Propuesta Metodológica para evaluar la seguridad del entorno informático de la Caja Central de cooperativas mediante procesos de Hardening.

Iza Sanhueza, Leyla Jennifer Maribel

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro De Posgrados

Maestría en Gerencia de Sistemas

Trabajo de Titulación, previo a la obtención del título de Magíster en Gerencia de Sistemas

Msc. Díaz Zúñiga, Magi Paúl

21 de septiembre del 2020

Curiginal

Document Information

Analyzed document	TesisLeylalzaSanhueza.pdf (D108308797)
Submitted	6/8/2021 10:30:00 PM
Submitted by	DIAZ ZUÑIGA PAUL
Submitter email	mpdiaz@espe.edu.ec
Similarity	3%
Analysis address	mpdiaz.espe@analysis.urkund.com

MAGI PAUL DIAZ

Sources included in the report

W	URL: https://hal.inria.fr/hal-01684351/document Fetched: 6/8/2021 10:32:00 PM	1
W	URL: https://patentimages.storage.googleapis.com/6b/9a/c3/e97f643448406b/US10181029.pdf Fetched: 6/8/2021 10:32:00 PM	1
W	URL: https://docplayer.es/74208916-Implementacion-de-pruebas-de-penetracion-a-los-sistemas-informaticos-de-una-entidad-gubernamental-lina-maria-salinas-galindo-jennifer-vasquez-ortiz.html Fetched: 2/23/2021 4:31:20 AM	1
W	URL: https://www.redbubble.com/shop/microsoft%252Bwindows%252Bposters Fetched: 6/8/2021 10:32:00 PM	1
W	URL: https://www.cyber.gov.au/acsc/view-all-content/publications/hardening-microsoft-windows-10-version-1909-workstations Fetched: 6/8/2021 10:32:00 PM	7
W	URL: https://www.microsoft.com/security/blog/2019/04/11/introducing-the-security-configuration-framework-a-prioritized-guide-to-hardening-windows-10/ Fetched: 6/8/2021 10:32:00 PM	2

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

CERTIFICACIÓN

Certifico que el trabajo de titulación, **"Propuesta Metodológica para evaluar la seguridad del entorno informático de la Caja Central de cooperativas mediante procesos de Hardening"** fue realizado por la señorita **Iza Sanhueza, Leyla Jennifer Maribel** el mismo que ha sido revisado y analizado en su totalidad, por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 21 de septiembre del 2020

Firma:

.....

MAGI PAUL DIAZ

Díaz Zúñiga, Magi Paúl

Director

C.C.: 1707249072

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

RESPONSABILIDAD DE AUTORÍA

Yo **Iza Sanhueza, Leyla Jennifer Maribel**, con cédula de ciudadanía n° 1716810872, declaro que el contenido, ideas y criterios del trabajo de titulación: **Propuesta Metodológica para evaluar la seguridad del entorno informático de la Caja Central de cooperativas mediante procesos de Hardening** es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 21 de Septiembre del 2020

Firma

.....

Iza Sanhueza, Leyla Jennifer Maribel

C.C.: 1716810872

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

AUTORIZACIÓN DE PUBLICACIÓN

Yo **Iza Sanhueza, Leyla Jennifer Maribel,** con cédula de ciudadanía n° 1716810872, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **Título**: **Propuesta Metodológica para evaluar la seguridad del entorno informático de la Caja Central de cooperativas mediante procesos de Hardening** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 21 de Septiembre del 2020

Firma

.....

Iza Sanhueza, Leyla Jennifer Maribel

C.C.:1716810872

AGRADECIMIENTO

Agradezco a mi familia por su apoyo incondicional, su paciencia y sus enseñanzas, por la unión que representamos y ha servido para ir logrando cada una de las metas propuestas

Al Ing. Paúl Díaz, por la orientación brindada en el desarrollo del presente proyecto, el mismo que representa el cumplimiento de la meta planteada.

Leyla Jennifer Maribel Iza Sanhueza

DEDICATORIA

A mis padres que me han inculcado el mejor regalo que pudieron brindarme es la sed por aprender y superarme cada día, por su amor, fuerza y apoyo.

A mis hermanos y al pequeño Mati que son mi apoyo incondicional por la confianza que me brindan día a día.

A mis amigas por ser mi soporte e incentivarme a seguir adelante cumpliendo mis metas académicas y personales

Gracias.

Leyla Jennifer Maribel Iza Sanhueza

Tabla de contenidos

Índice de Tablas

Índice de Figuras

RESUMEN

El presente trabajo de titulación consiste en realizar una propuesta metodológica que se desarrollará en base a la evaluación de la seguridad en un entorno informático, en este caso se efectuará la práctica en una entidad financiera como lo es la Caja Central realizando un levantamiento de información en base a las vulnerabilidades que están consideradas en los lineamientos del Hardening utilizando el framework CIS Benchmark en el que se detallan los procesos a seguir en base a la clasificación de activos se consideran el software y comunicaciones.

La metodología a utilizar es inductiva, es decir se procederá con la recolección de información sobre los activos que conforman el entorno informático y se los clasificará de acuerdo a su tipo; con dicho detalle se aplicará la definición de los frameworks de hardening para determinar los estándares de configuración segura para plantear políticas, mejores prácticas, guías y procedimientos, los que se describen para la propuesta metodológica; y se plasmara cada uno de ellos con el objetivo de minimizar los riesgos de seguridad que pueden enfrentar la Caja Central en su entorno informático.

En base a lo expuesto se generarán conclusiones y recomendaciones que se deben aplicar en el entorno informático, considerando salvaguardar la información que es el activo más importante de la institución y como un plan futuro poder dar a conocer en las Cooperativas de Ahorro y Crédito socias.

***Palabras Clave*:**

- **HARDENING**
- **SEGURIDAD DE LA INFORMACIÓN**
- **CONFIGURACIONES DE SEGURIDAD**
- **INVENTARIO DE ACTIVOS INFORMÁTICOS**

ABSTRACT

In the present project consists of making a methodological proposal which will be developed based on the evaluation of security in a computing environment, in this case the practice of the same will be carried out in a financial entity such as the “Caja Central”, making a Information gathering based on the vulnerabilities that are considered in the Hardening guidelines using the CIS Benchmark framework in which the processes to be followed are detailed based on the classification of assets in which software and communications are considered.

The methodology to be used is inductive, that is it will proceed with the collection of information on the information assets that make up the computing environment, each one of them will be classified according to their type; with this detail the definition of the hardening frameworks will be applied in which the safe configuration standards can be determined to propose policies, best practices, guides and procedures, which are detailed for the methodological proposal; and each one of them was shaped with the objective of minimizing the security risks that the Caja Central may face in its computing environment.

Based on the above, conclusions and recommendations will be generated that should be applied in the computing environment, considering safeguarding the information that is the most important asset of the institution and as a future plan to be able to make it known in the Cooperativas de Ahorro y Crédito members.

***Key words*:**

- **HARDENING**
- **INFORMATION SECURITY**
- **SECURITY SETTINGS**
- **IT ASSET INVENTORY**

Capítulo I.

Planteamiento del problema de investigación

Antecedentes

Hoy en día, con el avance la tecnología se tiene que tener presente el tema de la seguridad de la información, se ha evidenciado que han ido creciendo de forma exponencial los ataques a los entornos informáticos es por ellos que deben ser tratados las vulnerabilidades de los mismos en las instituciones de forma general, en este caso específicamente en las que prestan servicios financieros, es por ello que las instituciones deben precautelar la seguridad por los riesgos a los que se puede exponer el entorno informático de una institución, para lo cual se recomienda el uso de metodologías que puedan minimizar las vulnerabilidades; en este caso con procesos de hardening que se aplicaran en la Caja Central de cooperativas tanto por disolver amenazas y dar cumplimiento a regulaciones por los entes de control.

Problema Macro

El problema del presente proyecto se lo plantea con referencia a la seguridad informática, en las entidades financieras en este caso la Caja Central de cooperativas cuenta y adquiere activos de información para diversos proyectos y desarrollo de nuevos productos, pero se centran en dar funcionalidad al mismo sin revisar las configuraciones de forma que se disminuyan las brechas de seguridad al utilizar activos con configuraciones por default y adicional validar los actuales de forma de establecer una propuesta metodológica, la cual se la generaría con

procesos de hardening de forma de utilizar un estándar para el uso dentro del entorno informático de la institución.

Por lo que el problema planteado se lo desarrollara en base a las vulnerabilidades que se pueden presentar en el entorno informático que se ha identificado como primer punto el clasificar los activos según las categorizaciones utilizadas que son software y comunicaciones, utilizando normas para el desarrollo de las misma en este caso tenemos los Framework CIS[1] las que abarcan el análisis de sistemas operativos, bases de datos, dispositivos de red, software de servidores y equipos de escritorio; nos servirán para contar con políticas, mejores prácticas y recomendaciones que deben ser tomadas para minimizar los riesgos de seguridad, con el objetivo salvaguardar la información.

En el análisis de vulnerabilidades se realizarán revisión de servidores, configuraciones de los sistemas operativos, revisión de puertos, equipos de comunicación, accesos de usuarios, de donde se obtendrán los resultados que permitirán plantear medidas de seguridad que sean parte de la propuesta metodológica de forma de aplicarla en entornos informático de este tipo de instituciones.

Objetivo General

Generar una propuesta metodológica aplicable a la Caja Central en base a los procesos de hardening establecidos que permitan plantear estándares de configuración para poder solventar vulnerabilidades en el entorno informático de la institución.

Objetivos Específicos

- ✓ Clasificar los activos informáticos para identificar los ítems que pueden generar vulnerabilidades por lo que se realizará el levantamiento de los activos informáticos.

- ✓ Proteger los activos de información aplicando procedimientos de Hardening; que permitirán plantear estándares de configuración en los dispositivos del entorno informático y definir los ítems que se deben considerar por cada activo revisado.

- ✓ Generar un listado de puntos de verificación que debe ser incluido dentro de los procesos de ingreso de activos al entorno informático de la institución para su correspondiente aplicabilidad según la evaluación obtenida del hardening bajo el framework CIS benchmark.

Capítulo II.

Marco Teórico

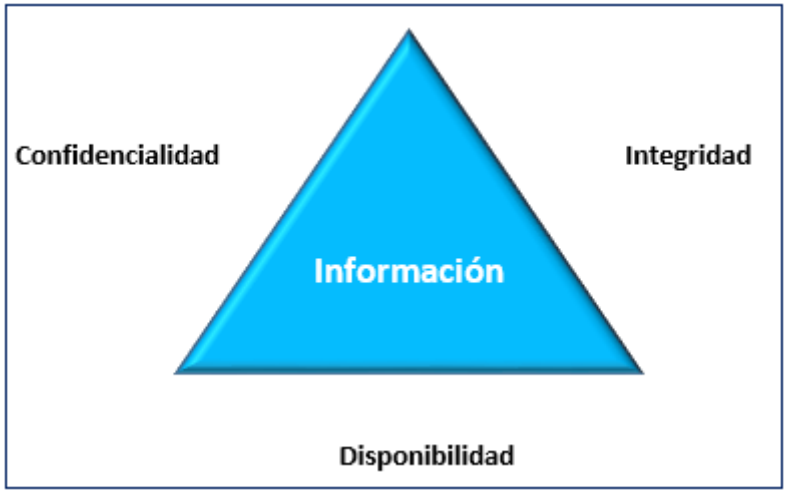
Seguridad de la Información

La seguridad de la información se basa en las medidas y controles que se apliquen en un entorno informático con el objetivo de salvaguardar la información; el activo más importante y sensible dentro de las organizaciones.

La seguridad informática se basa en tres principios básicos como lo indica el triángulo de la seguridad que son confidencialidad, integridad y disponibilidad, entre ellos debe existir un equilibrio para el correcto funcionamiento de un entorno informático, es decir no disminuir usabilidad por seguridad y viceversa.

Figura 1.

Triángulo de la seguridad de la información



Fuente: ***(Charles, 2019)***

La confidencialidad: es el estado en que la información debe ser conocida solo por las áreas y/o personas autorizadas

La integridad: Trata sobre que la información no debe ser manipulada y permanecer auténtica en todo su ciclo.

La disponibilidad es el hecho de que siempre se pueda tener el acceso a la información.

Vulnerabilidades, amenazas y riesgos informáticos

El objetivo de incluir políticas de seguridad dentro de un entorno informático es poder mitigar las amenazas y vulnerabilidades, analizando el impacto de riesgo que pueden generar dentro de una institución.

Vulnerabilidad informática

Las vulnerabilidades son debilidades que ponen en riesgo el entorno informático, al permitir que se pierda las condiciones primordiales de la seguridad de la información como lo es la confidencialidad, integridad y disponibilidad. (Incibe, 2017)

Clasificación de vulnerabilidades.

- Vulnerabilidades ya conocidas en recursos instalados
- Vulnerabilidades ya conocidas en recursos no instalados
- Vulnerabilidades no conocidas

En la actualidad las que causan mayor impacto son las no conocidas porque aún no se ha aplicado un plan de acción para mitigarlas y/o eliminarlas; pueden ser aprovechadas por personal malintencionado. (VIU, 2018)

Amenazas informáticas

La amenaza informática se la puede considerar como las acciones que pueden producir un fallo en la seguridad informática, estas aparecen en base a la existencia de vulnerabilidades, es decir cuando una de ellas puede ser aprovechada para producir riesgo en el entorno informático. (Luján, s.f.)

Se pueden presentar amenazas en base a procesos de ingeniería social, falta de cultura en cuanto a la seguridad informática para los usuarios y ataques intencionales que han crecido de forma exponencial en los últimos años.

Tipos de amenazas informáticas.

Los tipos de amenazas pueden ser agrupados en dos grupos

- Intencionales: Son las que se enfocan en causar daño o pérdida de información
    - Trashing
    - Ingenieria social
    - Código de seguridad
- No intencionales: Son las que se producen por omisiones o acciones no consideradas y no ejecutadas a propósito

Amenazas intencionales.

Trashing

Es la recolección de información de cestos de basura, ya sea física como son los papeles o desperdicios que se generan en una institución; y el lógico al revisar la papelera de reciclaje o historial de navegación en un equipo sin protección.

Ingeniería social

Es la obtención de información por varias vías como por ejemplo telefónica o personal utilizando la persuasión o la falta de precaución de la persona para obtener información sensible realizando un sin número de preguntas que a un futuro puede generarse un ataque.

