# UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

## FACULTAD DE INGENIERÍA

**Definición de políticas de seguridad informática para el fortalecimiento de infraestructura cómputo con sistema operativo Linux**

## INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

**Ingeniero en Computación**

**P R E S E N T A**

César Arian Ortega Arias

## ASESOR DE INFORME

M. C. Alejandro Velázquez Mena

**Ciudad Universitaria, Cd. Mx., 2016**

# Contenido

# Introducción

La administración de infraestructura GNU/Linux y los temas seguridad informática siempre fueron parte de mi interés como estudiante de la Facultad de Ingeniería de la Universidad Nacional Autónoma de México, en la cual gracias a programas extracurriculares, como el Programa de Tecnología y Cómputo (PROTECO), me permitieron desarrollar el interés y habilidades en estos temas, sobretodo en seguridad informática el cual es considerado un tema tan crítico, sensible y medular en todas las organizaciones (empresariales, gubernamentales, académicas, etc.). Estas habilidades adquiridas y complementadas con temas de desarrollo de aplicaciones, planteamiento y solución de problemas, toma de decisiones me han permitido desarrollarme como un ingeniero especializado en temas de seguridad e infraestructura.

Este informe tiene como objetivo mostrar la experiencia que he adquirido como ingeniero en los de los diferentes lugares que he trabajado y las aportaciones que he dado a diferentes proyectos en los que he participado de manera operativa y en otros como coordinador y responsable de estos, siendo el sector financiero y gubernamental el lugar en donde se han desarrollado la mayor parte de mis actividades como profesionista.

El Capítulo I describe las funciones y organigrama de la institución en la cual actualmente me encuentro laborando y el rol que actualmente desempeño dentro de la Dirección de Sistemas de Pagos en el Banco de México.

El Capítulo II hace una descripción de los proyectos más significativos en los cuales he participado a lo largo de mi experiencia como profesionista, en algunos casos siendo parte del grupo de trabajo y en otros siendo el responsable y coordinador.

El Capítulo III describe el proyecto “Definición de políticas de seguridad informática para el fortalecimiento de infraestructura cómputo con sistema operativo Linux” para operar en una red de telecomunicaciones que permite a las instituciones financieras intercomunicarse con los sistemas de pagos operados por Banco de México.

El Capítulo IV describe los resultados de la implementación de las políticas y fortalecimiento de la infraestructura de cómputo Red Hat Enterprise Linux a cargo de mi equipo de trabajo en la Dirección de Sistemas de Pagos de Banco de México.

El Capítulo V dará conclusiones sobre la elaboración de este informe, recopilando los aprendizajes y experiencias obtenidas durante la participación del proyecto descrito.

# Capítulo 1 Banco de México.

El Banco de México, ahora en adelante llamado como El Banco, es el banco central del Estado Mexicano. Por mandato constitucional, es autónomo en sus funciones y administración. Su finalidad es proveer a la economía del país de moneda nacional y su objetivo prioritario es procurar la estabilidad del poder adquisitivo de dicha moneda. Adicionalmente, le corresponde promover el sano desarrollo del sistema financiero y propiciar el buen funcionamiento de los sistemas de pago.

La visión de El Banco es: ser una institución de excelencia merecedora de la confianza de la sociedad por lograr el cabal cumplimiento de su misión, por su actuación transparente, así como por su capacidad técnica y compromiso ético.

