FACULTAD DE ARQUITECTURA E INGENIERÍAS

Trabajo de Investigación de fin de carrera titulado:

DISEÑO DE UN PROCESO DE HARDENING DE SERVIDORES PARA UNA INSTITUCIÓN FINANCIERA DEL SECTOR PUBLICO

Realizado por:

Ana Gabriela Caiza Navas

Director del proyecto:

Dr. Frankie Erikson Catota

Como requisito para la obtención del título de:

MAGISTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN SEGURIDAD DE REDES Y COMUNICACIÓN

QUITO, 27 de Marzo de 2019

DECLARACIÓN JURAMENTADA

Yo, Ana Gabriela Caiza Navas, con cédula de identidad 1719370536, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y, que ha consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, cedo los derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

_____
Ana Gabriela Caiza Navas
C.C: 1719370536

DECLARACIÓN DEL DIRECTOR DE TESIS

Declaro haber dirigido este trabajo a través de reuniones periódicas con los estudiantes, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.

Dr. Frankie Erikson Catota.

MBA

LOS PROFESORES INFORMANTES

Ing. Diego Riofrío

Ing, Edison Estrella

Después de revisar el trabajo presentado lo han calificado

como apto para su defensa oral ante el tribunal examinador

Ing. Diego Riofrío	Ing, Edison Estrella

Quito, 27 de marzo de 2019

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

Declaro que este trabajo es original, de nuestra autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.

_____
Ana Gabriela Caiza Navas
C.C: 1719370536

AGRADECIMIENTOS

Agradezco a Dios por la fortaleza brindad, para culminar mi meta profesional.

A la familia, por ser el apoyo constante en cada paso profesional y personal.

A los ingenieros, Diego, Edison y Erickson, por la paciencia, por su experiencia y conocimientos que fueron de gran aporte para culminar este trabajo.

A la Universidad Internacional SEK, que con sus gestiones y guías ayudaron en la consecución de este trabajo.

DEDICATORIA

Para mi querido Andrés, esposo, compañero y cómplice, sin su apoyo incondicional, paciencia y sobre todo amor no hubiese sido posible alcanzar esta meta.

Para Mery, César, Nena, Rocío, Patito, con sus consejos asertivos y apoyo que fortalecieron mis ánimos para no desmayar ante este objetivo.

A la memoria de Chelo, que predijo que esta meta llegaría a mi vida.

RESUMEN

El objetivo principal de este proyecto es diseñar el proceso de hardening de servidores para una institución financiera gubernamental; para ello, se ha realizado un análisis de la situación actual del proceso de instalación de servidores, identificando las debilidades administrativas y de seguridad, estas debilidades son mitigadas con controles de seguridad.

Para la conformación de la línea base de seguridad se utiliza los controles propuestos en las guías, CIS Benchmark, NIST y los fabricantes, Microsoft y Red Hat.

En el presente trabajo se realiza un estudio del número de controles propuestos por cada una de las guías y agrupándolos en categorías, se analiza cada control sugerido por las guías, proponiendo la adopción de controles a la institución. Se realiza la comparación de alto nivel entre las líneas de base de Windows y Red Hat.

Las líneas base de seguridad obtenidas de la comparativa de controles comprenden la estructura principal para la aplicación del proceso de aseguramiento de los servidores que se estudian en este trabajo, esta propuesta cuenta con 4 pasos que son: 1. Solicitud o requerimiento de la instalación del servidor, 2. Selección de la línea base de seguridad, 3. Fortalecimiento del activo y 4. Revisión del activo.

Los resultados de este documento muestran que la línea de base de seguridad es mejor cuando tiene diferentes puntos de vista sobre los controles estudiados, lo que proporciona la ayuda para crear una línea de base específica para el negocio.

Claves: Hardening, NIST, CIS, Windows, Red Hat

ABSTRACT

The main goal of this project is to design a hardening process for a financial goverment institution, to do that, an analysis of the current situation has been made to the server installation process, identifying administrative and security weaknesses.

The security controls used in this security baseline are included in international guides like: CIS Benchmark, NIST and the manufacturers, Microsoft and Red Hat.

An analysis is made using the number of controls listed by each of the guides and grouping into categories, an analysis of each control suggested by the guides is also studied, advising the use by the financial institution of those controls. The high-level comparison between the Windows and Red Hat baselines is also performed.

The security baselines obtained from the comparison of controls comprise the main structure for the application of the hardening process of the servers that are studied in this document, this proposal has 4 steps that are: 1. Requirement of the installation of the server, 2. Selection of the baseline of security, 3. Strengthening of the asset and 4. Review of the asset.

The results regarding this document show that the security baseline is better when you have different points of view about the studied controls, providing the help to create a specific baseline for the business.

Tabla de Contenidos

Lista de Figuras

Lista de Tablas

Capítulo I

Introducción

1.1. Planteamiento del Problema

La institución financiera actualmente tiene en producción infraestructura vulnerable misma que se identificó mediante un proceso de análisis de vulnerabilidades de infraestructura (Jefe de Seguridad, comunicación personal, 16 de noviembre de 2018), adicionalmente, la infraestructura nueva está siendo instalada sin una adecuada configuración de seguridad del sistema operativo, base de datos y/o software web.

La infraestructura vulnerable es el conjunto de hardware y software sobre el que se instala las diferentes aplicaciones y servicios que ayudan al manejo, almacenamiento y distribución de la información de la institución financiera, misma que tiene controles débiles de seguridad o carece de los mismos (Jefe de Seguridad, comunicación personal, 16 de noviembre de 2018).

Un sub grupo importante del grupo de infraestructura son los servidores y estos son también vulnerables, este sub grupo tiene instalado sistema operativo, base de datos, software web o aplicaciones y son vulnerables por una inadecuada configuración de seguridad, servicios y puertos activados y que no son necesarios, inexistente control de actualización de software y parches de seguridad de los servidores.

Los factores antes mencionados implican que la institución financiera quede expuesta a (Jefe de Seguridad, comunicación personal, 16 de noviembre de 2018):

- Vulnerabilidades de fácil explotación.
- Robo de Información confidencial de clientes.

- Daño de imagen o reputación de la institución.
- Indisponibilidad de los servicios de brinda a sus clientes.
- Pérdida económica
- Implicaciones legales

1.2. Objetivo General

Diseñar el proceso de hardening de servidores mediante el análisis de la situación actual del proceso de instalación de infraestructura para la implementación de medidas de seguridad basadas en configuración segura que permitan reducir las vulnerabilidades por inadecuada configuración.

1.3. Objetivos Específicos

- Identificar las falencias de seguridad en el proceso de instalación de infraestructura que actualmente realiza la institución financiera mediante entrevista con el administrador de infraestructura.
- Priorizar dos plataformas a nivel de sistema operativo o base de datos o software web mediante la aplicación de la metodología de Riesgo Operativo de la institución financiera.
- Identificar las fuentes adecuadas sobre configuración segura de las plataformas de sistemas operativos o base de datos o web, mediante un análisis para la recolección de recomendaciones y buenas prácticas de seguridad.
- Diseñar el proceso de hardening de servidores mediante la inclusión de controles de seguridad para el mejoramiento de seguridad en la instalación de servidores.

1.4. Justificación

El diseño del proceso de hardening de servidores existe por la necesidad de eliminar el problema de tener infraestructura con configuraciones no seguras este proceso es un control que ayudará a mitigar la existencia de configuraciones por defecto (Jefe de Seguridad, comunicación personal, 16 de noviembre de 2018),

Adicional mediante resolución JB-2014-3066 de la Junta Bancaria de la Superintendencia de Bancos del Ecuador (SB) emitida el 2 de septiembre y publicada el 3 de octubre en el Registro Oficial Nº 347, se dispuso que el sistema financiero nacional debe incrementar los niveles de seguridad en los canales electrónicos, mejorar los controles de gestión de la infraestructura de tecnología de la información y la gestión del riesgo operativo.

1.5. Método

Para lograr la propuesta de esta investigación se ejecutará diferentes actividades cuyos resultados ayudan a construir la propuesta del diseño del proceso de hardening de servidores:

1. Realizar el análisis de la situación actual del proceso de instalación de servidores de la institución financiera, obteniendo como entregable la identificación de los actores, actividades, controles de seguridad o carencias de las mismas.
2. Priorizar dos plataformas de sistema operativo, base de datos o software web para la creación de los checklist de hardening mediante la aplicación de la metodología de Riesgos que tiene la institución.
3. Identificar las fuentes adecuadas mediante un análisis para la recolección de recomendaciones y buenas prácticas de seguridad a nivel de configuración de las plataformas priorizadas.

4. Diseñar el proceso de hardening de servidores mediante la inclusión de controles de seguridad para mejorar el nivel de seguridad en la instalación de nuevos servidores.

1.6. Estado del Arte

Existe varia documentación con diferentes perspectivas de aseguramiento de infraestructura Tecnológica, de acuerdo a la investigación realizada, Jaison Fache en su documento" ESTUDIO SOBRE LA APLICACIÓN DE HARDENING PARA MEJORAR LA SEGURIDAD INFORMÁTICA EN EL CENTRO TECNICO LABORAL DE TUNJACOTEL " (Fache, 2016) señala:

1. Que su trabajo está enfocado en realizar primero un análisis de seguridad de la red informática.
2. Contempla indagar medidas de hardening para estaciones de trabajo basados en Windows y Linux, describiendo sus características, ventajas y usos de las mismas.
3. Considera presentar un informe con las recomendaciones necearías para aumentar el nivel de seguridad a nivel de un modelo de defensa en profundidad.
4. Expone al hardening como una excelente respuesta para robustecer la seguridad en la infraestructura haciendo uso de barreras en hardware o software que garanticen mediadas efectivas ante los ataque o daños.

Javier Robayo en su documento "ASEGURAMIENTO DE LOS SISTEMAS COMPUTACIONALES DE LA EMPRESA SITIOSDIMA.NET" (Robayo, 2015) señala:

1. Conocer el método de Hardening e identificar implicaciones de implementar en un sistema Operativo Windows.
2. Entender el concepto de defensa en profundidad e Indagar herramientas que permitan cumplir con esto.

3. Por ultimo considera estudiar políticas generales de seguridad informática, sus elementos y consideraciones de aseguramiento tecnológico.
4. Para implementar hardening en una empresa se requiere conocer detalles sobre aplicaciones o servicios de la organización con el fin de aplicar al máximo la seguridad de acuerdo a las necesidades del negocio.
5. Expone que el enfoque de hardening es la implantación de seguridad basado en defensa en profundidad.
    - Configuraciones para protegerse de posibles ataques físicos.
    - Instalación segura del sistema Operativo.
    - Activación y/o configuración adecuada de servicios de actualizaciones automáticas.
    - Instalar, mantener u monitorear programas de seguridad como Antivirus, Antimalware y Antispam.
6. Las compañías deberían blindar sus sistemas y establecer que deben cumplir al menos los estándares mínimos satisfactorios.

Carlos Frías en su documento “HARDENING A SERVIDORES CRITICOS DE LA PARTE TRANSACCIONAL WEB DE UNA ENTIDAD FINANCIERA” (Morales, 2018) señala:

1. Identificar vulnerabilidades a las que está expuesta una entidad financiera.
2. Mediante la combinación de herramientas, hardware, software minimizar las vulnerabilidades identificadas en el punto anterior
3. Implementar los resultados producto de la investigación realizada en su documento.
4. Expone que el hardening a servidores críticos se implementará con un enfoque basado en defensa en profundidad.

En este trabajo se realizará el diseño del proceso de hardening de servidores para la institución financiera basado en un marco de referencia COBIT; considerando el giro de negocio que la institución desempeña actualmente.

Capítulo II

Marco Teórico

2.1. Infraestructura Tecnológica

Es un conjunto de hardware y software que ayuda a la institución a prestar sus servicios a los usuarios finales, es decir, es donde se instalan las aplicaciones que necesita la institución para su funcionamiento bancario y su gestión interna.

El conjunto de hardware es todo dispositivo físico que ayude la comunicación, procesamiento y almacenamiento de información, por ejemplo: routers, switch, firewall, repetidores, cámaras, estaciones de trabajo, impresoras, teléfonos, servidores.

El conjunto de software son todos los programas y sistemas que ayuda o facilita la prestación de servicios, comunicación, manipulación, procesamiento y almacenamiento de la información, como por ejemplo: sistema operativo, motor de base de datos, aplicaciones, software web, programas de oficina, plataformas administrativas y operativas (Asociación Catalana de Universidades Públicas, 2012).

2.1.1. Servidor

Un servidor es “una unidad informática que proporciona diversos servicios a computadoras conectadas con ella a través de una red” (Española, 2018). Los servidores atienden y contestan peticiones constantemente a otros dispositivos, por consiguiente, los servidores deben permanecer activos la mayor parte de su tiempo de vida (Gutiérrez Cañizares).

Un servidor es un ordenador, computadora o equipo informático que pone sus recursos a disposición en la red para otros ordenados o equipos informáticos, llamados clientes (Torres, 2017).

Tipos de Servidores

Los servidores pueden clasificarse de diferentes maneras tomando en cuenta sus características como por ejemplo por su capacidad de procesamiento como expone en su texto Sandra Jara (Jara, 2005):

- Supercomputadoras
- Macro computadoras
- Minicomputadoras
- Microcomputadoras

Como expone Sandoval (2018) y Valdivia (2014) los servidores dependiendo del servicio que brinden, de su función a desempeñar en la red puede clasificarse en:

- Servidor Web
- Servidor Proxy
- Servidor de Acceso Remoto
- Servidor de Correo
- Servidores de base de Datos
- Servidores de Archivos

A continuación, se resume cada uno de los tipos de servidor de acuerdo a su funcionalidad.

- **Servidor web**: Es un sistema que recibe requests (peticiones) desde varios clientes locales o de internet y almacena archivos web como texto, imágenes, videos que pueden ser visualizados a través del navegador, el servidor permanece conectado ejecutando el servicio www "World Wide Web" (Cómez, 2014, Villada,2014)

- **Servidor proxy**: Es un ordenador dedicado a la tarea de filtración de paquetes, es un intermediario entre la petición del cliente y el servidor web, es decir realiza un control de acceso hacia el servidor web (Villada, 2014, Laudon,2004).
- **Servidor de base de datos:** Es un sistema utilizado para el almacenamiento y archivo de datos basado en una arquitectura de cliente/servidor que ejecuta tareas requeridas por quien hace uso de este (Sandoval, 2018).
- **Servidor del acceso remoto (RAS)**: Es un sistema que recibe las peticiones de conexión remota hacia los dispositivos de la red local (Caballero, 1998).
- **Servidor de correo**: Es un ordenador que permite el envío y recepción de mensajes por medio del internet facilitando la comunicación ágil entre usuarios internos y externos de una organización (Desongles, 2006).
- **Servidor de Archivos**: Es un sistema que permite la transferencia de ficheros entre un cliente y el servidor utilizando los protocolos FTP o SFTP.

2.1.2. Instalación de Servidores

La instalación de servidores se refiere a una serie de actividades o pasos a seguir que permitan garantizar calidad en la entrega de un servidor. Los pasos que se deberían considerar son los siguientes:

- Identificación el hardware en el cual se realizará la instalación.
- Seleccionar el sistema Operativo que va ser instalado.
- Validar compatibilidad.
- Configuración.
- Definir variables de entornos.
- Realizar pruebas de conectividad

2.1.3. Configuración de Servidores

La configuración en el ámbito de la informática es lo que hace que cada parte de la computadora cumpla una función por lo general es preexistente a la instalación del mismo. (Bembibre, 2009)

Esta configuración será lo que determine cómo, a través de qué medios y con qué recursos funcionará el elemento, sin embargo, este conjunto de información puede ser alterado para dar nuevas funciones o redefinir el elemento en diferentes modos. (Bembibre, 2009).

2.2. Seguridad Informática

Es una disciplina que debe garantizar y proteger la integridad, confidencialidad y disponibilidad de la información que se encuentra almacenada en un sistema informático, esta disciplina también se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir su fin (Purificación, Seguridad Informática, 2010, Porto, 2008).

Tipos de seguridad

- **Activa**: Comprende las medidas y conjunto de defensas cuyo alcance es evitar o reducir los riesgos que amenazan a los sistemas (Purificación, Seguridad Informática, 2010).
- **Pasiva**: Comprende las medidas implementadas una vez producido el incidente de seguridad, esto ayuda a que en caso de suceder nuevamente pueda facilitar su recuperación (Purificación, Seguridad Informática, 2010).

2.2.1. Amenaza

Es un suceso que puede llegar a desencadenar un incidente no deseado en la organización, ocasionando pérdidas y daños materiales (Colobran, 2008).

Es cualquier factor que pueda causar daño a una organización mediante la modificación, eliminación de la información o mediante la denegación de servicios (Iglesias, 2006).

Según lo expuesto por Purificación en su texto las amenazas pueden ser clasificadas en cuatro grandes grupos:

- De Interrupción: su objetivo es deshabilitar el acceso a la Información.
- De Intercepción: Es cuando personas, programas o equipos no autorizados podrían acceder a un determinado recurso del sistema y obtener información confidencial de la organización.
- De modificación: Es cuando personas, programas o equipos no autorizados a más de obtener acceso no autorizado a la información puedan modificarla.
- De Fabricación: Su objetivo es agregar información falsa en los datos de la organización.

Las amenazas pueden ser causadas por:

a) Usuario: causa del mayor problema en la seguridad de un sistema informático, sus acciones pueden causar incidentes de seguridad, la mayoría de veces se debe porque se sobredimensiona sus permisos. (ICORP, 2018)
b) Virus informático: Definiéndolos como «un programa de ordenador que puede infectar otros programas modificándolos para incluir una copia de sí mismo». Los virus informáticos tienen básicamente la función de propagarse, replicándose, pero algunos contienen además una carga dañina (payload) con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil. (Institución, 2017)
c) Personal técnico interno: Los administradores de la infraestructura, sistema operativo, bases de datos o software web, técnicos de desarrollo, etc. Los motivos que se encuentran entre los habituales son: disputas internas, problemas laborales, despidos, fines lucrativos, espionaje, curiosidad, poco interés en la seguridad etc. (ICORP, 2018)

d) Ransomware: Es un tipo de malware informático, el cual cifra la información del usuario infectado y solicita un rescate económico para descifrar la información. Generalmente este tipo de malware se distribuye mediante archivos infectados que el usuario obtiene desde el internet. (Oceano IT, 2014)

e) Phishing: Es el envío de un correo mal intencionado que aprovecha la confianza y emociones del usuario final, accionando que se extraiga información personal o de la organización (Oceano IT, 2014).

f) Cracker. Es un individuo que aprovecha de sus habilidades informáticas para violar la seguridad de un sistema informático de forma similar como un hacker, la diferencia es que el cracker realiza la intrusión con fines de beneficio personal o para hacer daño a su objetivo. (Purificación, Seguridad Informática, 2010)

g) Hacker. Son personas que tienen habilidades para realizar pruebas de intrusión sobre los sistemas e infraestructura de red. (Institución, 2017).

2.2.2. Vulnerabilidad Informática

Para una institución financiera es cualquier debilidad que signifique un riesgo para la seguridad de la información, es decir, son fallos en el diseño del sistema, de la arquitectura de la red que pueden ser utilizadas para causar daño y afectar la "confidencialidad, disponibilidad e integridad de la información de un individuo o empresa" (Gisbert, 2015).

Las vulnerabilidades solo por existir o estar ahí no significa que el daño que pueda causar se realice de forma automática, lo que significa es que un atacante puede aprovechar esta vulnerabilidad para realizar daño (Espinoza, 2012).

Las vulnerabilidades son explotadas o identificadas ejecutando el siguiente proceso:

- Reconocimiento
- Escaneo
- Obtener Acceso
- Escribir Informe
- Presentar Informe

Figura 1 - Proceso de Identificación de Vulnerabilidades basado en OWASP

Fuente: Elaborado por el autor de la investigación

Tipos de Vulnerabilidades

Existen varias formas de clasificar a las vulnerabilidades, por su naturaleza, por su tipo de acceso, por su impacto, o por su localización (Areitio, 2008).

Las vulnerabilidades también pueden clasificarse como vulnerabilidades lógicas y físicas como se expone en el texto "INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES" (Martha Romero, 2018):

Vulnerabilidades Físicas: Son vulnerabilidades que puedan perturbar a la infraestructura de manera física como por ejemplo que el centro de datos o de operación se encuentre en una zona de alto sismo o que por generalmente sufre de inundaciones, esto puede causar una indisponibilidad en el servicio.

Vulnerabilidades Lógicas: Son las pueden afectar directamente a la infraestructura y desarrollo de la operación, estas pueden ser:

- Configuración: Son las configuraciones por defecto del sistema o de las aplicaciones del servidor que se tengan expuestas, configuración de componentes perimetrales.
- Actualización: Son vulnerabilidades que las empresas e incluso las financieras pueden llegar adquirir por no actualizar los sistemas operativos, las aplicaciones, componentes.
- Desarrollo: Son todas aquellos errores u omisiones que se producen en la generación o modificación del código.

2.2.3. Riesgo

Es la posibilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad, es decir, si no existe una de las dos variables (vulnerabilidad, amenaza) no existe un riesgo (Purificación, Seguridad Informática, 2010).

Sobre los riesgos se puede ejercer diferentes niveles de control según lo expuesto por Xiomar Delgado en su texto (Delgado, 1998):

- Asumir o aceptar el riesgo: Sucede cuando el valor de afectación o perjuicio tiene valor muy bajo, o cuando el costo de mitigación o eliminación del riesgo es más alto que la reparación del daño.
- Eliminar el riesgo: En algunas ocasiones cuando los controles o medidas de seguridad eliminan la vulnerabilidad o la amenaza.
- Disminuir el riesgo: Cuando los controles o medidas reducen el daño.
- Transferir el riesgo: cuando el riesgo es transferido a terceros para ser gestionado.

2.3. Aseguramiento de Servidores

Son una serie de actividades que se realizan para generar un servidor o equipo con configuraciones de seguridad, esto también se lo puede llamar endurecimeito de sistema operativo.

2.3.1. Controles de Infraestructura

Un control en el ámbito la seguridad informática es cualquier acción o serie de acciones que ayudan a garantizar la confidencialidad, integridad y disponibilidad de la información, estas pueden ser ejecutadas automáticamente por sistemas o pueden ser ejecutadas manualmente por personal con habilidades y criterios de seguridad de la información.

Para garantizar los 3 principios de la seguridad de la información CID (Confidencialidad, Integridad, Disponibilidad) antes mencionados en la infraestructura de la organización es necesario considerar los siguientes controles (Rodrigo, 2014), la siguiente lista es una de las varias que puede existir para elevar el nivel de seguridad de la infraestructura de red de una institución:

- Firewall de red y de aplicación (filtrado de paquetes, comprobación de estado de conexión, inspección de paquetes, control de usuarios administradores)
- IPS (implementación de firmas)
- Switch de Core (Listas de control de acceso, control de usuarios administradores)
- Switch de piso (control de acceso por MAC, control de usuarios administradores)
- Servidores (Hardening de Sistema Operativo, BDD o software web, control de usuarios administradores)
- Infraestructura Física (Control de acceso)
- Enrutadores Perimetrales (ACL, implementación de protocoles de conexión segura, control de usuarios administradores)

- Antivirus y Antispyware (Amplia base de datos de conocimiento).