Código malicioso

Los códigos maliciosos son diversos, pueden identificarse los scripts que permiten utilizar las vulnerabilidades en los sistemas; permitir la apertura de puertas traseras, brechas de seguridad, robo de información, datos y virus. (Kaspersky, 2019)

Riesgo

El riesgo es la probabilidad de que una amenaza y/o vulnerabilidad se materialice produciendo pérdidas y/o daños, en nuestro caso en el entorno informático.

Figura 2.

Amenazas y vulnerabilidades

Fuente: *(Incibe, 2017)*

Sistemas de Información y entornos informáticos

Sistemas de Información (SI)

Son conjuntos de datos o mecanismos que interactúan entre sí para un resultado común; estos sirven para administrar la información y sea procesada de forma ágil y ayude en el desarrollo de la institución.

Entorno informático

El entorno informático son todos los componentes de hardware, software y comunicaciones que se utilizan en el área informática.

Al tratar el tema de la seguridad de la información, es importante conocer los dominios que se destacan en el desarrollo del presente proyecto, se identifican los estándares que existen actualmente en la ISO 27001, el mismo que nos sirve para marcar pautas dentro de una institución.

Figura 3.

Entorno informático

Fuente: *(Definicion ABC, 2019)*

ISO 27001

La ISO 27001 es un estándar en el cual se basa el sistema de gestión de seguridad de la información, mismo que debe generarse mediante procesos sistematizados, documentados y que sean conocidos por toda la institución.

Es una norma española, en nuestro país ha sido adoptada por la norma técnica ecuatoriana denominada INEN-ISO/IEC 27001.

Los ítems que se consideran en base a la norma son los que van enfocados a los siguientes controles. (Ecuatoriana, 2017)

Seguridad de las comunicaciones - ítem 6

En el punto 6 de la norma sobre la organización en la seguridad de la información es un ítem que se acopla en el desarrollo del presente proyecto ya que define la gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.

En cuanto a la implantación de dicho control detallado en la norma es el tema de identificar y definir los activos y procesos de seguridad de la información y documentarse los niveles de autorización

Gestión de Activos - ítem 8

Es el proceso de administración de activos que se manejan dentro de la institución entre los cuales se pueden considerar el software, hardware y comunicaciones, estos deben estar bien detallados dentro de un inventario y como objetivo principal identificar las protecciones que requiere cada uno de ellos, adicional deben ser clasificados de forma de reconocer el impacto que se generaría en el caso de que los activos no se encuentren protegidos de forma correcta.

Figura 4.

Entorno informático

Fuente: *(Pandora, 2019)*

Hardening

El hardening es el proceso de endurecer y/o fortalecer las seguridades en una etapa inicial de configuración de los activos que conforman el entorno informático de una institución, dicho proceso se lo realiza al minimizar las vulnerabilidades como por ejemplo eliminar usuarios, software o servicios que no deben estar activos; así también el cierre de puertos por default para esto se debe realizar un análisis en base al inventario que se encuentre en la institución.

Los beneficios que se obtienen al realizar dicho proceso en etapas iniciales es el aseguramiento de los recursos críticos dentro de la institución, ejemplos de su aplicación se pueden definir el tener los parches de seguridad actualizados, de esta forma el recurso puede defenderse de ataques conocidos, también se puede considerar que si se requiere realizar un cambio podrá facilitar dicho proceso al conocer las configuraciones de cada recurso, adicional se mejora la seguridad de los sistemas frente a amenazas internas y/o externas y minimiza el riesgo que involucra el factor humano y fraudes que podrían generarse.

Para identificar los ítems a analizar en el hardening se revisará los puntos de estudio dentro del framework CIS benchmark, según el punto de estudio dentro del entorno informático.

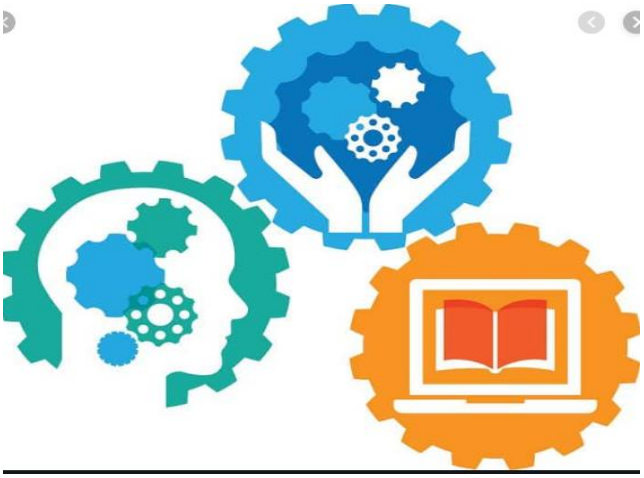
Framework Cis Benchmarking

Framework

Es un marco de referencia que se puede optar porque cuenta con pasos descritos de forma organizada para el desarrollo de diversos tipos de proyectos, estos se desarrollan en varias áreas de la informática; en este caso se tomará como base el framework Cis Benchmarking que se lo aplica en el desarrollo del hardening y se lo puede identificar para los componentes del entorno informático.

Figura 5.

Framework



Fuente *(cero, 2019)*

Framework Cis Benchmark

Actualmente el centro de seguridad de internet ha desarrollado el framework cis benchmark aplicable en el hardening; se han considerado el análisis de los siguientes ítems para su desarrollo

- Sistemas operativos
- Proveedores de sistemas en la nube
- Software de servidores
- Dispositivos móviles
- Dispositivos de red
- Software de equipos para usuarios finales
- Dispositivos de impresión (Cis-benchmarks, 2019)

Para un mayor detalle de los ítems que se consideran en el cis benchmark se detalla el siguiente software.

Tabla 1.

Software base de análisis de Benchmark

Ítem Análisis	Detalle Software
Sistemas operativos	Amazon Linux
	Apple OS
	CentOS Linux
	Debian Linux
	Distribution independiente linux
	IBM AIX
	Microsoft Windows desktop
	Microsoft Windows Server
	Oracle Linux
	Oracle Solaris
	Red Hat Linux
Proveedores de sistemas en la nube	Amazon Web Services
	Google Cloud Computing Plataform
	Microsoft Azure
Software de servidores	Apache Cassandra
	Apache Http Server
	Apache Tomcat
	Bind
	Docker
	IBM DB2
	Kubernetes
	Mir Kerberos
	Microsoft IIS
	Microsoft SQL Server
	Microsoft Sharepoint
	Mongo DB
	NGINX
	Oracle Database
	Oracle Mysql
	Postgre SQL
Dispositivos móviles	Apple IOS
	Google Android
Dispositivos de red	Cisco
	Juniper
	Palo Alto Networks

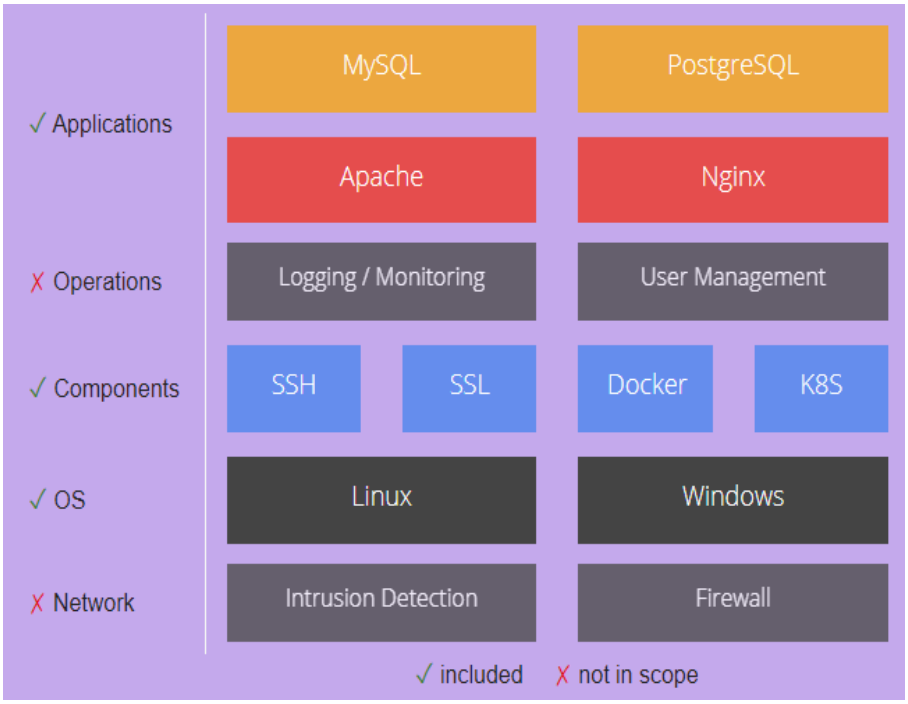
Software de equipos para usuarios finales	Google Chrome Microsoft Exchange Server Microsoft internet explorer Microsoft Office Mozilla Firefox
Dispositivos de impresión Multifunción	Dispositivos de impresión

DevSec Hardening Framework

Generado por una comunidad el hardening DevSec (Richter Dominik, 2020) es un marco de automatización, que se configura en sistemas operativos y varios servicios, brindando las pautas de cumplimiento de configuraciones, recomendaciones de criptografía y valores predeterminados seguros. (Adkins, 2020)

Figura 6.

DevSec Hardening Frameworks Baselines



Fuente *(Hartmann, 2020)*

Hardening Windows 10

Es un marco de seguridad generado por Microsoft con el objetivo de simplificar la configuración de seguridad y al mismo tiempo permitir la flexibilidad suficiente para permitirle equilibrar la seguridad, la productividad y experiencia del usuario; por lo que Microsoft desarrolla configuraciones prescriptivas que funcionen en varios escenarios según los requerimientos comunes que se visualizan en las empresas. (Jackson, 2019).

Microsoft ha planteado cinco escenarios con diferentes alertas de seguridad subdivididos en dispositivos de productividad y privilegios de accesos de estaciones de trabajo

Figura 7.

Framework configuración de seguridad Windows 10

Fuente *(Microsoft, 2019)*

Hardening Framework

El hardening framework (Puppet Forge, 2015) está compuesto de cuatro módulos que se subdividen en:

- ✓ OS Hardening: Configuración de sistemas operativos con hardening, como son: Redhat, Ubuntu, Debian, CentOS, OracleLinux, OpenSuse,

(Hardening framework, 2020), se puede evidenciar que son sistemas operativos basados en Linux.

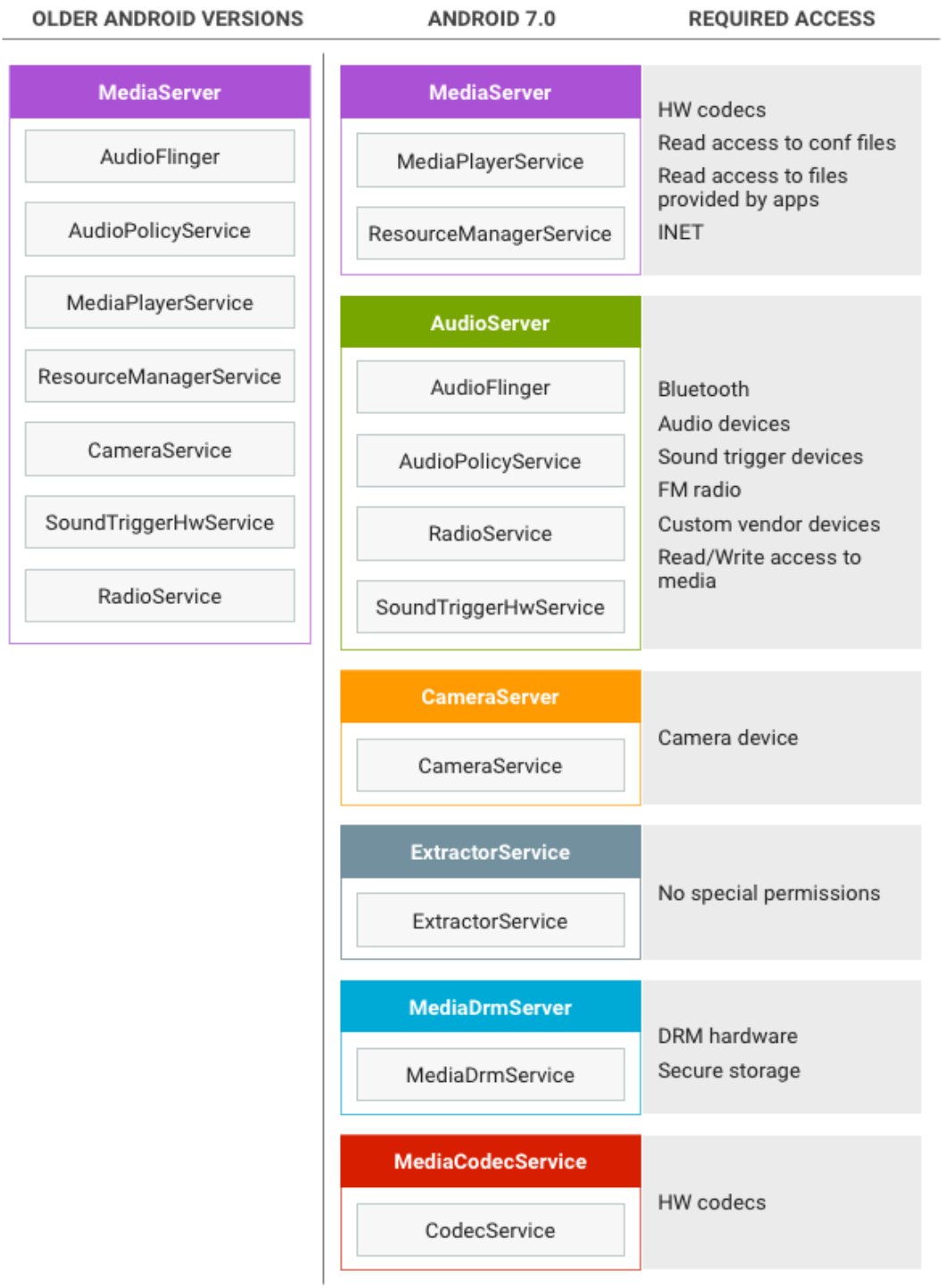
- ✓ Ssh hardening: Instalación y configuración segura de clientes y servidores con ssh. (Puppet Forge, 2015)
- ✓ Hardening stdlib (Puppet Forge, 2014)
- ✓ Mysql Hardening: Configuraciones de Mysql con hardening. (Framework, 2016)

Hardening Media Framework

Hardening del marco de medios es el mejoramiento de la seguridad en dispositivos con sistema operativo Android; con el objetivo de mejorar la seguridad para los usuarios finales en las aplicaciones. (Developers, 2020).