El Banco, tiene la siguiente estructura:

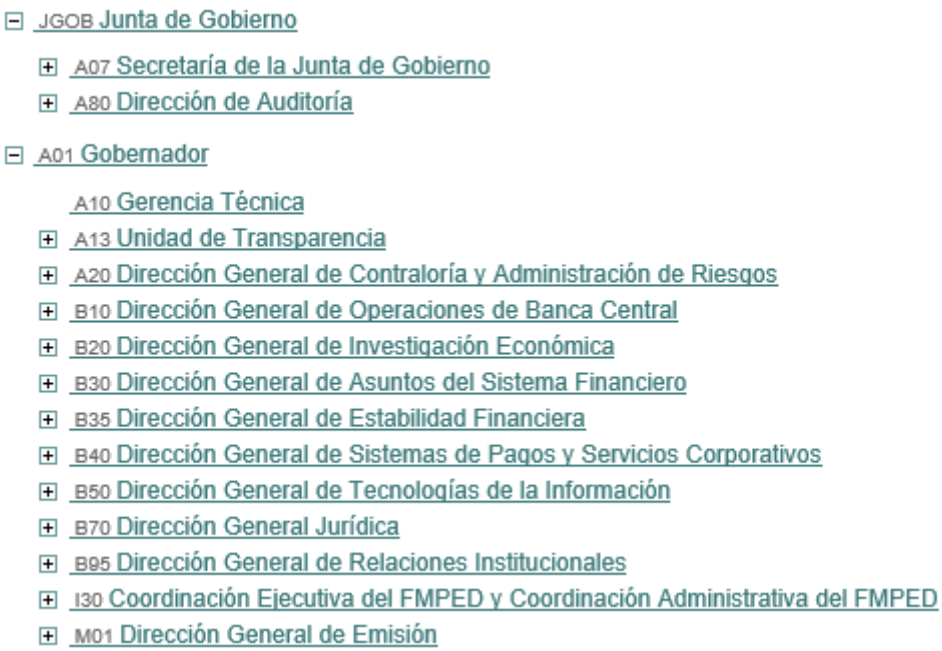



***Figura 1. Organigrama general de El Banco***

Las funciones que desempeño dependen de la Dirección de Sistemas de Pagos, la cual depende directamente de la Dirección General de Sistemas de Pagos y Servicios Corporativos, la cual tiene la siguiente estructura.

- B40 Dirección General de Sistemas de Pagos y Servicios Corporativos
  - D01 Dirección de Sistemas de Pagos
    - D10 Gerencia de Política y Vigilancia de los Sistemas de Pagos
      - D11 Subgerencia de Sistemas de Pagos de Importancia Sistémica
      - D12 Subgerencia de Sistemas de Liquidación de Valores y Contrapartes Centrales
      - D13 Subgerencia de Medios de Pago al Menudeo
    - D20 Gerencia de Tecnología de los Sistemas de Pagos
      - D21 Subgerencia de Desarrollo Tecnológico de los Sistemas de Pagos A
      - D22 Subgerencia de Desarrollo Tecnológico de los Sistemas de Pagos B
    - D30 Gerencia de Operación y Continuidad de Negocio de los Sistemas de Pagos
      - D31 Subgerencia de Operación de Sistemas de Pagos
      - D34 Subgerencia de Continuidad de la Operación de Sistemas de Pagos
    - D40 Gerencia de Estudios de Sistemas de Pagos

***Figura 2. Organigrama de la Dirección General De los Sistemas de Pagos y Servicios Corporativos.***

La Dirección de Sistemas de Pagos es la encargada de operar, regular y supervisar los sistemas de pagos, siempre procurando que su operación sea segura y eficiente.

La Gerencia de Tecnología de los Sistemas de Pagos (GTSP), es la encargada de desarrollar los sistemas informáticos que permiten la operación de los sistemas de pagos y es responsable de parte de la infraestructura de cómputo en la que operan los sistemas. La Gerencia tiene la siguiente estructura.