2.3.2. Hardening de Servidores

Hardening (palabra en ingles que significa endurecimiento), en seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo. Esto se logra eliminando software, servicios, usuarios, etc. innecesarios en el sistema así como cerrando puertos que tampoco estén en uso (Smartekh, 2012).

El aseguramiento de servidores (conocido también como "Server Hardening") se ocupa de revisar todos estos componentes que forman parte de una solución y testear si están correctamente configurados en los aspectos de seguridad y que no existan grietas de esa índole. Como las aplicaciones web confían en el servidor web y el sistema operativo subyacente, si hay problemas en ellos, entonces toda la seguridad a nivel de la aplicación sirve de muy poco (Arduinosecurity, 2016).

Los beneficios que nos brinda el hardening de servidores es reducir los riesgos asociados con fraude y error humano, facilita un despliegue de configuración más limpio y seguro, certifica que los recursos críticos se encuentren con parches actualizados y sean capaces de defenderse contra vulnerabilidades conocidas.

Cada organización o empresa consiente de la seguridad tendrá sus propios métodos o mecanismo o controles para mantener la seguridad adecuada en la red y el sistema; se presenta ciertas consideraciones a tomar al momento de blindar los servidores:

- Para sus comunicaciones se deberá usar cifrado de datos.
- Evite utilizar protocolos inseguros de transmisión de información sensible.
- Desinstalar o desactivar software innecesario en los servidores

- Actualizar los sistemas a versiones vigentes y principalmente los parches de seguridad.
- Usar extensiones de seguridad
- Deshabilitar binarios no deseados de SUID, SGID
- Las credenciales de los administradores de los sistemas deben ser fuertes y de no fácil deducción.
- No permitir contraseñas en vacío.
- Bloquear la cuenta después de un número de intentos fallidos
- Establecer un periodo frecuente de cambio de contraseña
- Deshabilitar y no utilizar puestos por defecto
- Deshabilitar los servicios innecesarios.
- Deshabilitar los inicios de sesión directos a root
- Ocultar la versión del sistema Operativo y contenedor web
- Establecer controles perimetrales como firewall, sistema de detección de intrusos.
- Usar protocolo SSH para comunicación.

2.4. Dominios de COBIT

Los dominios de COBIT orientados a procesos ayudan a incluir un modelo operacional y un lenguaje común para todas las partes involucradas en la instalación de servidores, brinda también un marco de trabajo para la medición y monitoreo del proceso. Este enfoque fomenta el uso de las mejores prácticas administrativas permitiendo que se defina las responsabilidades.

Tabla 1 - Dominios de COBIT que apoyan al diseño del proceso de hardening

Fuente: ISACA – COBIT5

Alinear, Planificar y Organizar

- Cubre las estrategias y las tácticas identificando la manera en que TI puede contribuir a los objetivos del negocio.

Constriur, Adquirir e Implementar

- Para llevar a cabo la estrategia de Ti, se requeire identificar, desarrollar, adquirir e integrar los procesos de negocio para cumpliento de la meta de IT asociada a la seguridad de la información, infraestructura de procesamiento y aplicaciones.

Entregar, dar Servicio y Soporte

- Cubre la entrega de los servicios requeridos para la instalación de servidores con linea base de seguridad, la administración de los datos y la instalación de operaciones.

Supervisar, Evaluar y Valorar

- Cubre la evalaución de forma regular de las actividades, entregables, calidad y cumplimiento del proceso de hardening; monitoreo y control interno de la ejecución del flujo de bliandaje.

Capítulo III

Análisis Situacional

3.1. Generalidades

La institución financiera pertenece al sector público, brinda servicios bajo los criterios de Banca de inversión, crece paulatinamente en servicios bancarios para sus clientes; sus principales servicios son préstamos Hipotecario, Quirografarios y Prendarios; los mismos que son soportados por infraestructura y aplicaciones tecnológicas.

El departamento de tecnología es el encargado de monitorear la infraestructura y aplicaciones del negocio, el departamento se encuentra estructurado por diferentes unidades, Producción y Soporte, Infraestructura y Canales, Control de Calidad y Desarrollo.

3.2. Estructura Organizacional de TI

Obteniendo un extracto del organigrama general de la institución en la siguiente ilustración se podrá observar cómo se encuentra posicionado TI dentro de la institución (Jefe de Seguridad, comunicación personal, 16 de noviembre de 2018); para ver todo el organigrama de la empresa referirse al Anexo I.

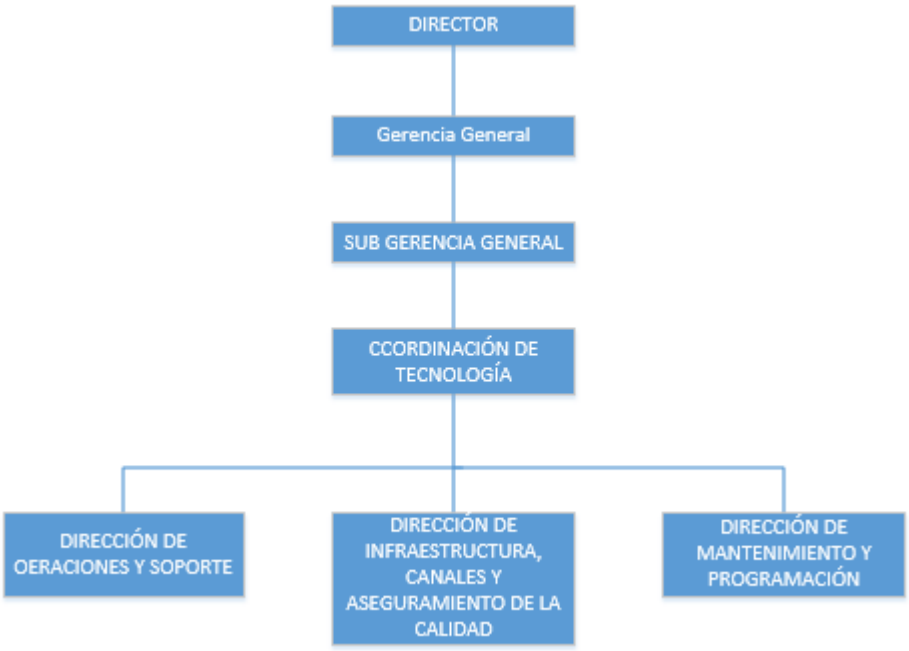


Figura 2 - Organigrama del departamento de tecnología

Fuente: Por el autor

Como se puede observar en la ilustración, el departamento cuenta con 3 direcciones, es responsabilidad de la dirección de infraestructura, canales y aseguramiento de la calidad, la ejecución del proceso de instalación de nuevos servidores.

3.3. Proceso de Instalación de Servidores

La coordinación de Tecnología cuenta con los siguientes procesos que ayudan al cumplimiento de sus objetivos:

- Gestión de la planificación, alineación y organización
- Gestión de la construcción, adquisición e implementación
- Gestión de la entrega del servicio y soporte

Gestión de la construcción, adquisición e implementación, proceso que abarca el subproceso de Administración de la Configuración donde se indica que debe ser considerado los siguientes documentos para lograr su objetivo, que es mantener un registro actualizado de todos los elementos de configuración de la infraestructura de TI:

- Política de Tecnología de la Información: Donde indica en su Art. 12 "La valoración, planificación, priorización y aprobación de los cambios estándar deberá ser realizado por una Comisión de Cambios, definido en el artículo 13 de esta Política, en función de su impacto sobre el negocio y la infraestructura de TI". (Institución, 2015)
- Política de Seguridad de la Información: Donde indica en su Art. 30 "Los requisitos, criterios y controles de seguridad deberán ser incorporados en los sistemas de información e incluirán: infraestructura tecnológica, adquisición de aplicaciones comerciales y desarrollos internos. {..}". (Institución, 2015)
- Reglamento de Seguridad de la Información: Donde indica en sus artículos 95.2 y 95.3 "No se permitirá la puesta en producción de ningún elemento de red que no haya sido configurado con los lineamientos de seguridad vigentes para la plataforma, sistema o equipo de conectividad. Los procedimientos de instalación y configuración de seguridad deberán ser respaldados con documentación vigente emitida oficialmente por el fabricante."
- Instructivo de Administración de Cambios de software: Garantizar que los cambios a la infraestructura sean controlados y disminuyendo el impacto negativo en la integridad y estabilidad de la infraestructura.

A continuación, se presenta y detalla el flujo actual de Administración de la configuración de acuerdo al documento formal aprobado por la institución financiera:

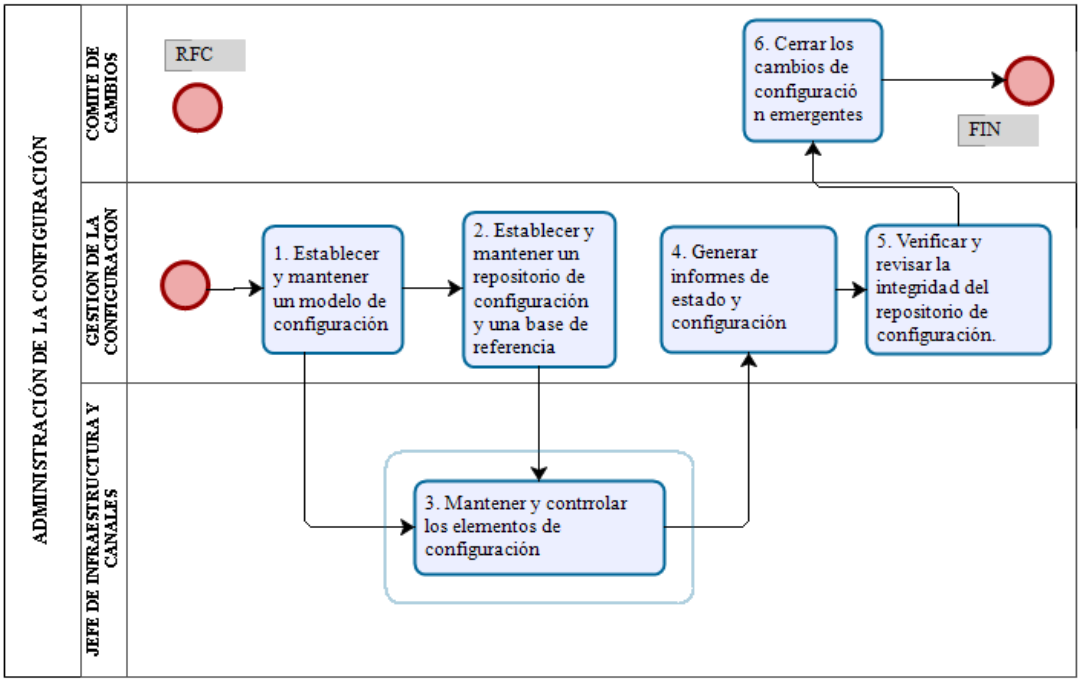


Figura 3 - Flujo del proceso de instalación de servidores.

Fuente: Elaborado por la Institución Financiera

Establecer y mantener un modelo de configuración: Esta actividad inicia con el inventario de infraestructura, en esta actividad se definirá conjuntamente con el Gestor de la configuración y el administrador de la plataforma el nivel de configuración (básica o avanzada), parches lógicos de seguridad, configuración en alta disponibilidad con respuestas de SI/NO..

En esta misma actividad debe establecer un modelo lógico de la infraestructura o servicio para la gestión del a configuración, la misma que debe ser aprobada por la dirección de infraestructura. La salida de la actividad es el modelo lógico (diagrama de flujo) de la configuración con su aprobación respectiva.

Establecer y mantener un repositorio de configuración y una base de referencia: crea o actualiza el registro en la CMDB (Configuration Management Database) (es un archivo Excel), en este documento se registra a detalle cada elemento de configuración con sus interrelaciones, dependencias y acuerdo; para iniciar esta actividad se requiere el modelo lógico que es salida del punto anterior y como resultado entrega o libera la CMDB actualizada. No se evidencia que exista un documento con el detalle que se expone en el procedimiento.

Mantener y controlar los elementos de configuración: La dirección de infraestructura revisa trimestralmente la CMDB, y en caso de existir controles de cambios emergentes solicita al gestor de la configuración que revise los cambios solicitados a los elementos de configuración caso contrario el requerimiento debe seguir el flujo de incidentes. Los documentos habilitantes para el inicio de esta actividad es la CMDB, requerimiento de cambio y como salida se libera el plan de implementación y marcha atrás.

Generar informes de estado de configuración: El gestor de configuración debe identificar cambios en el estado de los elementos de configuración y contrastar con los cambios emergentes autorizados con la finalidad de garantizar que no existe cambios no autorizados; la entrada para iniciar esta actividad es el plan de implantación y marchas atrás y como resultado se entrega el informe de novedades, en caso de no existir novedades no debe generarse el reporte pero debe notificar a la dirección de infraestructura.

Verificar y revisar la integridad del repositorio de configuración: Esta actividad se encarga de verificar semestralmente los elementos de configuración contra la CMDB comparando configuraciones físicas y lógicas, identifica todas las desviaciones de las correcciones; la entrada para iniciar esta actividad es el informe de novedades y la CMDB, como resultado se emite el memorando de desviaciones.

Cerrar los cambios de configuración emergente: El gestor de configuración realiza un seguimiento manual a cada uno de los cambios emergentes de configuración y gestiona las aprobaciones para el cierre del cambio emergente.

La institución Financiera contempla para cambios de configuración en la infraestructura del Banco aplicar el proceso de administración de cambios de Hardware, el mismos que indica que el cambio debe ser aprobado, documentado y probado antes de ponerlo en ambiente productivo; las actualizaciones de parches de los sistemas ingresan por este proceso.

3.4. Proceso de Gestión de Cambios de Hardware

El objetivo principal de este proceso es que se realicen los cambios a hardware de manera controlada disminuyendo cualquier impacto en la estabilidad de la infraestructura tecnológica.

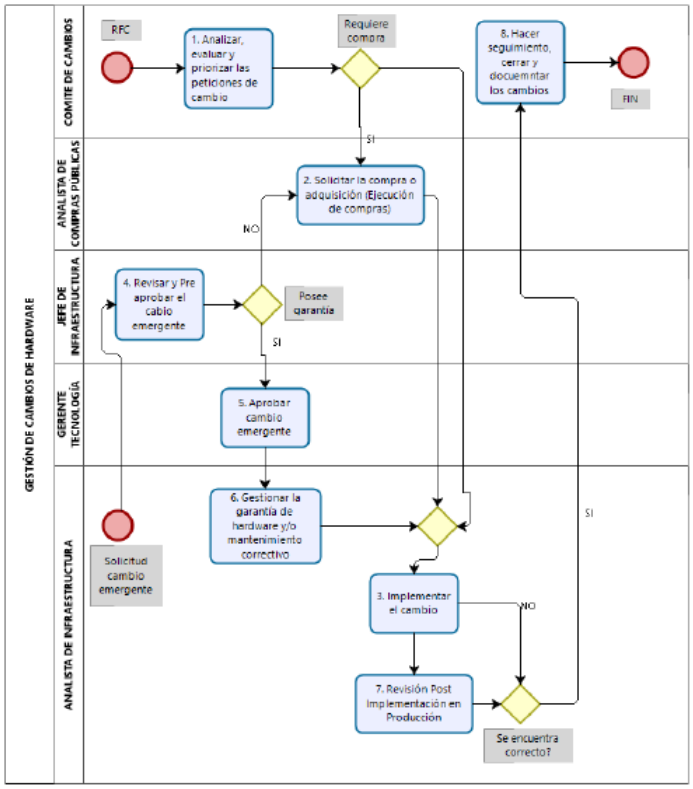


Figura 4 - Flujo del proceso de gestión de cambios a Hardware

Fuente: Elaborado por la Institución Financiera.

A continuación, se detalla el flujo actual de Gestión de cambios de hardware mismo que interactúa con el proceso de instalación de servidores antes visto:

Analizar, evaluar y priorizar las peticiones de cambio: Varios procesos pueden iniciar este proceso, pero en caso de que sea iniciado por el proceso de gestión de configuración y sea un cambio a la configuración de la infraestructura o adquisición de infraestructura, realiza lo siguiente:

- Si existe más de una petición es necesario priorizar
- Registrar en una bitácora la petición de cambio
- Planificar y programas los cambios.

- Crear el plan de implantación y marcha atrás
- En caso de compra fundamentar correctamente la compra
- El coordinador de TI debe solicitar mediante memo incluyendo ofertas, informes técnicos y ejecutar el instructivo del proceso de administración de comparas públicas.

Implementar el Cambio: se procede a implementar el cambio de hardware y se notifica por correo electrónico a los involucrados el estado del cambio.

Revisión post implementación en producción: realizan pruebas de funcionamiento, una vez revisado y certificado el cambio emiten un informe con las revisiones realizadas; notifican a la comisión de cambios el estado del cambio para que se proceda a realizar el cambio.

Hacer seguimiento, cerrar y documentar los cambios: La comisión de cambios valida el informe, realiza un seguimiento de todos los cambios programados para su implementación hayan concluido y actualiza inventario de infraestructura.

Cambios emergentes: Estos pueden ser originados solo por mesa de servicio y el analista de Infraestructura, mismo que revisa antes de ser solicitada la aprobación de la jefatura de Infraestructura. Se debe revisar si existe garantía técnica y en caso que requiera una adquisición deben cumplir con el proceso de compras públicas; posterior a la aprobación sigue el flujo normal de un cambio.

3.5. Relevamiento del proceso operativo

Mediante entrevista con el administrador de infraestructura se realizó el levantamiento del proceso con las actividades que realiza el operador de infraestructura con respecto a la instalación de servidores.

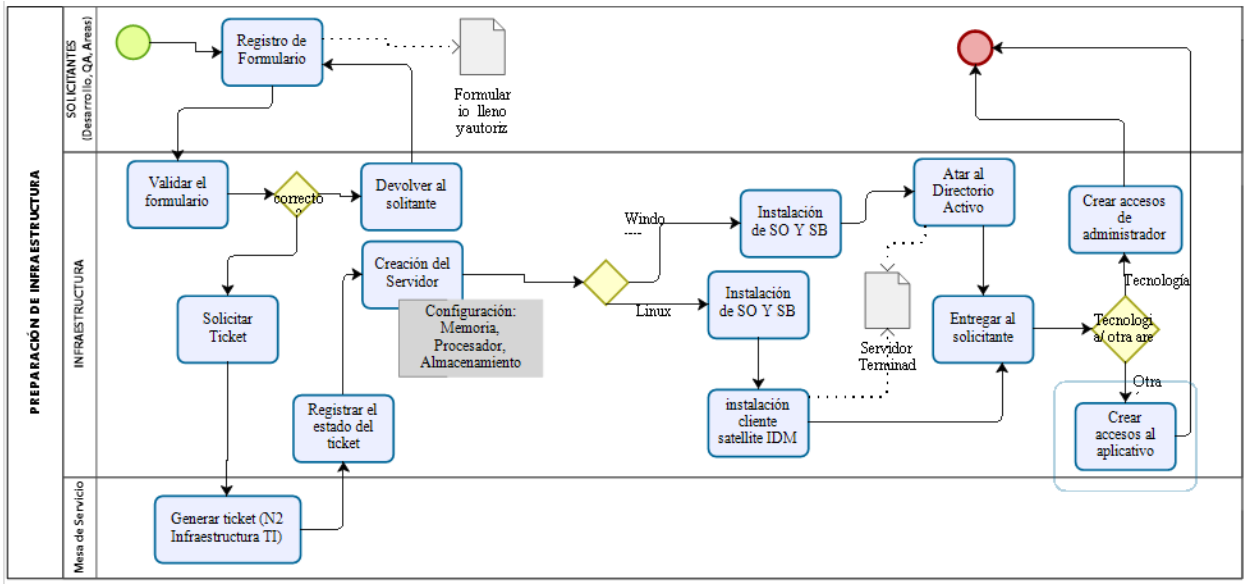


Figura 5 - Flujo de actividades que realizan actualmente en la instalación de servidores.
Fuente: Elaborado por la Institución Financiera

Los solicitantes que pueden pedir la preparación de servidores son las áreas de negocio, la unidad de QA y desarrollo. Los solicitantes deben llenar el formulario de requerimiento de hardware donde se especifica la arquitectura y las especificaciones técnicas como CPU y RAM. Ref. Anexo II

Luego de registrar el formulario con las firmas correspondientes deben solicitar a mesa de servicio la apertura de un ticket a infraestructura para la atención adjuntando el formulario anteriormente llenado.

El operador de infraestructura valida el requerimiento y en caso de existir observaciones devuelve a mesa de servicios para que se contacte con el solicitante, caso contrario, procede a la creación del servidor con las especificaciones técnicas y posterior a esta actividad se inicia la instalación del sistema Operativo y Software Base.

Como parte del punto anterior es responsabilidad del operador actualizar los parches de seguridad, como actividad final en caso de Windows es subir el servidor al dominio y en caso del Linux instalar el agente de monitoreo y con esta actividad se finaliza la instalación del servidor.

Antes de la entrega del servidor a los solicitantes se realiza la actividad de creación de accesos, en caso de que el solicitante sea un área de negocio se crea el acceso al aplicativo y en caso de que los solicitantes sea el área de QA o desarrollo se crea accesos de administrador para que realicen las configuraciones que requieren; siempre que se trate de ambientes no productivos, ya que para los productivos solo los administradores de infraestructura tienen acceso.

3.6. Debilidades Actuales

Si bien se cuenta con la documentación donde se detalla lo que se debería ejecutar de forma general para garantizar una adecuada instalación de servidor e incluso en caso de cambios en la infraestructura pueda ser de una manera confiable; en la práctica no se realiza, adicional no se cuenta con la información completa necesaria para realizar dichas actividades, las debilidades identificadas en el proceso actual de instalación de servidores versus las actividades que se realizan en el día a día al momento de instalar un servidor son:

a. Cuando se realiza la instalación de un nuevo servidor las únicas actividades que se contemplan de seguridad es que el servidor debe salir a producción con los últimos parches de seguridad.
b. En la documentación interna de seguridad se indica que la infraestructura debe ser configurada bajo los lineamientos de seguridad, no existe requerimiento o documento donde se solicite lo que debe configurarse en el servidor a nivel de seguridad en el sistema operativo, software web o base de datos.

c. Internamente no existe una clarificación de las responsabilidades de los roles de seguridad, Seguridad Informática y Seguridad de la información; actualmente estos roles están en diferentes direcciones, la primera está en la dirección de Infraestructura y la segunda en la dirección de Seguridad de la información, pero no existe una definición clara de quien debe hacerse responsable de aplicar y velar por el blindaje de la infraestructura.
d. El área de infraestructura no cuenta con el personal suficiente para realizar todas las actividades que se encuentran bajo su responsabilidad, esto también es una limitante para implementar un proceso de hardening de servidores.
e. No se cuenta con un inventario y una CMDB (Configuration Management Database) actualizada, esto dará un alcance irreal de seguridad.

