACC /]# ll
total 182
dr-xr-xr-x.   2 root root  4096 May 26 03:26 bin
dr-xr-xr-x.   5 root root  1024 May 25 16:29 boot
drwxr-xr-x.   2 root root  4096 Aug  7  2014 cgroup
drwxr-xr-x.   3 root root  4096 Mar 16 16:01 data1
drwxr-xr-x.   3 root root  4096 Mar 16 16:01 data2
drwxr-xr-x.  23 root root  4280 Jun 30 14:27 dev
drwxr-xr-x. 106 root root 12288 Jul 14 17:33 etc
drwxr-xr-x.   3 root root  4096 Mar 16 16:02 fra1
drwxr-xr-x.   3 root root  4096 Mar 16 16:02 fra2
drwxr-xr-x.   3 root root  4096 Jun 28  2011 home
drwx-w----.   2 root root  4096 Mar 27 12:48 instaladores
dr-xr-xr-x.  13 root root  4096 May 26 03:26 lib
dr-xr-xr-x.   9 root root 12288 May 26 03:26 lib64
drwx------.   2 root root 16384 Mar 16 16:02 lost+found
drwxr-xr-x.   2 root root  4096 Jun 28  2011 media
drwxr-xr-x.   2 root root  4096 Aug 21  2014 misc
drwxr-xr-x.   2 root root  4096 Jun 28  2011 mnt
drwxr-xr-x.   2 root root  4096 Aug 21  2014 net
drwxr-xr-x.   2 root root  4096 Jun 28  2011 opt
dr-xr-xr-x. 153 root root     0 Jun 30 14:26 proc
dr-xr-x---.   4 root root  4096 Jun  2 16:12 root
dr-xr-xr-x.   2 root root 12288 May 26 03:26 sbin
drwxr-xr-x.   7 root root     0 Jun 30 14:26 selinux
drwxr-xr-x.   2 root root  4096 Jun 28  2011 srv
drwxr-xr-x.   3 root root  4096 Mar 16 16:01 stage
drwxr-xr-x.  13 root root     0 Jun 30 14:26 sys
-r-x------.   1 root root  1217 Mar 26 11:56 system-auth-politicas
drwxrwxrwt.   4 root root  4096 Jul 14 17:40 tmp
drwxr-xr-x.   3 root root  4096 Mar 16 16:00 u01
drwxr-xr-x.  13 root root  4096 May 25 16:19 usr
drwxr-xr-x.  21 root root  4096 May 25 16:28 var
[root@SGGMORACC /]#
```

Figura 5.22 Configuración de permisos en directorio de archivos.

Verificación

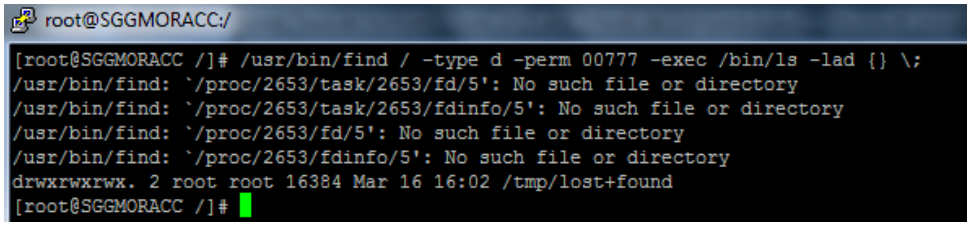


Figura 5.23 Verificación de permisos de escritura para otros.

5.1.1. VERIFICACIÓN DE ASEGURAMIENTO INFORMÁTICO IMPLEMENTADO.

La verificación se realiza mediante una revisión específica para la confirmación de la correcta implementación del esquema de aseguramiento informático.

Se usa la plantilla descrita en la tabla en la cual mediante la confirmación manual se procede a determinar el cumplimiento de cada una de las premisas del esquema de aseguramiento.

Tabla 4. Plantilla de verificación de aseguramiento informático Linux.

DETALLE	ACCIÓN DE VERIFICACIÓN	Cumple	
		SI	NO
Parámetros generales			
BIOS			
Confirmar en el bios, el menú de administración cuente con contraseña.	El ingreso directo al menú es confirmación de que no está configurada la contraseña.	SI	
Verificar que el primer dispositivo de arranque sean los discos rígidos del servidor.	Revisar el orden de los dispositivos de arranque, siempre los discos locales deben ser primero	SI	
Periféricos USB			

Verificar que no se encuentren habilitados los puertos USB.	Confirmar mediante la conexión de una unidad de almacenamiento USB externa	SI	
Usuarios y grupos			
Cuentas por defecto			
Confirmar la configuración indicada del procedimiento de aseguramiento informático para las cuentas de usuario por defecto.	Verificar el archivo “etc_passwd”, y confirmar los shell de los usuarios.	SI	
Cuenta de usuarios deshabilitadas			
Confirmar la configuración indicada del procedimiento de aseguramiento informático para usuarios deshabilitados.	Verificar el archivo “etc_shadow”, y confirmar usuarios desactivados.	SI	
Grupos de sistema			
Confirmar la configuración indicada del procedimiento de aseguramiento informático para los grupos del sistema.	Verificar el archivo “etc_group”, y confirmar la configuración de grupos.	SI	
Restricción del comando “su”			
Confirmar que en el archivo /etc/pam.d/su este agregada la línea del grupo administrador que únicamente usara su	Verificar el archivo “/etc/pam.d/su”, y confirmar la configuración del grupo con privilegio su.	SI	
Configuración del comando SUDO			
Confirmar que solo los administradores tengan el privilegio sudo %TI_UNIX_ADMIN ALL=(ALL) ALL	Verificar el archivo “etc/sudoers”, y confirmar la configuración del grupo con privilegio sudo	SI	
Configuración de inittab			
Verificar este implementada la configuración que evita el reinicio sin identificación de usuario. ca::ctrlaltdel:/sbin/shutdown -t3 -r no	Verificar el archivo “/etc/inittab”, y confirmar la configuración.	SI	
Configuración de SELiux			
Confirmar los parámetros SELINUX=enforcing y SELINUXTYPE=targeted en el archivo **“/etc/sysconfig/selinux”**	Verificar el archivo “/etc/sysconfig/selinux”, y confirmar la configuración.	SI	
Políticas de cuentas			
Políticas de contraseñas y cuentas de usuarios			
Verificar los parámetros indicados en el procedimiento de aseguramiento informático para la implementación de política de contraseñas.	Verificar los parámetros indicados en el procedimiento de aseguramiento informático en "/etc/login.defs" y "/etc/pam.d/system-auth"	SI	
Administración de recursos			

Servicios de red			
Verificar los servicios nivel 3 y 5 de ejecución del sistema permitidos e indicados por el procedimiento de aseguramiento informático.	Revisar mediante la consola grafica usando el comando "system-config-services"	SI	
directorios, permisos			
Permisos de acceso a archivos			
Confirmar que los permisos del aseguramiento informático estén implementados.	Verificar los permisos de los directorios principales indicados en el aseguramiento informático, adicional verificar que no exista permisos de escritura para otros con los siguientes comandos: /usr/bin/find / -type d -perm 00777 -exec /bin/ls -lad {} \; /usr/bin/find / -type f -perm -00002 -exec /bin/ls -la {} \;	SI	
Auditoría			
Objetos			
Confirmar la configuración del syslog y que se esté enviando la información a la central de recolección de logs	Verificar los parámetros indicados en el procedimiento de aseguramiento informático en "/etc/syslog.conf"	SI	

Si existiera el incumplimiento en unos de los ítem de la plantilla, la cual está estrictamente vinculada al procedimiento de aseguramiento informático, esta debe ser tratada y corregida, o en su defecto manejarla con la autorización del responsable de seguridad como excepción considerando acciones compensatorias que puedan minimizar los riegos latentes vinculantes.

5.1.2. PRUEBAS DE ASEGURAMIENTO INFORMÁTICO IMPLEMENTADO.

Las pruebas efectuadas al servidor con el sistema operativo Red Hat son acciones manuales en la cual se intenta acceder a las cuentas de usuario que deben estar deshabilitadas, confirmar que no puede modificar permisos a directorios principales del sistema, verificar que los logs de auditoría estén siendo enviados a la central de recolección de log configurada, que un usuarios normal no pueda acceder a privilegios como su y sudo, que no esté habilitado el servicio de telnet, que no se pueda hacer uso del usuario root vía ssh.

Se adjunta capturas de estas acciones.

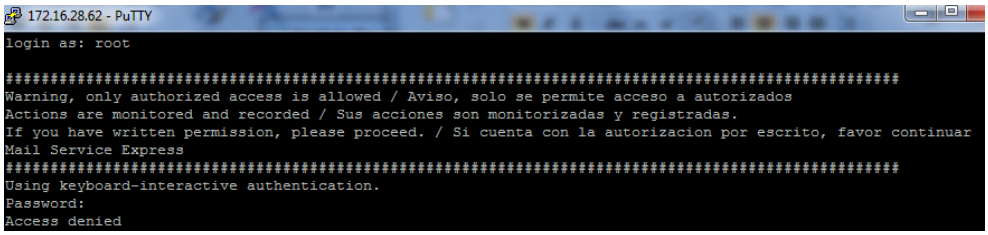


Figura 5.24 Verificación de no ingreso con credenciales root.

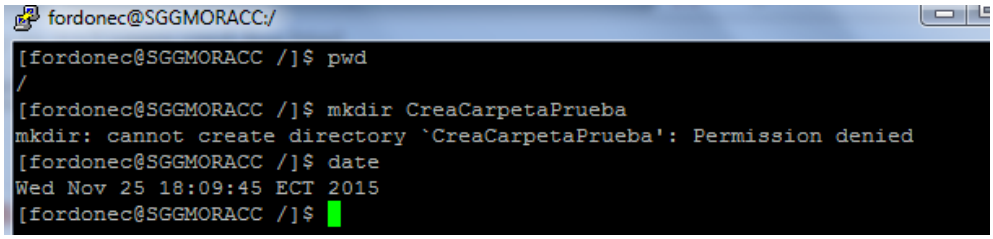


Figura 5.25 Verificación de no creación de carpeta

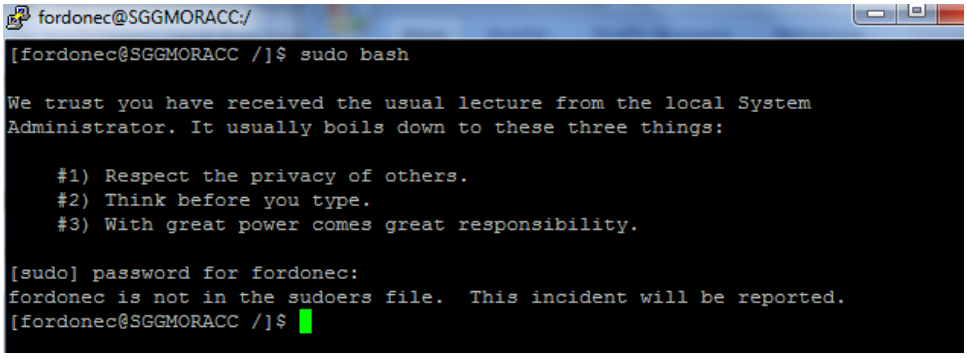


Figura 5.26 Verificación de no uso del privilegio sudo por usuario normal.

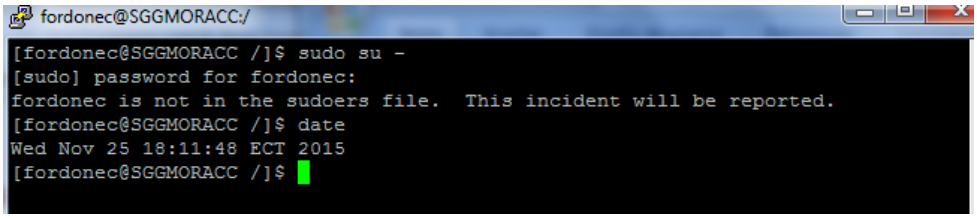


Figura 5.27 Verificación de no uso del privilegio su por usuario normal.