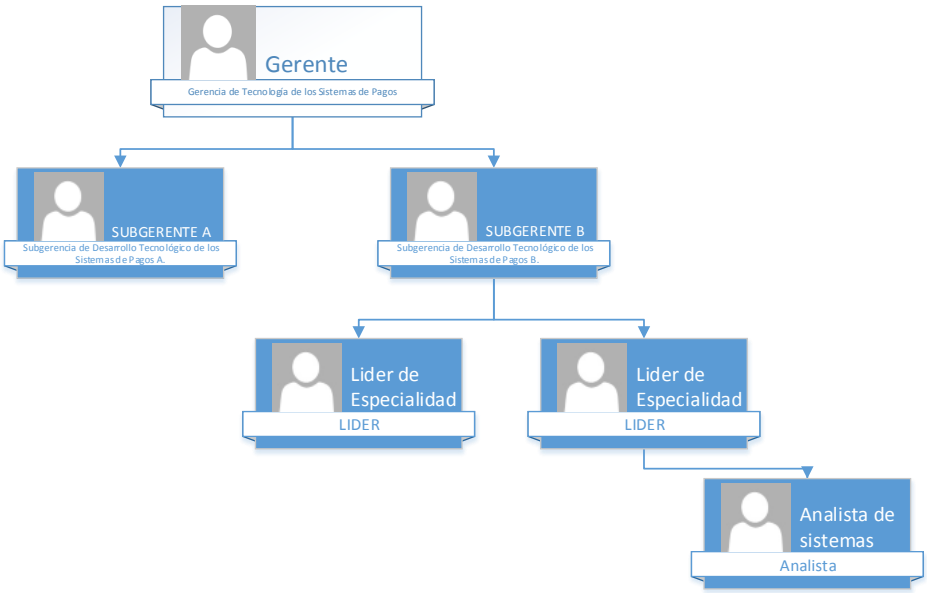


*Figura 3. Organigrama de la Gerencia de Tecnología de los Sistemas de Pagos*

Yo me desempeño como Líder de Especialidad adscrito a la Subgerencia de Desarrollo Tecnológico de los Sistemas de Pagos B.

## Rol dentro de El Banco y los sistemas de pagos

**Sistemas de pagos.**
Un sistema de pago es un conjunto de instrumentos, procedimientos bancarios y, por lo general, sistemas interbancarios de transferencia de fondos que aseguran la circulación del dinero.

Los sistemas de pagos tradicionalmente se clasifican en dos grupos, los de alto valor y los de bajo valor.

Los de alto valor son aquellos que pueden liquidarse el mismo día y por otro lado los de bajo valor son aquellos que se liquidan de manera diferida.

Algunos de los servicios que son ofrecidos por la Dirección de Sistemas de Pagos al público en general son:

- SPEI® (Sistema de Pagos Electrónicos Interbancarios) es un sistema desarrollado y operado por El Banco de México que permite al público en general realizar en cuestión de segundos pagos electrónicos, también llamados transferencias electrónicas, a través de la banca por internet o de la banca móvil. Este sistema permite transferir dinero electrónicamente entre cuentas de depósito de los bancos de manera casi instantánea.

- SPID (Sistema de Pagos Interbancarios en Dólares) es un sistema de pagos que permite realizar transferencias electrónicas interbancarias denominadas en dólares entre cuentas de depósito a la vista en dólares en la República Mexicana, correspondientes a personas morales que tengan su domicilio en territorio nacional.

- CEP (Comprobante Electrónico de Pago) es un comprobante o documento electrónico que emite el Banco de México con fines informativos para avalar la realización de un pago por medio del SPEI®. El CEP se genera con la información que el banco que recibió el pago envía al SPEI como confirmación del depósito del pago, la cual puede tardar hasta un máximo de 30 minutos. También, el CEP puede consultarse para pagos por SPEI® realizados en los últimos 45 días hábiles.

- MI-SPEI es un servicio de información a través del cual se puede consultar el estado de un pago mediante la clave de rastreo o el número de referencia que el banco proporciona al momento de realizarlo. Este módulo de información te permite conocer, por ejemplo, si el pago fue devuelto por alguna razón o si nunca se dio. Con esta información es posible acudir al banco para conocer mayor detalle sobre el estado de un pago y darle seguimiento.