Capítulo IV

Propuesta

4.1. Priorización de Plataformas

En esta sección se realiza la priorización de dos plataformas de sistema operativo o base de datos o web, de las cuales se obtendrá las mejores prácticas y/o recomendaciones de seguridad.

Para priorizar consideraremos los procesos críticos del negocio, la clasificación de la información que tiene la intuición: restringida, confidencial, pública y de uso interno, también en donde se almacena, físico o digital .

4.1.1. Activos de información a proteger

4.1.1.1. Información

La información en la actualidad es considerada como un bien o activo principal ya que es considerado como el motor que mueve a la institución empresa u organización, con este antecedente la institución como aparte del proceso de catalogación de información estima que tiene 45% de su información está catalogada como restringida y confidencial y un 51% adicional es información de uso interno de la institución y muy poca información que es de conocimiento público.

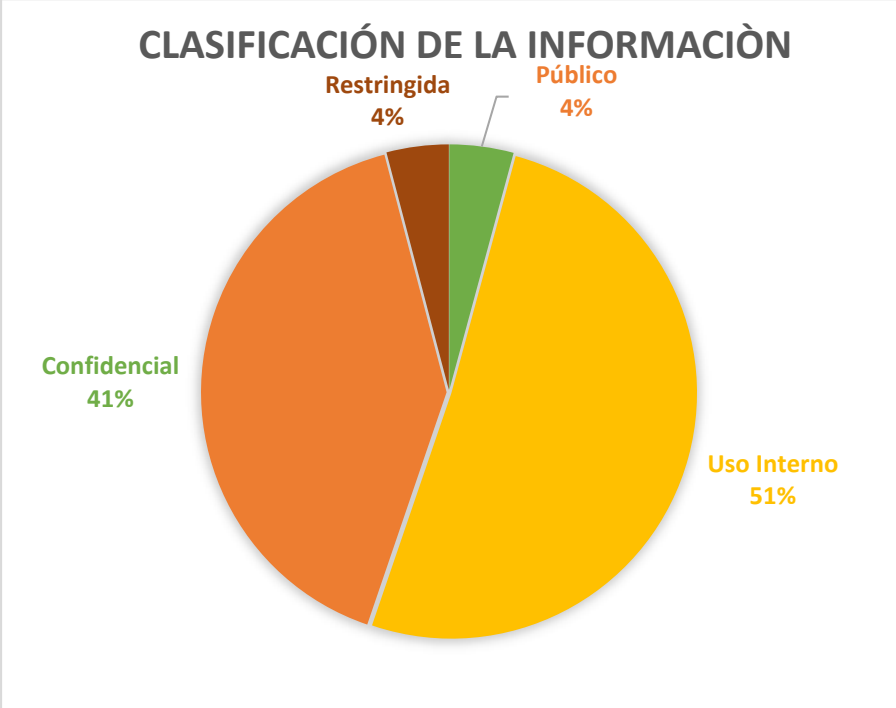


Figura 6 - Gráfico sobre la clasificación de la información

Fuente: Elaborado por la Institución Financiera

4.1.1.2. Almacenamiento de Información

La información puede ser almacenada de forma digital y/o física; en la siguiente gráfica como parte del proceso de clasificación de la información se puede decir que tenemos 78% aproximadamente de información que se almacena de forma digital, por consiguiente, podemos asumir que la tecnología es un motor importante para la generación de valor en su giro de negocio.

Ahora los elementos tecnológicos en las que se puede almacenar la información son Servidores, computadores personales, dispositivos extraíbles, cintas, entre otros.

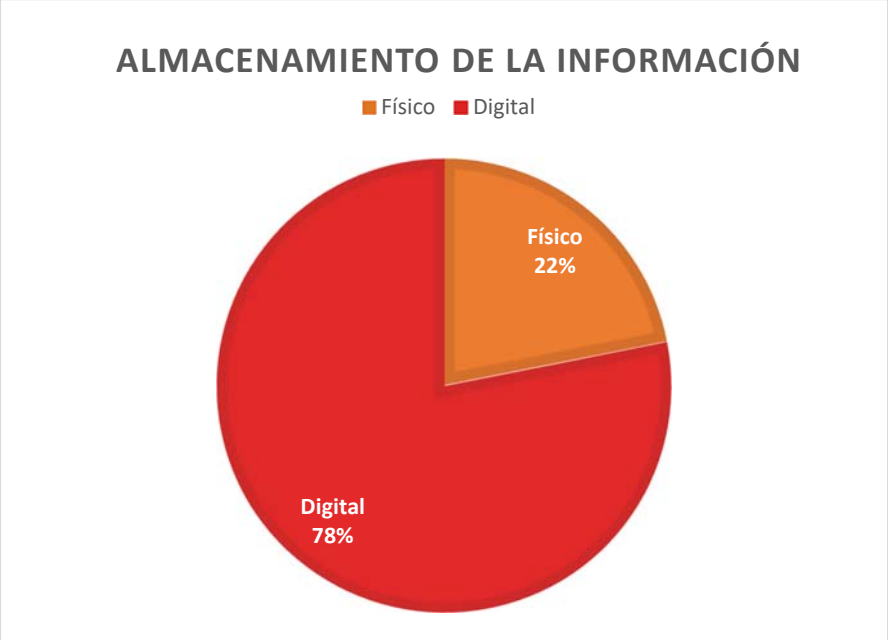


Figura 7 - Gráfico sobre donde se encuentra almacenada la información

Fuente: Elaborado por la Institución Financiera

4.1.2. Servicios Críticos

Por temas de confidencialidad con la institución financiera no se colocará los nombres exactos de las aplicaciones críticas, mismas que serán abreviadas.

Como resultado de este análisis de continuidad del negocio se ha identificado que los servicios críticos PH y PQ, mismos que guardan relación con créditos de vivienda y consumo directo, son los más característicos para la institución considerando el monto y número de transacciones que éstos manejan.

Figura 8 - Transacciones de aplicaciones.

Fuente: Elaborado por la Institución Financiera

4.1.3. Infraestructura de servicios críticos

Considerando solo los servicios críticos, se identificaron 25 recursos tecnológicos, de los cuales:

- 6 base de datos transaccional
- 9 son aplicaciones.
- 8 web services.

De los recursos tecnológicos de los servicios críticos, se identificó las plataformas que lo soportan y estas son:

- 18 sistemas Operativos: RedHat versiones 6 y 7,
- 7 sistemas Operativos: Windows server 2012
- 6 Base de Datos: SQL Server 2012

- 9 plataforma web: Jboss 7

Del análisis realizado se define que las plataformas Windows Server y Red Hat serán las consideradas para ser desarrolladas en el punto 4.2.5 “Estándares de seguridad”, que es la recolección de buenas prácticas de seguridad para la creación de una plantilla de seguridaddenominado como hardening.

4.2. Diseño de un proceso de hardening de servidores

El proceso de hardening de servidores considera mitigar las siguientes debilidades identificadas en la sección 3.6 de este documento:

1. No tienen estándar de seguridad
2. No existe una clarificación de las responsabilidades de seguridad informática y seguridad de la información.

Para la mitigación de la primera debilidad se crea de la línea base de seguridad, la que se evaluará en la sección 4.2.5. Para la segunda debilidad se considera detallar dentro del proceso de hardening el o los responsables de cada actividad para el cumplimiento del proceso.

Esta sección se enfoca en el proceso de Hardening, para lo cual se utiliza como marco de referencia en COBIT 5.0, iniciando con la identificación de los dominios que ayudan en el proceso de aseguramiento, se define el proceso de hardening global y posteriormente se detalla cada uno de los pasos del proceso de blindaje de servidores, que es el objetivo de este trabajo.

Como parte del último punto se definió la plantilla o línea base de seguridad de las plataformas priorizadas, artefacto considerado dentro del proceso de blindaje.

Como se mencionó en el marco teórico los dominios que apoyan al diseño del proceso de hardening son:

- Alinear, Planificar y Organizar
- Constriur, Adquirir e Implementar
- Entregar, dar Servicio y Soporte
- Supervisar, Evaluar y Valorar

Los procesos que nos facilita los dominios de COBIT y que ayuda al diseñodel proceso de hardening son:

- Gestión de la Seguridad
- Gestión de la definición de requisitos
- Gestión de Cambios
- Gestión de Operaciones
- Gestión de Riesgos
- Supervisar, evaluar y valorar el sistema el sistema de control Interno

Figura 9 - Procesos de COBIT para hardening de servidores

Fuente: Elaborado por el autor

El proceso de hardening debe apoyar al cumplimiento del objetivo del negocio que está enfocado al incremento de la rentabilidad considerando lo principios de seguridad, solvencia, eficiencia y control de riesgos. La institución financiera en la actualidad cuenta con los procesos de COBIT, APO12 Gestionar el Riesgo y APO13 Gestionar la Seguridad.

APO12 Gestionar el riesgo

Este proceso tiene como objetivo identificar, evaluar y reducir los riesgos de TI, considerando como meta de TI, la seguridad de la información, infraestructura de procesamiento y aplicaciones.

La institución financiera adoptado este proceso de COBIT aplicado por el área de Riesgo Operativo; el proceso de hardening ayudará a la práctica de identificar, analizar y gestionar el riesgo de los servidores a nivel de configuración.

La institución mediante la adopción de los procesos de COBIT requiere que como parte del plan operativo de Seguridad de la Información el realizar el diseño e implementación de blindaje de servidores iniciando por la infraestructura que soporta los servicios críticos del negocio, logrando así identificar el posible riesgo al que podría estar expuesto a nivel de configuración de servidores.

APO13 Gestionar la Seguridad

El objetivo de este proceso es definir, operar y supervisar el sistema de gestión de la seguridad de la información que considera como meta de TI asociada, la seguridad de la información, infraestructura de procesamiento y aplicaciones; la institución financiera adoptado el SGSI (Sistema de Gestión de la Seguridad de la Información), como parte de sus objetivos se considera realizar la gestión necesaria para la implementación del proceso de hardening.

El proceso de blindaje de servidores está conformado por 4 actividades:

Solicitud o Requerimiento: es la creación, validación del pedido que puede generar el negocio para la instalación y blindaje de servidores; es también enteder que realmente necesita el negocio con respecto al servidor.

Selección de línea base de seguridad: es identificar la o las líneas base de seguridad que un servidor debería cumplir.

Fortalecimiento del Activo: Implementar las líneas base en el servidor e identificar su nivel de cumplimiento.

Revisión del activo: validar que la configuración de seguridad cumple con la o las líneas base de seguridad que se aplicaron al servidor.

A continuación de detalla cada uno de los pasos del proceso de hardening de servidores.

4.2.1. Solicitud / Requerimiento

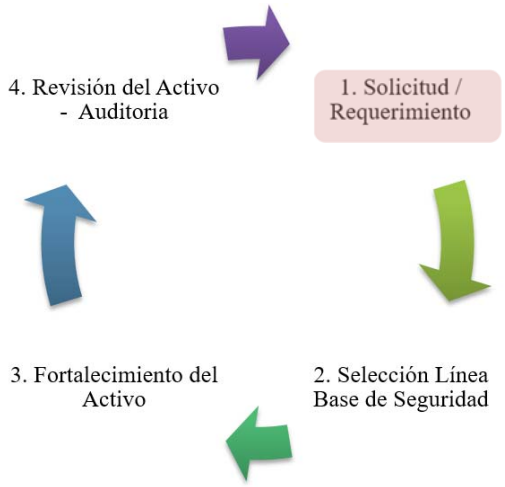


Figura 10 - Proceso de Hardening de servidores, paso 1.

Fuente: Elaborado por el autor de la investigación

Los procesos COBIT que ayudarán a la gestión de las solicitudes y requerimientos son BIA02 Gestionar la Definición de Requisitos, BAI06 Gestionar los Cambios.

BAI02 Gestionar la definición de Requisitos

Las solicitudes de nueva infraestructura o modificación sobre la existente pueden surgir por dos vías, la primera por proyectos o necesidades puntuales de las áreas de negocio y la segunda por soluciones que mitigan problemas, incidentes.

El proceso BAI02 nos ayudará a enfocarnos en la primera, para lograr una adecuada compresión, identificación y gestión de la necesidad que requiere el negocio. Las actividades que hay que considerar realizar son:

- El levantamiento del requerimiento sobre la infraestructura debe ser realizado por un equipo de trabajo conformado por personal de negocio y/o personal de proveedores y personal de TI.
- Los requerimientos deben ser claros, acordados, con la formalidad que la institución financiera lo ejecute, en este caso mediante un documento formal de análisis de requerimientos.
- El administrador de TI debe definir que la nueva infraestructura debe cumplir con la línea base de seguridad y que dentro de las pruebas a realizar sobre la solución debe ser considerado la de identificación y gestión de cierre de los incumplimientos a la línea base de seguridad.
- Realizar seguimiento y controlar el alcance de los requerimientos y los cambios a lo largo del ciclo de vida del requerimiento.
- Una vez realizado el requerimiento debe ser actualizada información interna como, inventario de servidores, procesos, aplicaciones con sus respectivas relaciones, versiones y estado de cumplimiento de la línea base de seguridad.

BAI06 Gestionar los cambios

El objetivo principal de este proceso es gestionar todos los cambios estándar o de mantenimiento en relación, a procesos, infraestructura y aplicaciones de manera controlada, esto nos ayudará a enfocarnos en la segunda alternativa de solicitud que son para solventar problemas y/o incidentes.

Las actividades que hay que considerar realizar son:

- La petición de cambio de configuración sobre infraestructura existente debe ser avaluado, priorizado, y autorizado por el dueño de la información y jefatura de infraestructura y producción.
- El analista de infraestructura y el oficial de seguridad deben participar activamente para identificar el impacto del cambio y en caso de llegar a un incumplimiento de la línea base de seguridad, de acuerdo al instructivo del Riesgo Operativo tecnológico de la institución, el nuevo riesgo deberá ser identificado, aprobado y tener un plan de acción o controles mitigantes.
- Los cambios debes ser programados, documentados y para lograr esto, el área responsable dentro de la institución financiera es la dirección de Control de calidad.
- Una vez realizado el cambio debe ser actualizada la información interna como, inventario de servidores, procesos, aplicaciones con sus respectivas relaciones, versiones y estado de cumplimiento de la línea base de seguridad.

4.2.2. Selección Línea Base de Seguridad

Figura 11 - Proceso de Hardening de servidores, paso 2.

Fuente: Elaborado por el autor de la investigación

Esta sección está enfocada a seleccionar la línea o líneas bases de seguridad que se aplicará:

- Si es para una nueva infraestructura, debe existir un requerimiento con las autorizaciones correspondientes, el requerimiento debe especificar el software que se requiere instalar, características de hardware, implementación de blindaje.
- El Administrador de las plataformas debe identificar la o las líneas bases de seguridad que deberán implementarse, por ejemplo, si a un servidor se instala el sistema operativo Windows, y base de datos SQL, las líneas base que deben aplicar son de cada una de las plataformas instaladas.
- En caso de que se trate de un cambio, se debe identificar línea base de seguridad que afecta el cambio. Esta actividad es responsabilidad del Administrador de las plataformas, y con ayuda del analista de seguridad deben identificar el impacto del cambio; si la modificación a realizar es un incumplimiento de la línea base de seguridad, el analista de seguridad debe ejecutar el

proceso de Riesgo Operativo de la institución; el nuevo riesgo deberá ser identificado, aprobado y tener un plan de acción o controles mitigantes.

Como parte de este trabajo también es realizar el levantamiento de dos líneas bases de seguridad de las plataformas priorizadas en el punto 4.1 que son Windows y Linux, esta actividad se realizará en la sección 4.2.5.

4.2.3. Fortalecimiento del activo

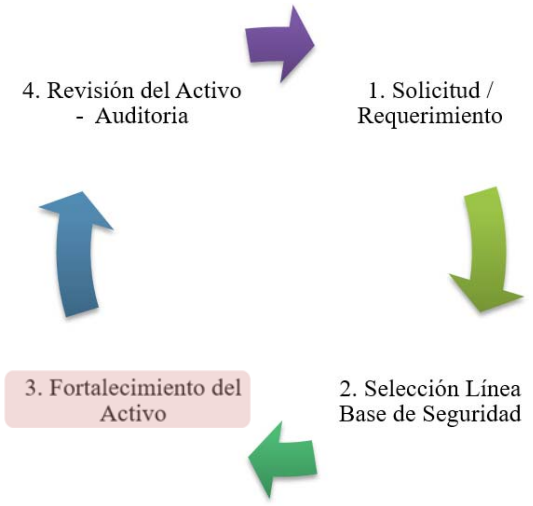


Figura 12 - Proceso de Hardening de servidores, paso 3.
Fuente: Elaborado por el autor de la investigación

Esta sección está enfocada a la implementación de la línea base de seguridad, el proceso que ayudará a brindar el servicio de blindaje de servidores es el DSS01 Gestionar Operaciones.

DSS01 Gestionar Operaciones

Este proceso tiene como objetivo coordinar y ejecutar las actividades y procedimientos operativos con el fin de entregar el servicio de TI a internos como externos.

La aplicación de la línea base de seguridad, es decir, configurar el servidor de acuerdo al estándar de seguridad, al final es una actividad operativa, que deriva en un servicio interno de TI.

Para la ejecución de la línea base de seguridad existe algunos prerrequisitos:

- Debe existir un requerimiento o una solicitud de cambio.
- Debe existir una validación del requerimiento o solicitud, con las aprobaciones respectivas.
- En caso de ser infraestructura nueva debe estar instalado el sistema Operativo y/o software base.
- En caso de ser un cambio, adicional debe existir la validación del impacto del cambio sobre software que ya exista en el servidor.

Con el cumplimiento de los prerrequisitos antes mencionados, el Administrador de infraestructura puede ejecutar la actividad de blindaje de acuerdo a lo programado internamente por el área. Las actividades que debe ejecutar el Administrador al aplicar la línea base de seguridad son:

1. Validar que todos prerrequisitos se encuentren listos.
2. Aplicar la o las líneas bases de seguridad en la nueva infraestructura.
3. En caso de tratarse de un cambio en la configuración de un servidor existente, obtener primero un respaldo de los archivos y configuraciones que van a ser modificadas y aplicar el cambio.
4. Reiniciar el servidor para que todas las configuraciones se apliquen.
5. Realizar pruebas de funcionalidad y operatividad del servidor y aplicación.
6. En la lista de verificación indicar si la configuración fue aplicada de manera exitosa (S) o no se puedo aplicar la configuración (N).

7. En caso de existir configuraciones que no se pudieron aplicar, notificar a la unidad de seguridad de la información para su análisis e identificación de controles complementarios e iniciar el proceso de riesgo operativo para la notificación y aceptación del riesgo.
8. Registrar en la ejecución de la actividad el número de configuraciones aplicadas y no aplicadas.
9. Actualizar el inventario de activos, indicando el estado de cumplimiento del servidor con respecto a la línea base de seguridad (número de ítems aplicados y número de ítems no aplicados).

4.2.4. Revisión del Activo - Auditoría

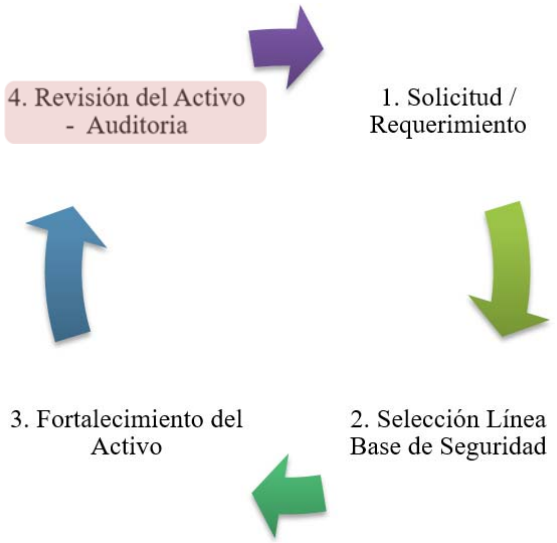


Figura 13 - Proceso de Hardening de servidores, paso 4.
Fuente: Elaborado por el autor de la investigación

Esta sección está enfocada a la revisión del cumplimiento de la línea base de seguridad, el proceso de COBIT que ayudará a realizar es MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno.

MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno

Este proceso tiene como propósito ofrecer transparencia a las partes interesada para generar confianza en las operaciones; una de las prácticas claves que considera este proceso es realizar auto evaluaciones del control.

La revisión del activo consiste es realizar una evaluación a lo implementado por el Administrador de las plataformas Windows o Unix, el área responsable de realizar la validación o verificación es la unidad de seguridad de la información de la institución financiera.

Para la revisión de la línea base de seguridad existe algunos prerrequisitos:

- El servidor se encuentre ejecutado el blindaje y el administrador haya notificado la terminación de sus actividades.
- El activo de estar registrado en el inventario con el estado de la implementación de blindaje de seguridad.

Con el cumplimiento de los prerrequisitos antes mencionados, la analista de Seguridad de la Información puede ejecutar la actividad de revisión de acuerdo a lo programado internamente por la unidad y tomando el checklist de la línea base ejecutada por el administrador de plataformas. Las actividades que debe ejecutar el Analista de seguridad de la información son:

1. Validar que todos prerrequisitos se encuentren listos.
2. Revisar de acuerdo a la lista de verificación de seguridad si todas las configuraciones se encuentran aplicadas.
3. Actualizar el estado del servidor con respecto al cumplimiento del blindaje en el inventario.
4. En caso de existir configuraciones que no pudieron ser implantadas, analizar el impacto y si existe controles complementarios para reducir su probabilidad de ocurrencia y/o su impacto.
5. Gestionar con el área de Riesgo operativo de la institución financiera la aceptación del riesgo.

4.2.5. Estándares de seguridad Windows / Linux

Existen varias fuentes para obtener información sobre configuración segura de una plataforma, buenas prácticas, recomendaciones de seguridad, mismas que están disponibles en el internet, publicadas en documentos electrónicos por grupos de profesionales como CIS® (Center for Internet Security, Inc.), entidades gubernamentales internacionales como NIST (National Institute of Standards and Technology), fabricantes de las plataformas como Microsoft, RedHat entre otros.

Para realizar la línea base de seguridad para la institución financiera se considerará las recomendaciones realizadas por NIST, ya que es un instituto dedicado a la administración de la tecnología del gobierno de Estados Unidos, su misión es promover la innovación y competitividad industrial para el gobierno.

NIST genera estándares para las industrias y productos que están relacionados de alguna manera con la tecnología, mismas que han sido reconocidas y aplicadas desde la creación de registros de salud electrónicos, relojes atómicos, industrias de ensamblaje de carros, creación de dispositivos a nano escala, entre otros. El aplicar las recomendaciones que propone NIST significa que el producto cumple con las especificaciones mínimas de seguridad de la información para ser utilizado en USA.

De la investigación realizada se identificaron varios fabricantes de herramientas de seguridad como Tenable (Dunn, 2017), Checkpoint, Fortinet, Juniper, Qualys (Qualys, 2019), Cisco entre otros, que brindan servicios de seguridad y recomiendan aplicar como mínimo las prácticas de seguridad de CIS Benchmark (Microsoft, 2018), la cual está conformada por una comunidad global de profesionales de TI experimentados y voluntarios del medio.