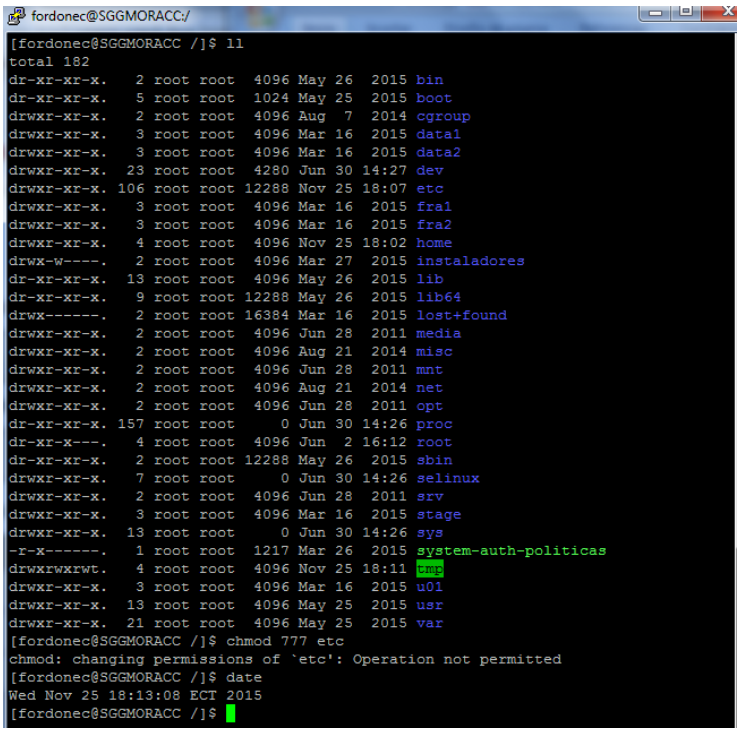


Figura 5.28 Verificación de no cambio de permisos a directorio.

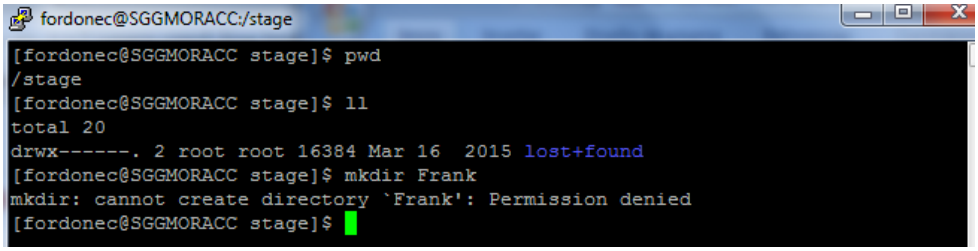


Figura 5.29 Verificación de no creación de carpeta dentro de filesytem.

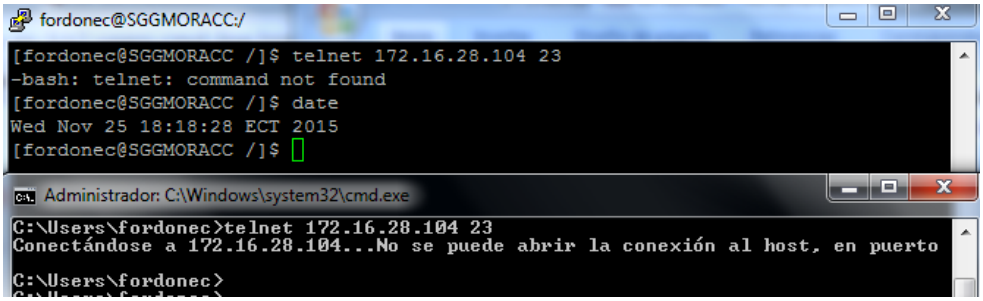


Figura 5.30 Verificación de no acceso mediante protocolos desactivados.

5.2. IMPLEMENTACIÓN DE ASEGURAMIENTO DE SISTEMA OPERATIVO WINDOWS SERVER.

El sistema operativo Windows server es muy diferente a Linux desde un punto de vista general, tiene un uso más amplio en infraestructuras tecnológicas, debido a su relativa facilidad de uso, a un mayor número de aplicaciones de negocio disponibles comparado con Linux. También incluye una interfaz gráfica más elaborada con un menú de opciones que incluye tareas totalmente automatizadas lo cual brinda ayuda al personal de TI con poca experiencia.

Debido a que el sistema operativo Windows tiene un mayor uso en el ámbito tecnológico y teniendo un historial de muchas vulnerabilidades que fueron explotadas, en los últimos años Microsoft ha corregido de forma temprana y recurrente la mayoría de ellas, inclusive de forma periódica libera parches de actualización las cuales contienen correcciones al core del sistema operativo, por ellos es de vital importancia realizar un adecuado aseguramiento informático el cual se complemente e incremente la seguridad y mantenga la fiabilidad del servidor.

Se realiza la implementación del aseguramiento informático al sistema operativo Windows server 2008 R2.

PERIFÉRICOS Y DISPOSITIVOS ADICIONALES.

El servidor no tiene conectado ningún periférico, unidad USB externa e impresora, solo tiene conexión al KVM del rack.

ARRANQUE DEL SISTEMA.

El servidor inicia desde el disco duro local, la unidad DVD fue desactivada por BIOS una vez instalado el sistema operativo.

CONTRASEÑA DE INICIO.

El servidor al iniciar no tiene configurada contraseña alguna, verificado mediante reinicio del servidor.

CONTRASEÑA DE CONFIGURACIÓN DE SERVIDOR.

Se habilita contraseña para acceder a la configuración (BIOS) del servidor, esta contraseña queda a resguardo del responsable de seguridad con su debida identificación en el inventario de contraseñas de equipos del centro de cómputo

FORMATO DE ARCHIVOS.

Las unidades de almacenamiento están en formato NTFS

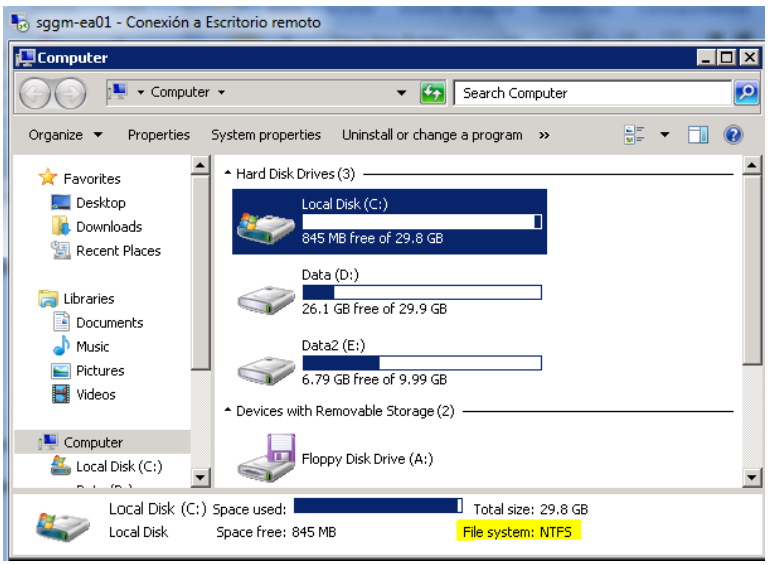


Figura 5.31 Verificación de formato en unidades de almacenamiento.

DOMINIOS.

Esta únicamente activo el dominio msexpress.com y el servidor esta agregado a este dominio.

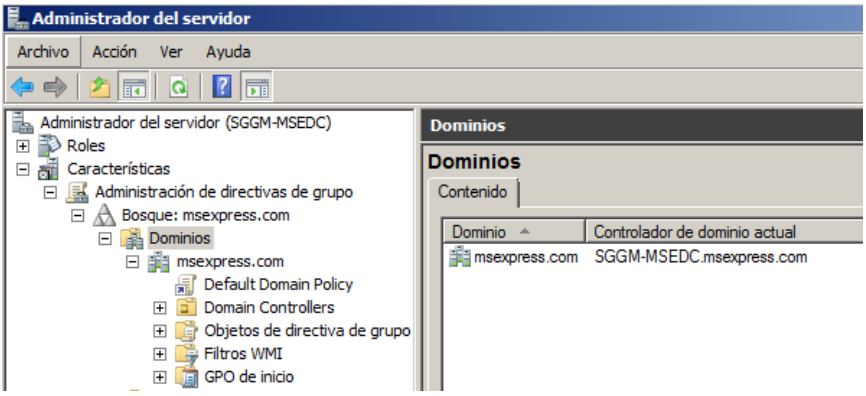


Figura 5.32 Verificación de dominio activo.

También se realizó una clasificación de los servidores acorde a la versión del sistema operativo junto una clasificación adecuada de los usuarios existentes.

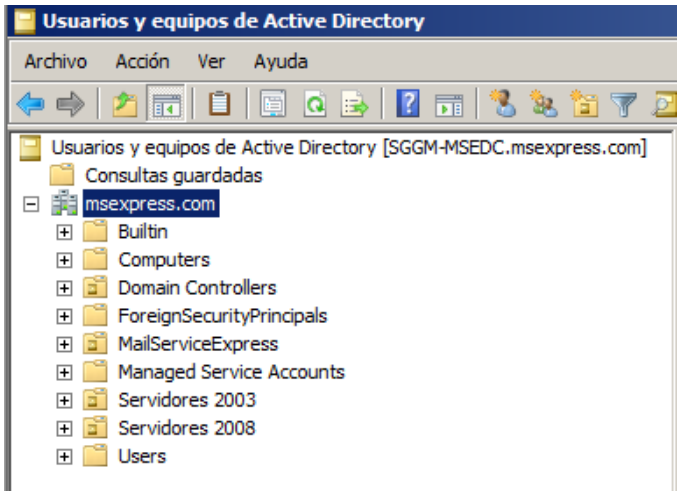


Figura 5.33 Clasificación de servidores por versión.

GESTIÓN DE USUARIOS Y GRUPOS.

Se establece un identificador único cada usuario de la red institucional,

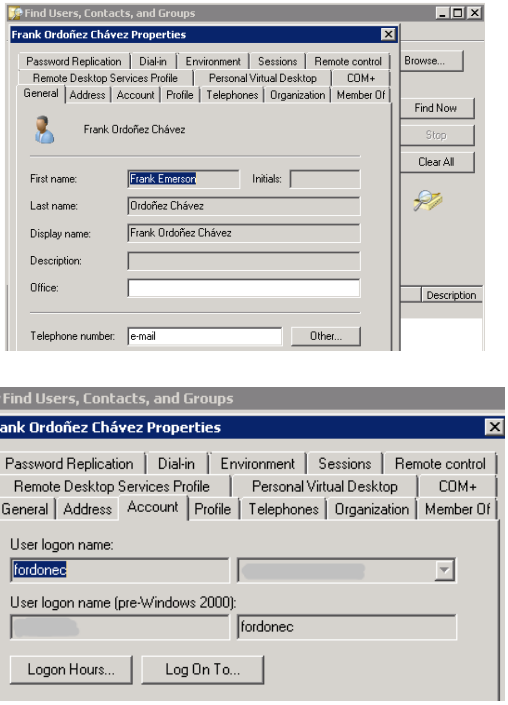


Figura 5.34 Identificación única por cada usuario.

La cuentas no expiran, caducan cada 90 días lo cual requiere cambio, el usuario también puede cambiar la calve cuando estime conveniente.

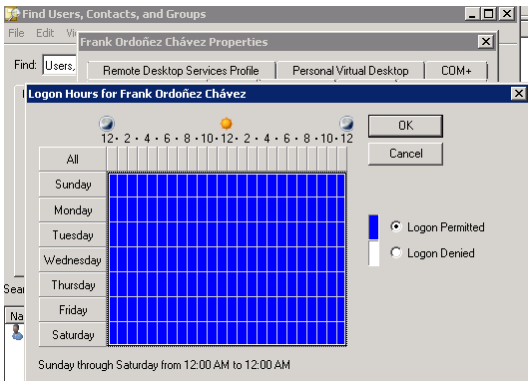


Figura 5.35 Se Configuración de horario por usuario.