- IES (Infraestructura Extendida de Seguridad) es la infraestructura de clave pública (o PKI por sus siglas en inglés: Public Key Infrastructure) del Sistema de Pagos mexicano. Dentro de sus principales funciones es dar seguridad a las transacciones de pagos en el sistema financiero y da el servicio de unicidad de clave pública a la firma electrónica del México. La IES es un sistema diseñado y administrado por Banco de México.

Es importante mencionar que parte de los programas y aplicaciones de los servicios comentados anteriormente se ejecutan en la infraestructura que está bajo la responsabilidad de mi equipo de trabajo.

**Participación en los sistemas de pagos.**

Mi rol dentro de El Banco y sistemas de pagos, es desenvolverme como Líder de especialidad dentro de la Subgerencia de Desarrollo Tecnológico de los Sistemas de Pagos B.

Dentro de mis actividades más destacadas están:

- Supervisar, coordinar y administrar la infraestructura de cómputo a cargo de la Gerencia de Tecnología de Sistemas de Pagos (GTSP).

    - Alrededor de 50 servidores con sistema operativo Red Hat Enterprise Linux.
- Coordinar, investigar e implementar nuevas tecnologías, la mayoría de software libre, que permitan optimizar y mejorar los procesos de aseguramiento, optimización y administración de la infraestructura de cómputo.
- Supervisar, coordinar e implementar mecanismos para disminuir los riesgos informáticos en la infraestructura de cómputo a cargo de la GTSP.
- Apoyar y colaborar en temas de Seguridad Informática relacionados con los sistemas de pagos a nivel mundial.
    - Asistencia a convenciones internacionales relacionada con la seguridad informática.
    - Seguimiento a sucesos relevantes en temas de seguridad informática en el ámbito financiero.
    - Elaboración de notas y reportes para la alta dirección y gubernatura sobre temas de seguridad informática.
- Apoyar, coordinar y colaborar en la supervisión de los elementos de seguridad informática de las instituciones financieras que participan en los sistemas de pagos.
    - Dar seguimiento para que la infraestructura de cómputo y telecomunicaciones de las instituciones financieras cumplan con requisitos mínimos de seguridad informática establecidos por El Banco para la operación e interconexión con los sistemas de pagos.
- Apoyar, colaborar y coordinar en el soporte a la infraestructura de cómputo a cargo de la GTSP.
- Apoyar y colaborar en el soporte a la operación de los sistemas de pagos.

Actualmente cuento con un equipo de dos personas que me apoyan en la atención de todos estos temas.

# Capítulo II Descripción de Proyectos

Desde mi incorporación al ámbito profesional hasta el día de hoy he estado participando en diferentes proyectos los cuales me han ayudado a desarrollarme como profesionista. En un principio en la industria privada colaborando como desarrollador y después en el sector gubernamental desarrollándome como administrador de infraestructura y especialista en seguridad.

A continuación, se listan los proyectos más significativos en los que he colaborado.

## Proyecto 1

- Fecha: diciembre de 2004 - 2005.

- Nombre: Sistema de facturación en línea (SOFIA) para Movistar

- Empresa: Accenture

- Rol: Becario y Desarrollador Junior

- Alcance del proyecto: Implementar el portal para que los clientes de la empresa Telefónica Movistar puedan ver sus facturas desde internet con un explorador de internet, este portal incluía un módulo para que el personal de Movistar pudiera dar seguimiento a los clientes que tenían adeudos.

- Actividades realizadas: Desarrollo de scripts para la automatización de tareas en los servidores Solaris y desarrollo de procedimientos con Oracle y Pro C.

- Resultado del proyecto: El sistema se puso en ambientes productivos y dio servicios a los usuarios de Telefónica Movistar.

## Proyecto 2

- Fecha: 2006 – 2007

- Nombre: Distribución de los servicios de la Infraestructura Extendida de Seguridad (IES) para optimizar la inserción de claves públicas.