Figura 8.

Arquitectura para el endurecimiento de servidor de medios



Fuente *(Media, 2020)*

Artículos científicos utilizados en Hardening

Adicional se puede verificar artículos científicos en donde se aplica hardening en diferentes entornos informáticos que pueden revisarse con el objetivo de tener un mayor panorama de su aplicabilidad y de lo relacionado con las debilidades que puedan presentarse.

- ✓ Un artículo publicado por la Feria internacional para la transformación digital del 2020 en la Habana Cuba con tema *Configuraciones Internas para el fortalecimiento de la seguridad en NGXIS* (Blanco, Chang, & Brito, 2020), en el cual se evidencia un fortalecimiento en servidores web con NGXIS que presenta seguridades mejoradas y acelera la entrega del contenido y aplicaciones.

- ✓ Debilidades de seguridad comúnmente explotadas. (Mieles, 2009); para poder realizar la identificación o levantamiento de ítems de fortalecimiento es importante reconocer las debilidades comunes.

- ✓ Defensa en profundidad aplicado a un entorno empresarial publicado en la revista ESPACIOS (GUIJARRO-Rodríguez, YEPEZ-Holgin, PERALTA-Guaraca, & Mirella, 2018), el cual contempla los ítems de la red que deben ser validados.

- ✓ El Sistema Financiero y la Seguridad Informática. (Hernández & Rocio, 2013), donde puede evidenciarse temas de cibercrimen y estándares de gestión tecnológica en entidades financieras.

- ✓ Hardening en dispositivos de red: Routers y Switch. (Martínez Cruz, 2015) el análisis está enfocado en dichos dispositivos al considerarse la columna vertebral de infraestructuras de tecnologías de información.

- ✓ Refuerzo óptimo de la seguridad de la red mediante Attack Graph - Optimal Network Security Hardening Using Attack Graph Games (Karel Durkota, 2015).

- ✓ Protección de las redes contra lo desconocido y lo inalcanzable, vulnerabilidades que utilizan opciones de hardening heterogéneas -Securing Networks Against Unpatchable and Unknown Vulnerabilities Using Heterogeneous Hardening Options. (Daniel Borbor, 2017)

- ✓ Hardening de bóvedas con acceso de huellas digitales mediante contraseñas – Hardening Fingerprint Fuzzy Vault Using Password. (Jain, 2007)

- ✓ Hardening de seguridad de software de código abierto - Security Hardening of Open Source Software. (Azzam Mourad, 2014).

- ✓ Fortalecimiento de la robustez y seguridad de las bibliotecas de software COTS - Robustness and Security Hardening of COTS Software Libraries. (Susskraut, 2007).

- ✓ Hardening de seguridad en la nube de software de aplicaciones móviles - Security cloud service framework for hardening in the field code of mobile software applications. (Osman Abdoul Ismae, 2017)

Capítulo III.

Desarrollo de Metodología

Para el desarrollo del presente proyecto se realizará el análisis en base al framework CIS Benchmark presentado en el marco teórico y en comparación con el resto de framework analizados, como son:

Tabla 2.

Comparativo de frameworks

Frameworks	Sistema Operativo			Bases de Datos	Servidores Web	Ofimática
	Linux	Microsoft	Dispositivos móviles			
Cis Benchmarking framework	√	√	√	√	√	√
DevSec Hardening Framework	√			√	√	√
Hardening Windows 10		√				
Hardening Framework	√					
Hardening Media Framework			√			

Se escogió el Cis Benchmark framework por ser el más completo al abarcar la mayoría de ítems que componen el entorno informático de la institución que se trabaja con plataformas Microsoft por políticas internas determinadas dentro del manual de la institución, pese a esto es compleja y extensa su aplicación por lo que se planteó la generación de la metodología propuesta, la cual debe ser práctica para su uso; por lo que el levantamiento de la metodología siendo está más clara para las instituciones que requieren su aplicabilidad y dando cumplimiento a la normativa requerida por el ente de control como lo es la Superintendencia de Economía Popular y Solidaria (SEPS) de Riesgo Operativo. (SEPS, 2018)

Desarrollo inventario de activos tecnológicos

El levantamiento del inventario de activos tecnológicos es la línea base que se debe obtener y mantener dentro de un área de tecnología de forma de contar con su registro y las configuraciones de cada dispositivo en cuanto a seguridad y aplicar el hardening propuesto.

En la institución se cuenta con equipos host de 33 dispositivos y servidores para los servicios internos de reportes, inversiones, Core central para intermediación financiera y los servicios transaccionales que se ofertan a los clientes.

Po lo que para el levantamiento de los activos tecnológicos lo podemos realizar de varias formas, lo primordial es identificar que debe existir el proceso y su ejecución, puede iniciarse con un registro en una matriz donde se cuenten con los datos, por ejemplo:

- Tipo de dispositivo
    - Servidor
    - Equipos host (all in one, de escritorio, laptop)
    - Equipos de comunicaciones (switch, router, firewall, Access point, etc)
- Sistema Operativo
- Memoria
- Disco duro
- Procesador

El objetivo es poder incluir los ítems que genera la metodología por lo que siempre que sea incluido un nuevo dispositivo sea aplicable la metodología.

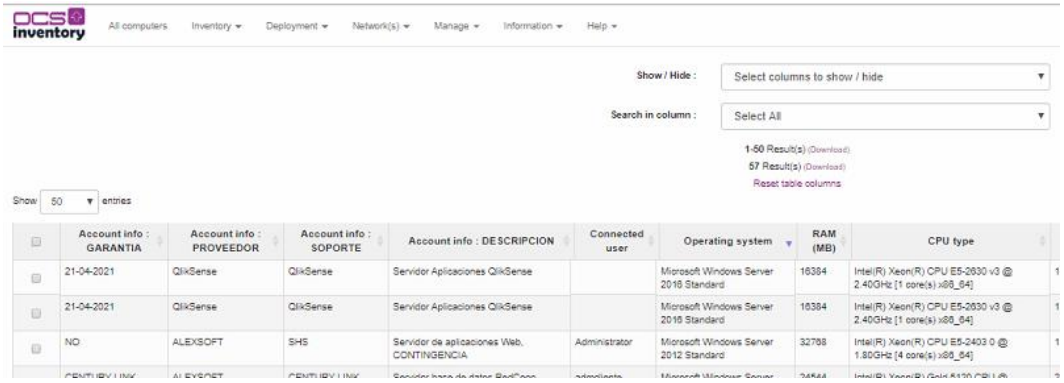
Existes varias herramientas para la gestión de activos informáticos (Freshservice, 2020), y su automatización para lo cual se tienen varias opciones, como, por ejemplo:

- ✓ OCS Inventory (Source, 2017)
- ✓ GLPI (Teclib, 2015 - 2020)
- ✓ Network Inventory Advisor (Blume, 1999-2020)

De las herramientas indicadas se escogió utilizar la herramienta free OCS Inventory (Source, 2017), esto se definió internamente en la institución porque la versión free es más completa sobre la información que se puede recolectar de las herramientas indicadas tiene una consola gráfica que permite un mayor entendimiento y validación en el caso de auditorías, pero es un ejemplo para la práctica en otras organizaciones se puede utilizar la que se adapte a la realidad de la organización al tener claro que el objetivo es la recolección de información de forma automática de los equipos que se utilizan dentro del entorno informático de la institución.

Figura 6.

Captura herramienta OCS Inventory



De forma general para tener la perspectiva de los dispositivos que conforman el entorno informático de la institución, se visualiza en el Anexo 1 del diagrama de red.

Los servidores se han ingresado por su usabilidad dentro del entorno informático, en el mismo se ha detallado el sistema operativo que es el primer ítem que se debe identificar en el análisis a realizar dentro del framework para ir desarrollando la metodología del hardening.

Como se puede identificar en la Tabla 2, se verifica que se utilizan sistemas operativos bajo plataformas Windows y según su funcionalidad se los ha clasificado entre web, aplicaciones y bases de datos, adicional cabe indicar que los servidores especificados se encuentran considerados los ambientes de certificación, contingencia y producción.

Tabla 3.

Detalle de servidores con sistema operativo

Núm.	Tipo de Servidor	Sistema Operativo
1	Servidor de Aplicaciones Web	Microsoft Windows Server
2	Servidor Directorio Activo	Microsoft Windows Server
3	Servidor Base de Datos	Microsoft Windows Server
4	Servidor Base de Datos	Microsoft Windows Server
5	Servidor Base de Datos	Microsoft Windows Server
6	Servidor de Aplicaciones Web	Microsoft Windows Server
7	Servidor Base de Datos	Microsoft Windows Server
8	Servidor de aplicaciones Web	Microsoft Windows Server
9	Servidor de aplicaciones Web	Microsoft Windows Server
10	Servidor de aplicaciones Web	Microsoft Windows Server
11	Servidor de Aplicaciones	Microsoft Windows Server
12	Servidor Web	Microsoft Windows Server
13	Servidor Base de Datos	Microsoft Windows Server
14	Servidor Base de Datos	Microsoft Windows Server
15	Servidor Branch - Aplicaciones	Microsoft Windows Server
16	Servidor imágenes	Microsoft Windows Server

17	Servidor Branch – Aplicaciones	Microsoft Windows Server
18	Servidor de aplicaciones Web	Microsoft Windows Server
19	Servidor Base de Datos	Microsoft Windows Server
20	Servidor Aplicaciones	Microsoft Windows Server

Adicional en el análisis a realizar se va a obtener también las especificaciones de los equipos de los funcionarios de manera detallada como se verifica en la Tabla 3, se evidencia que hay un total de 31 equipos

Tabla 4.

Equipos de funcionarios

Núm.	Modelo	Sistema Operativo
1	HP ProOne AiO	Microsoft Windows 10 Pro
2	Latitude	Microsoft Windows 10 Pro
3	All Series	Microsoft Windows 7 Professional
4	HP ProBook G2	Microsoft Windows 7 Professional
5	HP ProBook G1	Microsoft Windows 7 Professional
6	HP EliteDesk G1 SFF	Microsoft Windows 7 Professional
7	HP EliteDesk G1 SFF	Microsoft Windows 7 Professional
8	HP EliteDesk G1 SFF	Microsoft Windows 7 Professional
9	OptiPlex	Microsoft Windows 10 Pro
10	Latitude	Microsoft Windows 10 Pro
11	Inspiron	Microsoft Windows 7 Professional
12	Inspiron	Microsoft Windows 7 Professional
13	Latitude	Microsoft Windows 10 Pro
14	Inspiron	Microsoft Windows 10 Pro
15	OptiPlex AIO	Microsoft Windows 10 Pro
16	Latitude	Microsoft Windows 10 Pro
17	HP ProBook G5	Microsoft Windows 10 Pro
18	Latitude	Microsoft Windows 10 Pro
19	HP ProDesk G3 SFF	Microsoft Windows 10 Pro
20	Inspiron	Microsoft Windows 7 Professional
21	OptiPlex AIO	Microsoft Windows 10 Pro
22	Latitude	Microsoft Windows 10 Pro
23	OptiPlex AIO	Microsoft Windows 10 Pro
24	OptiPlex AIO	Microsoft Windows 10 Pro
25	HP ProBook G5	Microsoft Windows 10 Pro

26	Latitude	Microsoft Windows 10 Pro
27	Latitude	Microsoft Windows 10 Pro
28	81B0	Microsoft Windows 10 Pro
29	HP ProBook G1	Microsoft Windows 10 Pro
30	OptiPlex AIO	Microsoft Windows 10 Pro
31	HP ProBook G2	Microsoft Windows 7 Professional

Como adicional también se deben analizar los equipos de comunicaciones que se utilizan en la institución.

Tabla 5.

Dispositivos de comunicaciones

TIPO DE DISPOSITIVO	MARCA	MODELO
ACCESS POINT	CISCO	WAP
SWITH	CISCO	SG
FIREWALL	SOPHOS	XG230
ROUTER	MIKROTIK	RB

Identificación de recursos dentro del entorno informático

La identificación de recursos dentro del entorno informático es clasificar los dispositivos según su funcionalidad en base al inventario levantado en el paso anterior, entre ellos de manera general se cuenta con:

- Servidor de directorio activo
- Servidores de aplicaciones
- Servidores web
- Servidores de base de datos
- Equipos de escritorio

Servidor de directorio activo: Su funcionalidad se basa directamente en poder aplicar funciones de autorización, autenticación para los empleados de la institución.

Servidor de directorio activo	Sistema Operativo	Ambiente
	Microsoft Windows Server 2012 R2 Standard	Producción

Servidores de aplicaciones: En dichos servidores se encuentran cargados los aplicativos que se utilizan tanto para usuarios internos y externos.

Servidores web: Se encuentran publicados los servicios para los usuarios internos y externos según su usabilidad.

En el caso de la institución se tienen algunos servidores en donde se encuentran levantados tanto los servicios web y aplicaciones como son el portafolio de inversiones, reportería y los servidores donde se realizan pruebas y certificación de aplicativos que se encuentran dentro de la red LAN, en el caso de los servicios publicados para los socios se encuentran los servicios en tres capas ya son estos web, aplicaciones y base de datos.

Tabla 6.

Servidores de aplicaciones y web

Tipo de Servidor	Software Adicional	Sistema Operativo	Ambiente
Servidor de Aplicaciones Web	Internet Information Services	Microsoft Windows Server Standard	Contingencia
Servidor de Aplicaciones Web	Internet Information Services / Sw – Propietario	Microsoft Windows Server Standard	Certificación
Servidor de aplicaciones Web	Oracle Web Logic	Microsoft Windows Server Standard	Producción
Servidor de aplicaciones Web	Internet Information Services / Sw – Propietario	Microsoft Windows Server Standard	Certificación
Servidor de aplicaciones Web	Internet Information Services / Sw – Propietario	Microsoft Windows Server Standard	Certificación
Servidor de Aplicaciones	Aplicativo Web	Microsoft Windows Server Standard	Producción

Servidor Web	Internet Information Services	Microsoft Windows Server Standard	Producción
Servidor Branch – Aplicaciones	Aplicativo Core central / Microsoft Office	Microsoft Windows Server Standard	Contingencia
Servidor Branch – Aplicaciones	Aplicativo Core central / Microsoft Office	Microsoft Windows Server Standard	Producción
Servidor de aplicaciones Web	Internet Information Services	Microsoft Windows Server Standard	Producción
Servidor de Aplicaciones	Eset	Microsoft Windows Server Standard	Producción

Servidores de Base de Datos: Estos servidores son utilizados por las aplicaciones para almacenar la información que ellos generan, en cuanto a las bases de datos se pueden trabajar con diferentes motores.