CIS crea estándares reconocidos a nivel mundial que contiene las mejores prácticas las cuales son refinadas, verificadas y comprobadas, esta fuente también será considerada para la generación de la línea base de seguridad propuesto en este documento de investigación.

Para conformar la línea base de seguridad (LBS) tanto para los sistemas operativos Windows como para Linux que mantiene la entidad financiera, se realizará una tabla comparativa de la existencias de controles de seguridad propuestos por NIST SP 800-123 (Karen Scarfone, 2008), CIS Benchmark (Benchmarks, 2018) y los propuestos por los propios fabricantes que para el caso de investigación son Microsoft y RedHat. Se definirá los controles que se recomendará a la institución financiera, mediante el análisis de lo propuesto en cada control por las guías consideradas.

En las siguientes secciones se muestran los cuadros comparativos junto con su análisis para conformar la línea base.

4.2.6. Línea base de seguridad plataforma Windows Server

De forma general, los documentos estudiados para el aseguramiento de Windows Server están conformados de la siguiente manera:

CIS Microsoft Windows Server 2012 Benchmark en su alcance abarca a servidores y controladores de dominio (Active Directory), el alcance para la institución es para servidores; la guía cuenta con 19 secciones; cada control está estructurado con descripción, configuración, auditoria e impacto que ayuda al lector a interpretar el objetivo del control (CIS Benchmark - Windows 2012, 2018).

En la figura 15 se muestra que las configuraciones de seguridad propuestas por CIS Benchmark siguen la estructura de “Directivas de Seguridad Local” que se encuentra en todo servidor Windows.

Para poder acceder a estas configuraciones es necesario ejecutar el comando “secpol.msc” en el inicio de Windows.

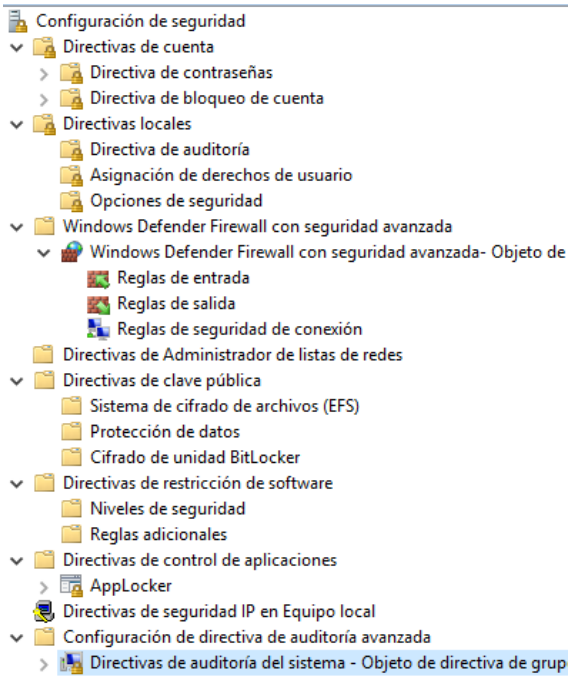


Figura 14 - Directivas de seguridad local, Windows

Fuente: Autor

NIST 800-123 su alcance está orientado a brindar recomendaciones para seleccionar, implementar y mantener los controles de seguridad necesarios en un servidor, el documento cuenta con 6 secciones de las cuales 2 están orientadas a la introducción y antecedentes, 4 secciones están orientadas a las recomendaciones de aseguramiento del sistema operativo (Karen Scarfone, 2008).

Microsoft Baseline está estructurado por varios documentos entre ellos el denominado SCM "Security Compliance Manager" que consta de las siguientes secciones: "Security Template, Advanced Auditing, Windows firewall, Computer, User", se detallan las recomendaciones para robustecer la seguridad del servidor (Margosis, Microsoft TechNet, 2014).

4.2.6.1. Análisis Comparativo de Guías Internacionales

Debido a la existencia de apartados comunes en las guías NIST, CIS y Microsoft Baseline, el siguiente cuadro muestra la existencia de cada control en cada una de ellas.

Las categorías propuestas en la tabla 2 fueron obtenidas de la agrupación lógica de los controles propuestos en cada una de las guías, por ejemplo, en las guías hablan de los tópicos de bloquear la cuenta cuando supere un número de intentos fallidos, la contraseña nueva del usuario no debe ser una contraseña antes utilizada, el equipo debe ser accedido localmente por personal autorizado como los administradores.

Los dos primeros tópico del ejemplo está enfocado a las características de la cuenta del usuario, serán agrupadas en la categoría política de cuenta el tercer tópico está enfocado a los accesos que debe tener el o los usuarios, será agrupada en la categoría derechos de usuario, sucesivamente se realiza con los controles de las guías hasta obtener a tabla 2 que se presenta a continuación.

Tabla 2 - Comparativa de guías de seguridad (CIS, NIST, Microsoft)
Fuente: Elaborado por el autor de la investigación

Categorías/ Controles	Nombre del Control	CIS	NIST	Microsoft
CAT1	**Preparación e Instalación**			
C1	Aislar el servidor en un segmento de red diferente al de producción		✔	

Categorías/ Controles	Nombre del Control	CIS	NIST	Microsoft
CAT2	**Parches de Seguridad**			
C2	Actualizar el Sistema Operativo		✔	
C3	Instalar parches de seguridad vigentes		✔	
CAT3	**Política de Cuentas**			
C4	Configurar longitud mínima de contraseña	✔	✔	✔
C5	Configurar el historial de contraseña	✔	✔	✔
C6	Habilitar complejidad de contraseña	✔	✔	✔
C7	Desactivar almacenamiento de contraseña con método de cifrado reversible.	✔	✔	✔
C8	Configurar política de bloqueo de cuenta	✔	✔	✔
CAT4	**Asignación de Derechos de Usuarios**			
C9	Permitir el acceso al servidor desde la red solo a los Administradores.	✔	✔	✔
C10	No otorgar a ningún usuario el privilegio “Act as part of the operating System”	✔	✔	✔
C11	Permitir logon local solo a los administradores.	✔	✔	✔
C12	Bloquear el uso de conexiones por RDP.	✔	✔	✔
C13	Permitir el cambio de zona horaria solo al administrador.	✔	✔	✔
C14	Permitir carga y descarga de controladores solo a los administradores	✔	✔	✔
C15	Administrar registros de auditoria y seguridad	✔	✔	✔
CAT5	**Opciones de Seguridad**			
C16	Deshabilitar cuenta invitado	✔	✔	✔
C17	Deshabilitar el apagado del equipo al no registrar las auditorías	✔	✔	✔
C18	Permitir expulsar y formatear medios extraíbles a los administradores	✔	✔	✔
C19	Restringir la instalación de controladores	✔	✔	✔
C20	Deshabilitar el envío de datos sin cifrar por SMB.	✔	✔	✔
C21	Renombrar la cuenta administrador.	✔	✔	✔
C22	Configurar mensaje de advertencia para el usuario que intenten ingresar al equipo.	✔	✔	✔
C23	Restringir visibilidad de último acceso	✔	✔	✔
C24	Establecer límite de inactividad del equipo	✔	✔	✔
CAT6	**Configuraciones de Seguridad de Red**			

Categorías/ Controles	Nombre del Control	CIS	NIST	Microsoft
C25	Configurar niveles de cifrado de Kerberos	✔	✔	✔
C26	Deshabilitar sesiones de tipo NULL.	✔	✔	✔
C27	No almacenar valores de hash de “LAN Manager”	✔	✔	✔
C28	Configurar cifrado de contraseñas utilizando MTLMv2	✔	✔	✔
C29	Desconectar los usuarios al expirar su tiempo de sesión.	✔	✔	✔
C30	Restringir el acceso a servicios como RDP y VNC.	✔	✔	✔
C31	Restringir el acceso anónimo a los recursos compartidos	✔	✔	✔
CAT7	**Configuraciones de Firewall**			
C32	Habilitar el firewall de Windows	✔	✔	✔
C33	Restringir conexiones entrantes	✔	✔	✔
C34	Permitir conexiones de salida	✔	✔	✔
C35	Registrar conexiones exitosas	✔	✔	✔
CAT8	**Configuraciones de políticas de Auditorías**			
C36	Registrar inicio y cierre de sesión	✔	✔	✔
C37	Registrar creación y finalización de procesos	✔	✔	✔
C38	Registrar la administración de cuentas	✔	✔	✔
C39	Registrar modificaciones en las políticas	✔	✔	✔
C40	Registrar actividades de usuarios privilegiados.	✔	✔	✔
C41	Registrar eventos de acceso a los objetos	✔	✔	
CAT9	**Configuraciones Adicionales**			
C42	Registrar eventos	✔		
C43	Restringir acceso mediante grupos	✔		
C44	Deshabilitar o desinstalar servicios no utilizados	✔	✔	
C45	Asegurar que todos los volúmenes utilicen NTFS	✔		
C46	Controlar el acceso a las redes que interactúan con el equipo	✔		
C47	Configurar directivas de clave pública	✔		
C48	Configurar directivas de restricción de software	✔		
C49	Configurar directivas de control de aplicaciones	✔	✔	

Categorías/ Controles	Nombre del Control	CIS	NIST	Microsoft
C50	Configurar directivas de seguridad de IP (VPN)	✔		

De la tabla anterior, se puede decir que tanto la guía de CIS Benchmark y Microsoft Baseline utilizan muchos controles similares para el aseguramiento de un equipo Windows, sin embargo, el Baseline no está limitado a una determinada versión de sistema operativo pudiendo ser aplicado no sólo a servidores sino a equipos de usuario final.

Los controles de la guía de CIS se centran específicamente en servidores por lo que es un fuerte complemento a lo propuestos por Microsoft.

Si evaluamos la propuesta de los controles de NIST 800-123, se puede evidenciar que esta guía considera pasos preliminares que ayudan a proteger al servidor de amenazas desde su instalación, las recomendaciones son de alto nivel, es decir sus recomendaciones definen que debe tener la institución para asegurar el sistema operativo, mas no como se debe implementar el blindaje, los controles de la guía NIST se armonizan con controles previamente implementados por otras guías de seguridad.

Así mismo, se puede evidenciar que CIS cuenta con controles adicionales de seguridad que están enfocados en registro de eventos, directivas de control de programas entre otros que se encuentran listados en la categoría 9 (Configuraciones adicionales) y que no son completamente estudiados por el resto de guías pero que son de gran utilidad al momento de analizar eventos de seguridad en equipos de producción ya que pueden ser correlacionados para obtener información oportuna de accesos no autorizados.

De forma general, las categorías obtenidas de las 3 guías de seguridad estudiadas, se puede resumir en el gráfico 16, en donde se puede ver que NIST tiene mayor número de categorías que

se pueden utilizar, sin embargo, la diferencia con las otras guías no es muy grande, por lo que pueden ser complementarias al estudio de la línea base de seguridad.

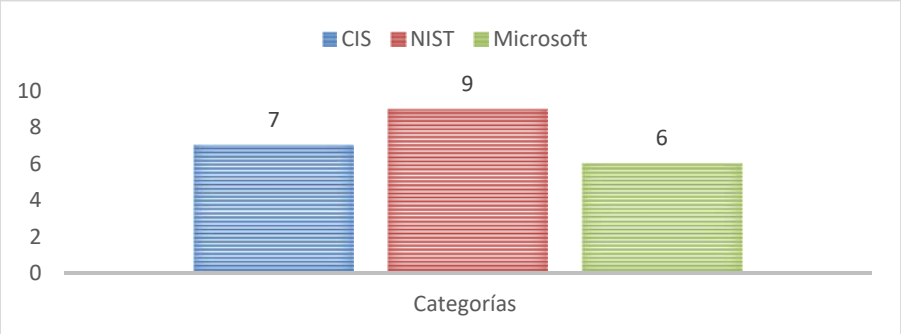


Figura 15 – Categorías de CIS, NIST, Microsoft baseline

Fuente: Elaborado por el autor de la investigación

En la figura 17 que muestra el porcentaje de controles por guía, donde se puede ver que, NIST800-123 como CIS Benchmark proponen la mayor cantidad de recomendaciones para fortalecer la seguridad en el sistema operativo Windows.

Además, se puede visualizar que si se adopta una u otra guía, estaríamos omitiendo configuraciones y el nivel de seguridad del sistema operativo se afectaría.

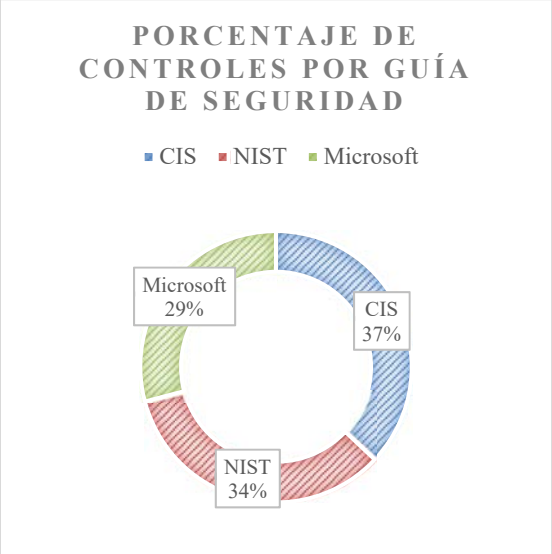


Figura 16 – Porcentaje de controles de las guías (CIS, NIST, Microsoft)

Fuente: Elaborado por el autor de la investigación

En la figura 18 se muestra la cantidad de controles por categoría y por guía de seguridad; en la que se puede observar que se tiene similar número de controles en las categorías 3 al 7.

Esta similitud se genera principalmente porque las guías de CIS Benchmark y Microsoft utilizan para su propuesta de controles la estructura las directivas de seguridad local de la plataforma Windows como se muestra en la figura 15.

NIST 800-123 propone recomendaciones de alto nivel en las categorías 3 al 7, por ejemplo, la configuración de longitud de contraseña de acuerdo a CIS y Microsoft es de 14 o más caracteres, pero de acuerdo a los editores de NIST 800-123 en lugar de sugerir un valor a la longitud de contraseña indica que “Longitud: establecer una longitud mínima para las contraseñas.” (Karen Scarfone, 2008, págs. 4-5).

Del ejemplo antes expuesto se puede concluir que las 3 guías contemplan el tópico de establecer una longitud de contraseña.

También se puede ver que las categorías 1 y 2, que corresponden a la preparación y validación de parches, muestran únicamente controles aplicables mediante NIST 800-123, esto surge ya que esta guía incluye un conjunto de controles de alto nivel y no muestra un detalle técnico a profundidad de las configuraciones de seguridad.

En la categoría 9 que trata de configuraciones adicionales se observa que CIS tiene mayor prevalencia en contraste con el resto de guías, pero en este documento se puede ver que no existen configuraciones técnicas y solo lo sugiere como complemento a la directiva local de seguridad, además también se puede ver que el proveedor no expresa ningún control es la categoría 9.

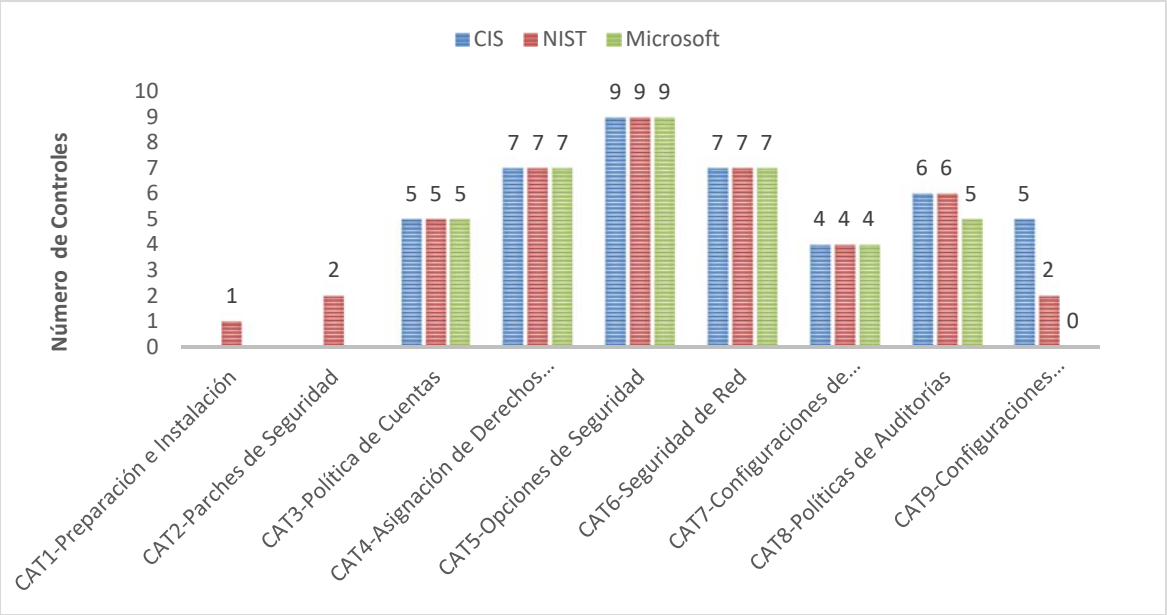


Figura 17 - Cantidad de controles por categoría (CIS, NIST, Microsoft)

Fuente: Elaborado por el autor de la investigación

La figura 18 también muestra que NIST 800-123 está presente en todas las categorías mientras que la guía de CIS Benchmark no está presente en las categorias1 y 2; de igual manera la guía de Microsoft no está presente en las categorías 1, 2 y 9.

Otro punto de interés es que con la unión de controles de las categorías 4, 5 y 6 se abarcarían 25 controles de los 50 propuestos en la tabla 2, esto representa el 50%; podríamos a atrevernos a decir que estas categorías son esenciales para formar la línea base de seguridad para la institución.

Para la conformación de la propuesta en relación al aseguramiento de Windows Server, se realiza un estudio de las categorías y controles listados previamente en la tabla 2.

4.2.6.2. Diseño Línea Base Windows

En las siguientes tablas se realizará el análisis de los controles por categoría, cada tabla estará conformada por: el nombre de la categoría, a la izquierda el número de control, seguido del control y a la derecha se encuentra las referencias de cada una de las guías según aplique para cada control.

Tabla 3 - Análisis categoría 1- Preparación e Instalación

Fuente: Elaborado por el autor de la investigación

CAT1	Preparación e Instalación	
Categorías/ Controles	Control	Evaluación de Guías de Seguridad
C1	Aislar el servidor en un segmento de red diferente al de producción	2.3 NIST 800-123
Análisis: Validaciones para este apartado existen únicamente en NIST, en donde se propone una planificación previa antes de realizar los procesos de aseguramiento del servidor. Una de las recomendaciones hace relación al uso de firewalls, routers para filtrado de paquetes y proxy para el aislamiento y posterior protección del nuevo servidor. Además NIST tiene un documento específico dedicado íntegramente a la configuración de firewalls que se denomina NIST SP 800-41, Guidelines on Firewalls and Firewall Policy.		

Tabla 4 - Análisis categoría 2 - Parches de Seguridad

Fuente: Elaborado por el autor de la investigación

CAT2	Parches de Seguridad	
Categorías/ Controles	Control	Evaluación de Guías de Seguridad

C2	Actualizar el Sistema Operativo	4.1 NIST 800-123
C3	Instalar parches de seguridad vigentes	

Análisis:
De acuerdo a NIST, una vez que el sistema ha sido instalado, se deben aplicar los parches y actualizaciones de sistema para solventar problemas de seguridad.
La entidad financiera debe validar que una actualización o aplicación de determinado parche no interfiera con las funcionalidades del servidor, por ejemplo, servicio web, base de datos, correo electrónico entre otros.

Tabla 5 - Análisis Categoría 3 - Política de Cuentas

Fuente: Elaborado por el autor de la investigación

CAT3	**Política de Cuentas**			
Categorías/ Controles	Control	Evaluación de Guías de Seguridad		
		CIS Benchmark	NIST 800-123	Microsoft Baseline
C4	Configurar longitud mínima de contraseña	1.1	4.2	Security Template
		14 o más caracteres	No definido	14 caracteres
Análisis: Definir una longitud grande de caracteres para passwords ayuda a evitar ataques de fuerza bruta que permita el acceso no autorizado al servidor. De acuerdo a un estudio realizado en el año 2010 por ingenieros del Georgia Institute of Technology en donde ¨los investigadores utilizaron agrupaciones de tarjetas gráficas para romper claves de 8 caracteres en menos de 2 horas; pero usando el mismo método con 12 caracteres, romper la contraseña tomaría 17134 años.” (Sutter, 2010), se puede concluir que una contraseña de 14 caracteres según lo propuesto por las guías CIS y Microsoft es adecuada, ya que, si consideramos que en el 2019 contamos con hardware más potente que el usado en los experimentos citados en el 2010, romper claves de menor longitud no sería mayor complejidad para un atacante.				
C5	Configurar el historial de contraseña	1.1	4.2	Security Template
		60 o menos	No definido	60
Análisis:				

<table>
<tr><th>CAT3</th><th colspan="4">Política de Cuentas</th></tr>
<tr><td rowspan="2">Categorías/ Controles</td><td rowspan="2">Control</td><td colspan="3">Evaluación de Guías de Seguridad</td></tr>
<tr><td>CIS Benchmark</td><td>NIST 800-123</td><td>Microsoft Baseline</td></tr>
<tr><td colspan="5">El historial de contraseña representa el número de passwords que el sistema recordará antes que pueda ser reutilizada.
Esta característica es importante para evitar que un atacante pueda romper credenciales siguiendo un patrón establecido, pero justamente este es el problema que se enfrentan todas las instituciones, de acuerdo a un estudio propuesto por SANS en donde la empresa evaluada indica que “pedimos a los usuarios que roten sus contraseñas con más frecuencia que la mayoría. Para nuestros usuarios más sensibles, eso es cada 30 días.” (Stevens, 2017), sin embargo, en los resultados de Stevens se muestra que durante el proceso de cracking la diferencia entre una política de rotación de 30 días y algo más no va a hacer mucha diferencia, esto por el uso de claves como password1, password2, password3 sucesivamente.
Para la conformación de la línea base, se propone el uso de 60 veces con la final.</td></tr>
<tr><td>C6</td><td>Habilitar complejidad de contraseña</td><td>1.1 CIS</td><td>4.2 NIST</td><td>Security Template - Microsoft</td></tr>
<tr><td colspan="5">Análisis:
De acuerdo al estudio realizado en 2017 en la publicación NIST 800-63B en donde se identifica que esta atributo de complejidad de contraseña requiere que se implemente también el control de validar la contraseña con un listado de passwords inaceptables “lista negra”, el motivo es porque los usuarios son predecibles al momento de generar su contraseña (Paul A. Grassi, 2017).
Se propone que la institución financiera adopte este control y la recomendación adicional realizada en la publicación NIST 800-63B.</td></tr>
<tr><td>C7</td><td>Desactivar almacenamiento de contraseña con método de cifrado reversible.</td><td>1.1 CIS</td><td>4.2 NIST</td><td>Security Template - Microsoft</td></tr>
<tr><td colspan="5">Análisis:
Desactivando esta característica se obliga al sistema a utilizar un método de cifrado de contraseñas robusto que es menos susceptible a ataques, es decir si la contraseña se almacena con cifrado reversibles un atacante puede romper este cifrado y utilizar el acceso a los recursos de la red con la cuenta comprometida (Microsoft, 2017).
Se propone que la institución financiera adopte este control, ayuda a fortalecer la confidencialidad de la contraseña.</td></tr>
<tr><td rowspan="2">C8</td><td rowspan="2">Configurar política de bloqueo de cuenta</td><td>1.1 CIS</td><td>4.2 NIST</td><td>Security Template - Microsoft</td></tr>
<tr><td>10 o menos intentos</td><td>3 intentos</td><td>10 intentos</td></tr>
</table>

CAT3	Política de Cuentas			
Categorías/ Controles	Control	Evaluación de Guías de Seguridad		
		CIS Benchmark	NIST 800-123	Microsoft Baseline
Análisis: Para contrarrestar técnicas de cracking de contraseñas las instituciones generalmente definen un número de intentos antes que el password quede inhabilitado. De acuerdo a la publicación de NIST 800-63B establecer un número de intentos de inicio de sesión es una mitigante para evitar que un atacante mediante fuerza bruta pueda conseguir acceso no autorizado (Paul A. Grassi, 2017). Las guías de CIS Benchmark y Microsoft proponen 10 intentos fallidos, sin embargo, este número puede permitir una ventana de ataque suficiente para un individuo mal intencionado y con conocimiento en este tipo de ataques, por lo que reducir la cantidad de pruebas que pueda realizar un atacante es importante para la seguridad del servidor por ello se sugiere adoptar el uso de 3 intentos como lo indica NIST 800-123.				