- Empresa: Banco de México

- Rol: Analista de Sistemas.

- Alcance del proyecto: Diseñar la distribución de la base de datos para optimizar la inserción de las claves públicas de la IES.
  Implementación de un nuevo componente y algoritmo que permitiera la distribución de la base de datos de manera uniforme.
  Migración de la base de datos a un manejador de base de datos libres que permitiera tener varias instancias corriendo en un mismo servidor.
  Implementación de un mecanismo de replicación asíncrona que permitiera tener las claves publicas replicadas en el sitio alterno.

- Actividades Realizadas: Evaluación de alternativas en manejadores de base de datos.
  Migración de la base de datos de claves públicas de Sybase Adaptive Server a PostgreSql.
  Implementación de una herramienta que permitiera la replicación asíncrona de los datos al sitio alterno.
  Pruebas de los componentes y operatividad con el SAT.

- Resultados del proyecto. Se logró la distribución de los datos en diferentes instancias de manejadores de base de datos, se logró la replicación de datos al sitio alterno y la distribución de los datos fue uniforme, lo cual indicaba que el algoritmo implementado era el óptimo. Sin embargo, al hacer solo ajustes, adicionar productos y no hacer reingeniería a algunos componentes fue mantener la operación y dar seguimiento a un incidente.

## Proyecto 3

- Fecha: 2007 – 2008

- Nombre: Reforzamiento de la Infraestructura Extendida de Seguridad (IES).

- Empresa: Banco de México

- Rol: Analista de Sistemas.

- Alcance del proyecto: Reingeniería de los componentes de la IES para mejorar su desempeño y operatividad. Alcanzar la taza de registro de 20 certificados por segundo, esto estimando el posible crecimiento del uso de la Firma electrónica en el país.
  Utilizar las herramientas nativas del manejador de base de datos para implementar una replicación de datos asíncrona.

- Actividades Realizadas: Implementación de una replicación asíncrona con las herramientas nativas del manejador de base de datos.
  Pruebas de volumen y validación con las agencias certificadoras participantes. (SAT y CECOBAN).

- Resultados del proyecto: La reconstrucción de algunos elementos de la IES permitió que estos lograran un funcionamiento más estable y eficiente. Se logró una taza de registro de 50 certificados por segundo y la replicación de datos asíncrona era casi instantánea. El soporte y seguimiento a la operación era bastante ágil y el número de incidentes bajó significativamente.

## Proyecto 4

- Fecha: 2010 – 2011

- Nombre: Implementación de esquemas de alta disponibilidad y de cambio de servidor para dar continuidad a la operación.

- Empresa: Banco de México

- Rol: Analista de Sistemas. Este el primer proyecto donde desempeñé el rol de líder de proyecto.

- Alcance del proyecto: Diseño de un esquema que permitiera el cambio de servidor de manera eficiente y reduciendo en su máximo posible la perdida de

comunicación de la infraestructura de computo, esto con el objetivo de reducir las afectaciones de la operación.
Debido al crecimiento del uso de la firma electrónica, ante una incidencia en el servidor principal, el cambio de servidor se llevaba a cabo en alrededor de 20 minutos, lo cual representaba que en el país se tuvieran 20 minutos sin los servicios de la firma electrónica.

- Actividades Realizadas: Colaboración en el diseño e implementación de herramientas nativas del sistema operativo para lograr virtualizar las direcciones IP y así el cambio del servidor no representara hacer cambios a los clientes que se conectan a los servicios.
  Configuración de direcciones físicas de red (MAC ADDRESS) para evitar reconfiguraciones en los firewalls (actualización de tablas ARP) y de esta manera la reconexión de los clientes fuera en el momento del cambio.
  Coordinación y apoyo en la implementación de herramientas y utilerías que permitían que el cambio del servidor se diera de manera automática en menos de 5 segundos una vez detectada la caída del servidor primario. Estas herramientas tienen la capacidad de configurarse y así encender los servicios que se ejecutan en los servidores para lograr un cambio completo de servidor.