Tabla 7.

Servidores de base de datos

Tipo de Servidor	Software Adicional	Sistema Operativo	Ambiente
Servidor Base de Datos	Sql Server	Microsoft Windows Server Standard	Contingencia
Servidor Base de Datos	Sql Server	Microsoft Windows Server Standard	Contingencia
Servidor Base de Datos	Sql Server	Microsoft Windows Server Standard	Certificación
Servidor Base de Datos	Oracle	Microsoft Windows Server Standard	Producción
Servidor Base de Datos	Sql Server	Microsoft Windows Server Standard	Producción
Servidor Base de Datos	Sql Server	Microsoft Windows Server Standard	Producción
Servidor Base de Datos	PostgreSQL	Microsoft Windows Server Standard	Producción

En este caso para el análisis del framework CIS benchmarking para obtener la metodología del hardening se resumirá el software que se utiliza en los servidores detallados.

Tabla 8.

Resumen de software utilizado

Tipo de software	Nombre
Sistema operativo	Microsoft Windows Server Standard
Sistema operativo	Microsoft Windows Server Standard
Servidor Web	Internet Information Services
Servidor Web	Oracle Web Logic
Consola de bloqueo y antivirus	Eset Deslock
Motor de base de datos	Sql Server
Motor de base de datos	Sql Server
Motor de base de datos	Oracle
Motor de base de datos	PostgreSQL

Equipos de escritorio y laptop: Son los equipos que utilizan los usuarios finales de la institución según su ocupación contienen diferentes aplicaciones.

En este caso se utilizan los sistemas operativos Windows 7 Pro y Windows 10 Pro

Tabla 9.

Software de equipos de escritorio

Detalle	Software	Tipo
Word, Excel, Power Point y Outlook	Office 365	
Navegadores	Internet Explorer, Google Chrome	
Aplicativo central	Core Bancario	Cliente – Servidor
Aplicativo de portafolio	Gestor	Cliente – Servidor
Centralización de información	Sistema de reportes	Web
Servicios transaccionales	Switch	Web

Aplicación de framework CIS Benchmarking

Según cada uno de los activos tecnológicos, para la aplicación del framework se identificarán los procesos del hardening y se validará la funcionalidad dentro del entorno informático.

Se iniciará el análisis con el sistema operativo de los servidores que se utilizan.

- ✓ Windows Server 2008
- ✓ Windows server 2012
- ✓ Windows server 2016

Validación de framework en sistemas operativos

Esta aplicación se la realiza en el servidor del directorio activo porque en el mismo se configuran políticas que son aplicadas en los equipos con los que cuenta la institución.

Aplicación de políticas de cuentas de acceso.

Para la aplicación de políticas en cuanto a accesos y contraseñas nos hemos basado en las buenas prácticas que determina la norma ISO27001 sobre Sistemas de Gestión de la Seguridad de la información. (EXCELLENCE, 2020), de la cual se ha obtenido el Manual de Seguridad de la información de la institución. (Financoop, 2019)

Políticas de contraseñas

Las políticas de contraseñas deben ser aplicadas; con el objetivo de evitar especialmente los ataques de fuerza bruta y ataques de diccionario, por lo que la configuración se la realiza en el servidor del directorio activo, y estas políticas se replican a todos los equipos de la red, las políticas establecidas son parte del Manual se seguridad de la información de la institución, numeral 10.5.3 Administración de contraseñas. (Financoop, 2019)

Tabla 10*.*

Políticas de contraseñas

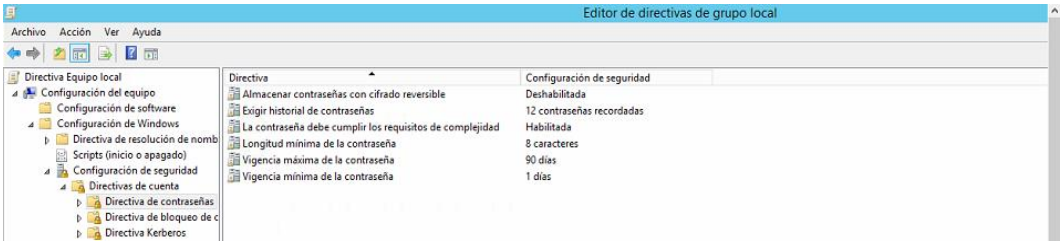
Políticas de contraseñas	Aplicar historial de contraseñas se aplica a las últimas 24 aplicadas
	Tiempo de vigencia de contraseñas de 60 días
	Tiempo mínimo de contraseña 1 día, antes de su primer cambio
	Longitud mínima de contraseñas 14 caracteres
	Cumplimiento de complejidad de contraseña

En el caso de que no exista directorio activo se recomienda realizar las configuraciones en cada uno de los equipos, pero es importante la inclusión del servidor para poder administrar las políticas.

> *Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy.*

Figura 7.

Configuración de políticas de contraseña



Políticas de bloqueo de cuentas.

Las políticas de bloqueo de cuentas deben ser configuradas para disminuir ataques de fuerza bruta y de denegación de servicios; de igual manera se lo realiza en el servidor de directorio activo y se replica a los equipos conectados en la red y están especificadas en el manual de seguridad de la información de la institución, numeral 10.3.3 (Financoop, 2019)

Tabla 11.

Políticas de bloqueo de cuentas

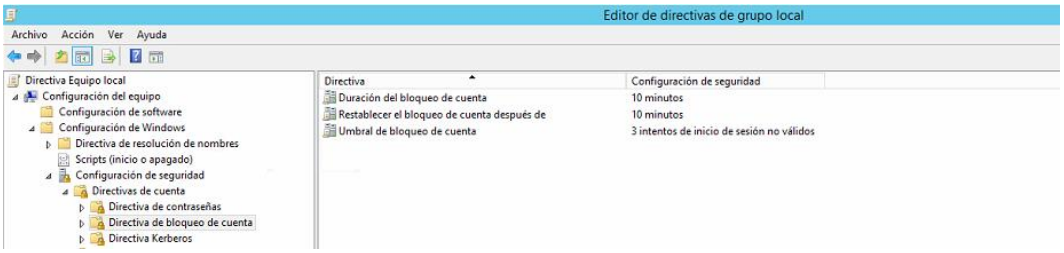
Políticas de bloqueo de cuentas	Duración del tiempo de desbloqueo automático de usuario en 15 minutos
	Umbral de intentos fallidos para bloqueo de cuenta
	Restablecer contador de bloqueo de cuenta después de tiempo determinado 15 minutos

En el caso de que no exista un directorio activo se recomienda realizar las configuraciones en cada uno de los equipos.

Computer Configuration\Windows Settings\Security Settings\Account Policies\ Account Lockout Policy.

Figura 8.

Configuración de bloqueo de cuentas.



Aplicación de políticas locales.

Políticas de auditoria.

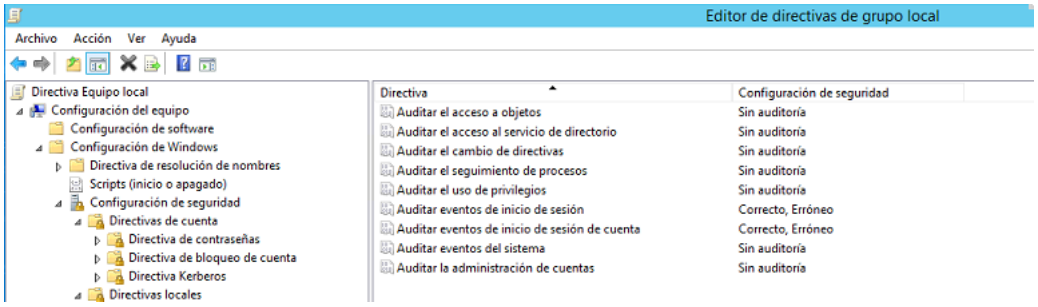
Entre las políticas de auditoria se debe tomar en cuenta la Administración de credenciales que sirve para realizar una copia de seguridad, por lo que ningún usuario debe mantener activa la política, de igual manera se lo establece en el active directory.

El objetivo de la política es que no exista la posibilidad de que un usuario al obtener dicho acceso; pueda diseñar un aplicativo que obtenga credenciales de otros usuarios, para su activación de forma manual se lo realiza en la siguiente opción:

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Access Credential Manager as a trusted caller

Figura 9.

Configuración de directivas de auditoria

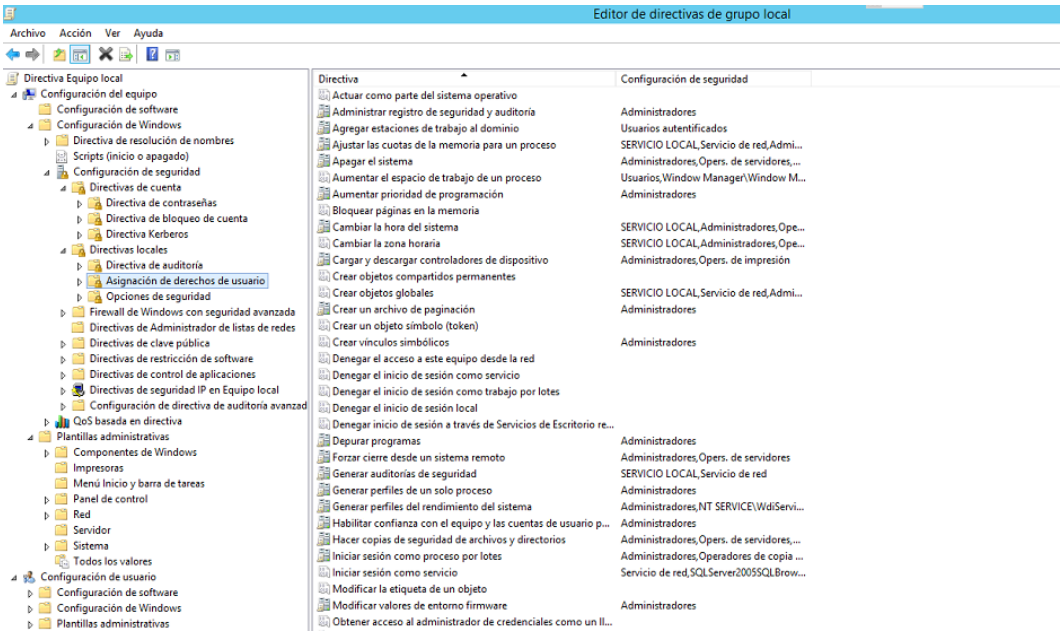


Acceso del computador desde la red.

El acceso debe ser controlado, porque al tener permisos hacia la red podría ingresar a la documentación compartida de áreas que no se encuentre autorizado, es por eso por lo que debe ser restringido a los que necesita, de igual manera se lo configura en el servidor de directorio activo para que se replique la política, también aplica el compartir dispositivos como impresoras.

Figura 10.

Configuración de accesos de red



Añadir usuarios como Administradores

Un administrador dentro del active directory puede crear usuarios de las estaciones de trabajo, el framework recomienda que se debiera establecer un máximo de 10 usuarios, pero por la estructura de la institución un funcionario realiza dicho proceso y es controlado por solicitudes y autorizaciones de las áreas de control.

Permitir acceso mediante el escritorio remoto

El acceso remoto solo se debería habilitar si es que las áreas de soporte necesitan acceder a los equipos de la institución, en la Caja Central es autorizado dicho proceso exclusivamente para usuarios administradores y está descrito en las políticas institucionales.

Configuración de hora

Dicho permiso debe ser desactivado para los usuarios finales, en el caso de los administradores debe estar configurado en la directiva correspondiente del servidor con un NTP conocido, por ejemplo, las directivas del directorio activo, al ejecutar la política puede existir alteración de horas en los registros para evidencia de procesos que se ejecuten en los dispositivos.

Modificación de registro

La opción debe tener acceso el Administrador para evitar que usuarios finales accedan a la opción del REGEDIT y realicen cambios al mismo ocasionando mal funcionamiento de los equipos.

Modificación de variables de entorno.

La opción debe estar activa para los administradores, en usuarios finales puede ocasionar afectaciones en las configuraciones de hardware lo que puede generar denegación de servicios.

Realización de actividades de mantenimiento

La opción debe estar activa para el Administrador, el usuario final si tiene activa la opción puede llegar a eliminar una unidad de disco y así presentar un ataque de Denegación de servicios.

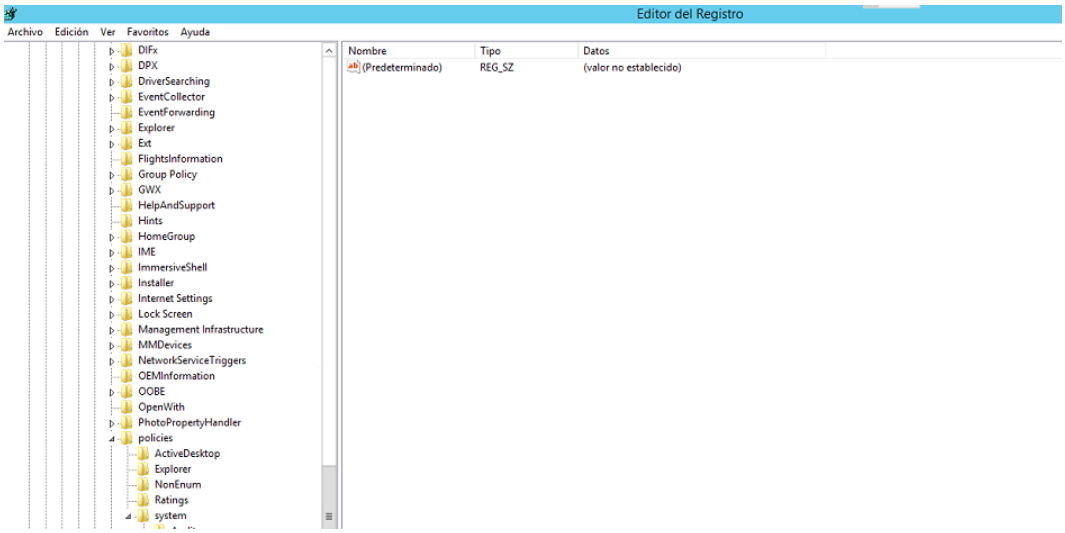
Opciones de Seguridad - Bloqueo de cuentas de Microsoft

La configuración se la genera para que los usuarios no puedan crear cuentas de Microsoft para su acceso local sin restricciones, deben utilizar la cuenta habilitada dentro del active directory la cual es asignada en el momento del ingreso a la institución, bajo las políticas de registro de usuarios, esta configuración se la realiza en:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\NoConnect edUser

Figura 11.