Tabla 6 - Análisis de la categoría 4 - Asignación de Derechos de Usuarios

Fuente: Elaborado por el autor de la investigación

CAT4	Asignación de Derechos de Usuarios			
Categorías/ Controles	Control	Evaluación de Guías de Seguridad		
		CIS Benchmark	NIST 800-123	Microsoft Baseline
C9	Permitir el acceso al servidor desde la red solo a los Administradores.	2.2	5.2	Security Template
C10	No otorgar a ningún usuario el privilegio “Act as part of the operating System”	2.2	5.2	Security Template
C11	Permitir logon local solo a los administradores.	2.2	5.2	Security Template
C12	Bloquear el uso de conexiones por RDP.	2.2	5.2	Security Template
C13	Permitir el cambio de zona horaria solo al administrador.	2.2	5.2	Security Template
C14	Permitir carga y descarga de controladores solo a los administradores	2.2	5.2	Security Template
C15	Administrar registros de auditoria y seguridad	2.2	5.2	Security Template

CAT4	Asignación de Derechos de Usuarios			
Categorías/ Controles	Control	Evaluación de Guías de Seguridad		
		CIS Benchmark	NIST 800-123	Microsoft Baseline
Análisis: La guía NIS 800-123 detalla la recomendación de manera global como deben limitarse los accesos al recurso del servidor, por lo cual se sugiere adoptar las directrices indicadas por las guías de CIS Benchmaks y del proveedor Microsoft, ya que en ellas se evidencia los parámetros que debe configurase. De acuerdo a la publicación de Andrea Bichsel técnico sénior de Microsoft en donde indica que estos controles permiten establecer las directrices mediante las cuales un usuarios puede iniciar sesión con credenciales de administrador, acceder a recursos del equipo, administrar cuotas de memoria, así como añadir estaciones de trabajo al dominio entre otros (Andrea Bichsel - Microsoft, 2017).				

Tabla 7 - Análisis de categoría 5 - Opciones de Seguridad

Fuente: Elaborado por el autor de la investigación

CAT5	Opciones de Seguridad			
Categorías/ Controles	Control	Evaluación de Guías de Seguridad		
		CIS Benchmark	NIST 800-123	Microsoft Baseline
C16	Deshabilitar cuenta invitado	2.3	4.2 y 5.1	Security Template
C17	Deshabilitar el apagado del equipo al no registrar las auditorías	2.3	4.2 y 5.1	Security Template
C18	Permitir expulsar y formatear medios extraíbles a los administradores	2.3	4.2 y 5.1	Security Template
C19	Restringir la instalación de controladores	2.3	4.2 y 5.1	Security Template
C20	Deshabilitar el envío de datos sin cifrar por SMB.	2.3	4.2 y 5.1	Security Template
C21	Renombrar la cuenta administrador.	2.3	4.2 y 5.1	Security Template
C22	Configurar mensaje de advertencia para el usuario que intenten ingresar al equipo.	2.3	4.2 y 5.1	Security Template
C23	Restringir visibilidad de último acceso	2.3	4.2 y 5.1	Security Template
C24	Establecer límite de inactividad del equipo	2.3	4.2 y 5.1	Security Template

CAT5	Opciones de Seguridad			
Categorías/ Controles	Control	Evaluación de Guías de Seguridad		
		CIS Benchmark	NIST 800-123	Microsoft Baseline
C16	Deshabilitar cuenta invitado	2.3	4.2 y 5.1	Security Template
Análisis: Las guías técnicas proponen los controles expuestos en esta categoría, de los cuales se puede evidenciar que su objetivo es definir el comportamiento del equipo localmente como, por ejemplo, el estado de cuenta del usuario "invitado", que permite acceso a usuarios que no necesariamente tienen acceso al equipo. Restringir la instalación de software fortalece que se active, servicios, puertos e incluso usuarios no autorizados, auditar los objetos del sistema, permite monitorear la actividad que se realiza con los objetos. De los ejemplos que hemos dado se puede evidenciar que los controles que se encuentran en esta categoría son esenciales para el blindaje del sistema operativo.				
C24	Establecer límite de inactividad del equipo	2.3 CIS	4.2 y 5.1 NIST	Security Template - Microsoft
		900 segundos o menos	No definido	900 segundos
Análisis: El tiempo de inactividad ayuda a bloquear la pantalla del usuario solicitando el ingreso nuevamente de sus credenciales, esto en caso de olvido de bloqueo en caso de quedar desatendido el equipo. El tiempo propuesto por CIS y Microsoft es de 15 minutos, en algunas empresas podrá suponer un corto tiempo, sin embargo, hay que considerar las nuevas técnicas de intrusión mediante dispositivos USB que ejecutan acciones sin interacción del usuario, como es USB Rubber Ducky, de acuerdo al fabricante de esta herramienta "15 segundos de acceso físico y un USB Rubber Ducky es todo lo que se necesita para robar las contraseñas de una PC desatendida." (Hack5, 2017) Por lo expuesto, se ha considerado recomendar a la institución un tiempo de 3 minutos para protección de sesiones, considerando que con este valor aún quedan brechas de seguridad para este tipo de dispositivos sin embargo, un tiempo menor dificultaría las tareas de gestión en sitio del servidor.				

Tabla 8 – Análisis de la categoría 6 - Configuraciones de Seguridad de Red

Fuente: Elaborado por el autor de la investigación

CAT6	Configuraciones de Seguridad de Red			
Categorías/ Controles	Control	Evaluación de Guías de Seguridad		
		CIS Benchmark	NIST 800-123	Microsoft Baseline

C25	Configurar niveles de cifrado de Kerberos	2.3	4.2 y 4.3	Security Template
C26	Deshabilitar sesiones de tipo NULL.	2.3	4.2 y 4.3	Security Template
C27	No almacenar valores de hash de "LAN Manager"	2.3	4.2 y 4.3	Security Template
C28	Configurar cifrado de contraseñas utilizando MTLMv2	2.3	4.2 y 4.3	Security Template
C29	Desconectar los usuarios al expirar su tiempo de sesión.	2.3	4.2 y 4.3	Security Template
C30	Restringir el acceso a servicios como RDP y VNC.	2.3	4.2 y 4.3	Security Template
C31	Restringir el acceso anónimo a los recursos compartidos	2.3	4.2 y 4.3	Security Template

Análisis:
Los controles que se encuentran en esta categoría están orientados a la restricción de servicios o protocolos como SMB "Server Message Block", RDP "Remote Desktop Protocol", también considera evitar que usuarios no autorizados enumeren credenciales que se encuentren en cache, mantener la comunicación entre servidores sea lo más segura posible, e incluso evitando que un usuario esté conectado fuera de su horario de inicio de sesión asignadas.
Los controles pretenden evitar que los atacantes mediante la suplantación de identidad, sesión o por protocolos activos innecesarios puedan obtener acceso no autorizado a modificar paquetes o realizar una denegación del servicio.
De acuerdo a lo expuesto por Jakub Kroustek analista de ingeniería inversa de Avast indica que el vector de infección de ransomware WannaCriptOr 2.0 es mediante el aprovechamiento de la vulnerabilidad de Windows en el protocolo SMB, "el ransomware se vuelve particularmente molesto cuando infecta instituciones como hospitales, donde puede poner en riesgo la vida de los pacientes" (Kroustek, 2017).

Tabla 9 - Análisis de la categoría 7 - Configuraciones de Firewall

Fuente: Elaborado por el autor de la investigación

CAT7	Configuraciones de Firewall			
Categorías/ Controles	Control	Evaluación de Guías de Seguridad		
		CIS Benchmark	NIST 800-123	Microsoft Baseline
C32	Habilitar el firewall de Windows	9	5.3	Windows Firewall
C33	Restringir conexiones entrantes	9	5.3	Windows Firewall
C34	Permitir conexiones de salida	9	5.3	Windows Firewall

CAT7	Configuraciones de Firewall			
Categorías/ Controles	Control	Evaluación de Guías de Seguridad		
		CIS Benchmark	NIST 800-123	Microsoft Baseline
C35	Registrar conexiones exitosas	9	5.3	Windows Firewall
Análisis: Los controles de esta categoría proporcionan un filtrado de tráfico de red bidireccional basado en el host (Andrea Bichsel - Microsoft, 2017). Las reglas personalizadas permiten un mejor nivel de control sobre el tráfico entrante y saliente. De acuerdo a lo expuesto por Manoj Kumar indica que el firewall es una barrera por la cual pasa el tráfico de red y que mediante políticas permite o no el paso del tráfico, además, ante el descubrimiento de una falla de seguridad, cada sistema potencialmente afectado debe actualizarse para corregir esa falla, el firewall es una solución que se inserta entre la red local y el Internet para establecer un enlace controlado. El objetivo de este perímetro es proteger la red de accesos no autorizados por los ataques y proporcionar un único punto de mitigación donde se pueda establecer una regla de seguridad (Kumar, 2008).				

Tabla 10 - Análisis de la categoría 8 - Políticas de Auditorías

Fuente: Elaborado por el autor de la investigación

CAT8	Configuraciones de políticas de Auditorías			
Categorías/ Controles	Control	Evaluación de Guías de Seguridad		
		CIS Benchmark	NIST 800-123	Microsoft Baseline
C36	Registrar inicio y cierre de sesión	17	3.3	Advanced Auditing
C37	Registrar creación y finalización de procesos	17	3.3	Advanced Auditing
C38	Registrar la administración de cuentas	17	3.3	Advanced Auditing
C39	Registrar modificaciones en las políticas	17	3.3	Advanced Auditing
C40	Registrar actividades de usuarios privilegiados.	17	3.3	Advanced Auditing
C41	Registrar eventos de acceso a los objetos	17	3.3	No definido
Análisis: Los controles que se encuentran en esta categoría están orientados a registrar los distintos eventos como, inicio y cierre de sesión, actividades de los usuarios administradores, modificaciones sobre configuraciones, servicios, procesos entre otros.				

CAT8	Configuraciones de políticas de Auditorías			
Categorías/ Controles	Control	Evaluación de Guías de Seguridad		
		CIS Benchmark	NIST 800-123	Microsoft Baseline
Como expone Shruchi Mistry en su documento "La auditoría en un sistema operativo se puede utilizar para la identificación de actividades maliciosas del usuario, investigación forense del sistema y el cumplimiento de la seguridad" (Mistry, 2018) Los controles mostrados en las categorías deben ser adoptadas por la institución financiera				

Tabla 11 - Análisis de categoría 9 - Configuraciones Adicionales

Fuente: Elaborado por el autor de la investigación

CAT9	Configuraciones Adicionales			
Categorías/ Controles	Control	Evaluación de Guías de Seguridad		
		CIS Benchmark	NIST 800-123	Microsoft Baseline
C42	Registrar eventos	3		
C43	Restringir acceso mediante grupos	4		
C44	Deshabilitar o desinstalar servicios no utilizados	5	4.2	
C45	Asegurar que todos los volúmenes utilicen NTFS	6		
C46	Controlar el acceso a las redes que interactúan con el equipo	10		
C47	Configurar directivas de clave pública	12		
C48	Configurar directivas de restricción de software	13		
C49	Configurar directivas de control de aplicaciones	15	5	
C50	Configurar directivas de seguridad de IP (VPN)	16		
Análisis: Los controles que se encuentran en esta categoría corresponden a configuraciones que para su aplicación requiere un análisis más detallado por parte de la institución. Su aplicación no corresponde únicamente a activar o desactivar sus parámetros, en algunos controles es necesario más detalle de la función que desempeñará el servidor. Para la conformación de la línea base se utilizarán estos controles para cerrar el ciclo de validaciones que son propuestas por la guía de CIS en sistemas Windows.				

4.2.7. Línea base de seguridad plataforma RedHat

De forma similar a la línea base de Windows, los documentos estudiados para conformar las recomendaciones de aseguramiento de Red Hat son CIS Benchamark, NIST 800-123 y las validaciones proporcionadas por el fabricante.

La diferencia en relación a las configuraciones de seguridad para este sistema operativo radica en el uso de archivos destinados para el aseguramiento del equipo mientras que en Windows las configuraciones de seguridad son estructuradas en base a la directiva local de la plataforma.

4.2.7.1. Análisis Comparativo de Guías Internacionales

La siguiente tabla muestra la distribución de categorías y controles que fueron obtenidas de las distintas guías.

Hay que recordar que el aporte de recomendaciones de alto nivel viene dado por NIST 800-123 mientras que las directrices técnicas son proporcionadas por CIS Benchmark y Red Hat.

Las categorías propuestas en la tabla 12 fueron obtenidas de la agrupación lógica de los controles propuestos en cada una de las guías, por ejemplo, las guías recomiendan establecer una contraseña para el BIOS, al igual que se debe considerar particiones distintas para algunos directorios, también indican que se restrinja o elimine servicios innecesarios. Los dos primeros controles están enfocados al momento de la instalación, se crea una categoría “Preparación e instalación”, el tercer control pertenecerá a la categoría “Configuración de servicios”, así para todos los controles identificados de las 3 guías.

Tabla 12 - Comparativa de guías de seguridad (CIS, NIST, RedHat)

Fuente: Elaborado por el autor de la investigación

Categorías /Controles	Control	CIS Benchmark	NIST 800-123	REDHAT
CAT1	**Preparación e Instalación**			
C1	Aislar el servidor en un segmento de red diferente al de producción		✔	✔
C2	Configurar password para BIOS/firmware	✔		✔
C3	Crear particiones separadas para los directorios / boot, /, / home / tmp y / var / tmp /	✔		✔
CAT2	**Parches de Seguridad**			
C4	Actualizar el Sistema Operativo	✔	✔	✔
C5	Instalar parches de seguridad vigentes	✔	✔	✔
C6	Limitar la descarga automática de actualizaciones	✔		
CAT3	**Configuración Sistema de archivos**			
C7	Restringir el montaje de sistemas de archivos no necesarios como cramnfs, freevxfs, entre otros	✔	✔	
C8	Restringir la ejecución de aplicaciones en los directorios temporales y home	✔		✔
C9	Restringir el montaje automático de directorios.	✔		
C10	Verificar la integridad de los archivos de configuración	✔		✔
C11	Configurar advertencias de seguridad	✔		
CAT4	**Configuración de Servicios**			
C12	Deshabilitar servicios de red innecesarios	✔	✔	✔
C13	Configurar la sincronización automática de la hora	✔	✔	
CAT5	**Configuraciones de Seguridad de Red**			
C14	Desactivar IP Forwarding	✔		✔
C15	Deshabilitar reenvío de paquetes	✔		✔
C16	Ignorar respuestas de broadcast de ICMP	✔		✔
C17	Permitir acceso solo a las IP's autorizadas	✔		✔
C18	Restringir el acceso a los archivos /etc/hosts.allow y /etc/hosts.deny	✔		✔
CAT6	**Configuraciones de Firewall**			
C19	Instalar iptables	✔		
C20	Restringir conexiones entrantes ICMP	✔		✔

Categorías /Controles	Control	CIS Benchmark	NIST 800-123	REDHAT
C21	Configurar las conexiones salientes permitidas	✔	✔	✔
CAT7	**Registro y Auditorias**			
C22	Configurar el tamaño de los archivos de registro.	✔		✔
C23	Deshabilitar el sistema cuando los registros de auditoria estén completos	✔		✔
C24	Restringir la eliminación automática de los registros de auditoria	✔		✔
C25	Activar el servicio de auditoria	✔		✔
C26	Registrar modificaciones a fecha y hora del equipo	✔		
C27	Registrar modificaciones a usuarios y grupos	✔		✔
C28	Registrar modificaciones a la configuración del entorno red.	✔		
C29	Registrar inicio/cierre de sesiones	✔		
C30	Registrar intentos de acceso no autorizado.	✔	✔	
C31	Registrar uso de comandos privilegiados	✔		
C32	Registrar cambios en el ámbito de administración del sistema (sudoers)	✔		
C33	Registrar acciones del administrador	✔		
C34	Restringir los cambios sobre la configuración de auditoria.	✔	✔	
C35	Activar los servicios de rsyslog, syslog-ng	✔		
C36	Permitir el acceso controlado al archivo rsyslog	✔		
C37	Revisar los permisos a los log files estén configurados	✔		
CAT8	**Configuración de SSH**			
C38	Permitir el acceso controlado al archivo /etc/ssh / sshd_config	✔		
C39	Activar el protocolo SSH versión 2	✔		
C40	Registrar inicio y cierre de sesión ssh	✔		
C41	Restringir el inicio de sesión directo con el usuario root.	✔		✔
C42	Restringir el inicio de sesión a usuarios sin contraseña	✔		
C43	Restringir a los usuarios a establecer variables de entorno	✔	✔	
C44	Establecer tiempo de inactividad de la sesión SSH	✔		

Categorías /Controles	Control	CIS Benchmark	NIST 800-123	REDHAT
C45	Restringir los usuarios puede acceder a través de SSH.	✔	✔	
CAT9	**Política de Cuentas**			
C46	Configurar longitud mínima de contraseña	✔	✔	✔
C47	Configurar el historial de contraseña	✔	✔	✔
C48	Habilitar complejidad de contraseña		✔	
C49	Activar el algoritmo SHA-512 para contraseñas	✔		
C50	Configurar política de bloqueo de cuenta	✔	✔	✔
C51	Definir vigencia de contraseña	✔		✔
C52	Restringir el login a cuentas del sistema	✔		✔
C53	Advertir el cambio de contraseña antes de su caducidad	✔		
C54	Bloquear contraseñas inactivas	✔		
C55	Restringir el acceso al comando su	✔		
C56	Validar que el grupo GID 0 sea solo del usuario root	✔		
CAT10	**Mantenimiento del sistema**			
C57	Restringir el acceso a los archivos sensibles (passwd, shadow,group, gshadow) y a sus backups	✔	✔	
C58	Validar que no exista directorios sin propietario	✔		
C59	Validar que los campos de contraseñas no estén vacíos	✔		
C60	Validar que solo el usuarios root tenga UID 0	✔		
C61	Validar que los accesos a directorios personales existan y estén restringidos.	✔		
C62	Validar que no exista usuarios y grupos duplicados	✔		

Como se puede observar, la tabla 12 muestra una mayor cantidad de controles que son propuestos mediante las guías de CIS Benchmark, sin embargo, existen controles en NIST 800-123 y Red Hat que se complementan tanto en el lineamiento teórico como en lo técnico, por ejemplo, el control 50 de la configuración de la política de bloqueo de cuenta, en este

caso NIST 800-123 da las recomendaciones teóricas mientras que CIS y Red Hat abordan con mayor detalle técnico las configuraciones de seguridad.

En la figura 18 se presenta la cantidad de controles que abarcan cada una de las guías, evidenciando que las validaciones que más cubren aspectos de seguridad está contenida en la guía de CIS Benchmark, esto se debe principalmente a que esta organización desarrolla documentos específicos para cada sistema operativo, mientras que NIST 800-123 son recomendaciones de alto nivel sin entrar a mayor detalle de la configuración.

Por otro lado, la guía de Red Hat tiene entre sus documentos una guía de aseguramiento para su sistema operativo, pero al compararlo con CIS se observa que tiene menor propuesta de controles, pero no necesariamente están embebidas dentro de CIS como por ejemplo el control 1 que trata sobre aislar en un segmento de red diferente al de producción, este control no existe en CIS Benchmark.

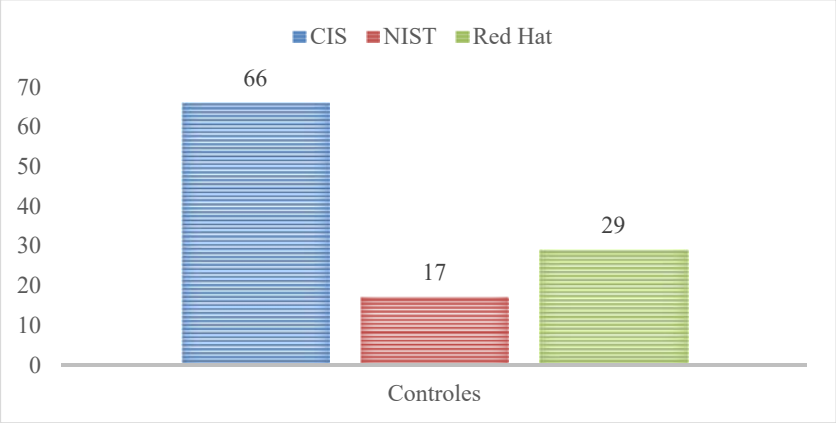


Figura 18 - Controles por cada guía (CIS, NIST, RedHat)

Fuente: Elaborado por el autor de la investigación

En la figura 19 se puede evidenciar que la totalidad de controles propuestos en la tabla 12, CIS Benchmark tiene el 59% de los controles propuestos, mientras que la guía del fabricante Red Hat tiene el 26% y NIST 800-123 el 15%. También se puede interpretar que la guía CIS Benchmark

por sí sola no cubre la totalidad de los controles de seguridad identificados en la tabla 12, entonces para la línea base de seguridad para la institución se propone considerar una combinación de los controles propuestos por las 3 guías.