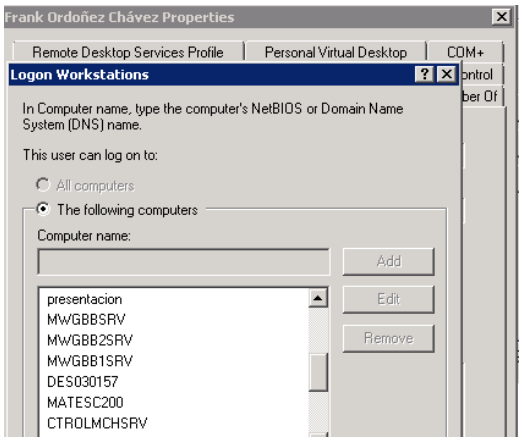


Figura 5.36 Logon especifico usuario.

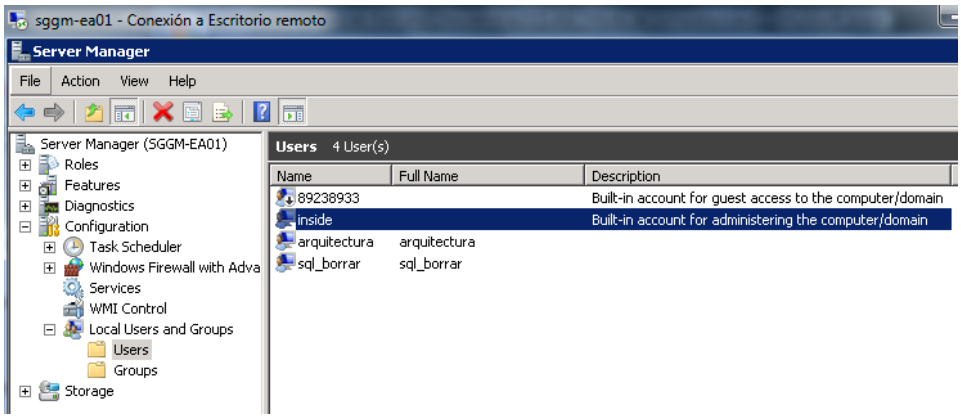


Figura 5.37 Renombre de cuentas administrador e invitado.

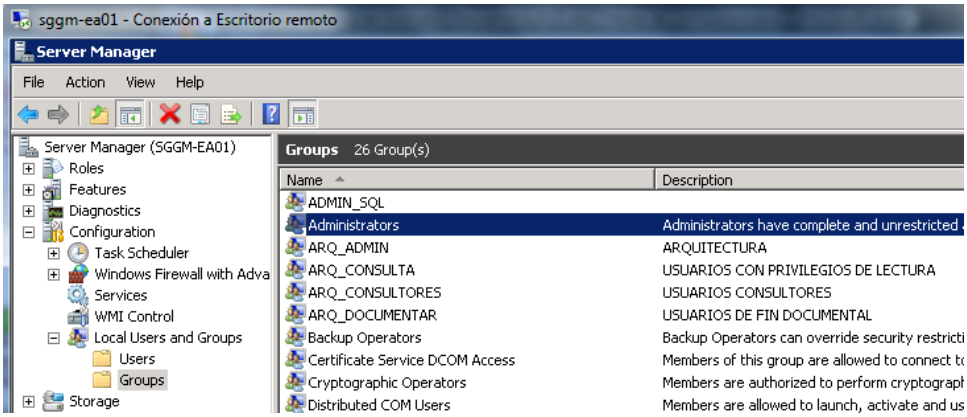


Figura 5.38 Clasificación de usuarios por grupos.

ALERTA DE INICIO.

Se establece la advertencia al inicio de sesión de los usuarios al ingresar al servidor.

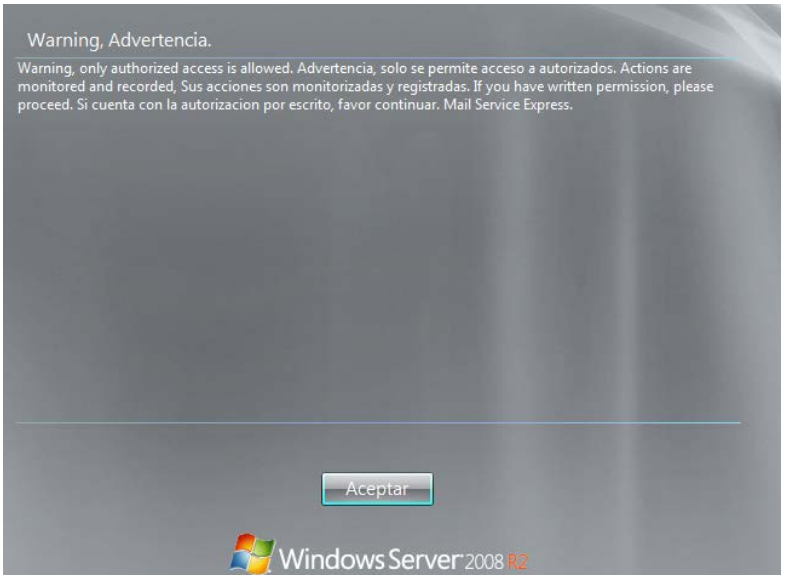


Figura 5.39 Alerta de sesión al ingresar al sistema operativo.

ADMINISTRACIÓN DE SERVICIOS.

Se establecieron la configuración de los estados del servicio acorde al esquema de aseguramiento informático.

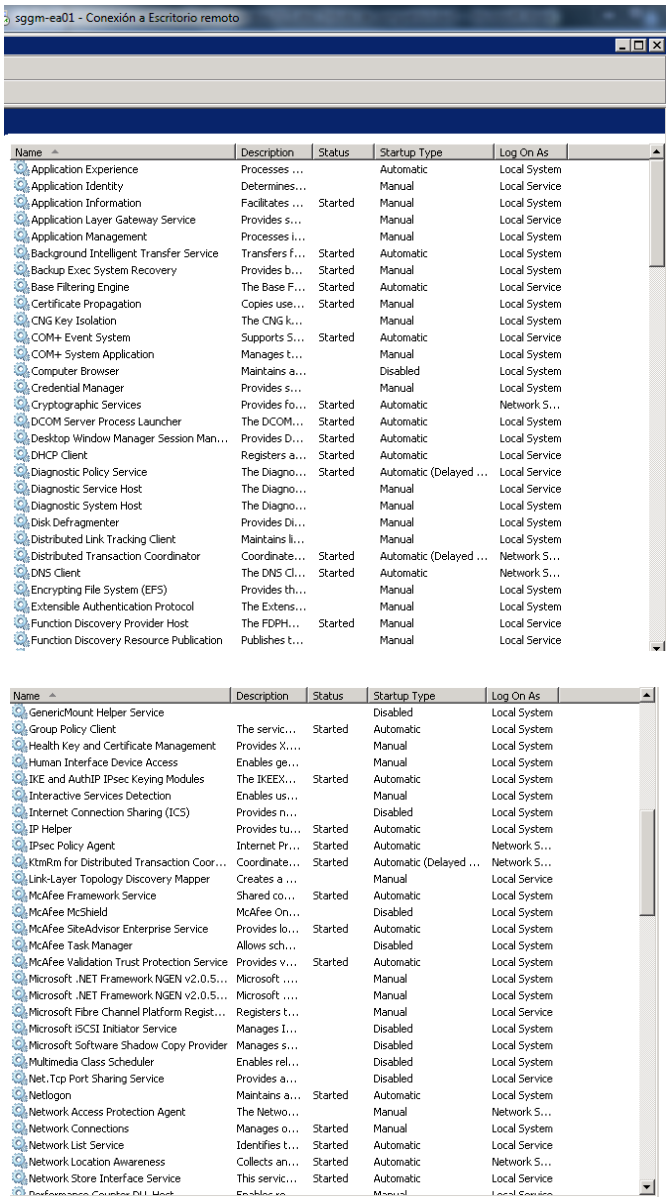


Figura 5.40 Configuración de servicios del sistema operativo.

PARAMETRIZACIÓN DE POLÍTICA DE CONTRASEÑAS.

Se realizó la configuración acorde a lo indicado en el esquema de aseguramiento informático.

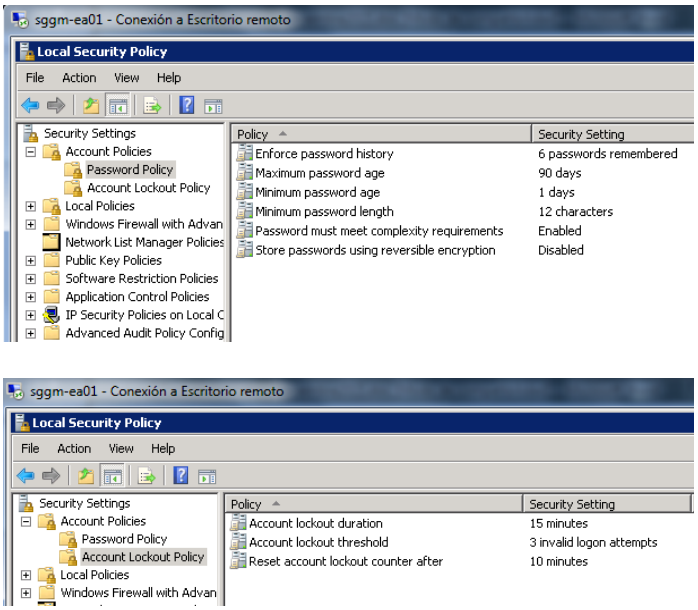


Figura 5.41 Configuración de política de contraseña.

AUDITORIA DE OBJETOS Y EVENTOS.

Se realizó la configuración acorde a lo indicado en el esquema de aseguramiento informático.

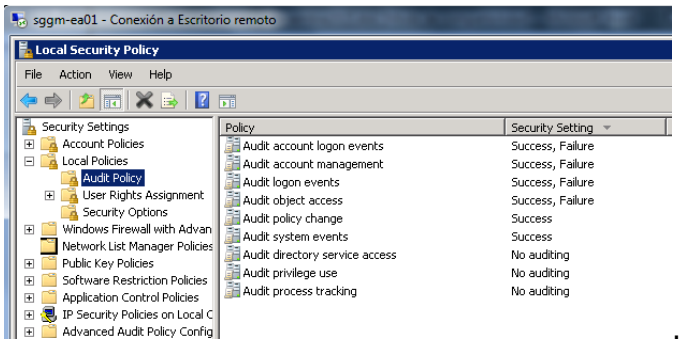


Figura 5.42 Configuración de auditoría al sistema operativo.

OPCIONES DE SEGURIDAD.

Se realizó la configuración acorde a lo indicado en el esquema de aseguramiento informático.

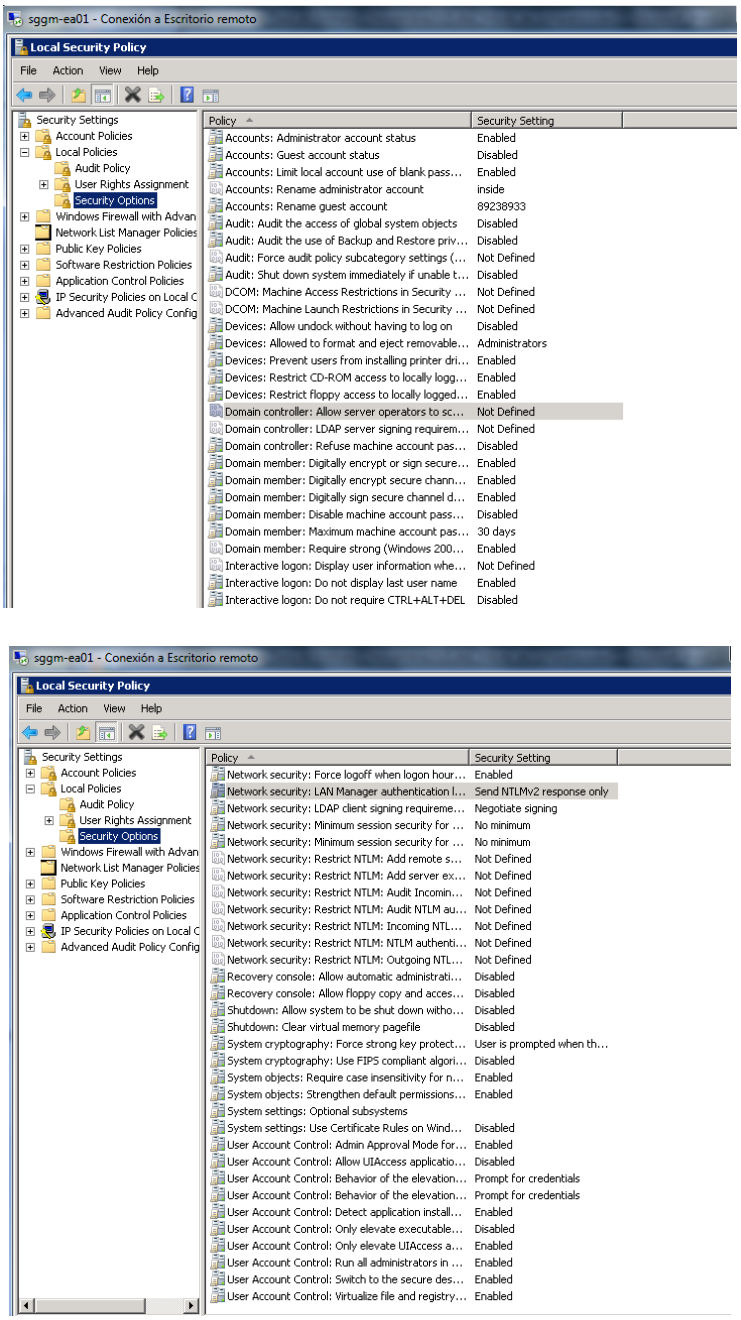


Figura 5.43 Configuración de las opciones de seguridad.