Registro de desactivación de cuentas de Microsoft

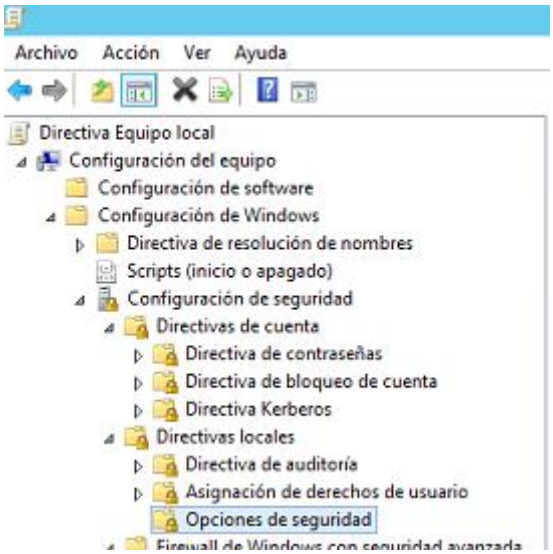


O en el directorio activo en las Opciones de Seguridad

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Block Microsoft accounts

Figura 12.

Opciones de seguridad en servidor de directorio Activo



Des habilitación de cuentas de invitado

Dentro del directorio activo se inactiva la opción de cuentas de invitado, de esta forma no se podrá ingresar con la misma, el riesgo se genera que al estar activa el tipo de cuenta no solicita contraseña.

Se lo ejecuta en el directorio activo en:

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Guest account status

Renombrar cuenta de Administrador

De manera general las cuentas se crean como Administrador a quien maneja dicha cuenta, es recomendable realizar el cambio del nombre para minimizar la vulnerabilidad del acceso conociendo el nombre por default que se crea en los equipos.

Esto se puede realizar en la opción del directorio activo:

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename administrator account

Bloqueo de instalación de controladores y/o programas

Se debe bloquear la instalación de controladores de dispositivos como las impresoras y de programas en general porque los hackers pueden enmascarar dichos controladores enviando virus que pueden posterior esparcirse en la red.

En el caso de impresoras se lo configura en el directorio activo:

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Prevent users from installing printer drivers

Accesos de Red

Permitir nombres de SID anónimas

La configuración debe estar desactivada de forma que no puedan acceder o crear SID nuevas en los equipos.

La activación en el directorio activo debe ser ejecutada en:

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Allow anonymous SID/Name translation

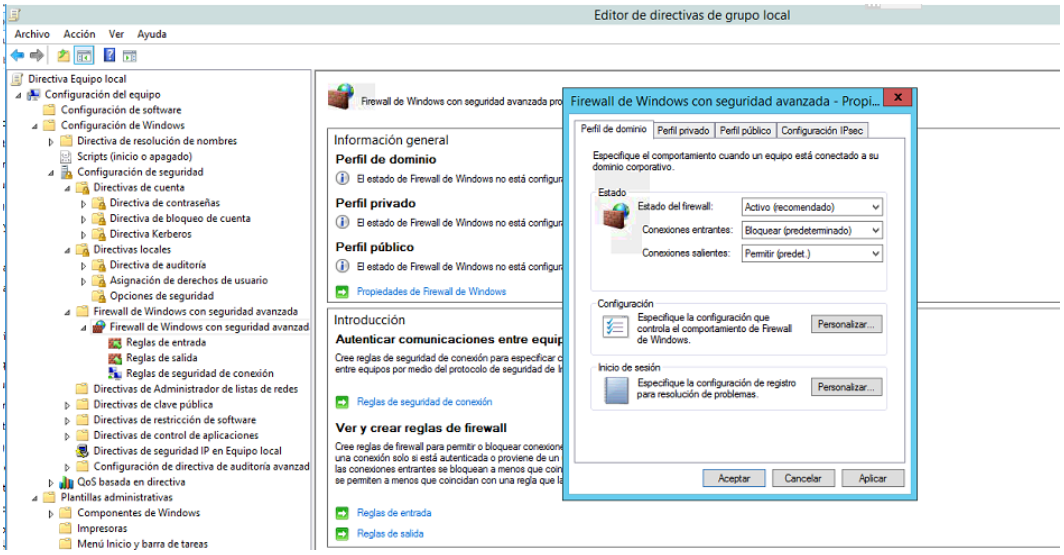
En otra sección donde se analizará las configuraciones de la red es en los dispositivos de comunicaciones correspondientes

Firewall de Windows y seguridad avanzada

Por default en el active directory se debe tener habilitado el firewall de Windows de forma de tener dicha protección de software, aunque dentro de la institución actualmente se tiene el antivirus que maneja el firewall de los equipos institucionales.

Figura 13.

Configuración recomendada del Firewall de Windows



Aplicación del benchmark hardening en servidores de aplicaciones y Web

Los servidores de aplicaciones y web en el entorno informático de la institución manejan los siguientes servicios.

- ✓ Internet information Services 8.0
- ✓ Oracle web Logic

Aplicación de configuración hardening en Internet information Services

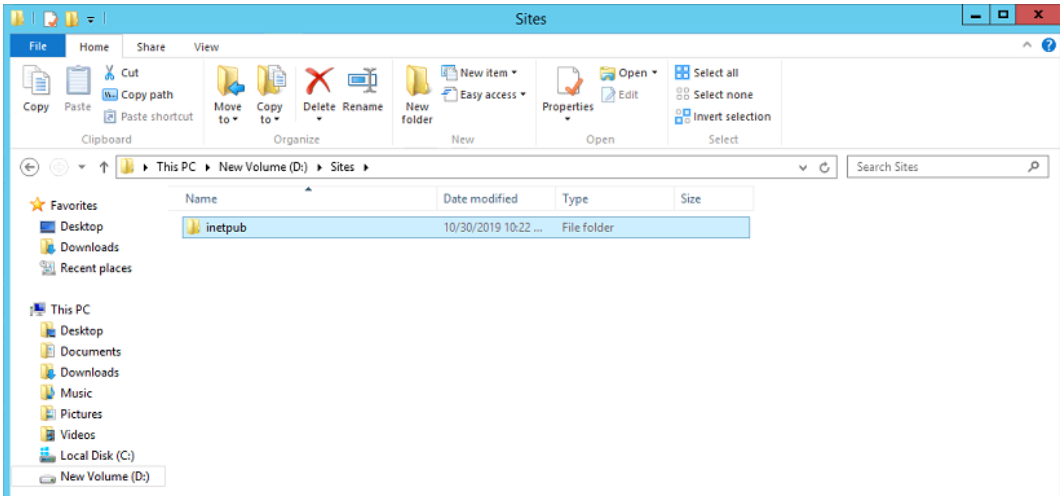
Para el análisis y validación se verifica en el framework para el IIS con el objetivo de mantener una configuración segura, la última versión de IIS es la 10, actualmente se trabaja en la institución con versión 8.0.

Carpeta inetpub

La carpeta inetpub es un directorio virtual donde se publican los servicios, es por lo que hay que asegurarse que el mismo sea creado en una unidad de almacenamiento diferente de la que se encuentra instalado el sistema operativo, en este caso se encuentra en la unidad D.

Figura 14.

Ubicación de directorio de publicación de servicios

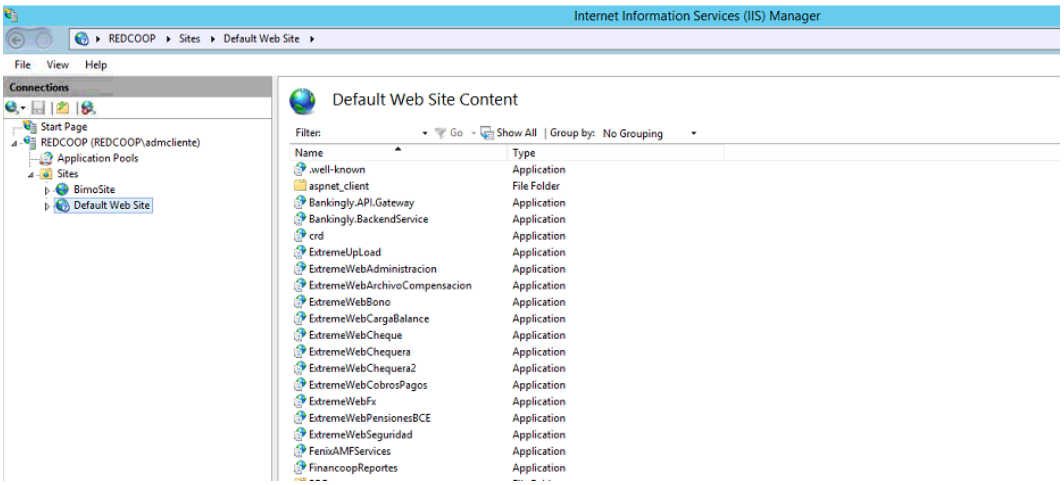


Encabezados de host

En un directorio virtual se pueden manejar varios servicios donde se deben establecer que se encuentren bajo el directorio; asignando la dirección IP y puerto, pueden existir aplicativos publicados en el puerto 80 con http, pero al mantener un certificado de seguridad se lo publica con protocolo https en el puerto 443.

Figura 15.

IIS Default web site



Exploración de directorios

La exploración de directorios debe estar deshabilitada de forma que los clientes finales no puedan encontrar un directorio con el nombre específico del listado de documentos predeterminados del IIS, en la configuración de los sitios se debe ingresar las siguientes líneas de configuración, en nuestro caso los aplicamos en los web.config de cada sitio.

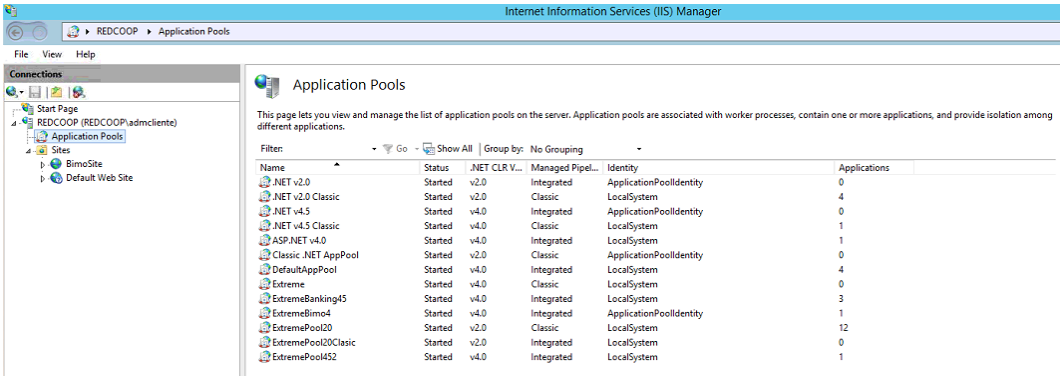
```
<system.webServer>
        <directoryBrowse enabled=”false” />
<system.webServer>
```

Identidad del grupo de aplicaciones

Los pools que se crean para las aplicaciones son procesos que trabajan en conjunto para levantar un sitio web dependiendo de las necesidades; esto se crea para poder reforzar la privacidad específica para un sitio sin tener que proporcionar un acceso general, con esto el servidor es más eficiente y se sugiere que se lo maneje bajo identidades únicas que se configuran en el servidor.

Figura 16.

Pool de aplicaciones

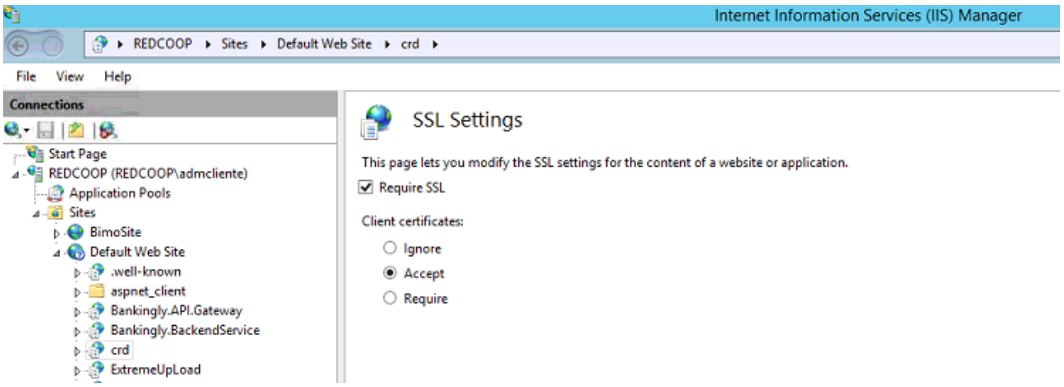


Autenticación de formularios SSL

El tráfico que se genera en los servicios que se exponen deben contar con cifrado SSL, esto se lo ejecuta para mantener confidencialidad en procesos de logueo o inicio se sesión.

Figura 17.

Aplicar configuración de SSL en sitio web.



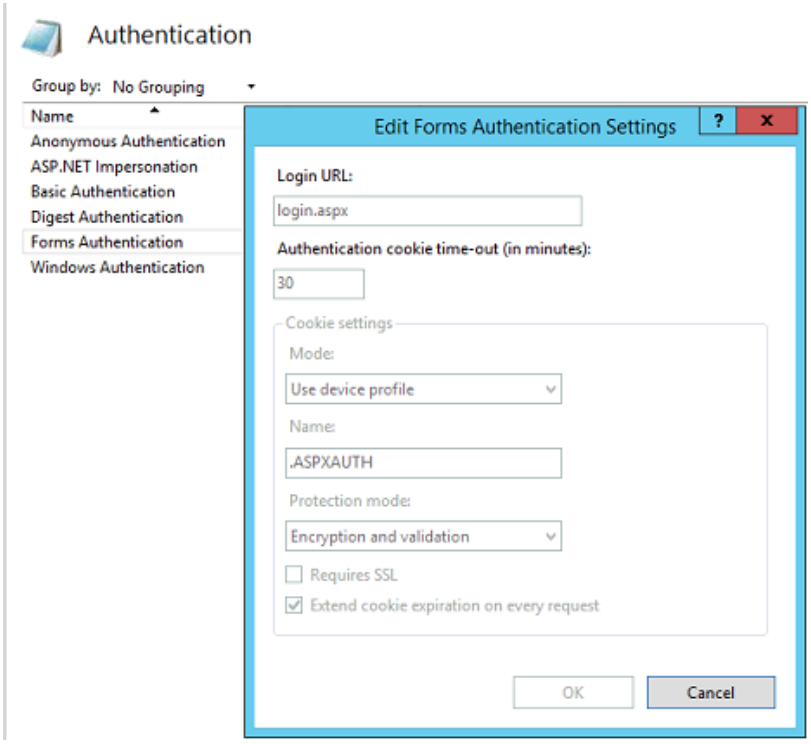
Autenticación de formularios para uso de Cookies

La activación del uso de cookies sirve para evitar el riesgo de secuestro de sesiones para modificar las páginas de inicio establecidas y generar ataques de DoS, por lo que se establece la configuración dentro del IIS o en los archivos de web.config de los sitios web.

```
<system.web>
    <authentication>
        <forms cookieless=”UseCookies” requireSSL=”true” timeout=”30” />
    </authentication>
</system.web>
```

Figura 18.