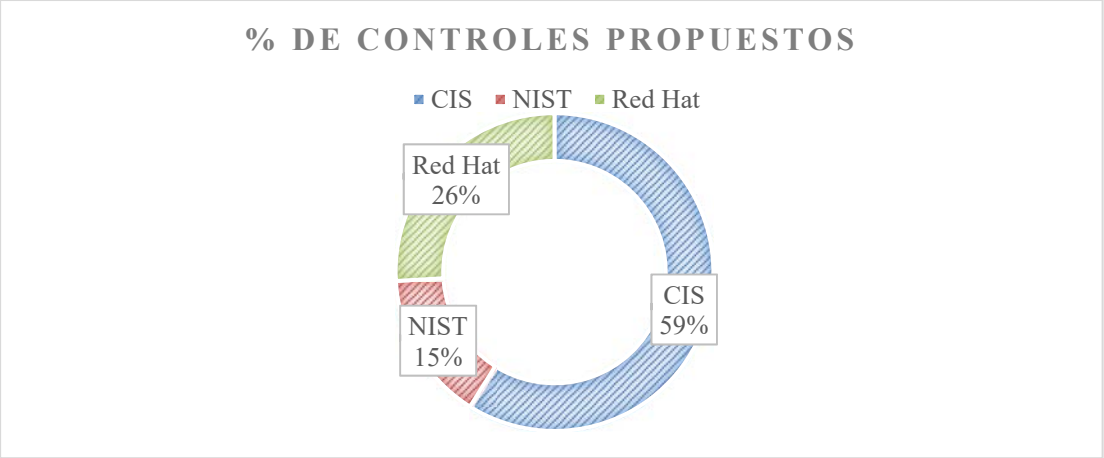


Figura 19 - Porcentaje de Controles propuestos (CIS, NIST, Red Hat)

Fuente: Elaborado por el autor de la investigación

La figura 20 muestra la cantidad de controles para cada una de las categorías, en ella se puede ver que CAT 10 relacionada a mantenimiento del sistema, no es abordada por Red Hat por tratarse de configuraciones que se realizan después del aseguramiento inicial del sistema operativo.

También se puede observar igual número de controles entre CIS Benchmark y Red Hat en la categoría 5 (Configuraciones de Seguridad de Red), esto es posible ya que en esta categoría existen configuraciones técnicas para evitar accesos desde direcciones IP no autorizadas o para evitar denegación de servicio y que se consideran importantes para el aseguramiento del sistema operativo Red Hat.

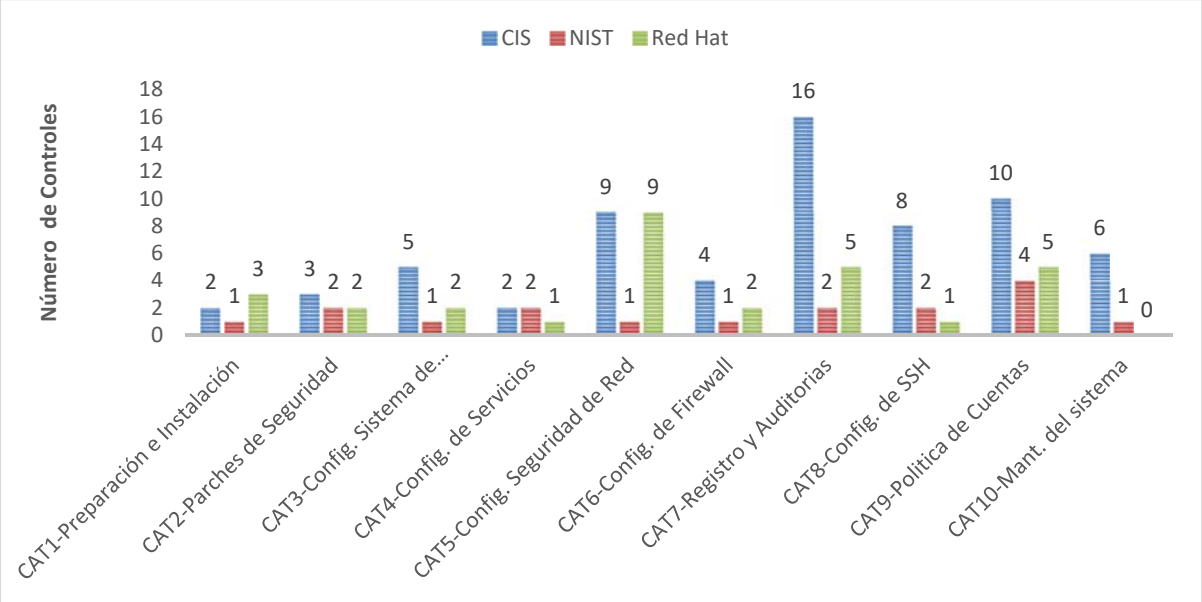


Figura 20 - Controles por categoría (CIS, NIST, RedHat)

Fuente: Autor

En la categoría 7 (Registro y Auditorías) se puede ver que existe más controles propuestos por la guía de CIS, principalmente porque esta guía además de establecer una política de auditoria recomienda el aseguramiento de la modificación y monitoreo de los registros de auditoría brindando integridad a los datos que se obtendrán por la aplicación de esta categoría.

En la categoría 2 (Parches de seguridad), la guía CIS sobre sale en número de controles porque aparte de proponer la actualización del sistema operativo e instalación de parches vigentes, propone limitar la descarga automática de actualizaciones, otorgando esta responsabilidad a la institución, de considerar primero una validación de las actualizaciones en ambiente de pruebas antes de ser aplicados al ambiente de producción.

Caso similar sucede con la categoría 4 (Configuración de Servicios), en donde las guías que mayor número de controles proponen es CIS Benchmark y NIST 800-123, el control adicional que

proponen estas guías es sobre la sincronización de la hora en los servidores, esto es importante para brindar la exactitud del tiempo en que sucedió un evento, esto es vital al momento de atender un incidente.

En CAT9 Política de cuentas, se observa que existe más controles propuestos por la guía CIS Benchmark, estos controles son configuraciones que ayudan al control de accesos no autorizados, como por ejemplo el advertir el cambio de contraseña al usuario, validar que en el grupo sensible GUI=0 solo exista el usuario autorizado, activar el cifrado de contraseñas.

Con estos resultados, es simple decidir que el sustento principal para la conformación de la propuesta para sistemas Linux es la guía CIS Benchamark, sin embargo, hay que considerar que para el presente proyecto de investigación se han realizado evaluaciones únicamente para Red Hat por tratarse del sistema operativo de la familia de Linux que más se ha implementado en la institución financiera, pero si en determinado momento surge la necesidad de instalar un sistema base, la institución deberá validar la aplicación de sus controles solicitando la guía respectiva de CIS Benchmark.

La evaluación de los controles por cada una de las categorías se muestra en las tablas mostradas a continuación en la siguiente sección.

4.2.7.2. Diseño Línea Base Linux

En las siguientes tablas se realizará el análisis de los controles por categoría, cada tabla estará conformada por: el nombre de la categoría, a la izquierda el número de control, seguido del control y a la derecha se encuentra las referencias de cada una de las guías según aplique para cada control.

Tabla 13 - Análisis categoría 1- Preparación e Instalación

Fuente: Elaborado por el autor de la investigación

CAT1	Preparación e Instalación			
Categorías/Controles	Control	Evaluación de Guías de Seguridad		
		CIS	NIST	Red Hat
C1	Aislar el servidor en un segmento de red diferente al de producción.	No definido	2.3	2.4
Análisis: Validaciones para este apartado existen únicamente en NIST 800-123 y RedHat, en donde se propone una planificación previa antes de realizar los procesos de aseguramiento del servidor. Una de las recomendaciones hace relación al uso de firewalls, routers para filtrado de paquetes y proxy para el aislamiento y posterior protección del nuevo servidor. Además, NIST tiene un documento específico dedicado íntegramente a la configuración de firewalls que se denomina NIST SP 800-41, Guidelines on Firewalls and Firewall Policy.				
C2	Configurar password para BIOS/firmware	1.4	No definido	2.1
Análisis: En este apartado tanto CIS como RedHat proponen el uso de un password para proteger el acceso a las configuraciones del BIOS del servidor, esto se utiliza para precautelar modificaciones que puedan permitir el acceso no autorizado al equipo. Ambas guías no especifican el tamaño del password, por lo que es recomendable utilizar las mismas políticas de longitud, complejidad dispuesta para usuarios. Adicional se recomienda que para no afectar la disponibilidad del servicio por procesos de mantenimiento la clave debe permanecer en sobre sellado y a custodio del jefe de infraestructura.				
C3	Crear particiones separadas para los directorios / boot, /, / home / tmp y / var / tmp /	1.1		2.2
Análisis: De acuerdo a Debian existen dos motivos por las que un administrador particionaría el sistema de archivos “La primera es por seguridad. Si algo ocurre y daña su sistema de ficheros, generalmente sólo afectará una partición. Así, sólo tendrá que sustituir solamente (desde los respaldos que cuidadosamente ha realizado) una parte de su sistema. La segunda, es generalmente más importante cuando se instala una máquina para trabajar, pero realmente depende del uso de su máquina. Por ejemplo, un servidor de correo que recibe una gran cantidad de correo no deseado, si coloca /var/mail en una partición separada, por lo general su sistema seguirá funcionado perfectamente, a pesar de recibir una gran cantidad de spam.” (Debian, 2017)				

Tabla 14 - Análisis categoría 2 - Parches de Seguridad

Fuente: Autor

CAT2	Parches de Seguridad			
Categorías/Controles	Control	Evaluación de Guías de Seguridad		
		CIS	NIST	REDHAT
C4	Actualizar el Sistema Operativo	1.2	4.1	2.5
C5	Instalar parches de seguridad vigentes	1.2	4.1	2.5
Análisis: De acuerdo a NIST, una vez que el sistema ha sido instalado, se deben aplicar los parches y actualizaciones de sistema para solventar problemas de seguridad. La entidad financiera debe validar que una actualización o aplicación de determinado parche no interfiera con las funcionalidades del servidor, por ejemplo, servicio web, base de datos, correo electrónico entre otros.				
C6	Limitar la descarga automática de actualizaciones	1.2		
Análisis: La descarga automatizada de actualizaciones debe ser controlada por la administración de la institución financiera, la aplicación automática de determinado parche podría ocasionar inestabilidad en el equipo y afectar en las funciones que debe desempeñar el servidor, ocasionando una indisponibilidad en los servicios de la institución.				

Tabla 15 - Análisis categoría 3 (Linux)

Fuente: Elaborado por el autor de la investigación

CAT3	Configuración Sistema de archivos			
Categorías/Controles	Control	Evaluación de Guías de		
		CIS	NIST	REDHAT
C7	Restringir el montaje de sistemas de archivos no necesarios como cramnfs, freevxfs, entre otros	1.1	4.2.3	
C8	Restringir la ejecución de aplicaciones en los directorios temporales y home	1.1		4.3.7
C9	Restringir el montaje automático de directorios.	1.1		
Análisis:				

CAT3	Configuración Sistema de archivos			
Categorías/Controles	Control	Evaluación de Guías de		
		CIS	NIST	REDHAT
El aseguramiento de los sistemas de archivos en relación a montaje y ejecución de archivos en ellos es importante para evitar la ejecución de rootkits o programas de escalamiento de privilegios. De acuerdo a CIS "si el sistema operativo ya está instalado, es recomendable obtener un backup completo antes de modificar las particiones" (CIS Benchmark - RedHat , 2017).				
C10	Verificar la integridad de los archivos de configuración	1.3 CIS		4.11 RedHat
Análisis: Es importante instalar y configurar un validador de integridad para tener una visión global de los archivos de sistema que puedan ser alterados. Esto es sumamente importante para validaciones por parte de analistas en caso de ocurrir un acceso no autorizado o por infección de malware. Las guías CIS Benchmark y RedHat proponen iniciar con la utilización de AIDE, herramienta que ayuda a monitorear los cambios realizados en los archivos y alertar, pero no evita la modificación (CIS Benchmark - RedHat , 2017).				
C11	Configurar advertencias de seguridad	1.7 CIS		
Análisis: La configuración de los denominados "banners" es importante para evitar que atacantes puedan capturar información relacionada a versiones de sistema operativo, aplicaciones o servicios en ejecución. CIS tiene un apartado completo dedicado a configurar estos mensajes.				

Tabla 16 - Análisis categoría 4 - Configuración de Servicios

Fuente: Elaborado por el autor de la investigación

CAT4	Configuración de Servicios			
Categorías/Controles	Control	Evaluación de Guías de Seguridad		
		CIS	NIST	REDHAT
C12	Deshabilitar servicios de red innecesarios	2	4.2.1	4.3
Análisis: La habilitación innecesaria de puertos expone al servidor a una gran variedad de ataques a través de la red interna o internet, la recomendación general que nos ofrece Red Hat es la siguiente "Para limitar la exposición a ataques a través de la red, todos los servicios que no se utilicen deben estar desactivados." (Red Hat, Inc., 2018).				

CAT4	Configuración de Servicios			
Categorías/Controles	Control	Evaluación de Guías de Seguridad		
		CIS	NIST	REDHAT
C13	Configurar la sincronización automática de la hora	2.2	4.2.2	
Análisis: Para poder dar un seguimiento oportuno a cualquier incidencia, es importante contar con logs de servidor y que se evidencie las horas exactas de cada evento. Para llevar a cabo este control es necesario disponer de un servicio NTP "Network Time Protocol" interno o en su defecto utilizar un servidor público para sincronizar sus equipos.				

Tabla 17 - Análisis categoría 5 - Configuraciones de Seguridad de Red

Fuente: Autor

CAT5	Configuraciones de Seguridad de Red			
Categorías/Controles	Control	Evaluación de Guías de Seguridad		
		CIS	NIST	REDHAT
C14	Desactivar IP Forwarding	3.1		4.4.3
C15	Deshabilitar reenvío de paquetes	3.1		5.11
C16	Ignorar respuestas de broadcast de ICMP	3.2		5.11
Análisis: Los controles están orientados a asegurar el equipo mediante configuraciones de los parámetros del kernel, de acuerdo a la guía de CIS benchmarck, estos controles son aplicables para servidores que entre sus funciones no está el funcionar como enrutador de paquetes. Ya que la institución financiera posee equipos utilizados únicamente como servidores y no como enrutadores, estas características deben ser deshabilitadas en el sistema operativo.				
C17	Permitir acceso solo a las IP's autorizadas	3.4 CIS		4.4.1 RedHat
C18	Restringir el acceso a los archivos /etc/hosts.allow y /etc/hosts.deny	3.4 CIS		4.4 RedHat
Análisis: El objetivo de estos controles es asegurar el equipo mediante la aplicación de listas de control de acceso. El acceso a la administración del servidor debe estar restringido para direcciones IP específicas. Este control previene algunos ataques de denegación de servicio (ICMPflood, SYN flood), cracking de passwords entre otras técnicas efectuadas desde redes no autorizadas.				

Tabla 18 - Análisis categoría 6 (Linux)

Fuente: Elaborado por el autor de la investigación

CAT6	Configuraciones de Firewall			
Controles	Control	Evaluación de Guías de Seguridad		
		CIS	NIST	REDHAT
C19	Instalar/ configurar iptables	3.6		
C20	Restringir conexiones entrantes ICMP	3.6		5.11
C21	Configurar conexiones salientes permitidas	3.6	4.3	5.11

Análisis:
Es importante controlar las conexiones que llegan y salen del servidor, por ello la configuración del firewall mediante iptables es muy importante para el aseguramiento del equipo.
Se debe permitir el acceso administrativo únicamente a direcciones IP de los administradores y permitir solamente los puertos de servicio necesarios, sin embargo Purificación, afirma. "Se debe prestar especial atención a la hora de configurar un firewall ya que este no protegerá de ataques internos ni de ataques a través de comunicaciones permitidas en la configuración del mismo" (Purificación, 2010, pág. 154). Para contención de ataques existen otros dispositivos de red que deben ser instalados por la administración de la institución financiera.

Tabla 19 - Análisis categoría 7- Registro y Auditorias

Fuente: Elaborado por el autor de la investigación

CAT7	Registro y Auditorias			
Controles	Control	Evaluación de Guías de Seguridad		
		CIS	NIST 800-123	REDHAT
C22	Configurar el tamaño de los archivos de registro.	4.1		6.3
C23	Deshabilitar el sistema cuando los registros de auditoria estén completos	4.1		6.3
C24	Restringir la eliminación automática de los registros de auditoria	4.1		6.3
C25	Activar el servicio de auditoria	4.1		6.4

CAT7	Registro y Auditorias			
Controles	Control	Evaluación de Guías de Seguridad		
		CIS	NIST 800-123	REDHAT
C26	Registrar modificaciones a fecha y hora del equipo	4.1		
C27	Registrar modificaciones a usuarios y grupos	4.1		6.5 RedHat
C28	Registrar modificaciones a la configuración del entorno red.	4.1		
C29	Registrar inicio/cierre de sesiones	4.1		
C30	Registrar intentos de acceso.	4.1	4.2.3	
C31	Registrar uso de comandos privilegiados	4.1		
C32	Registrar cambios en el ámbito de administración del sistema (sudoers)	4.1		
C33	Registrar acciones del administrador	4.1		
C34	Restringir los cambios sobre la configuración de auditoria.	4.1	5.2	
C35	Activar los servicios de rsyslog, syslog-ng	4.2		
C36	Permitir el acceso controlado al archivo rsyslog	4.2		
C37	Revisar los permisos a los log files estén configurados	4.2		

Análisis:
La habilitación de registros y auditoría es de vital importancia para investigaciones de eventos de seguridad, por ello el servidor debe mantener estos servicios en ejecución y conservarlos en un lugar seguro de acuerdo apolíticas internas de la institución.
El tamaño de logs no está establecido en las guías estudiadas, sin embargo, esto dependerá del propósito del servidor necesitando tamaños reducidos para servidores con pocas transacciones o grandes tamaños para base de datos, servidores web entre otros.
Ya que la generación de logs implica uso de espacio en el disco duro, las guías recomiendan utilizar syslog para su almacenaje, por ello la comunicación servidor con syslog Server debe cumplir las seguridades dispuestas en la categoría 6 de esta línea base.

Tabla 20 - Análisis categoría 8- Configuración de SSH

Fuente: Elaborado por el autor de la investigación

CAT8	Configuración de SSH			
Controles	Control	Evaluación de Guías de Seguridad		
		CIS	NIST	REDHAT
C38	Permitir el acceso controlado al archivo /etc/ssh / sshd_config	5.2		
C39	Activar el protocolo SSH versión 2	5.2		
C40	Registrar inicio y cierre de sesión ssh	5.2		
C41	Restringir el inicio de sesión directo con el usuario root.	5.2		4.2.1
C42	Restringir el inicio de sesión a usuarios sin contraseña	5.2		
C43	Restringir a los usuarios a establecer variables de entorno	5.2	6.5	
C44	Establecer tiempo de inactividad de la sesión SSH	5.2 300 segundos (5 minutos)		
C45	Restringir que usuarios pueden acceder a través de SSH.	5.2	4.2.2 , 6.5	

Análisis:
El protocolo SSH es muy utilizado para la administración remota de servidores Linux, sin embargo, debe ajustarse sus archivos de configuración para evitar usos indebidos o accesos no autorizados.
De acuerdo a CIS, todos los cambios para este protocolo en Red Hat debe realizarse en el archivo "etc/ssh/sshd_config" y después de ejecutar los cambios se debe recargar el servicio con "systemctl reload sshd".
El acceso mediante SSH debe ser controlado para un grupo específico de usuarios, esto debe estar alineado a las políticas internas y en medida de lo posible evitar el uso de usuarios genéricos para poder conocer detalladamente que usuarios acceden al servidor.
El tiempo de inactividad debe ser bajo para impedir actividades maliciosas en consolas que se encuentren abiertas por descuido, recordando el caso propuesto en Windows en la categoría 5 en donde se podría utilizar un dispositivo USB para ejecución de comandos, es recomendable establecer un tiempo de inactividad menor a 5 minutos y de esta forma minimizar el accionar de personal malintencionado con acceso físico al servidor.

Tabla 21 - Análisis categoría 9- Política de Cuentas

Fuente: Elaborado por el autor de la investigación

<table>
<tr><th>CAT9</th><th colspan="4">Política de Cuentas</th></tr>
<tr><td rowspan="2">Controles</td><td rowspan="2">Control</td><td colspan="3">Evaluación de Guías de Seguridad</td></tr>
<tr><td>CIS</td><td>NIST</td><td>REDHAT</td></tr>
<tr><td rowspan="2">C46</td><td rowspan="2">Configurar longitud mínima de contraseña</td><td>5.3</td><td>4.2</td><td>4.1.1</td></tr>
<tr><td>14 caracteres</td><td>No definido</td><td>8 caracteres</td></tr>
<tr><td colspan="5">Análisis:
De acuerdo al estudio bibliográfico desarrollado en la línea base de Windows (Categoría 3), en donde se muestra un experimento en relación a cracking de passwords por parte de la Georgia Institute of Technology, se ha adoptado la recomendación del uso de 14 caracteres propuesto por CIS.
Red Hat propone el uso de 8 caracteres, lo cual supone un alto riesgo considerando que se pueden romper contraseñas de esta longitud con computadoras con múltiples tarjetas gráficas.
Se recomienda que la institución adopte el control con un valor de 14 caracteres.</td></tr>
<tr><td rowspan="2">C47</td><td rowspan="2">Configurar el historial de contraseña</td><td>5.3</td><td>4.2</td><td>4.1.1.</td></tr>
<tr><td>No definido</td><td>No definido</td><td>3 veces.</td></tr>
<tr><td colspan="5">Análisis:
De forma similar al control anterior, el estudio del historial de contraseña fue desarrollado en el Control 5 de Windows, en donde CIS y el fabricante sugieren 60 días, sin embargo, en este apartado Red Hat sugiere utilizar 90 días, esta configuración si bien es útil para el usuario, ya que no necesita cambiar muy seguido su password, se convierte en un foco atractivo para el cracking de passwords ya que al no cambiar por tanto tiempo las credenciales en caso de que el ataque efectuado sea satisfactorio se podrá tener violación de acceso y muy posiblemente reutilización de contraseñas para realizar movimiento lateral en la red.
Por esta razón se sugiere adoptar el uso de 30 días como en la línea base de Windows.</td></tr>
<tr><td>C48</td><td>Habilitar complejidad de contraseña</td><td></td><td>4.2</td><td></td></tr>
<tr><td colspan="5">Análisis:
De acuerdo al estudio realizado en 2017 en la publicación NIST 800-63B en donde se identifica que esta atributo de complejidad de contraseña requiere que se implemente también el control de validar la contraseña con un listado de contraseñas inaceptables “lista negra”, el motivo es porque los usuarios son predecibles al momento de generar su contraseña (Paul A. Grassi, 2017).
Se propone que la institución financiera adopte este control y la recomendación adicional realizada en la publicación NIST 800-63B.</td></tr>
<tr><td>C49</td><td>Activar el algoritmo SHA-512 para contraseñas</td><td>5.3</td><td></td><td></td></tr>
<tr><td>C50</td><td></td><td></td><td>4.2</td><td>4.1.2.</td></tr>
</table>

CAT9	Política de Cuentas			
Controles	Control	Evaluación de Guías de Seguridad		
		CIS	NIST	REDHAT
	Configurar política de bloqueo de cuenta	3 intentos	No definido	3 intentos
Análisis: El aseguramiento utilizando un método de cifrado fuerte junto con la política de bloqueo es muy importantes en sistemas operativos Linux. Las guías estudiadas han determinado que 3 intentos son suficientes para bloquear la cuenta en caso de ataques de fuerza bruta. Se propone que la institución financiera adopte este control, ayuda a fortalecer la confidencialidad de la contraseña.				
C51	Definir vigencia de contraseña	5.4 365 o menos		4.1.1. 90 días
Análisis: En la guía de CIS Benchmark propone que sea de 365 días o menos y el fabricante RedHat sugieren 90 días, si bien esta configuración es útil para el usuario, ya que no necesita cambiar muy seguido su password, se convierte en un foco atractivo para el cracking de passwords ya que al no cambiar por tanto tiempo las credenciales en caso de que el ataque efectuado sea satisfactorio se podrá tener violación de acceso y muy posiblemente reutilización de contraseñas para realizar movimiento lateral en la red. Por esta razón se sugiere adoptar el uso de 30 días como vigencia del password.				
C52	Restringir el login a cuentas del sistema	5.4		
Análisis: En la plataforma Linux existe varios usuarios que vienen por defecto y en algunos de los casos son requeridos para el funcionamiento del sistema, se debe restringir el logueo con estos usuarios e incluso otra manera de restringirlos es asignándoles una Shell que no brinde acceso a línea de comando.				
C53	Advertir el cambio de contraseña antes de su caducidad	5.4 7 días o más	No definido	No definido
Análisis: De acuerdo a CIS, el sistema debe alertar al usuario 7 días antes del cambio de credenciales, esta configuración debe estar acorde a políticas internas de la institución, sin embargo, es recomendable que el recordatorio se realice 15, 7 y 3 días antes de la caducidad del password, de esta forma el administrador tiene la oportunidad de tomar las acciones respectivas teniendo alertas con un tiempo prudencial.				
C54	Bloquear contraseñas inactivas	5.4		

CAT9	Política de Cuentas			
Controles	Control	Evaluación de Guías de Seguridad		
		CIS	NIST	REDHAT
		30 días o menos	No definido	No definido
C55	Restringir el acceso al comando su	5.4		
C56	Validar que el grupo GID 0 sea solo del usuario root	5.4		
Análisis: Las contraseñas de usuarios que se encuentran inactivas deben ser bloqueadas para evitar su uso por parte de usuarios no autorizados que quieran aprovechar esta debilidad para escalar privilegios en el activo o en la red. El bloqueo de acuerdo a CIS debe ser a partir de los 30 días, pero esta configuración debe ser validada por la administración de la institución financiera en donde el número de días debe ser ajustado de acuerdo a sus necesidades empresariales y normativa interna. De igual forma, el comando su debe ser restringido a un número finito de usuarios que requieran escalar sus privilegios para tareas administrativas. En el aparatado correspondiente de CIS se puede observar las directrices para configurar el acceso a "su".				