ARCHIVOS COMPARTIDOS, DIRECTORIO Y UNIDADES DE DISCO.

Ningún servidor tiene instalado impresora, esto como regla general. Así mismo no tienen sus discos compartidos. Para las carpetas compartidas se creó un servidor en el cual se generan y solo se da acceso únicamente al área o usuario autorizado.

PERMISOS EN DIRECTORIOS.

Estos permisos son importantes para delimitar la manipulación de archivos vitales para el sistema operativo, los cuales fueron configuración acorde a lo indicado en el esquema de aseguramiento informático.

Fueron aplicados en la unidad C:\, C:\Windows, C:\Program Files, C:\Windows\Security, C:\Windows\System32\config, C:\Windows\System32\bcdedit.exe, C:\Windows\System32\winload.exe, C:\Windows\System32\ntoskml.exe, C:\Windows\System32\spool

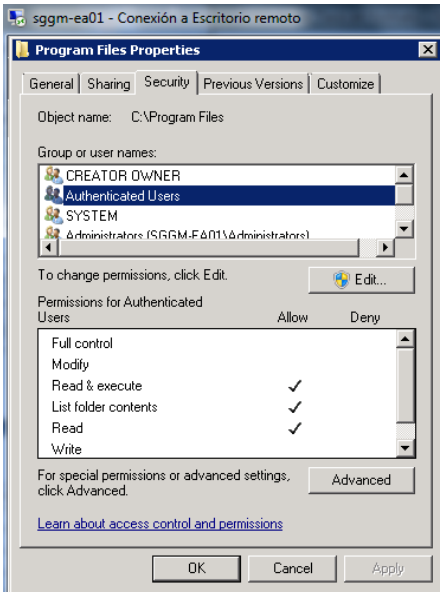


Figura 5.44 Configuración de permisos en directorios.

5.2.1. VERIFICACIÓN DE ASEGURAMIENTO INFORMÁTICO IMPLEMENTADO.

La verificación se realiza mediante una revisión específica para la confirmación de la correcta implementación del esquema de aseguramiento informático.

Se usa la plantilla descrita en las tablas en la cual mediante la confirmación manual se procede a determinar el cumplimiento de cada una de las premisas del esquema de aseguramiento.

Tabla 5. Plantilla de verificación de aseguramiento informático Windows.

DETALLE	ACCIÓN DE VERIFICACIÓN	Cumple	
		SI	NO
Parámetros generales			
Confirmar en el bios, el menú de administración cuente con contraseña.	El ingreso directo al menú es confirmación de que no está configurada la contraseña.	SI	
Verificar que el primer dispositivo de arranque sean los discos rígidos del servidor.	Revisar el orden de los dispositivos de arranque, siempre los discos locales deben ser primero	SI	
Verificar que no se encuentren habilitados los puertos USB.	Confirmar mediante la conexión de una unidad de almacenamiento USB externa	SI	
Verificar que todos los discos estén formateados en NTFS	Validar en propiedades de cada sistema de archivo.	SI	
Que los recursos compartidos y los usuarios que requieran el acceso a los mismos sean específicos y no generales.	Verificar en los recursos compartidos existentes.	SI	
Confirmar que se encuentren aplicados los parches de seguridad más recientes.	Verificar en historial de actualizaciones.	SI	
Usuarios y grupos			
Confirmar estén habilitadas únicamente las cuentas de usuario autorizadas.	Verificar las cuentas de usuario activas en administración de usuarios.	SI	
Confirmar que estén renombradas las cuentas de administrador e invitado.	Verificar estas cuentas de usuario en administración de usuarios.	SI	
Políticas de cuentas			
Políticas de contraseñas y cuentas de usuarios			
Verificar los parámetros indicados en el procedimiento de aseguramiento informático para la implementación de directiva de contraseñas.	Verificar los parámetros indicados en el procedimiento de aseguramiento, directiva de seguridad local, directiva de cuenta, directiva de contraseñas.	SI	
Verificar los parámetros indicados en el procedimiento de aseguramiento informático para la implementación de directiva de bloqueo de usuarios.	Verificar los parámetros indicados en el procedimiento de aseguramiento, directiva de seguridad local, directiva de cuenta, directiva de bloqueo de cuenta.	SI	
Permisos en directorios			

Verificar que estén correctamente implementados los permisos en directorios del sistema operativo como indica el esquema de aseguramiento informático.	Verificar cada uno de los directorios del sistema validando los permisos a usuarios y grupos.	SI	
Opciones de seguridad			
Verificar que estén correctamente implementadas las medidas de seguridad como indica el esquema de aseguramiento informático.	Verificar los parámetros indicados en el procedimiento de aseguramiento, directiva de seguridad local, directivas locales, opciones de seguridad.	SI	
Auditoría			
Verificar que este aplicado las directivas de auditoría.	Verificar los parámetros indicados en el procedimiento de aseguramiento, directiva de seguridad local, directiva locales, directiva de auditoría.	SI	
<verificar que el agente de syslogserver este iniciado	Confirmar que el syslogserver esté recibiendo los log del servidor		

5.2.2. PRUEBAS AL ASEGURAMIENTO IMPLEMENTADO.

Las pruebas efectuadas al servidor con el sistema operativo Windows server 2008 R2 son acciones manuales en la cual se intenta acceder a las cuentas de usuario que deben estar deshabilitadas, confirmar que no puede alterar directorios principales del sistema, verificar que los log de auditoría estén siendo enviados a la central de recolección de log configurada, que un usuarios normal no posea privilegios de administrador, que no esté habilitado el servicio de telnet o innecesarios.

Se adjunta capturas de estas acciones.

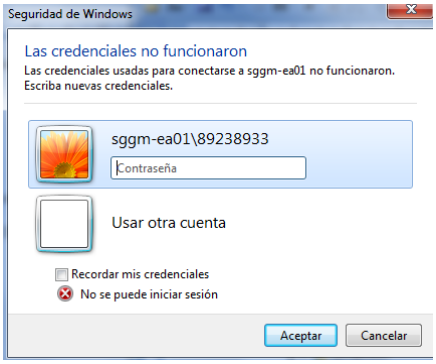


Figura 5.45 Prueba fallida con usuario invitado, la cual fue renombrada.

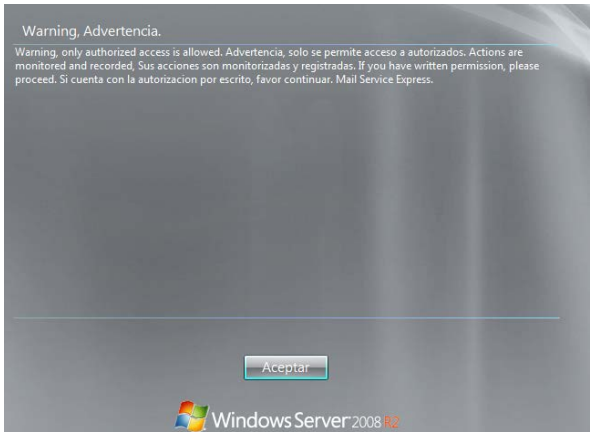


Figura 5.46. Prueba de acceso con cuenta de dominio, muestra de advertencia.

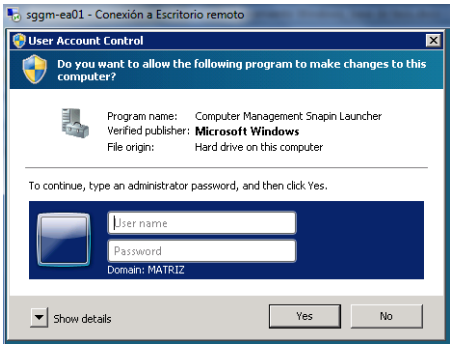


Figura 5.47. Solicitud de credenciales por acceder al administrador de equipo.

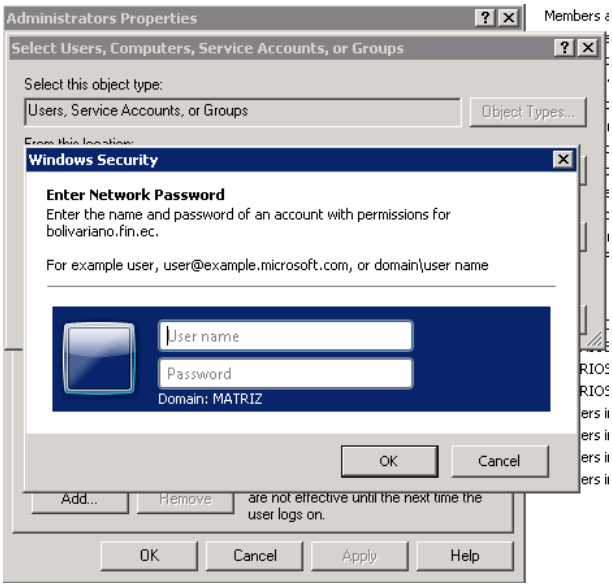


Figura 5.48 Solicitud de credenciales para modificar grupo de usuarios.

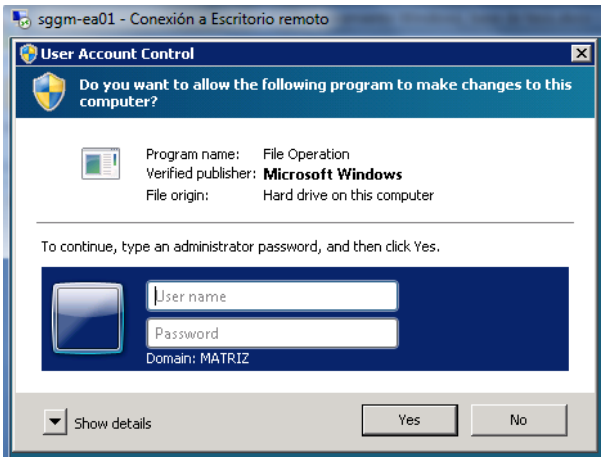


Figura 5.49 Solicitud de credenciales para modificar carpetas

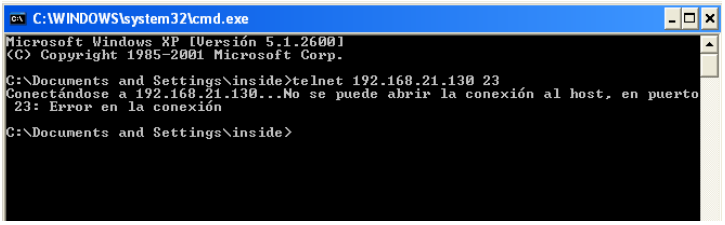


Figura 5.50 Prueba al servicio telnet, el cual esta desactivado.