Uso de cookies en sitio web

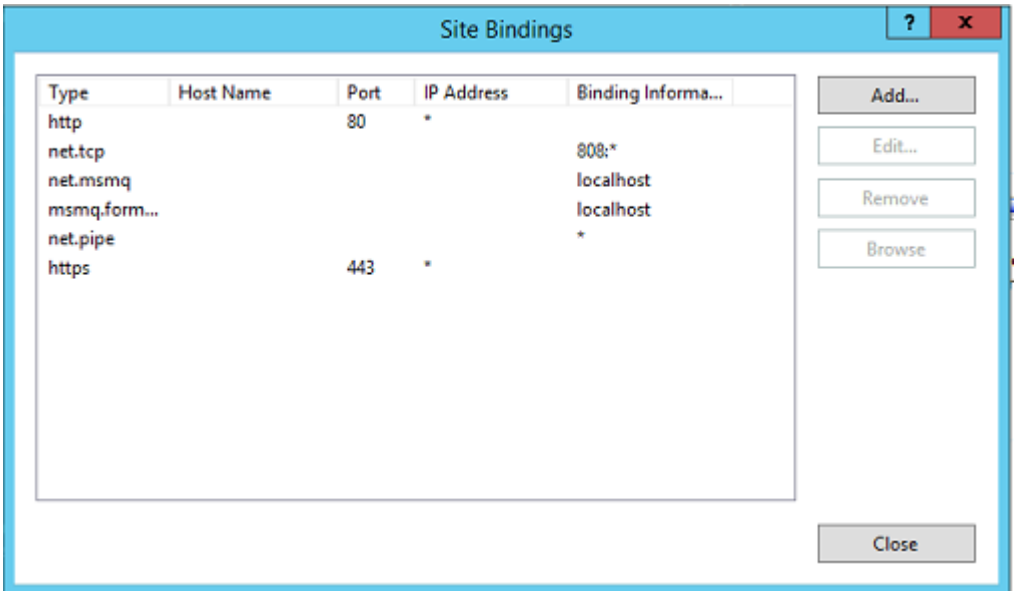


Configuración de capa de transporte

Es la aplicación de la configuración del TLS, esto minimiza ataques man in the midle, para mantener información verídica entre el cliente y el servidor; se requiere el uso de certificados de seguridad en donde se transporta la información con el protocolo https, que es aplicado en el sitio web.

Figura 19.

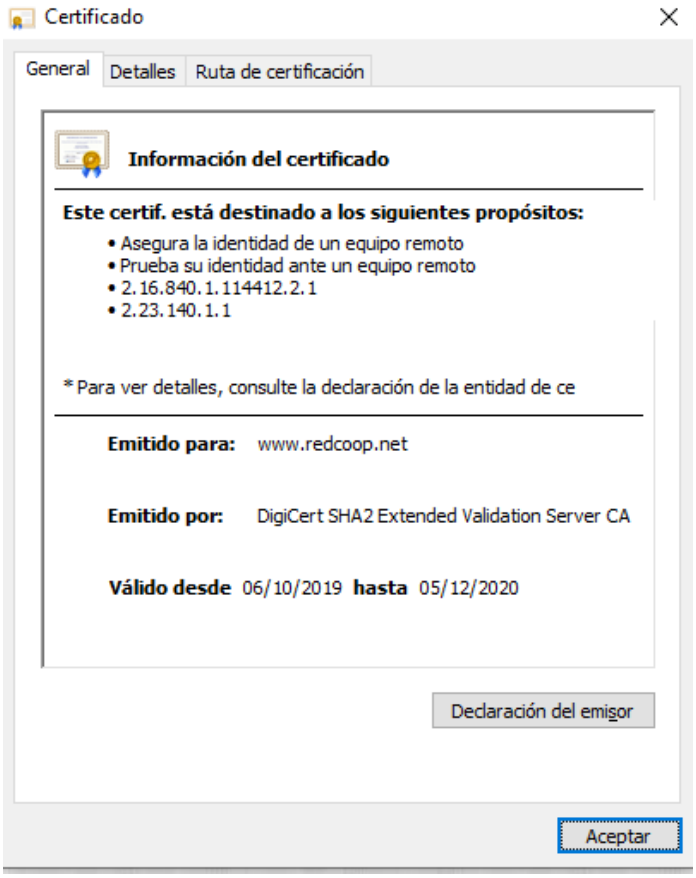
Configuración de puerto 443 en sitio web



Para su aplicación es necesario la adquisición de un certificado de seguridad que lo emiten las entidades certificadoras a nivel mundial, el proceso inicia con la obtención del request con los datos del sitio publicado y posterior la carga del certificado cuando se validan los datos de parte de dicha entidad, el mismo que cuenta con encriptación tipo SHA2

Figura 20.

Certificado de seguridad vigente de sitio web



Configuraciones del ASP.NET

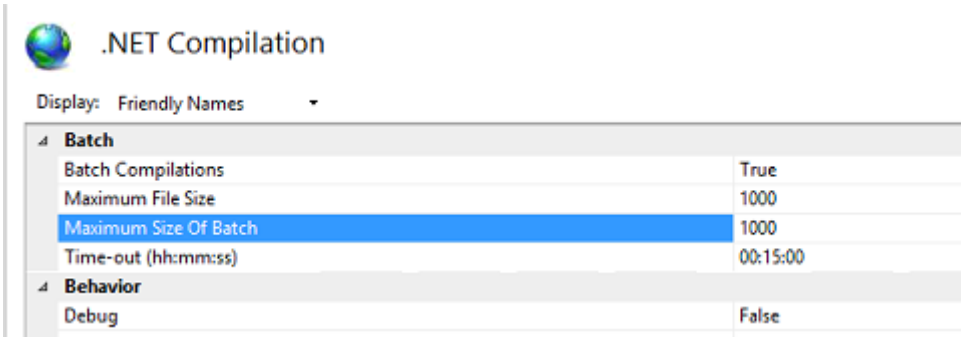
El ASP.NET es la versión con la que se carga el pool de aplicaciones, sirve para ejecutar el aplicativo de forma eficiente, en el desarrollo se utiliza para realizar pruebas de funcionalidad al activar el debug, pero en producción debe estar inactivo y esto se lo registra en el web config del sitio.

```
<configuration>
        <system.web>
                <compilation debug=”false” />
        </system.web>
</configuration>
```

O realizarlo directamente en el IIS en la opción de .net compilation

Figura 21.

Compilación de ASP. NET

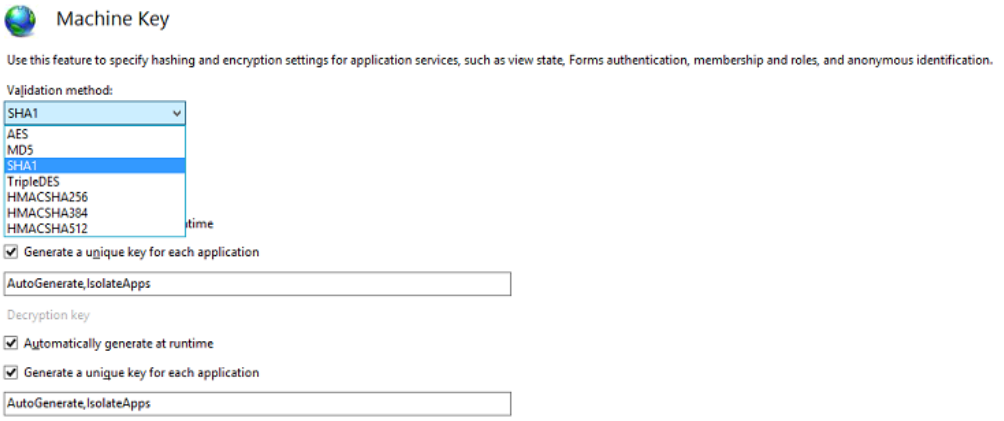


Método de validación de machine key

La validación es para identificar el algoritmo y cifrado para los servicios de aplicación, existen varios métodos como el AES, MD5, sha1, sha2, TripleDES; se recomienda el uso del SHA2, que se encuentra configurado en el certificado de seguridad.

Figura 22.

Configuración Machine Key



Aplicación del benchmark hardening en motor de base de datos

En la institución se utilizan varios motores de base de datos como son Sql Server 2012, 2014, Oracle 11G y Postgres 9.4

Motor de base de datos Sql Server

En primera instancia es necesario verificar la instalación, actualizaciones y parches del motor de base de datos.

Las bases de datos deben estar en servidores exclusivos por la información que mantienen, seguridad y mantener la arquitectura de las capas de software recomendadas.

En la institución los servidores de base de datos se manejan en equipos exclusivos, por lo que se procede a validar las configuraciones iniciales que se encuentran detalladas en el framework correspondiente al Sql Server, en este caso con el comando *sp_configure*

Figura 23.

Comando sp_configure en Sql Server

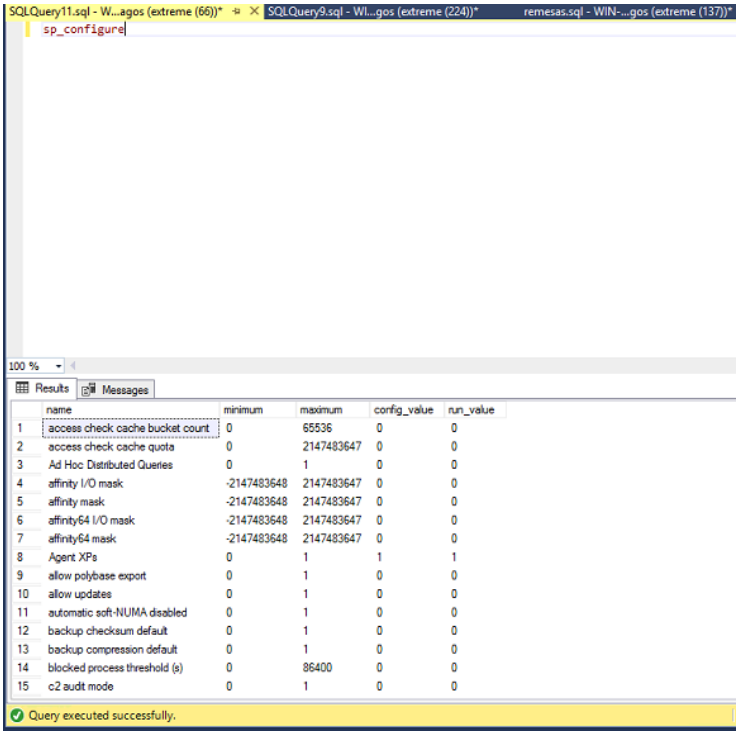


Tabla 12.

Configuraciones recomendadas en motor de base de datos

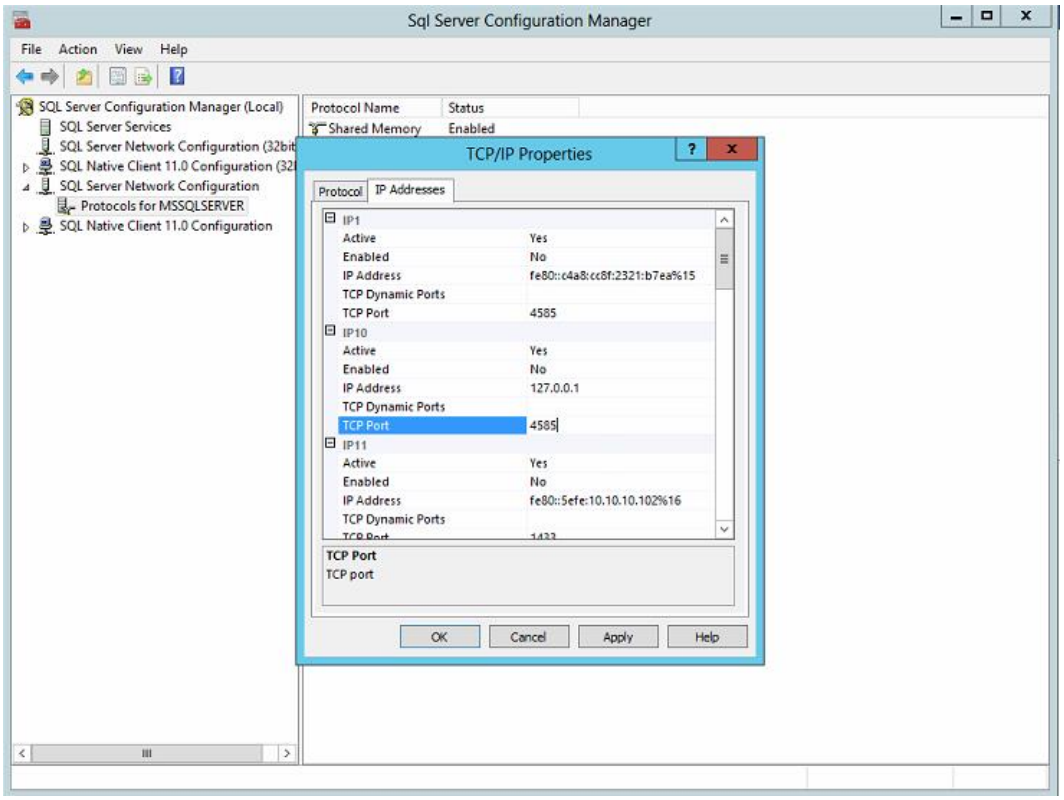
Detalle de configuración	Configuración recomendada	Riesgo
Ad hoc distributed queries	0	Si se encuentra activo permite ejecutar sentencias desde otras bases de datos
Show advanced options	1	Visualizar opciones de configuraciones avanzadas
Clr enabled	0	Minimiza seguridad en ejecución de procedimientos almacenados
cross db ownership chaining	0	un usuario con permiso db_owner podrá acceder a objetos de otra base de datos
Database mail	Disabled	Disminuye ataques de DoS
Remote Access	0	El uso de este puede generar ataques de DoS
Remote admin Connections	0	Uso exagerado de recursos

Configuración de puertos no estándar

El puerto por default que utiliza SQL Server es el 1433, por lo que se debe cambiar el mismo para minimizar la vulnerabilidad de puertos conocidos.