Tabla 22 - Análisis categoría 10 - Mantenimiento del sistema

Fuente: Elaborado por el autor de la investigación

CAT10	Mantenimiento del sistema			
Controles	Control	Evaluación de Guías de Seguridad		
		CIS	NIST	REDHAT
C55	Restringir el acceso a los archivos sensibles (passwd, shadow,group, gshadow) y a sus backups	6.1	4.2.3	
C56	Validar que no exista directorios sin propietario	6.1		
C57	Validar que los campos de contraseñas no estén vacíos	6.2		
C58	Validar que solo el usuarios root tenga UID 0	6.2		
C59	Validar que los accesos a directorios personales existan y estén restringidos.	6.2		
C60	Validar que no exista usuarios y grupos duplicados	6.2		
Análisis:				

La adopción de estos controles mostrados en las categorías 8 debe estar presentes en la línea base propuesta ya que todos ellos son validaciones adicionales de seguridad que refuerza los accesos a los recursos del servidor.

4.2.8. Comparación entre Líneas Base (Windows – Linux)

En los apartados anteriores se han realizado los análisis correspondientes a los controles y categorías que cada guía estudiada (CIS Benchmark, NIST 800-123, Microsoft Baseline y Red Hat Baseline), en esta sección se realiza una comparación a nivel macro de los controles presentados en las tablas 2 y 12 que corresponden a cada una de las plataformas analizadas Windows y Linux.

No se considerará realizar una comparación técnica de cada uno de las configuraciones ya que la forma de validar de Windows difiere con Linux principalmente en la estructura de archivos y accesos a las configuraciones en el servidor.

4.2.8.1. Cantidad de controles que aporta CIS Benchmarks a las Líneas base, Windows y RedHat

La figura 21 se indica el porcentaje de controles que aporta las guías de CIS Benchmark para las líneas base de Windows y RedHat, en la figura se puede observar que de todos los controles evaluados en este documento de investigación, las configuraciones definidas por CIS están presentes en un mayor porcentaje en el sistema Red Hat, esto sucede principalmente porque la guía no se enfoca únicamente en la configuración técnica del servidor sino que también recomienda temas de administración del equipo como aseguramiento de SSH entre otros servicios administrativos.

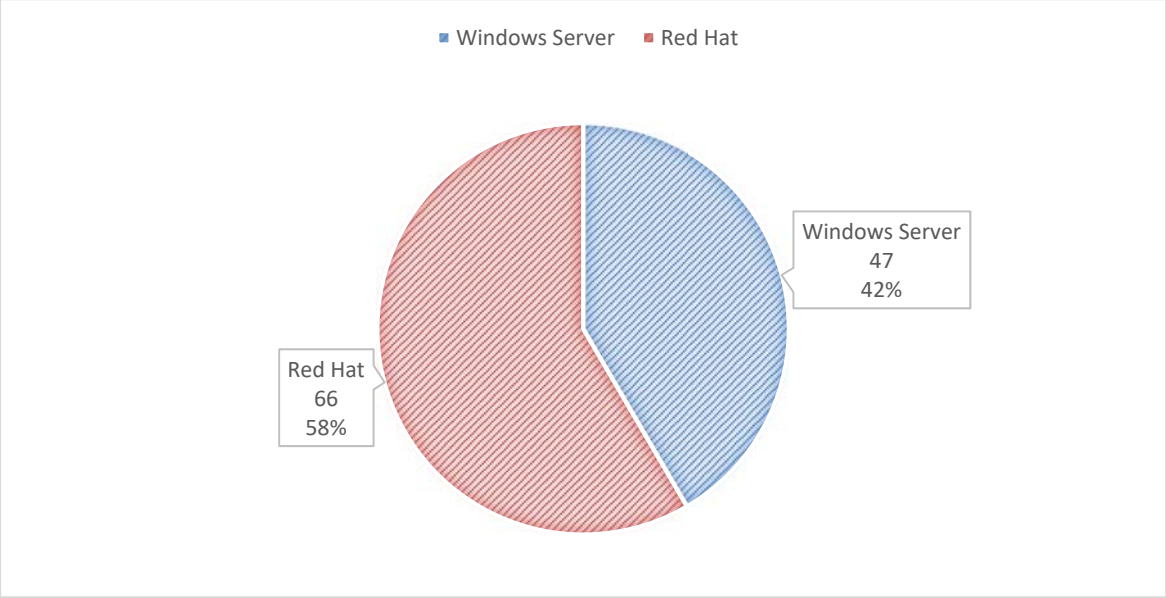


Figura 21 – Porcentaje de controles que aporta CIS Benchmark a las líneas base de Windows y RedHat

Fuente: Elaborado por el autor de la investigación

Las guías de Red Hat y Windows, si bien ambas tratan tópicos similares, la forma de configurar los parámetros de aseguramiento son distintos por lo que en Red Hat el desglose de las configuraciones hacen que se incremente el número de controles de la guía.

4.2.8.2. Cantidad de controles que aporta NIST a las líneas base, Windows y RedHat

En la figura 22 se puede observar el porcentaje de controles que aporta la guía NIST 800-123 al blindaje de las plataformas Windows y RedHat.

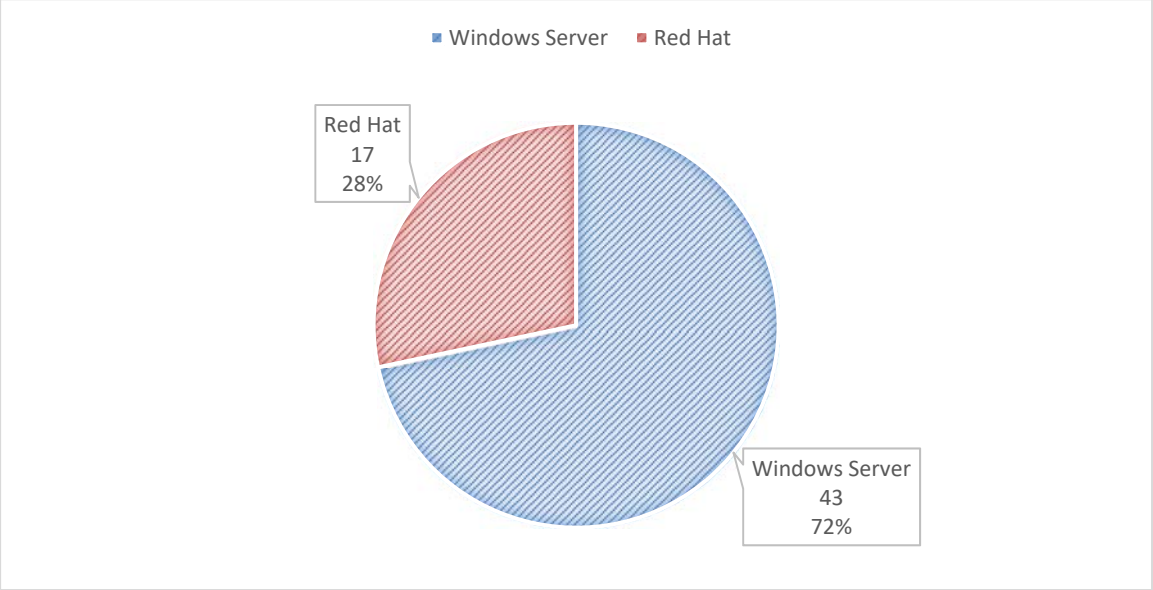


Figura 22 - Controles que aporta NIST 800-123

Fuente: Elaborado por el autor de la investigación

Para este caso, NIST 800-123 tiene mayor presencia de controles que se pueden aplicar en sistemas Windows, este comportamiento se da porque esta guía propone validaciones de muy alto nivel y ya que en el aseguramiento de Red Hat se necesitan recomendaciones más específicas que involucran parámetros en archivos del sistema operativo, se puede ver a NIST 800-123 con poco aporte para la conformación de la línea base si solo consideramos la parte técnica.

El tener pocos controles para RedHat no descarta el uso de esta guía, los controles en donde es aplicable aporta con definiciones teóricas que orientan al investigador a tomar decisiones para el correcto aseguramiento del sistema.

4.2.8.3. Cantidad de controles que aportan los fabricantes de cada Sistema Operativo, Windows y RedHat

Cada fabricante desarrolla sus propuestas de aseguramiento para sus servidores, independientemente del uso que se lo vaya a dar.

Para Windows, la propuesta de Microsoft es bastante técnica, en donde se ofrecen configuraciones muy específicas y siempre tomando como base a la directiva de seguridad local.

Por otro lado, la guía de aseguramiento de Red Hat propone cambios en los parámetros de configuración existentes en los archivos de sistema, pero el detalle técnico que se muestra no es muy profundo.

La siguiente figura muestra la comparación de controles para ambas tecnologías.

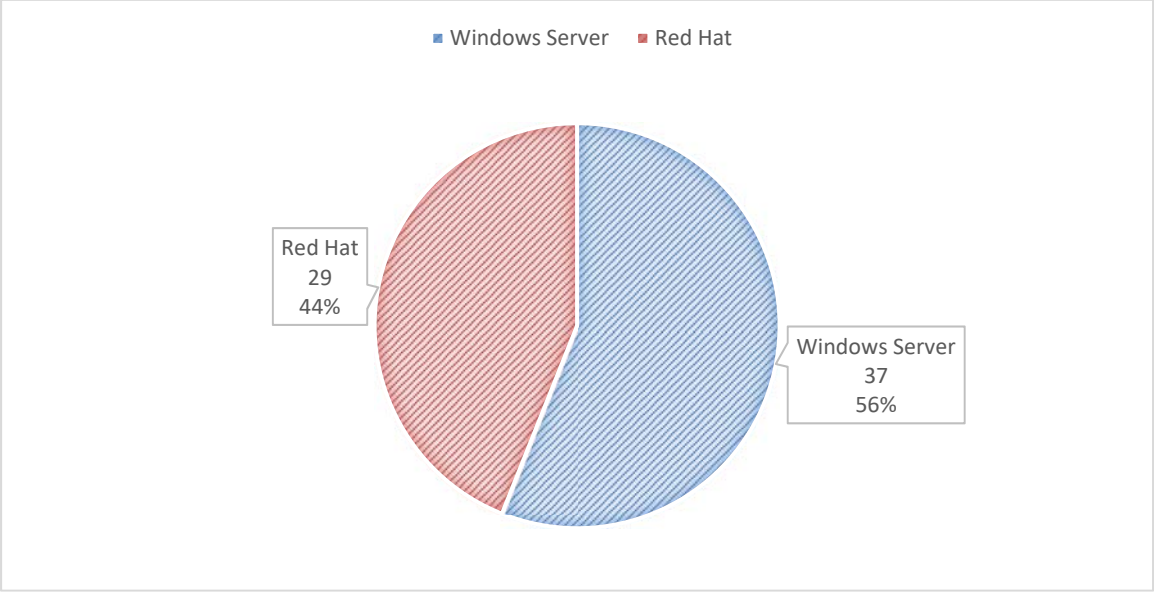


Figura 23 - Cantidad de controles que aportan los fabricantes a las líneas bases, Windows y RedHat

Fuente: Elaborado por el autor de la investigación

En la figura 23 se puede visualizar que el fabricante de Windows propone más controles que el fabricante de RedHat, esto puede ser porque al ser Linux un sistema open source depende de la investigación de la comunidad, es decir de los profesionales interesados en aportar con conocimiento al mejoramiento de la plataforma no solo a nivel funcional sino de seguridad; mientras que Windows cuenta con un equipo dedicado a generar mejora continua a sus productos.

4.2.8.4. Comparativo general de las guías estudiadas

La figura 24 muestra el porcentaje de controles que ha aportado cada una de las guías al proceso de identificación de líneas base de seguridad para las plataformas Windows y RedHat, en la figura se puede observar que del total de controles estudiados para conformar las líneas base para Windows y Red Hat, la mayor parte de controles propuestos son de las guías de CIS Microsoft Windows Benchmark y CIS Red Hat Benchmarck.

Este comportamiento se debe a que las guías de CIS son bastante detalladas y técnicas, cubren una cantidad grande de controles que ayudan a asegurar los sistemas operativos desde su instalación.

Un punto importante que acotar es la cantidad de controles propuestos NIST 800-123, es la segunda guía que más controles aportado a las líneas base de las plataformas Windows y RedHat, ya que, si bien no existe una recomendación técnica, sus propuestas son de alto nivel que nos ayuda a tener un conocimiento lineamientos de seguridad que el sistema operativo debería cumplir.

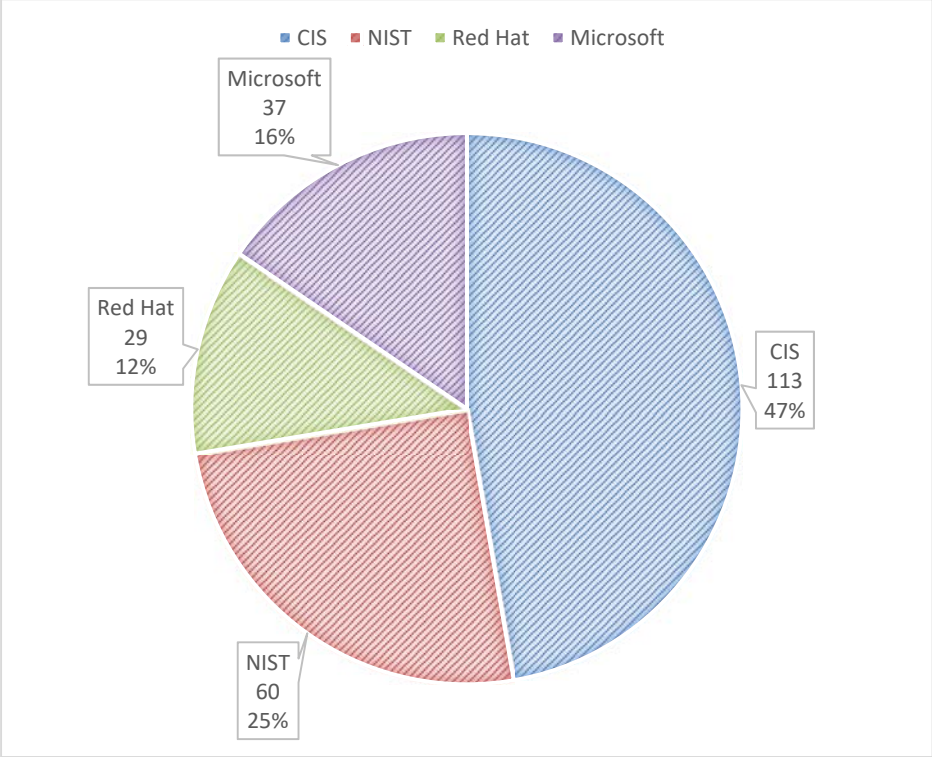


Figura 24 – Porcentaje de contrales de las guías de seguridad

Fuente: Elaborado por el autor de la investigación

De la figura 24 se puede deducir que la línea base de seguridad que se propone a la institución tiene más controles propuestos por la guía de CIS Benchmark, seguido de los lineamientos propuestos por NIST 800-123.

4.2.8.5. Categorías similares entre líneas base Windows y RedHat

Durante el desarrollo de las líneas base para Windows y Red Hat, se pudo observar que existen categorías similares para ambos sistemas, pero la cantidad de controles que contiene cada una de ellas son diferentes.

De acuerdo a la figura 26, muestra las 6 categorías similares que están presentes tanto en la línea base de Windows como Red Hat y estas son: Preparación e Instalación, Parches de Seguridad,

Política de Cuentas, Configuraciones de Seguridad de Red, Configuraciones de Firewall y Configuraciones de políticas de Auditorías.

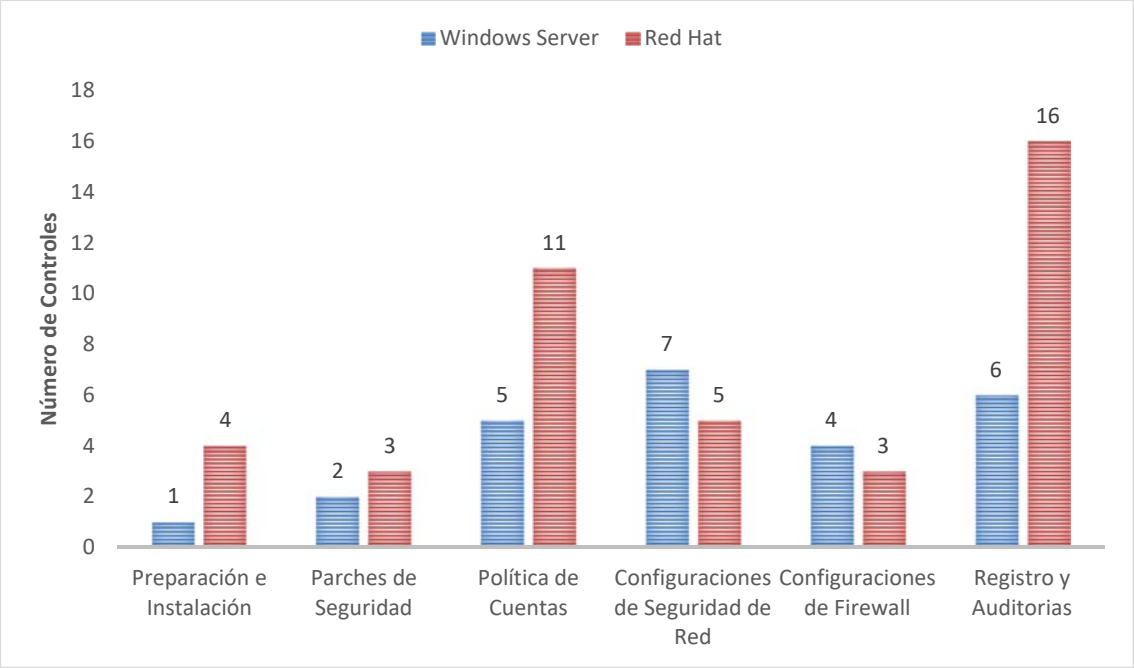


Figura 25 - Categorías similares entre Windows y Linux

Fuente: Elaborado por el autor de la investigación

En la figura 25 se puede observar que la línea base para Red Hat tiene mayor número de controles de las categorías similares en contraste con Windows, esto se da porque las configuraciones que se deben realizar en sistemas operativos Red Hat son más detallas en donde no basta únicamente activar o desactivar un botón y en su lugar se debe modificar archivos de sistema para lograr el aseguramiento deseado.

Los registros y auditorías que se deben habilitar en el servidor tiene más énfasis en Red Hat, puesto que en las guía se sugiere que se habilite no solo los registros para las configuraciones del sistema operativo sino también para otros servicios que se encuentren en ejecución, por ejemplo, si el servidor cuenta con Apache se sugiere habilitar estos logs tanto de accesos como de

conexiones fallidas, si el servidor ejecuta como servicio a SSH, también son considerados los logs de acceso mediante este protocolo.

También existen diferencias en las configuraciones sugeridas, por ejemplo: todas las guías usadas para Windows sugieren el uso de 14 o más caracteres para la contraseña, mientras que para la plataforma Red Hat el proveedor sugiere 8 caracteres, pero con el análisis realizado en la tabla 21 se analiza por que se propone el uso de 14 caracteres.

El análisis realizado en este capítulo nos ayuda a evidenciar que para obtener un nivel de blindaje adecuado para las plataformas Windows y Red Hat se propone que se adopte los controles identificados en las tablas 2 y 12, controles que han sido obtenidos de 3 guías de referencia CIS Benchmark, NIST 800-123 y la guía del fabricante (Microsoft y Red Hat).

El análisis de los controles que aportan al aseguramiento de los sistemas operativos Windows y Red Hat se encuentran detallados en las secciones 4.2.6.2 y 4.2.7.2 de este documento. Resultado que será tomado como artefacto en el proceso de blindaje del sistema operativo propuesto en las secciones 4.2.1.a 4.2.4 de este documento.

Capítulo V

Conclusiones y Trabajo Futuro.