5.3. IMPLEMENTACIÓN Y CONFIGURACIÓN BÁSICA DE UNA CENTRAL DE RECOLECCIÓN DE LOGS.

El esquema básico de implementación de una central de log es la que se describe en la figura, en la cual se visualiza, representativamente la interacción de los equipos de la LAN de empresa Mail Service Express.

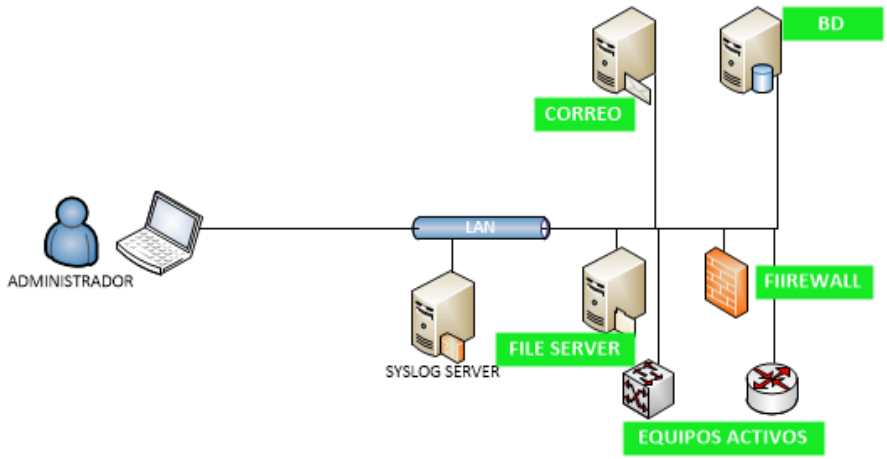


Figura 5.51 Central de recolección de log.

Se usó para este punto un equipo que inicialmente no estaba operativo, el cual siendo habilitado mediante reparación de sus dos fuentes se habilito para este fin. El equipo usado para función de logserver posee las siguientes características:

Marca: HP

Modelo: Proliant ML110

Tipo: Torre

Procesador: XEON, de 4 núcleos, 2.2GHz

Disco: 200GB

RAM: 8GB

Se instaló el sistema operativo Windows server 2008 estándar con su respectiva licencia. Se instala Datagram SyslogServer, se realiza la parametrización general y se configura el inicio automático del servicio en el sistema operativo.

En los servidores Windows que enviaran los log se instala el agente SyslogAgentConfig, se realiza la configuración de los parámetros generales del servicio y se confirma su correcto funcionamiento mediante la recepción de los log en el repositorio en el syslogserver.

5.3.1. VERIFICACIÓN DE ALMACENAMIENTO LOCAL DE LOG

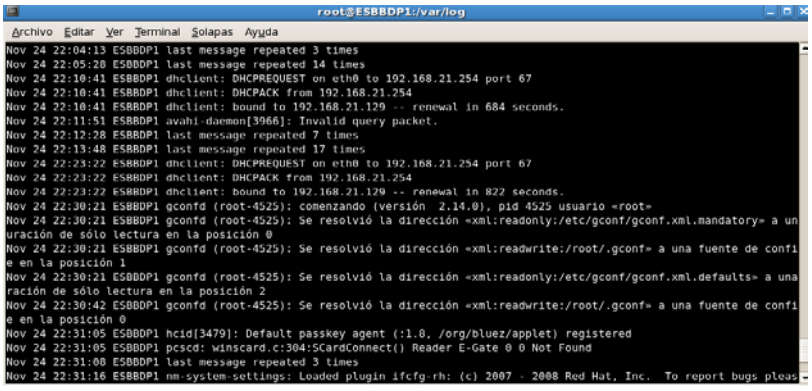


Figura 5.52. Verificación de almacenamiento activo de log en Linux.

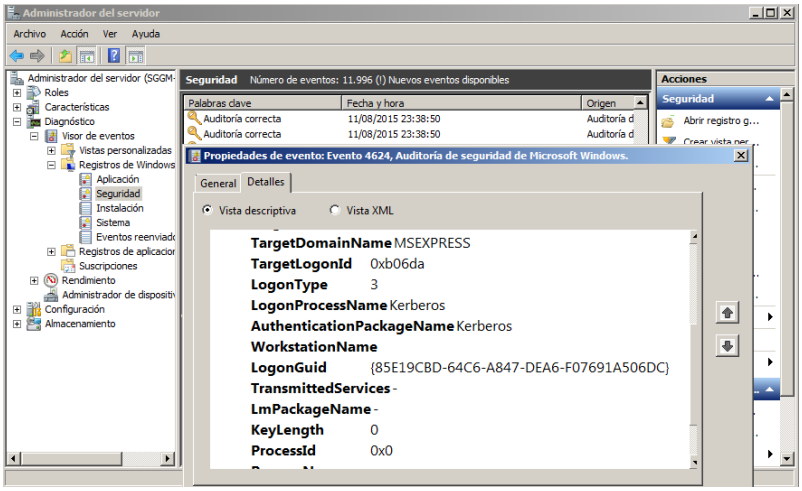


Figura 5.53 Verificación de registro activo de log en Windows, acorde a las directivas establecidas.

5.3.2. VERIFICACIÓN DE ALMACENAMIENTO REMOTO DE LOG

Los logs enviados por los sistemas operativos windows y linux esta siendo receptados y almacenados en el serverlog.

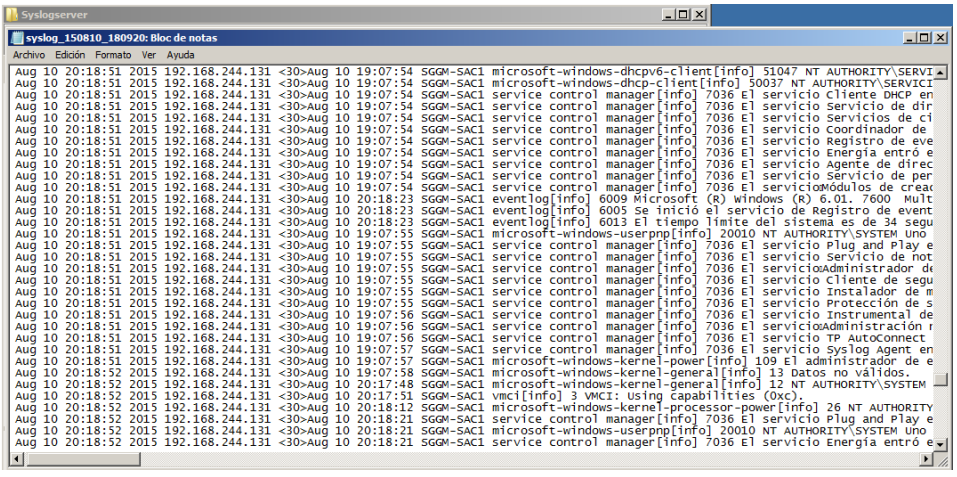
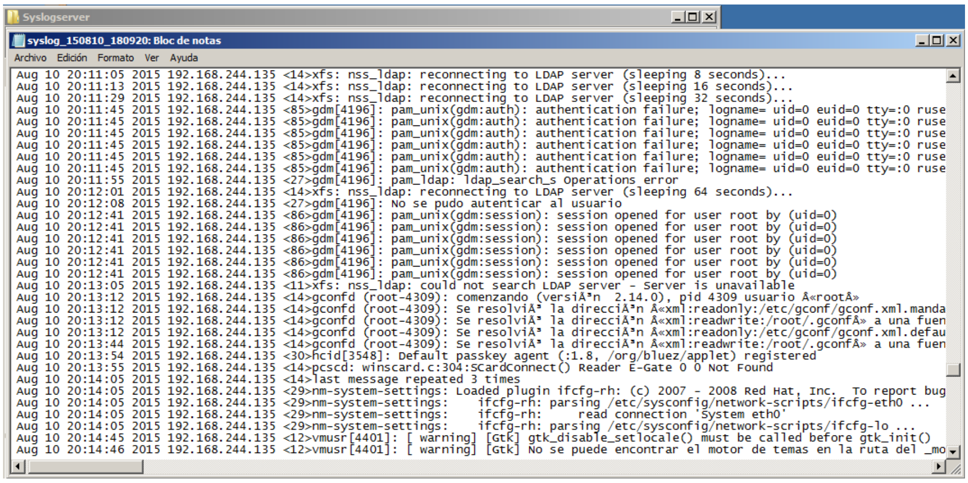


Figura 5.54 Verificación de almacenamiento de los log Windows.



Syslogserver

syslog_150810_180920: Bloc de notas

Archivo Edición Formato Ver Ayuda

```
Aug 10 20:11:05 2015 192.168.244.135 <14>xfs: nss_ldap: reconnecting to LDAP server (sleeping 8 seconds)...
Aug 10 20:11:13 2015 192.168.244.135 <14>xfs: nss_ldap: reconnecting to LDAP server (sleeping 16 seconds)...
Aug 10 20:11:29 2015 192.168.244.135 <14>xfs: nss_ldap: reconnecting to LDAP server (sleeping 32 seconds)...
Aug 10 20:11:45 2015 192.168.244.135 <85>gdm[4196]: pam_unix(gdm:auth): authentication failure; logname= uid=0 euid=0 tty=:0 ruse
Aug 10 20:11:45 2015 192.168.244.135 <85>gdm[4196]: pam_unix(gdm:auth): authentication failure; logname= uid=0 euid=0 tty=:0 ruse
Aug 10 20:11:45 2015 192.168.244.135 <85>gdm[4196]: pam_unix(gdm:auth): authentication failure; logname= uid=0 euid=0 tty=:0 ruse
Aug 10 20:11:45 2015 192.168.244.135 <85>gdm[4196]: pam_unix(gdm:auth): authentication failure; logname= uid=0 euid=0 tty=:0 ruse
Aug 10 20:11:45 2015 192.168.244.135 <85>gdm[4196]: pam_unix(gdm:auth): authentication failure; logname= uid=0 euid=0 tty=:0 ruse
Aug 10 20:11:45 2015 192.168.244.135 <85>gdm[4196]: pam_unix(gdm:auth): authentication failure; logname= uid=0 euid=0 tty=:0 ruse
Aug 10 20:11:55 2015 192.168.244.135 <27>gdm[4196]: pam_ldap: ldap_search_s Operations error
Aug 10 20:12:01 2015 192.168.244.135 <14>xfs: nss_ldap: reconnecting to LDAP server (sleeping 64 seconds)...
Aug 10 20:12:08 2015 192.168.244.135 <27>gdm[4196]: No se pudo autenticar al usuario
Aug 10 20:12:41 2015 192.168.244.135 <86>gdm[4196]: pam_unix(gdm:session): session opened for user root by (uid=0)
Aug 10 20:12:41 2015 192.168.244.135 <86>gdm[4196]: pam_unix(gdm:session): session opened for user root by (uid=0)
Aug 10 20:12:41 2015 192.168.244.135 <86>gdm[4196]: pam_unix(gdm:session): session opened for user root by (uid=0)
Aug 10 20:12:41 2015 192.168.244.135 <86>gdm[4196]: pam_unix(gdm:session): session opened for user root by (uid=0)
Aug 10 20:12:41 2015 192.168.244.135 <86>gdm[4196]: pam_unix(gdm:session): session opened for user root by (uid=0)
Aug 10 20:12:41 2015 192.168.244.135 <86>gdm[4196]: pam_unix(gdm:session): session opened for user root by (uid=0)
Aug 10 20:13:05 2015 192.168.244.135 <11>xfs: nss_ldap: could not search LDAP server - Server is unavailable
Aug 10 20:13:12 2015 192.168.244.135 <14>gconfd (root-4309): comenzando (versiÃ³n  2.14.0), pid 4309 usuario Â«rootÂ»
Aug 10 20:13:12 2015 192.168.244.135 <14>gconfd (root-4309): Se resolviÃ³ la direcciÃ³n Â«xml:readonly:/etc/gconf/gconf.xml.manda
Aug 10 20:13:12 2015 192.168.244.135 <14>gconfd (root-4309): Se resolviÃ³ la direcciÃ³n Â«xml:readwrite:/root/.gconfÂ» a una fuen
Aug 10 20:13:12 2015 192.168.244.135 <14>gconfd (root-4309): Se resolviÃ³ la direcciÃ³n Â«xml:readonly:/etc/gconf/gconf.xml.defau
Aug 10 20:13:44 2015 192.168.244.135 <14>gconfd (root-4309): Se resolviÃ³ la direcciÃ³n Â«xml:readwrite:/root/.gconfÂ» a una fuen
Aug 10 20:13:54 2015 192.168.244.135 <30>hcid[3548]: Default passkey agent (:1.8, /org/bluez/applet) registered
Aug 10 20:13:55 2015 192.168.244.135 <14>pcscd: winscard.c:304:SCardConnect() Reader E-Gate 0 0 Not Found
Aug 10 20:14:05 2015 192.168.244.135 <14>last message repeated 3 times
Aug 10 20:14:05 2015 192.168.244.135 <29>nm-system-settings: Loaded plugin ifcfg-rh: (c) 2007 - 2008 Red Hat, Inc.  To report bug
Aug 10 20:14:05 2015 192.168.244.135 <29>nm-system-settings:    ifcfg-rh: parsing /etc/sysconfig/network-scripts/ifcfg-eth0 ...