Figura 24.

Cambio de puerto default de SQL Server



Cuando se realiza dicha modificación debe reiniciar el servicio del SQL Server y ejecutar el cambio en los archivos de configuración de los aplicativos correspondientes, caso contrario podría perder conectividad.

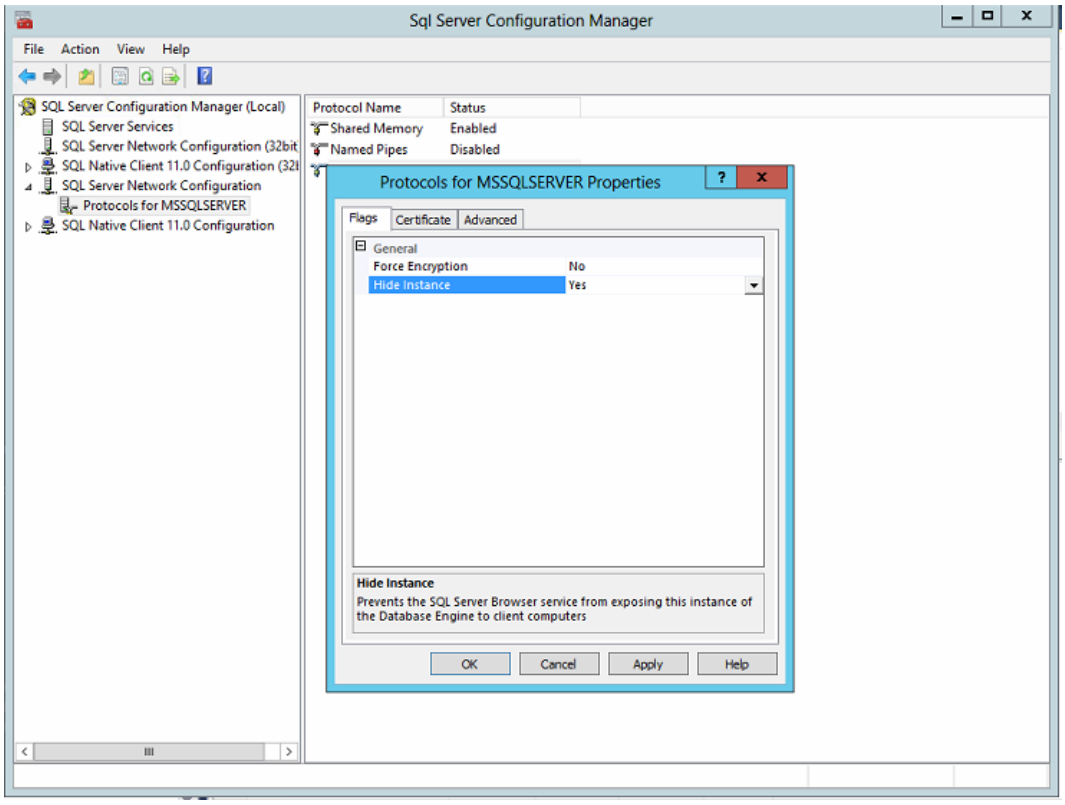
Para motores de base de datos como Oracle es necesario cambiar el puerto default 1521 y postgres el puerto 5432.

Ocultar nombre de instancia de SQL Server

Se debe ocultar la instancia de conexión en los ambientes de producción con el objetivo de que no se visualice la publicación del servicio y estos ítems son considerados en una instalación segura del motor de base de datos.

Figura 25.

Ocultar instancia de SQL Server



Cuenta *sa* debe estar deshabilitada

La cuenta **sa** es conocida y utilizada con privilegios de administrador; es por ello que se deshabilita, para evitar ataques de fuerza bruta al conocer el usuario login del motor de base de datos, también podría optarse por renombrar la cuenta de esa forma atacantes externos no obtendrían en login de una cuenta deshabilitada.

/deshabilita cuenta

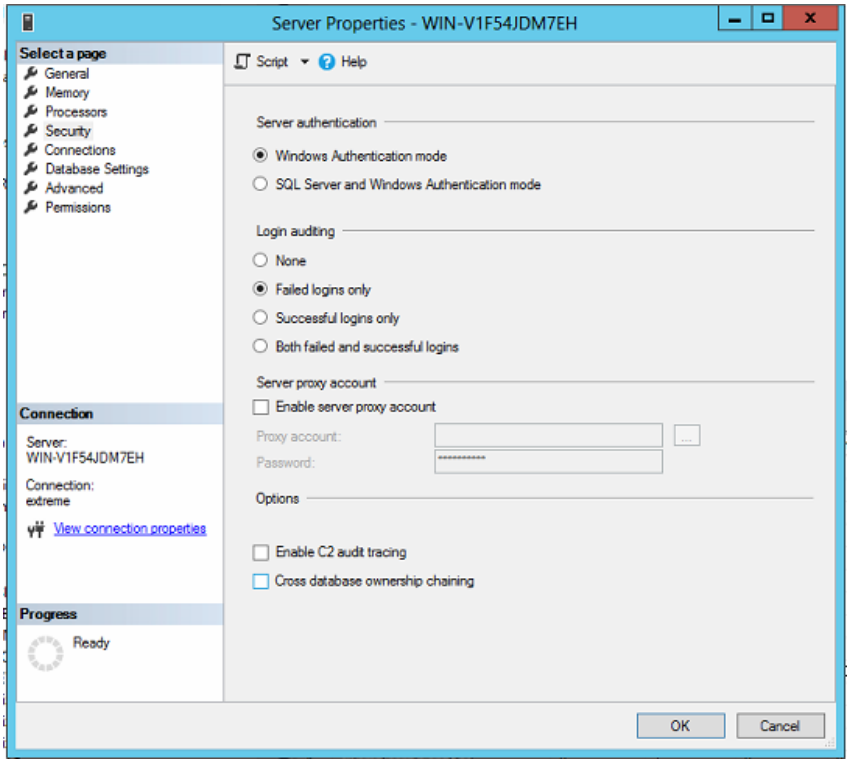
```
USE [master]
GO
DECLARE @tsql nvarchar(max)
SET @tsql = 'ALTER LOGIN ' + SUSER_NAME(0x01) + ' DISABLE'
EXEC (@tsql)
GO
/cambia nombre cuenta
ALTER LOGIN sa WITH NAME = <different_user>;
```

Autenticación del servidor

La autenticación debe estar configurada mediante el modo Windows al ser un mecanismo solido dentro del SQL Server.

Figura 26.

Modo de autenticación

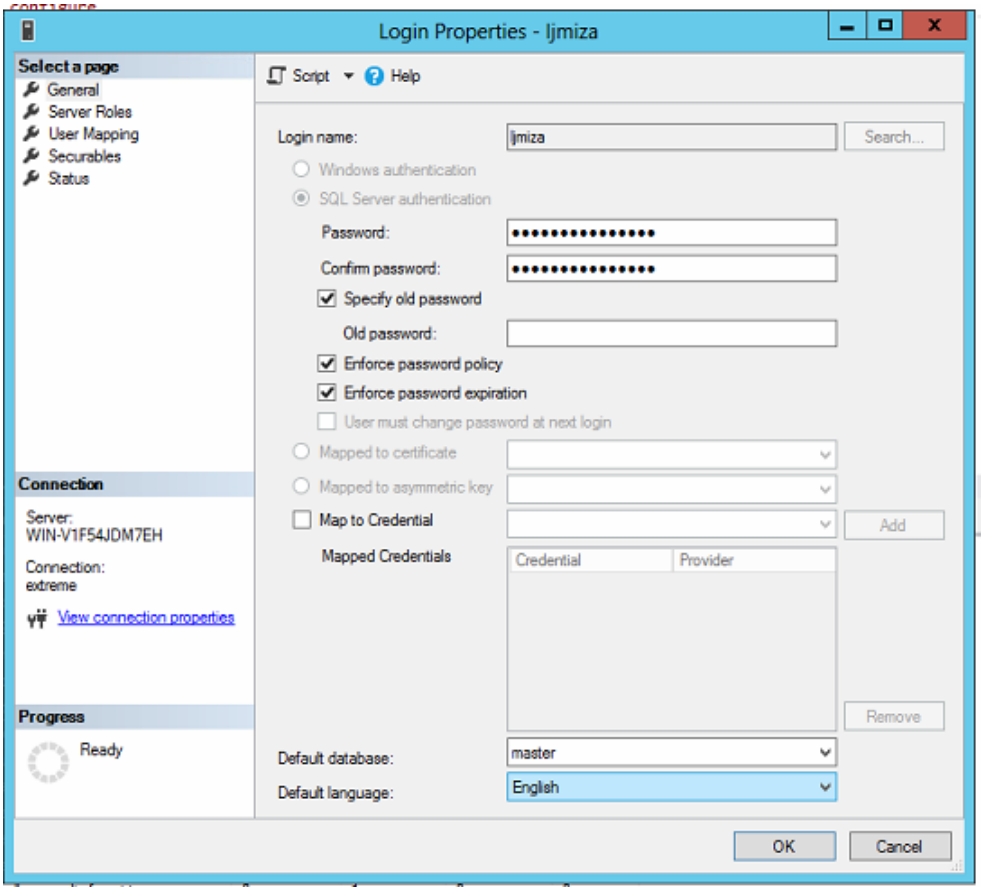


Política de contraseña

Las políticas de contraseñas se deben aplicar de forma similar al que se maneja con el sistema operativo; como es el cambio y complejidad de contraseñas, esto se lo habilita en las opciones de seguridad de los usuarios aplicando las políticas que brinda el motor de base de datos

Figura 27.

Políticas de contraseñas

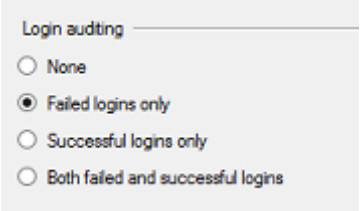


Activación de la auditoria de inicio de sesión

Se activa la auditoria por sesión para obtener los datos de los intentos de ingresos correctos e incorrectos, de forma de determinar el volumen de solicitudes erróneas que pueden ser a razón de un ataque de fuerza bruta.

Figura 28.

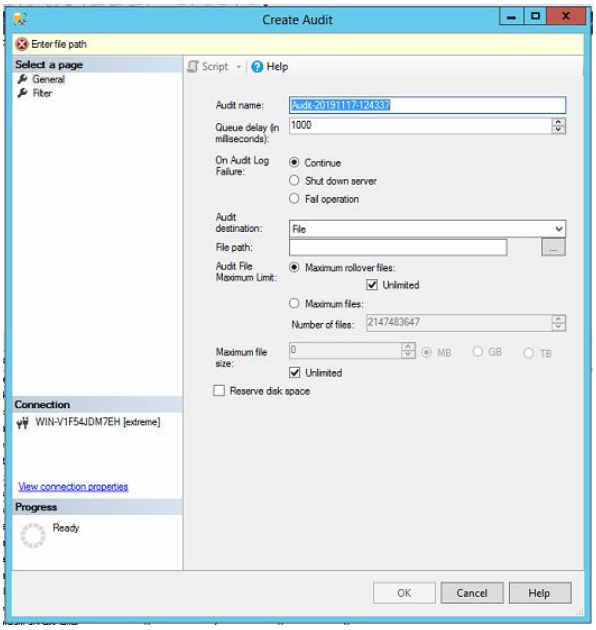
Login de auditoria



El motor de base de datos permite configurar auditorias especificas; dentro del explorador de objetos se cuenta con la opción de seguridad, se crea la nueva auditoría y se la ejecuta según las necesidades.

Figura 29.

Creación de una auditoria



Al validar los benchmark para motores de bases de datos adicionales como Oracle y Postgres; se verifica que los ítems revisados con el motor de base de datos analizado son generales y deben ser comprobados en las mismas.

Consideraciones del benchmark en sistemas operativo de estaciones de trabajo.

Para la aplicación de dicho ítem se debe verificar el sistema operativo de los usuarios finales.

- Microsoft Windows 10 Pro
- Microsoft Windows 7 Pro

En el análisis se puede utilizar la guía del framework para las estaciones de trabajo, en la institución todos los equipos se encuentran dentro de la red; la misma que es administrada desde el active directory, donde se aplica la configuración de la funcionalidad, controles y bloqueos que se emplearan en los equipos de trabajo de los usuarios finales.

Para el control de dichos dispositivos se maneja también los accesos a internet desde el firewall dependiendo el grupo al que pertenece, es por ello por lo que cuando un nuevo equipo va a ingresar a la red; es necesario contar con los pedidos correspondientes para la aplicación de políticas según su operatividad.

Consideraciones del benchmark en dispositivos de comunicaciones

Análisis de firewall de la institución

Se cuenta con un firewall de marca Sophos dentro del benchmark no se encuentra uno específico para dicha marca, se debe considerar los ítems que recomienda para este tipo de dispositivos.

Administración de contraseñas

El primer ítem independiente del dispositivo es la administración de contraseñas las cuales se indicaron en el análisis de servidores, se debe tener en cuenta que la contraseña tenga una longitud mínima, caducidad, complejidad, bloqueo por tiempo de inactividad, bloqueo por ingreso de contraseñas incorrectas, dentro del dashboard del firewall en la Administración permite el equipo realizar las configuraciones detalladas como se muestra en las imágenes.

Figura 30.