5.1 Conclusiones

- Si bien la institución financiera mantiene un procedimiento denominado "Administración de la Configuración", su aplicación no ha sido evidenciada en las actividades cotidianas que realizan los administradores de las plataformas con respecto a la instalación y aseguramiento de servidores, dejando en evidencia la inexistencia de una línea base de seguridad para las plataformas de la institución.
- El proceso de instalación de servidores que realiza la institución tiene varias debilidades como: carencia de definición de roles de seguridad informática y seguridad de la información, un único control de seguridad (instalación de parches), personal insuficiente para realizar las actividades del área mucho menos para implementar un proceso de blindaje de servidores. Este trabajo mitiga la inexistencia de controles de seguridad para las plataformas de Windows - Red Hat y brinda un proceso de hardening, que queda a disposición de la institución para su implementación.
- La institución cuenta con una variedad de plataformas tecnológicas que soportan los servicios críticos (Red Hat, Windows, SQL, Jboss), de las cuales se ha seleccionado Windows y Red Hat para realizar la propuesta de línea base de seguridad, los sistemas operativos fueron seleccionadas partiendo de los servicios críticos de la institución, considerando la cantidad de activos que soportan estos servicios y priorizando las plataformas.

- Las líneas base para Windows y Red Hat cuentan con controles de las tres guías en cada una de las categorías identificadas, esta diversidad de puntos de vista ayuda a aplicar controles más específicos de acuerdo a la necesidad de la institución; las líneas base brindan la visión de alto nivel de lo que debería cumplir un servidor, así como el detalle técnico facilita la aplicación de los controles, además, la combinación de estos controles fortalece la línea base de seguridad propuesta a la institución.
- Del análisis realizado para la identificación de controles para Windows Server, se pudo validar que las tres guías aportan con algunos apartados similares, existe cinco categorías con igual cantidad de controles, sin embargo, al examinar detenidamente cada guía se pueden encontrar distintas recomendaciones para un mismo control por lo cual la institución financiera debe validar su aplicabilidad de acuerdo a sus procesos internos que no interfieran con las actividades normales de los procesos en cada servidor.
- La línea base para Red Hat muestra la existencia de controles de las tres guías en cada una de las categorías identificadas, excepto para la categoría diez en donde solo hay controles de dos guías, esto evidencia que la guía del fabricante no considera controles que se realizan después de aseguramiento inicial.
- De acuerdo al análisis realizado para Windows y Red Hat, se puede ver que existe mayor cantidad de controles propuestos por CIS que aporta con el 47% del total de controles técnicos estudiados en el presente proyecto, sin embargo, NIST 800-123 aporta con 25% de controles proporcionando un complemento teórico para la toma de decisiones al momento de aplicar una configuración en el servidor.

- Al realizar la comparación de categorías similares que existen entre las líneas base de Windows y Red Hat se han identificado las siguientes: preparación e instalación, parches de seguridad, política de cuentas, configuraciones de seguridad de red, configuraciones de firewall y configuraciones de políticas de Auditorías, estas categorías no necesariamente tienen los mismos controles, es decir, que por la naturaleza de cada sistema operativo los controles que existen en cada una de las categorías no son iguales, como por ejemplo en la categoría de política de cuentas Windows tiene 5 controles mientras que Red Hat 11, difiere porque en la plataforma Red Hat considera la activación del cifrado de contraseñas, el bloqueo de cuentas des pues de una cantidad de tiempo transcurrido y la cuenta haya permanecido inactiva, entre otros controles adicionales
- En la propuesta se evidencia que para obtener un nivel de blindaje adecuado para los sistemas operativos Windows y Red Hat, se propone a la institución financiera aplicar los controles que se obtienen de la comparativa de seguridad (CIS Benchmark, NIST 800-123, Microsoft, Red Hat)

5.2 Recomendaciones

- El proceso propuesto en este trabajo de investigación puede ser replicado en otras instituciones que requieran iniciar con el aseguramiento de su infraestructura a nivel de configuraciones de los sistemas operativos, sin embargo, hay que tener en consideración que el levantamiento de la línea base propuesta debe ser ajustada a la realidad del giro de negocio de cada organización.

- Se recomienda complementar el proceso de hardening propuesto con evaluaciones continuas de vulnerabilidades sobre la infraestructura y de esta forma ayudar a la institución financiera a mejorar su postura de seguridad.
- Debido a que los fabricantes de plataformas tecnológicas desarrollan mejoras constantemente, es recomendable actualizar la línea base de seguridad conforme se hagan públicas las nuevas configuraciones recomendadas por los proveedores o grupos profesionales dedicados a la generación de estándares de seguridad.

5.3 Trabajo Futuro

- El presente trabajo conforma el estudio para el aseguramiento de dos sistemas operativos (Windows y Linux), este análisis puede ser ampliado evaluando el aseguramiento de otras plataformas como Solaris, AIX entre otros e incluyendo base de datos y software web.
- El trabajo realizado en este documento está orientado al diseño del proceso de hardening de servidores y la institución deberá realizar la gestión necesaria para implementar el proceso propuesto en nuevos servidores, así como en los existentes en ambiente productivo.

BIBLIOGRAFÍA

Andrea Bichsel - Microsoft. (18 de 04 de 2017). *User Rights Assignment*. Obtenido de https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/user-rights-assignment

Arduinosecurity. (2016). Obtenido de Aseguramiento de Servidores: https://arduinosecurity.com/es/services/hardening

Areitio, J. (2008). *Seguridad de la información. Redes, informática y sistemas de información.* Madrid: PARANINFO.

Asociación Catalana de Universidades Públicas. (2012). *Infraestructura Tecnológica*. Obtenido de http://www.uoc.edu/portal/es/tecnologia_uoc/infraestructures/index.html

Bembibre, V. (23 de 02 de 2009). *Configuración.* . Obtenido de Definición ABC: https://www.definicionabc.com/tecnologia/configuracion.php

Benchmarks, C. (30 de 03 de 2018). *www.cisecurity.org.* Obtenido de www.cisecurity.org: https://learn.cisecurity.org/benchmarks

Bernal, C. A. (2006). *Metodología de la investigación.* México: Pearson Education.

Better Buys. (2016). *Estimating Password-Cracking Times.* Obtenido de betterbuys.com: https://www.betterbuys.com/estimating-password-cracking-times/

Bonnet, N. (2014). *Windows Server 2012.* España: ENI.

Caballero, J. (1998). *Redes de banda ancha.* Barcelona: Marcombo S.A.

Center for Internet Security. (2018). Obtenido de https://www.cisecurity.org/about-us/

CIS Benchmark - RedHat . (27 de 12 de 2017). *www.cisecurity.org.* Obtenido de www.cisecurity.org: https://learn.cisecurity.org/benchmarks

CIS Benchmark - Windows 2012. (30 de 03 de 2018). *www.cisecurity.org.* Obtenido de www.cisecurity.org: https://learn.cisecurity.org/benchmarks

Colobran, M. (2008). *Administración de sistemas operativos en red.* Barcelona: UOC.

Cómez, Á. (2014). *Enciclopedia de la Seguridad Informática.* Madrid: RA - MA.

De Plablos Heredero, C. (2004). *Informática y comunicaciones en la empresa.* Madrid: ESIC.

Delgado, X. (1998). *Auditoría informatica.* Costa Rica: EUNED.

Desongles, J. (2006). *Tecnicos de Informatica.* Sevilla: Mad S.L.

Dunn, S. (27 de enero de 2017). *www.tenable.com*. Obtenido de https://www.tenable.com/sc-report-templates/cis-cisco-benchmark-reports

Española, R. A. (2018). *Real Academia Española*. Obtenido de http://dle.rae.es/?id=XhbjsNo

Espinoza, D. (17 de Noviembre de 2012). *Seguridad Informática*. Obtenido de ¿Qué es una vulnerabilidad, una amenaza y un riesgo?: http://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo#.UKexLOMSU0w

Fache, J. (2016). *Estudio sobre la aplicación de hardening para mejorar la seguridad informáticaen el centro técnico laboralde Tunjacotel*. Obtenido de https://campus0a.unad.edu.co/campus/

Gisbert, B. (2015). *Administración y auditoría de los servicios web.* ELEARNING S.L.

Gutiérrez Cañizares, J. J. (s.f.). *Instalación configuración del sofware de servidor web.* España: Elearning S.L.

Hack5. (2017). *15 Second Password Hack, Mr Robot Style*. Obtenido de Payloads and How-To: https://docs.hak5.org/hc/en-us/articles/360010471374-15-Second-Password-Hack-Mr-Robot-Style

ICORP. (2018). *Seguridad Informatica*. Obtenido de http://www.icorp.com.mx/solucionesTI/seguridad-informatica/

Iglesias, R. (2006). *Instalacion De Redes Informaticas e Ordenadores.* Ideaspropias.

Institución. (19 de 11 de 2015). Política de Tecnología de la información. QUITO.

Institución. (19 de 11 de 2015). Política Seguridad de la Información. Quito.

Institución. (3 de enero de 2017). *Amenazas informáticas: conoce las internas y externas*. Obtenido de https://www.tecnoxxi.com/blog/seguridad-informatica/amenazas-informaticas/

Jara, S. (2005). *Taller de Computo.* México: Umbral.

Karen Scarfone, W. J. (25 de julio de 2008). *www.nist.gov*. Obtenido de https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=890008

Kroustek, J. (12 de 05 de 2017). *Avast te protege del ransomware WanaCrypt0r 2.0 que ha infectado a NHS y Telefónica*. Obtenido de https://blog.avast.com/es/ransomware-telefonica-hospitales

Kumar, M. (12 de 2 de 2008). *Cryptography and Network Security.* India: Krishna Prakashan Media.

Laudon, K. (2004`). *Sistemas de información gerencial: administración de la empresa digital.* México: Pearson Educación.

Marchionni, E. (2011). *Administradores de Servidores.* Buenos Aires: Fox Andina.

Margosis, A. (13 de Agosto de 2014). *Microsoft TechNet*. Obtenido de https://blogs.technet.microsoft.com/secguide/2014/08/13/security-baselines-for-windows-8-1-windows-server-2012-r2-and-internet-explorer-11-final/

Margosis, A. (13 de 08 de 2014). *technet.microsoft.com.* Obtenido de https://blogs.technet.microsoft.com/secguide/2014/08/13/security-baselines-for-windows-8-1-windows-server-2012-r2-and-internet-explorer-11-final/

Martha Romero, G. F. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades.* ALICANTE: 3CIENCIAS.

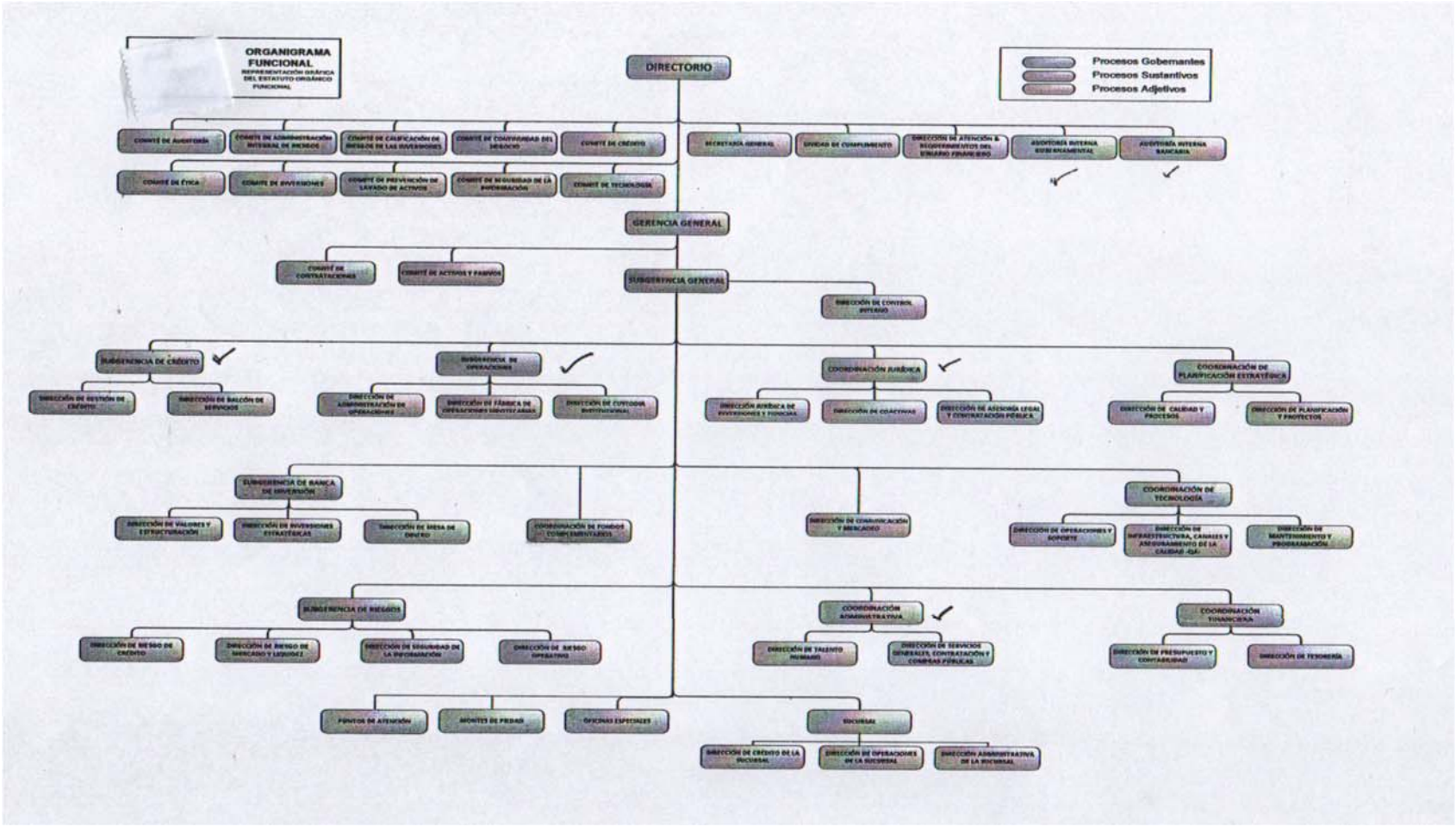
Microsoft. (18 de 04 de 2017). *Store passwords using reversible encryption*. Obtenido de https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/store-passwords-using-reversible-encryption

Microsoft. (26 de marzo de 2018). *azure.microsoft.com*. Obtenido de https://azure.microsoft.com/en-us/resources/cis-microsoft-azure-foundations-security-benchmark/

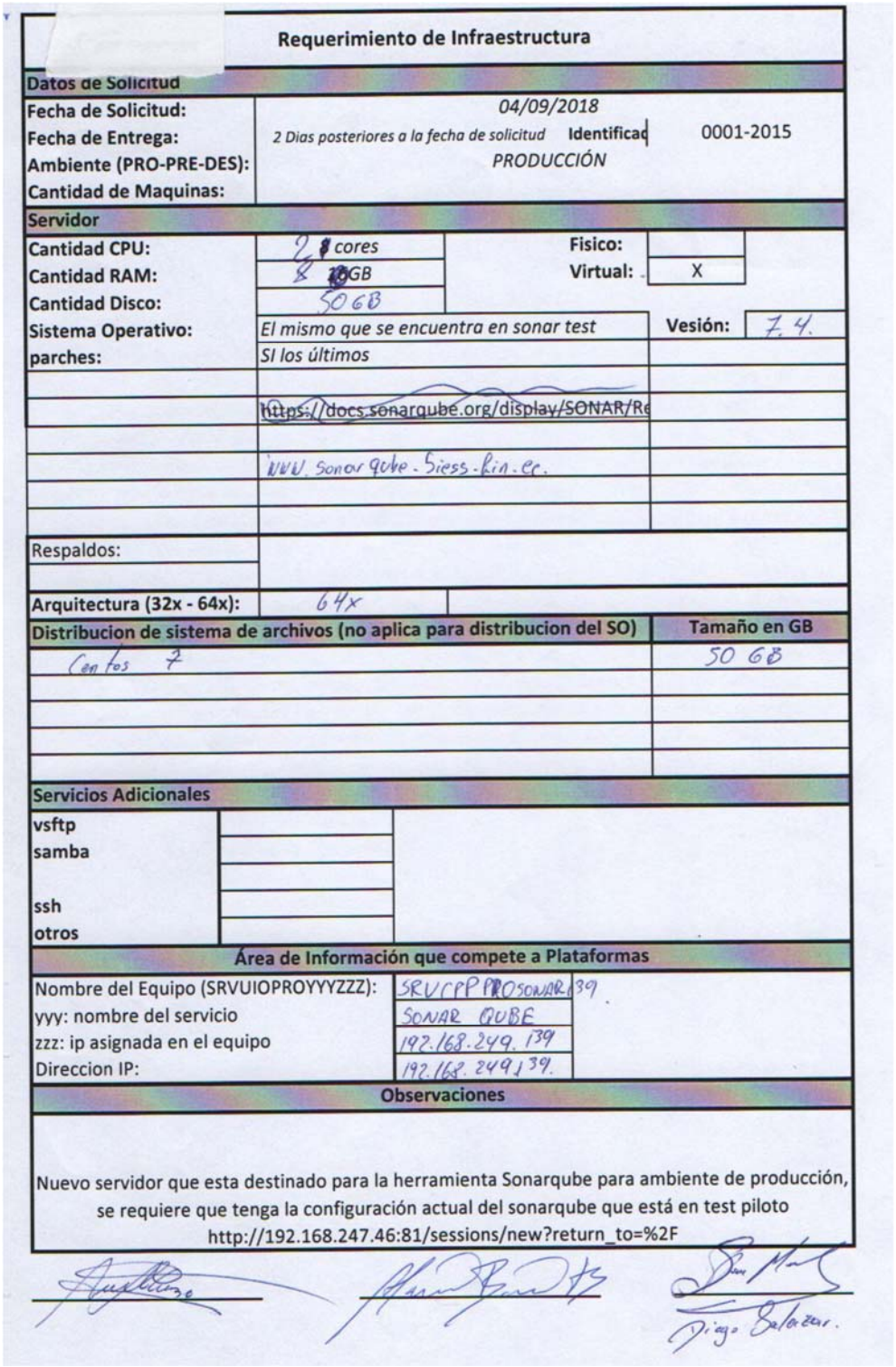
Mistry, S. (2018). Endpoint Protection through Windows Operating. *International Journal of Computer Applications Technology and Research*.
Morales, C. F. (2018). *repositorio.ug.edu.ec.* Obtenido de http://repositorio.ug.edu.ec/
Oceano IT. (2014). *Oceano IT © 2014*. Obtenido de https://www.oceano-it.es/news-individual/369/amenazas-informaticas-mas-comunes-en-la-actualidad
Paul A. Grassi. (Junio de 2017). Digital Identitu Guidelines. *NIST Special Publication 800 -63B*, 79.
Porto, J. (2008). *Seguridad Informatica*. Obtenido de https://definicion.de/seguridad-informatica/
Purificación, A. (2010). *Segruidad Informática.* EDITEX.
Purificación, A. (2010). *Seguridad Informática.* Madrid: EDITEX.
Qualys. (2019). *www.qualys.com*. Obtenido de https://www.qualys.com/apps/security-configuration-assessment/
Red Hat, Inc. (2018). *access.redhat.com.* Obtenido de Red Hat Customer Portal: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/
Robayo, J. (2015). *Aseguramiento de los istemas computacionales de la empresa SITIOSDIMA.NET*. Obtenido de https://repository.unad.edu.co/
Rodrigo, F. (2014). Recomendaciones para software e infraestructura segura. *SISTESEG*, 6. Obtenido de Recomendaciones para software e infraestructura segura.
Sandoval, D. (2018). *Cuáles son los tipos de servidores*. Obtenido de https://www.nextu.com/blog/tipos-de-servidores/
Smartekh. (3 de Mayo de 2012). *Hardening*. Obtenido de http://blog.smartekh.com/que-es-hardening
Stevens, D. (10 de 04 de 2017). *SANS ISC InfoSec Forums.* Obtenido de Password History: Insights Shared by a Reader: https://isc.sans.edu/forums/diary/Password+History+Insights+Shared+by+a+Reader/22278/
Sutter, J. (20 de 10 de 2010). *CNN*. Obtenido de How to create a 'super password': http://edition.cnn.com/2010/TECH/innovation/08/20/super.passwords/index.html
Torres, A. (2 de 09 de 2017). *¿Qué es un servidor y que tipos hay?* Obtenido de https://www.comparahosting.com/p/que-es-un-servidor/
Villada, J. L. (2014). *Instalación y configuración del software de servidor Web.* IC.

ANEXOS

Anexo I: Organigrama Funcional.



Anexo II: Formulario para instalación de un servidor



Requerimiento de Infraestructura

Datos de Solicitud

Fecha de Solicitud:	04/09/2018
Fecha de Entrega:	2 Dias posteriores a la fecha de solicitud **Identificad** 0001-2015
Ambiente (PRO-PRE-DES):	PRODUCCIÓN
Cantidad de Maquinas:	

Servidor

Cantidad CPU:	2 8 cores	**Fisico:**	
Cantidad RAM:	8 16GB	**Virtual:**	X
Cantidad Disco:	50 GB		
Sistema Operativo:	El mismo que se encuentra en sonar test	**Vesión:**	7.4.
parches:	SI los últimos		
	https://docs.sonarqube.org/display/SONAR/Re		
	www.sonarqube.5iess.fin.ec.		

Respaldos:	
Arquitectura (32x - 64x):	64x

Distribucion de sistema de archivos (no aplica para distribucion del SO)	**Tamaño en GB**
Centos 7	50 GB

Servicios Adicionales

vsftp		
samba		
ssh		
otros		

Área de Información que compete a Plataformas

Nombre del Equipo (SRVUIOPROYYYZZZ):	SRVCPPPROSONAR139
yyy: nombre del servicio	SONAR QUBE
zzz: ip asignada en el equipo	192.168.249.139
Direccion IP:	192.168.249.139

Observaciones

Nuevo servidor que esta destinado para la herramienta Sonarqube para ambiente de producción, se requiere que tenga la configuración actual del sonarqube que está en test piloto
http://192.168.247.46:81/sessions/new?return_to=%2F

Diego Salazar.

Glosario

Crowdsourcing: es un modelo de abastecimiento en el que individuos u organizaciones obtienen bienes y servicios. Estos servicios incluyen ideas y finanzas de un gran grupo de usuarios de Internet, relativamente abierto ya menudo en rápida evolución; divide el trabajo entre los participantes para lograr un resultado acumulativo.

CIS: Center for Internet Security, Inc. Entidad conformada por una comunidad global de profesionales de TI experimentados y voluntarios del medio.

NIST: National Institute of Standards and Technology, es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos.

SB: Superintendencia de Bancos del Ecuador, es la entidad encargada de controlar, regular y supervisar a las instituciones del sistema financiero del país

Vulnerabilidad: Es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo

Amenaza: Existen solo si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información.

Línea base de seguridad: conjunto de controles de seguridad orientados que son aplicados sobre los sistemas operativos.

CID: acrónimo que abrevia los principios de seguridad Confidencialidad, Integridad, Disponibilidad.

SUID: son permisos de acceso que pueden asignarse a archivos o directorios en un sistema operativo basado en Unix. Se utilizan principalmente para permitir a los usuarios del sistema ejecutar binarios con privilegios elevados temporalmente para realizar una tarea específica.

COBIT: Marco de referencia creado para ayudar a las organizaciones a obtener el valor óptimo de TI.

CMDB: Es un repositorio que relaciona todos los "elementos de configuración" de la organización y sus relaciones