Aug 10 20:14:05 2015 192.168.244.135 <29>nm-system-settings:    ifcfg-rh:     read connection 'System eth0'
Aug 10 20:14:05 2015 192.168.244.135 <29>nm-system-settings:    ifcfg-rh: parsing /etc/sysconfig/network-scripts/ifcfg-lo ...
Aug 10 20:14:45 2015 192.168.244.135 <12>vmusr[4401]: [ warning] [Gtk] gtk_disable_setlocale() must be called before gtk_init()
Aug 10 20:14:46 2015 192.168.244.135 <12>vmusr[4401]: [ warning] [Gtk] No se puede encontrar el motor de temas en la ruta del _mo
```

Figura 5.55 Verificación de almacenamiento de log Linux.

Se confirma la recepción satisfactoria de los log de los sistemas operativos Windows y Linux, en los actuales se ha instalado los agentes y configurado el syslog.conf respectivamente.

5.4. ANÁLISIS DE RESULTADOS.

Los dos esquemas de aseguramiento informático fueron desarrollados e implementados en seis servidores de producción de la empresa, dos con el sistema operativo Windows server 2008 R2, más uno donde se efectuaban las pruebas de verificación del aseguramiento, el cual paso por varias novedades hasta obtener el esquema final, y los tres restantes sobre Linux Red 5.4.

Estos servidores estuvieron como pilotos para comprobar que las medidas de seguridad en ellos implementados son fiables y que previenen eficientemente el acceso no autorizado.

Luego de tres meses, el 20 de noviembre del 2015, la jefatura de infraestructura tecnológica afianza el esquema de aseguramiento informático para que se inicie la formalización de este procedimiento solicitando a Gerencia de TI, Auditoria, Administración y Control su aprobación para que el mismo forme parte de los requisitos en la preparación de servidores para el ambiente de producción, inclusive que sea aplicado para ambientes de pruebas o pre-producción.

Realizaremos una descripción de resultados obtenidos gracias a este esquema.

5.4.1. VERIFICACIÓN DE CORRECCIÓN DE VULNERABILIDADES GENERALES.

Teniendo en claro los tipos de vulnerabilidades o amenazas siendo estas de hardware, software, de configuración y fallas humanas, es importante la validación y comprobación de mejoras de seguridad luego de la aplicación del esquema de aseguramiento informático.

Iniciando con la corrección de la instalación por defecto, se corrige y se establece directivas para el tratamiento de cuentas de usuarios durante la instalación del sistema operativo, específicamente se renombra la cuenta administrador junto con la de invitado en Windows, esta última se desactiva cambiando su clave. En Linux se desactivan todas las cuentas innecesarias como bin, daemon, ftp,

games, gopher, mail, man, news, nobody, uucp, lp. El objetivo de estas acciones es complicar actividades de escaneos no autorizados e intentos de usos de estas credenciales para obtener accesos a la plataforma tecnológica.

Entre las amenazas de configuración, con el esquema de aseguramiento informático se establece una mejor administración de grupos y usuarios en los servidores de producción, se limita y reduce a uno al usuario con privilegio de administrador de dominio y root en Windows y Linux respectivamente, anteriormente a esto, todo el personal de sistemas que incluye a soporte, desarrollo, infraestructura y administradores de servicio, sus privilegios eran de administrador de dominio y root.

Se crean perfiles adecuados para cada persona, formalizando esto con una solicitud y aprobación mediante el uso de una plantilla digital en Word. Adicionalmente se ensobran las cuentas de máximos privilegios.

Al implementar permisos a los filesystem y directorios principales de los sistemas operativos, se ha reducido los incidentes, errores involuntarios y actividades dañinas como eliminación de archivos, alteración de información o configuraciones.

La activación de los registros de auditoría y almacenamiento remoto de los log ayuda significativamente en el análisis de eventos en los

sistemas operativos, lo cual serviría como soporte para actividades de seguimiento o auditorias ante modificaciones sin controles de cambio.

La implementación de nuevos parches de seguridad y versiones de paquetes a Windows y Linux de forma periódica, incrementa la fiabilidad de los mismos al contar con las últimas actualizaciones que buscan corregir vulnerabilidades detectadas que pudieren ser explotadas por personal externo mediante ataques dirigidos y controlados.

5.4.2. ESTADÍSTICA, REDUCCIÓN DE ACCESOS NO AUTORIZADOS.

Se presenta dos cuadros donde se visualiza estadísticamente el cambio positivo en cuanto al uso de las credenciales con privilegios para ingresar a los servidores de producción que tienen instalado los sistemas operativos.

SIN ESQUEMA DE ASEGURAMIENTO INFORMÁTICO, Abril 2015					
Área	Número de personas	Acceso con Administrador Windows	Acceso con root Linux	Credencial usada en Windows	Credencial usada en Linux
Soporte	7	7	7	Administrador	root
Desarrollo	16	14	16	Administrador	root
Infraestructura	2	2	2	Administrador	root
BD	2	2	2	Administrador	root
A&C	3	3	1	Administrador	root

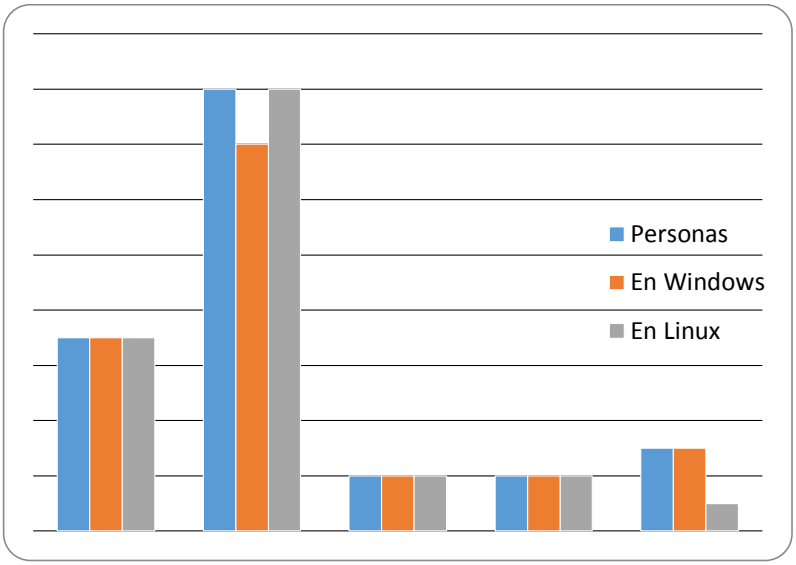


Figura 5.56. Acceso de máximo privilegios sin aseguramiento.

Las áreas de soporte, infraestructura y BD, la totalidad de sus integrantes hacen uso de las credenciales con máximos privilegios, así como el 88% del personal de desarrollo, lo cual requiere a prioridad una mejor gestión.

ASEGURAMIENTO INFORMÁTICO IMPLEMENTADO, Noviembre 2015					
Área	Número de personas	Acceso con Administrador Windows	Acceso con root Linux	Credencial usada en Windows	Credencial usada en Linux
Soporte	7	0	0	Cuenta personal	Cuenta personal
Desarrollo	16	0	0	Cuenta personal	Cuenta personal
Infraestructura	2	2	2	Cuenta admin creada para cada persona	Cuenta admin creada para cada persona
BD	2	0	0	Cuenta personal	Cuenta personal
A&C	3	0	0	Cuenta personal	Cuenta personal

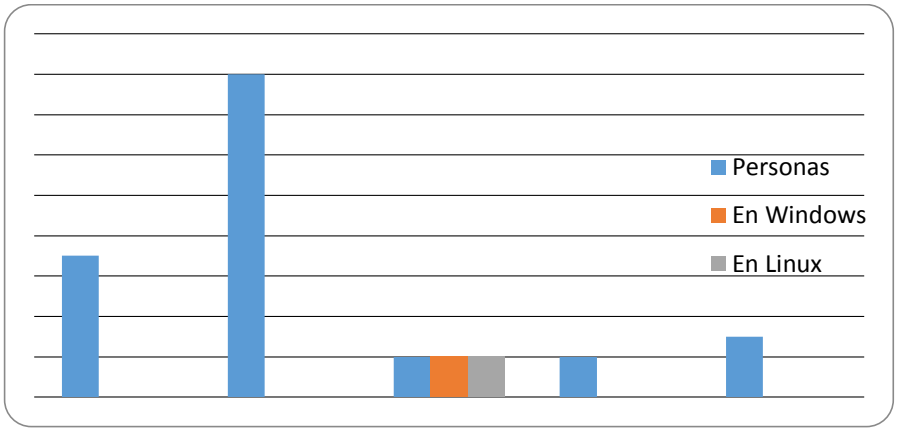


Figura 5.57. Acceso de máximo privilegios con aseguramiento.

Se visualiza y confirma una reducción drástica del acceso a los servidores haciendo uso de las credenciales administrativas con máximos privilegios. Fue necesario crear cuentas administrativas para el área de infraestructura.

PROPUESTA DE MEDIDA DE SEGURIDAD ADICIONAL.

Se recomienda la implementación de servidor seguro como complemento de seguridad, en el cual se concentrarían todas las conexiones a los servidores de producción.

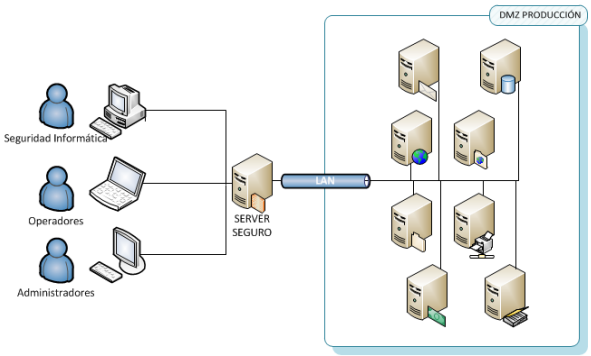


Figura 5.58 Server seguro de conexiones

Este esquema de conectividad evita la comunicación directa desde cualquier otro computador, como el de los administradores, operadores y usuarios finales, estos últimos pudieren ser personal interno o externo no autorizados.

El servidor seguro, a nivel de recurso deberá ser de buenas características para soportar varias conexiones simultaneas tener un nivel de aseguramiento superior al actual. También será necesaria la coordinación con el administrador de redes-firewall para solo tener habilitados los puertos TCP/IP y UDP necesarios bajo el siguiente esquema:

- Desde PC de administradores hacia el server seguro.
- Desde PC de operadores hacia el server seguro.
- Desde server seguro hacia servidores de producción.
- Desde estaciones de atención al cliente hacia servidores de producción, en el cual debe establecerse esquemas de re direccionamiento NAT.

CAPÍTULO 6

GESTIÓN DE CONTROL.

A los esquemas de aseguramiento para los sistemas operativos Windows server 2008 R2 y Linux Red Hat 5, la revisión anual de los mismos, su publicación y supervisión de implementación general está a cargo de la unidad de Administración y Control que también realiza seguimiento al departamento de sistemas, misma que entre todas sus funciones y actividades es la encargada de autorizar los pases a producción de nuevos servicios y aplicaciones.