Administración de contraseña de acceso

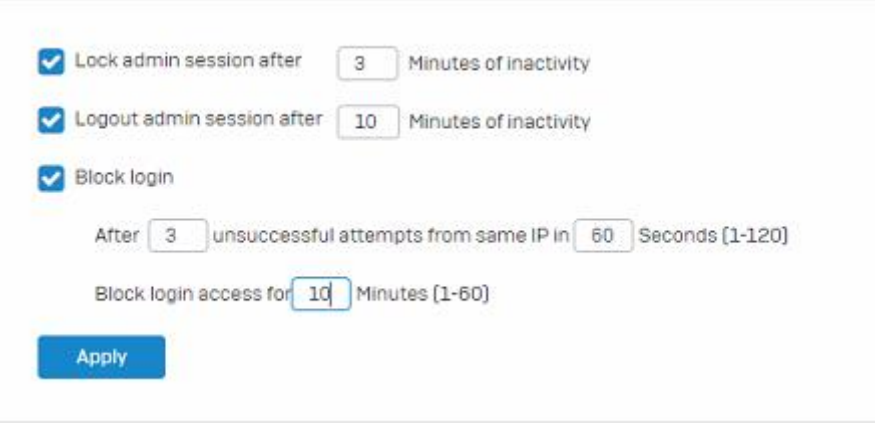


Figura 31.

Longitud de contraseña de administrador

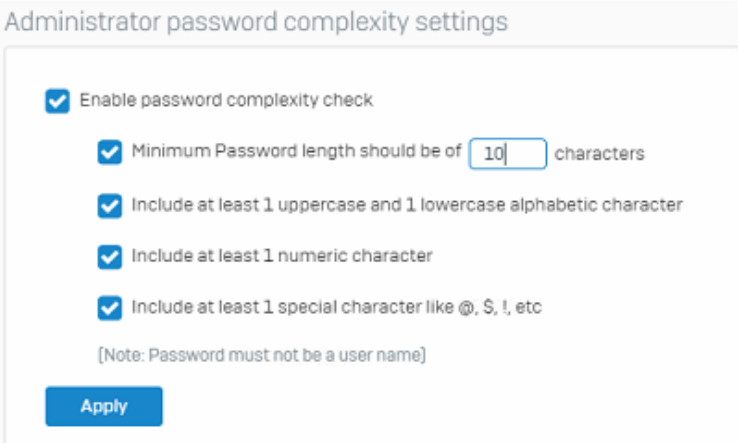
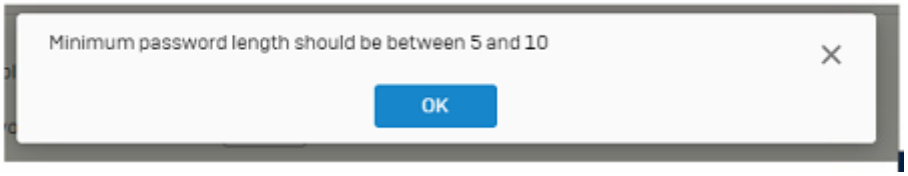


Figura 32.

Complejidad de contraseña



El firewall maneja la longitud de contraseña de cinco a diez caracteres por lo que se considere trabajar con el máximo tamaño y es necesario modificar la contraseña del usuario default.

La política de contraseñas debe ser aplicada en los equipos de seguridad al inicio de su configuración independiente de la marca que se utilice en las organizaciones.

Se debe deshabilitar las opciones que no son utilizadas de forma que no puedan generar huecos de seguridad; que puedan ser aprovechados por hackers.

En las configuraciones que se realizan en el firewall se debe establecer que los puertos de conectividad tanto TCP y UDP deben estar bloqueados al menos de que un aplicativo específico deba utilizar los mismos, el desbloqueo debe estar documentado y considerarse información restringida dentro de la institución.

Capítulo IV.

Metodología

En base al análisis realizado en el capítulo anterior; al revisar el framework CIS Benchmarking se puede obtener los ítems a aplicar de manera general según el tipo de dispositivo.

Como objetivo se planteó generar la política que va a ser parte del Manual de Tecnología de la información de la institución, que queda establecido como se detalla:

“Aplicar la metodología del hardening cuando ingrese un nuevo dispositivo que va a ser parte del entorno informático”

La metodología para el hardening dentro de la institución se define bajo el siguiente panorama.

1. Realizar el levantamiento del inventario de activos tecnológicos del entorno informático; es decir los componentes de software y comunicaciones de la institución, esto es para poder tener un punto de partida para aplicar los controles identificados con el framework CIS Benchmarking, posterior a esto cada activo que ingrese en la institución debe ser registrado.

2. En el inventario se obtiene la información de tipo de equipo es decir identificar el hardware, en este caso se puede indicar si es servidor, equipo de escritorio, laptop y dispositivo móviles como teléfono o Tablet; en cuanto al software se identifica inicialmente en los equipos el sistema operativo y en

base a su funcionamiento se obtendrá el software base y en cuanto a las comunicaciones el tipo de equipo.

Tabla 13.

Dispositivos de entorno informático

SOFTWARE	COMUNICACIONES
Sistema Operativo	Firewall
Motor de base de datos	Router
Servicios Web	Switch
Ofimática	
Aplicaciones propias	

3. Ubicar el dispositivo e ir completando la siguiente matriz de cumplimiento de las configuraciones realizadas bajo la metodología del hardening en los dispositivos, los ítems indicados se los ha obtenido del análisis del Framework CIS Benchmarking (Cis-benchmarks, 2019), como se indicó en el capítulo 2 es el más completo porque tiene en su mayoría el software utilizado.

ITEMS A VALIDAR
Actualización de Firmware, BIOS, contraseñas de arranque de los equipos.
Desactivación de unidades externas en servidores como pen drive o memorias USB
Aplicativo de encriptación de información
Instalación de antivirus
Instalación de agente de respaldos
Partición de unidades de almacenamiento
Protección y renombre de cuentas de Administración y deshabilitar o invalidar cuentas estándares, invitado, uso de cuentas limitadas.
Habilitar los sistemas de Auditorias y Monitoreo de logs.
Asegurar consolas de administración, accesos remotos; solo para administradores
Administración de paquetes de instalación, parches, updates.
Configuración de Protocolos, Puertos y Servicios (Solo los necesarios).
Asignación de contraseñas seguras
Registro en el directorio activo

Identificar grupo de privilegios de internet
Identificar vlan de registro
Asignar IP address con reservas de MAC

4. Al obtener el detalle del punto 3 se verifica cada ítem y se aplica las recomendaciones especificadas, de forma de incluir el dispositivo dentro del entorno informático de la institución cuidando de preservar la seguridad y evitar vulnerabilidades desde su instalación.

CAPÍTULO V.
Conclusiones y Recomendaciones

Conclusiones

- ✓ El presente proyecto se direccionó para el cumplimiento de normativas del ente de control SEPS de riesgo operativo en el tema de seguridad informática y se planteó la aplicación del CIS framework benchmark, el que se lo direccionó en el desarrollo del hardening.

- ✓ El hardening permitió identificar que es necesario aplicar configuraciones iniciales dentro del entorno informático de una institución; para minimizar vulnerabilidades en los nuevos dispositivos, es importante el proceso porque antes de tener un ataque se visualiza los riesgos de seguridad.

- ✓ En la Caja Central se procedió a levantar los ítems que permitió el desarrollo de la metodología en el entorno informático que se utiliza en la institución, y plantearlo como política institucional, adicional en los procesos se especificó los estándares de configuración inicial.

- ✓ En base a esto se mantiene el inventario actualizado en la institución de forma automatizada, ya que en el desarrollo de este se evidenció la necesidad, aplicabilidad y operatividad que nos brindaría dicha información.

- ✓ La metodología desarrollada permite que de forma secuencial se realice el análisis por cada activo y como valor agregado se genera la documentación como se lo requiere en la institución.

- ✓ Adicional al involucrar revisiones de vulnerabilidades iniciales en la institución se minimizan las brechas de seguridad que puedan presentarse.

Recomendaciones

- ✓ La aplicación de la metodología en la institución debe ser parte de las políticas y procesos que se aplican en el ingreso de activos informáticos.

- ✓ Es necesario mantener actualizado el inventario de activos informáticos para la aplicación del hardening, en el caso de que se realice un cambio o una baja en los dispositivos debe evidenciarse su registro.

- ✓ El hardening permite minimizar las vulnerabilidades que puedan presentarse en las configuraciones iniciales de los dispositivos; además se debe contar con herramientas como antivirus, firewalls que deben estar alineados adecuadamente a las políticas de seguridad para la protección de la información en el entorno informático.

- ✓ La seguridad informática es responsabilidad de todos los integrantes de las instituciones por lo que es importante siempre darles pautas para el manejo de información y dispositivos.

- ✓ Por cada nuevo dispositivo debe ser aplicada la política sobre el hardening, de forma que cuando sea parte del entorno informático de la institución sea integrado con las configuraciones de seguridad

iniciales, en el caso que dentro del benchmark no se encuentre establecido la marca o modelo se debe tener las referencias generales.

- ✓ Al ser una institución referente para el sector financiero de la economía popular y solidaria, puede recomendar su funcionalidad a sus socias y clientes.

REFERENCIAS

Bibliografía

Adkins, L. (2020). *Hardening Framework*. Obtenido de https://github.com/hardening-io

Azzam Mourad, M.-A. L. (30 de Mayo de 2014). *Computer Security Laboratory, CIISE*. Obtenido de https://laur.lau.edu.lb:8443/xmlui/bitstream/handle/10725/2692/Security.pdf?sequence=3&isAllowed=y

Blanco, L. A., Chang, L. R., & Brito, H. R. (2020). Configuraciones Internas para el fortalecimiento de la seguridad NGXIS. *Seminario Iberoamericano de Seguridad en las Tecnologías de la Información*.

Blume, J. (1999-2020). *Netwotk Inventory Advisor*. Obtenido de https://www.network-inventory-advisor.com/es/

cero, C. d. (2019).

Charles, P. (2019). *Triángulo de la seguridad de la información*. Obtenido de https://www.it-skull.com/2-seguridad-de-la-informacion-que-es/6-triangulo-de-la-seguridad-de-la-informacion.html

Cis-benchmarks. (2019). *Center for internet Security*. Obtenido de https://www.cisecurity.org/cis-benchmarks/

Daniel Borbor, L. W. (Julio de 2017). *Hal Archives - Ouveters*. Obtenido de https://hal.inria.fr/hal-01684351/document

Definicion ABC. (2019). Obtenido de https://www.definicionabc.com/tecnologia/entorno-informatico.php

Developers. (6 de Enero de 2020). *Source*. Obtenido de https://source.android.com/devices/media/framework-hardening

Ecuatoriana, N. T. (2017). *INEN.*

EXCELLENCE, I. T. (2020). *ISO TOOLS*. Obtenido de https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

Financoop. (2019). *Manual de Seguridad de la información.*

Framework, H. (2016). *Puppet Forge*. Obtenido de https://forge.puppet.com/hardening/mysql_hardening

Freshservice. (26 de 02 de 2020). *FreshService - Gestión de activos TI*. Obtenido de https://freshservice.com/es/it-asset-management-software/

GUIJARRO-Rodríguez, A. A., YEPEZ-Holgin, J. M., PERALTA-Guaraca, T. J., & Mirella. (2018). Defensa en profundidad aplicado a un. *Espacios*, 19.

Hardening framework. (Abril de 2020). *Puppet Forge*. Obtenido de https://forge.puppet.com/hardening/os_hardening

Hartmann, C. (2020). *DevSec Hardening Framework Baselines*. Obtenido de https://dev-sec.io/baselines/

Hernández, A., & Rocio, J. (2013). El sistema Financiero y la seguridad informática.

Incibe. (20 de Marzo de 2017). *Instituto Nacional de Ciberseguridad de España*. Obtenido de https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Jackson, C. (11 de Abril de 2019). *Hardening windows 10*. Obtenido de https://www.microsoft.com/security/blog/2019/04/11/introducing-the-security-configuration-framework-a-prioritized-guide-to-hardening-windows-10/

Jain, K. N. (2007). *Spronger Link*. Obtenido de https://link.springer.com/chapter/10.1007/978-3-540-74549-5_97

Karel Durkota, V. L. (2015). *Segundo Taller Internacional sobre Agentes y Ciberseguridad*. Obtenido de https://www.google.com/search?q=traductor&rlz=1C1CHBD_esEC886EC887&oq=traductor&aqs=chrome.0.35i39l2j0l6.1556j0j7&sourceid=chrome&ie=UTF-8

Kaspersky. (2019). *Karspersky*. Obtenido de https://latam.kaspersky.com/resource-center/definitions/malicious-code

Luján, U. N. (s.f.). *Departamento de Seguridad informatica*. Obtenido de http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

Martínez Cruz, J. L. (2015). Endurecimiento (hardening) en dispositivos de red: Routers y Switchs. *Universidad Piloto de Colombia*.

Media, H. (6 de Enero de 2020). *Source Medios*. Obtenido de https://source.android.com/devices/media

Microsoft. (2019). *Framework configuración de seguridad*. Obtenido de https://www.microsoft.com/security/blog/2019/04/11/introducing-the-security-configuration-framework-a-prioritized-guide-to-hardening-windows-10/

Mieles, J. (2009). Debilidades de seguridad comúnmente explotadas . *Evil Fingers*.

Osman Abdoul Ismae, D. S. (17 de Noviembre de 2017). *United States Patent*. Obtenido de https://patentimages.storage.googleapis.com/6b/9a/c3/e97f643448406b/US10181029.pdf

Pandora. (2019). *PandoraFMS*. Obtenido de https://pandorafms.com/blog/es/gestion-de-activos-de-ti/

Puppet Forge. (2014). *Hardening Framework*. Obtenido de https://forge.puppet.com/hardening/ssh_hardening

Puppet Forge. (2015). *Hardening Framework*. Obtenido de https://forge.puppet.com/hardening/ssh_hardening

Puppet Forge. (2015). *Puppet Forge*. Obtenido de https://forge.puppet.com/hardening

Richter Dominik, H. C. (2020). *DevSec Hardening Framework*. Obtenido de https://dev-sec.io/

SEPS. (2018). *Superintendencia de Economía Popular y Solidaria*. Obtenido de https://www.seps.gob.ec/

Source, O. (12 de 01 de 2017). *Ocs Inventory*. Obtenido de https://ocsinventory-ng.org/?lang=fr

Susskraut, M. (16 de Julio de 2007). *IEEE ORG*. Obtenido de https://ieeexplore.ieee.org/abstract/document/4272956

Teclib. (2015 - 2020). *GLPI*. Obtenido de https://glpi-project.org/

VIU. (24 de Abril de 2018). *Universidad Internacional de Valencia*. Obtenido de https://www.universidadviu.com/vulnerabilidad-informatica-tipos-debilidades-principales/

Carpeta Anexos