Esta unidad, en cada nuevo proyecto o servicio a implementarse, luego de la gestión y administración de proyectos, solicitará la implementación de los esquemas de aseguramiento en los nuevos servidores salientes al

ambiente de producción y receptara los informes, evidencia y confirmaciones de su implantación.

Administración y Control designara un recurso el cual realizará una revisión a los servidores que se implementó el esquema de aseguramiento, junto con personal técnico del departamento de sistemas.

6.1. REPORTE DE ASEGURAMIENTO INFORMÁTICO IMPLEMENTADO.

El reporte del aseguramiento informático es la evidencia física o digital que se obtendrá luego de la revisión realizada a los servidores actuales o salientes en el ambiente de producción, en este documento se describirá todos y cada uno de los ítems del esquema de aseguramiento que han sido cubiertos e implementados, de existir excepciones estas se documentaran y se deberá adjuntar en el mismo las medidas de mitigación de posibles riesgos que pudieren presentarse con la respectiva aprobación de la gerencia de sistemas y del responsable o designado de seguridad informática.

El reporte de la implementación del esquema de aseguramiento informático puede ser físico o digital, este último mediante uso del correo electrónico institucional, el cual manejará el siguiente formato.

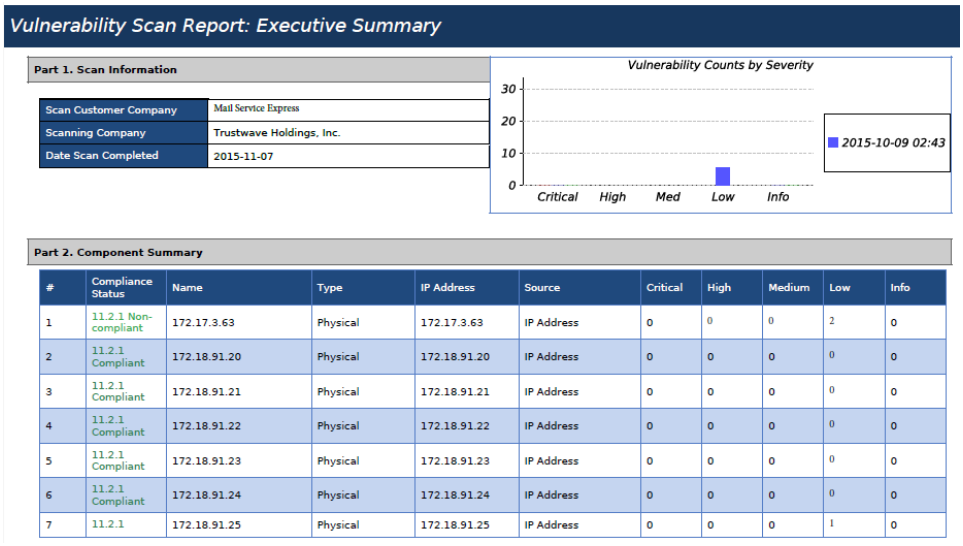
Tabla 6. Formato del reporte de aseguramiento informático.

Asunto: Fecha: Proyecto: Nombre de Servidor: Ip de servidor: Nombre de Gerente de Sistemas: Nombre de responsable de Seguridad Informática: Nombre de responsable de Administración y Control:	
Ítem	**Cumple (Si/ No), comentario.**
Seguridad de hardware	
Seguridad de inicio o arranque del sistema	
Contraseña de inicio	
Contraseña de configuración de servidor	
Acceso físico	
Gestión de usuarios	
Gestión de grupos	
Creación de grupo de administradores	
Alerta de bienvenida	
Configuración de variables	
Configuraciones de seguridad	
Configuración de contraseñas	
Actualizaciones criticas	
Configuración de servicios	
Configuración de auditoria	
Permisos de directorios	
Observaciones y Comentarios.	
Autoriza	**Autoriza**
Responsable de seguridad: Nombre	Responsable de sistemas: Nombre

6.2. AUDITORIAS AL ASEGURAMIENTO.

Una vez implementado el esquema de aseguramiento informático al sistema operativo, se realizó una auditoria al mismo para confirmar el tratamiento de las novedades y vulnerabilidades detectadas en el escaneo realizado inicialmente.

Se adjunta captura con el resultado del escaneo ejecutado un mes después del análisis inicial, donde se puede visualizar una drástica reducción de las observaciones debido a la efectiva implementación del aseguramiento.



Vulnerability Scan Report: Executive Summary

Part 1. Scan Information

Scan Customer Company	Mail Service Express
Scanning Company	Trustwave Holdings, Inc.
Date Scan Completed	2015-11-07

Part 2. Component Summary

#	Compliance Status	Name	Type	IP Address	Source	Critical	High	Medium	Low	Info
1	11.2.1 Non-compliant	172.17.3.63	Physical	172.17.3.63	IP Address	0	0	0	2	0
2	11.2.1 Compliant	172.18.91.20	Physical	172.18.91.20	IP Address	0	0	0	0	0
3	11.2.1 Compliant	172.18.91.21	Physical	172.18.91.21	IP Address	0	0	0	0	0
4	11.2.1 Compliant	172.18.91.22	Physical	172.18.91.22	IP Address	0	0	0	0	0
5	11.2.1 Compliant	172.18.91.23	Physical	172.18.91.23	IP Address	0	0	0	0	0
6	11.2.1 Compliant	172.18.91.24	Physical	172.18.91.24	IP Address	0	0	0	0	0
7	11.2.1	172.18.91.25	Physical	172.18.91.25	IP Address	0	0	0	1	0

Figura 5.59 Resultado del segundo análisis de vulnerabilidad.

Es recomendable realizar un escaneo cada 6 meses a cada uno de los servidores asegurados, con el objetivo de verificar no existan

nuevos riesgos de seguridad o de que se hayan realizado modificaciones o no autorizadas al aseguramiento realizado.

Es importante también indicar que todas las auditorias junto con los escaneos deberán coordinarse entre las áreas de sistemas, operaciones y todas aquellas que interactúan con el servicio o aplicación alojado en los servidores a revisarse, para evitar afectaciones mayores en cuanto a la disponibilidad de los servicios tecnológicos frente al usuario final.

6.3. MEDIDAS CONTINGENTES

Llamamos medidas contingentes a demás acciones que deben implementarse antes, durante y después de la aplicación del esquema de aseguramiento informático en servidores de producción, las cuales pueden ayudar a incrementar o mantener la seguridad de los esquemas se aseguramientos descritos aquí.

Se debe tener presente que ningún sistema informático es totalmente seguro, las mejores prácticas, estándares, políticas, esquemas y procedimientos que pudieren aplicarse solo buscan minimizar riesgos y probabilidades de que personas puedan aprovechar una o varias formas de acceder a equipos de una red para realizar acciones no autorizadas que perjudiquen o afecten la

disponibilidad, integridad y confidencialidad de nuestras aplicaciones, servicios e información.

ANTES.

Luego del análisis realizado sobre las funcionalidades aplicativas que tendrá el o los servidores existentes o salientes al ambiente de producción, es necesario validar e implementar las reglas de comunicación estrictamente necesarias, limitando los accesos a los puertos, recursos compartidos, servicios e ingreso remoto, limitando inclusive la comunicación directa desde otros servidores o estaciones de trabajo que no necesitarían interactuar con los equipos asegurados, DMZ.

Para ello es necesario contar con firewall, sean estos hardware, software o combinación de estos (Appliance) en los cuales estarán activas únicamente las reglas de firewall autorizadas clasificándolas entre temporales y permanentes, buscando controlar el acceso a equipos críticos o que contengan información sensible. Todo ello deberá tener un control e inventario para un seguimiento ante eventualidades que pudieren presentarse.

DURANTE.

Debe existir una coordinación adecuada entre las áreas, departamentos empresas, proveedores e inclusive clientes

(Stakeholder), dando a conocer que por temas de mejoras o trabajos en nuestra plataforma tecnológica uno o varios servicios/aplicaciones no estarán disponible en determinado momento de tiempo siempre especificando su inicio y final de actividades, esto debido que la implementación de un esquema de aseguramiento requiere reinicio de servicios, aplicaciones hasta inclusive servidor o hardware.

Debemos tener en cuenta también que muchas instituciones hacen uso de ventanas de tiempo llamadas “horario de mantenimiento”, en donde puede realizarse estas actividades con un mínimo de afectación a usuarios finales.

DESPUÉS.

La implementación de IPS (sistemas de prevención de intrusos) o IDS (sistemas de detección de intrusos) es también importante, la cual se sugiere para un monitoreo eficaz que nos ayudará a tomar decisiones acertadas respecto a ingresos no autorizados o de usuarios de nuestra red pero que presenta un comportamiento diferente del normal (perfil), para este último pudiere ser que se vio comprometido el user/clave o estaríamos ante una suplantación de identidad.

Igual de importante es llevar una bitácora de ingresos (siendo preventivos) a los equipos críticos, ver la posibilidad y factibilidad

económica de implementar reportes, alertas y estadistas (por monitoreo) de las acciones y actividades realizadas en nuestra plataforma.

6.4. MEJORAS CONTINUAS AL ASEGURAMIENTO INFORMÁTICO.

Invertir en conocimientos produce siempre los mejores beneficios. [5]

Benjamín Franklin (1706-1790)

La expresión de Benjamín Franklin es atemporal y totalmente aplicable a la rama informática, teniendo en cuenta que siempre deberá considerarse de forma prioritaria la actualización de los conocimientos plasmados en los dos esquemas de aseguramientos presentados, esto debido a nuevos descubrimientos que se dan a diario respecto a vulnerabilidades y fallas existentes tanto en hardware y software.

La actualización de procedimientos y esquemas de aseguramientos acompañado con una correcta gestión de seguridad mantendrá e inclusive fortalecerá la misma elevando su fiabilidad.

Es necesario revisar y actualizar estos esquemas bajo las siguientes premisas.

EN CADA NUEVA VERSIÓN DEL SISTEMA OPERATIVO.

Sabiendo que una nueva versión de sistema operativo trae nuevas funcionalidades, en muchas de las ocasiones contiene también errores de programación y falencias de seguridad, por estas razones es importante aplicar este esquema de aseguramiento a las nuevas versiones de los sistemas operativos, identificando que funciones y servicios quedan sin tratar para seguido revisar las misma, determinando la mejor medida preventiva aplicable comprobando está en un ambiente de pruebas y así certificar su funcionalidad para agregarlo en el revisado esquema de aseguramiento.

UNA VEZ CADA DOCE MESES.

Una vez al año se deberá evaluar y actualizar los esquemas de aseguramiento a los sistemas operativos, con el objetivo de afinar los mismos con las correcciones y medidas de tratamiento a las nuevas vulnerabilidades detectadas, corregidas y publicadas.

Los fabricantes como Microsoft y Red Hat realizan anualmente publicaciones de actualizaciones críticas para sus respectivos sistemas operativos, por lo cual los responsables, líderes y administradores de la plataforma tecnológica como de seguridades tienen que revisar los mismos, evaluarlos, comprobarlos y proponer cuales de todos ellos deberán incluirse en los esquemas de aseguramientos.

CONCLUSIONES Y RECOMENDACIONES.

La institución Mail Service Express al implementar los esquemas de aseguramiento informático incrementó las seguridades en los sistemas operativos Windows server y Linux Red Hat, reduciendo los accesos no autorizados y minimizando posibles amenazas que pudieren efectivizarse debido a un manejo inadecuado, involuntario o con fines nocivos de los servicios y aplicaciones de la plataforma tecnológica.

CONCLUSIONES.

1. Se mejoró la gestión de usuarios lo cual ha brindado una correcta asignación de permisos necesario a cada credencial de acceso acorde a su función o rol.

2. Desactivación de servicios innecesarios en los sistemas operativos, lo cual repercute positivamente en mejor rendimiento de los recursos del servidor.

3. Se maneja adecuadamente los permisos generales tanto en directorios y filesystem de los sistemas operativos Windows y Linux respectivamente.
4. Se cuenta con registros de auditoría locales y remotos para seguimiento de incidentes o problemas.

RECOMENDACIONES.

1. Los esquemas de aseguramiento informático deben ser revisados y renovados de forma periódica manteniéndolos actualizados en cada nueva versión de los sistemas operativos.

2. Realizar como mínimo dos escaneos anuales a los servidores de producción en horario de mantenimiento o en su defecto en una ventana de tiempo programada con su respectiva notificación a los interesados, con el objetivo de detectar nuevas vulnerabilidades.

3. La contratación y realización de un Ethical Hacking a la plataforma tecnológica de Mail Service Express mediante una empresa especializada permitirá obtener información detallada de posibles vulnerabilidades actuales o nuevas que no puedan ser cubiertas con el esquema de aseguramiento informático realizado.

BIBLIOGRAFÍA.

[1] Centro de prensa ESET, Incidentes de seguridad más relevantes, http://www.eset-la.com/centro-prensa/articulo/2015/eset-presenta-incidentes-seguridad-mas-relevantes-del-2014/3611 , fecha de consulta 2015.

[2] Balcázar Priscila, Magazcitum 1, Scitum Magazcitum, fecha de publicación Septiembre 2010, Pág. 26.

[3] Equipo de Investigación Eset Latinoamérica, Tendencias 2014 el desafío de la privacidad, fecha de consulta Abril 2015, Pág. 22.

[4] Morris P, Historia de la seguridad informática, http://www.latinoseguridad.com/LatinoSeguridad/HCyP/Morris.shtml , fecha de consulta Febrero 2015,

[5] Benjamín Franklin, Colección libre de citas y frases célebres, https://es.wikiquote.org/wiki/Benjamin_Franklin fecha de consulta Junio 2015.

[6] Red Hat, Base de conocimiento y soluciones generales Red Hat, https://access.redhat.com/solutions/759463?tour=6 fecha de consulta Febrero 2015.

[7] Microsoft., Base de conocimiento y soporte corporativo Windows server https://technet.microsoft.com/en-us/library/dn135243(v=ws.10).aspx, fecha de consulta Mayo 2015.

GLOSARIO.

Amenaza.

Es todo suceso, evento o persona que tiene la facultad de causar perjuicio a un sistema informático en forma de hurto, daño, divulgación, alteración de datos o negación de servicio (DoS).

Sistema de detección de intrusos.

Servicio que monitorea y analiza los eventos del sistema mediante hardware, software o la combinación de ambos para encontrar ataques o intentos de intrusión y proporcionar en tiempo casi real advertencias de intentos de acceso no autorizados a una red institucional.

Sistema de prevención de intrusos.

Es un dispositivo especializado de la combinación de hardware y software que inspecciona las actividades de la red lan o wan en busca de comportamientos anormales o maliciosos y así poder tomar acciones preventivas frente a estos.

Vulnerabilidad

Es una debilidad del sistema informático que puede ser aprovechada por terceros para actividades ilícitas o no autorizadas que afectan a la confidencialidad, integridad y disponibilidad de los sistemas. Una vulnerabilidad puede permitir ejecutar comandos de forma remota, acceso a información sensible, suplantación de identidad o denegación de servicio.

Agente.

Programa de computación que actúa para una aplicación u otro programa realizando un conjunto de operaciones con fines de monitorización y análisis de bajo nivel que sirven como fuente de información para otros programas o dispositivos. También los agentes se los conoce como sensores.

Análisis de vulnerabilidades.

Es la identificación de amenazas y determinación de niveles de riesgo internos o externos existentes sin tratar en una plataforma tecnológica, identifica la probabilidad de ocurrencia de o las amenazas estimando en lo posible los efectos que se tendrían en los recursos de la institución si estos se efectivizaren.

El análisis de vulnerabilidad también busca exponer los riesgos para que los mismos sean atendidos y corregidos.

Auditoría:

Es el proceso que consiste en inspeccionar, recoger, agrupar, evaluar evidencias y eventos del sistema para determinar su significado y saber si un sistema de información mantiene la integridad de los datos.

Autenticación.

Proceso de validar e inclusive revalidar la identificación de una entidad de sistema.

Cifrado.

Proceso mediante el cual información legible se transforma mediante la aplicación de una función matemática o algoritmo para obtener un mensaje codificado, ilegible o cifrado.

Control de acceso.

Consiste en la verificación de si una entidad sea esta persona, ordenador, aplicación o servicio, que solicitan acceso a un recurso tiene los derechos suficientes para hacerlo, limitándolo mediante definiciones estructuradas de identificación.

Analizador de vulnerabilidades:

Instrumento de hardware o software creado para llevar a cabo análisis de vulnerabilidades.

Advertencia.

Mensaje que indica a un usuario o grupo de estos que una acción que se está llevando a cabo puede ocasionar alteración, interrupción o perdida de datos del sistema.

Contraseña.

Código secreto que se ingresa en un equipo de procesamiento de información el cual siendo válido acciona nuevas funciones informática hasta ese momento inaccesible.

Incidente.

Generalmente un incidente es el intento de acceso, acceso, uso, divulgación, modificación, alteración, pérdida o destrucción no autorizada u no intencionada de datos e información; también los incidentes pueden ser por un impedimento en la operación normal de servicios, redes de comunicación y recursos informáticos.

Seguridad Informática.

Es la disciplina que vela por mantener el cumplimiento de los principios de Integridad, Disponibilidad y Confidencialidad de la información.

Ataque.

Cualquier método o acción deliberada de un individuo o grupo estos mediante el uso de sistemas informáticos con el objetivo de violar los mecanismos de seguridad para intentar tomar el control, desestabilizar o inutilizar un sistema de información, sea este privado o público.

Degradación.

Pérdida total o paulatina del valor de un activo como resultado de la materialización de una amenaza.

Frecuencia.

Tasa de ocurrencia de una amenaza.

ANEXOS.

ANEXOS

ANEXO 1

ASEGURAMIENTO LINUX, BASE DE TESIS

ANEXO 2

ASEGURAMIENTO WINDOWS, BASE DE TESIS

LOG WINDOWS

Mon Aug 10 18:09:20 2015 192.168.244.130 <30>Aug 10 18:09:20 SGGM-ADMSE SyslogServer Starting service Version 2.3.2 Licensed to:Invalid license! Using Trial version settings.

Mon Aug 10 18:09:38 2015 192.168.244.128 <30>Aug 10 18:09:31 zeuz service control manager[info] 7035 MSEXPRESS\inside Se ha enviado satisfactoriamente un control detener al□servicio Syslog Agent.

Mon Aug 10 18:09:38 2015 192.168.244.128 <30>Aug 10 18:09:33 zeuz service control manager[info] 7036 El servicio Syslog Agent entró en estado detenido.

Mon Aug 10 18:09:40 2015 192.168.244.128 <30>Aug 10 18:09:36 zeuz service control manager[info] 7035 MSEXPRESS\inside Se ha enviado satisfactoriamente un control iniciar al□servicio Syslog Agent.

Mon Aug 10 18:09:40 2015 192.168.244.128 <30>Aug 10 18:09:36 zeuz service control manager[info] 7036 El servicio Syslog Agent entró en estado Activo.

Mon Aug 10 18:13:14 2015 192.168.244.128 <30>Aug 10 18:13:05 zeuz thinprint autoconnect[info] 4002 MSEXPRESS\inside Error al importar desde el archivo.

Mon Aug 10 18:13:45 2015 192.168.244.128 <28>Aug 10 18:13:42 zeuz print[warning] 4 NT AUTHORITY\SYSTEM La impresora Adobe PDF#:8 está pendiente de eliminación.

Mon Aug 10 18:13:45 2015 192.168.244.128 <28>Aug 10 18:13:42 zeuz print[warning] 3 NT AUTHORITY\SYSTEM Se ha eliminado la impresora Adobe PDF#:8.

Mon Aug 10 18:13:45 2015 192.168.244.128 <28>Aug 10 18:13:42 zeuz print[warning] 4 NT AUTHORITY\SYSTEM La impresora Print to Evernote#:4 está pendiente de□eliminación.

Mon Aug 10 19:08:01 2015 192.168.244.128 <28>Aug 10 19:07:59 zeuz print[warning] 3 NT AUTHORITY\SYSTEM Se ha eliminado la impresora Enviar a OneNote 2013#:3.

Mon Aug 10 19:08:01 2015 192.168.244.128 <28>Aug 10 19:07:59 zeuz print[warning] 4 NT AUTHORITY\SYSTEM La impresora EPSON L355 Series#:7 está pendiente de□eliminación.

Mon Aug 10 19:08:01 2015 192.168.244.128 <28>Aug 10 19:07:59 zeuz print[warning] 3 NT AUTHORITY\SYSTEM Se ha eliminado la impresora EPSON L355 Series#:7.

LOG LINUX

Mon Aug 10 20:06:03 2015 192.168.244.135 <14>hpiod: 1.6.7 accepting connections at 2208...

Mon Aug 10 20:06:05 2015 192.168.244.135 <86>sshd[3730]: Server listening on :: port 22.

Mon Aug 10 20:06:05 2015 192.168.244.135 <86>sshd[3730]: Server listening on :: port 22.

Mon Aug 10 20:06:05 2015 192.168.244.135 <86>sshd[3730]: Server listening on :: port 22.

Mon Aug 10 20:06:05 2015 192.168.244.135 <86>sshd[3730]: Server listening on :: port 22.

Mon Aug 10 20:06:05 2015 192.168.244.135 <86>sshd[3730]: Server listening on :: port 22.

Mon Aug 10 20:06:05 2015 192.168.244.135 <86>sshd[3730]: Server listening on :: port 22.

Mon Aug 10 20:06:05 2015 192.168.244.135 <83>sshd[3730]: error: Bind to port 22 on 0.0.0.0 failed: Address already in use.

Mon Aug 10 20:06:05 2015 192.168.244.135 <83>sshd[3730]: error: Bind to port 22 on 0.0.0.0 failed: Address already in use.

Mon Aug 10 20:06:05 2015 192.168.244.135 <83>sshd[3730]: error: Bind to port 22 on 0.0.0.0 failed: Address already in use.

Mon Aug 10 20:06:05 2015 192.168.244.135 <83>sshd[3730]: error: Bind to port 22 on 0.0.0.0 failed: Address already in use.

Mon Aug 10 20:06:05 2015 192.168.244.135 <83>sshd[3730]: error: Bind to port 22 on 0.0.0.0 failed: Address already in use.

Mon Aug 10 20:06:05 2015 192.168.244.135 <83>sshd[3730]: error: Bind to port 22 on 0.0.0.0 failed: Address already in use.

Mon Aug 10 20:06:58 2015 127.0.0.1 <191>Kiwi Syslog Server - Test message number 0001

Mon Aug 10 20:07:14 2015 127.0.0.1 <191>Kiwi Syslog Server - Test message number 0002

Mon Aug 10 20:07:47 2015 192.168.244.135 <29>xinetd[3753]: xinetd Version 2.3.14 started with libwrap loadavg labeled-networking options compiled in.

Mon Aug 10 20:07:47 2015 192.168.244.135 <29>xinetd[3753]: Started working: 0 available services

Mon Aug 10 20:07:48 2015 192.168.244.135 <9>python: [3847] error: Unable to set locale.

Mon Aug 10 20:07:49 2015 192.168.244.135 <6>kernel: ppdev: user-space parallel port driver

Mon Aug 10 20:07:50 2015 192.168.244.135 <14>dbus-daemon: nss_ldap: reconnecting to LDAP server (sleeping 4 seconds)...

Mon Aug 10 20:07:54 2015 192.168.244.135 <14>dbus-daemon: nss_ldap: reconnecting to LDAP server (sleeping 8 seconds)...

Mon Aug 10 20:08:02 2015 192.168.244.135 <14>dbus-daemon: nss_ldap: reconnecting to LDAP server (sleeping 16 seconds)...

Mon Aug 10 20:08:18 2015 192.168.244.135 <14>dbus-daemon: nss_ldap: reconnecting to LDAP server (sleeping 32 seconds)...

Mon Aug 10 20:08:50 2015 192.168.244.135 <14>dbus-daemon: nss_ldap: reconnecting to LDAP server (sleeping 64 seconds)...