- Resultados del proyecto: Las pruebas con sistemas críticos como la IES, dieron resultados de un cambio de 8 servidores en un tiempo de 45 segundos, una vez que el servidor secundario detecta la caída del servidor principal. Esto permitió que los tiempos por falla del servidor principal, centro de cómputo o incluso de telecomunicaciones, no afectaran los niveles de servicio comprometidos para la operación.
  Dado los buenos resultados de este modelo de operación, parte de la infraestructura crítica de El Banco ha implementado este modelo con sus respectivas adecuaciones para ser compatible con el sistema operativo.

## Proyecto 5

- Fecha: 2011 - 2012 y 2014

- Nombre: Ley de Firma electrónica Avanzada. Reglamento de firma Electrónica Avanzada.

- Empresa: Banco de México

- Rol: Analista de Sistemas.

- Alcance del proyecto: Colaborar con el SAT para la instrumentación de un proyecto de Ley que regule la implementación y el uso de la firma electrónica en México.
  Como parte complementaria a la Ley de Firma Electrónica en México, se colabora en conjunto con el SAT en la elaboración del Reglamento de Ley de Firma Electrónica en México el cual pretende cubrir aspectos técnicos de la firma electrónica.

- Actividades Realizadas: Colaboración en la revisión y redacción de la Ley de Firma Electrónica en México.
  Colaboración en la revisión y redacción del Reglamento de la Ley de Firma Electrónica en México.

- Resultados. La ley de firma electrónica avanzada en México fue publicada en enero de 2012 y el reglamento en marzo de 2014, ambos en el Diario Oficial de la Federación.

## Proyecto 6

- Fecha: **2015**

- Nombre: Requerimientos mínimos de seguridad informática para la incorporación de instituciones financieras al SPEI.

- Alcance del proyecto: Definir los requerimientos mínimos de seguridad informática que deben de cumplir las instituciones financieras que estén interesadas en participar en el SPEI.

- Actividades Realizadas: Colaboración y revisión en la definición de requerimientos mínimos de seguridad informática para que una institución se

pueda conectar a la infraestructura de telecomunicaciones y cómputo con la que se interconectan y comunican todas las instituciones financieras.
De manera general los requerimientos de incorporación son:

- Contar con un área designada, responsable de la seguridad informática que verifique que la administración de la Infraestructura Tecnológica se lleva a cabo conforme a las políticas y procedimientos de seguridad informática establecidos.
- Contar con una política escrita que deberá seguir sobre el fortalecimiento de la Infraestructura Tecnológica.
- Contar con políticas que deberá seguir para un manejo seguro de la información electrónica.
- Contar con políticas que deberá seguir para implementar mecanismos robustos y seguros de control de acceso a la Infraestructura Tecnológica.
- Contar con políticas que deberá seguir para la gestión de una red de telecomunicaciones que permita la comunicación segura y eficiente con el Banco de México.

- Resultados: La definición y solicitud de estos requerimientos han permitido que El Banco como regulador de los sistemas de pagos, tenga un panorama de la seguridad informática de los participantes en el sector financiero y pueda elaborar programas de supervisión que ayuden a mantener un sistema financiero más saludable.

## Proyecto 7

- Fecha: 2015 -2016

- Empresa: Banco de México

- Rol: Analista de sistemas / Líder de especialidad.

- Nombre: SPID (Sistema de Pagos Interbancario en Dólares).

- Alcance del proyecto: Implementar un Sistema que permita realizar transferencias electrónicas en dólares entre cuentas de depósito a la vista en

dólares en la República Mexicana, correspondientes a personas morales que tengan su domicilio en territorio nacional.

- Instrumentar la regulación que incluya los requisitos de incorporación y permanencia, así como los esquemas de operación con el SPID.
    - En la regulación deberán incluirse requisitos de:
        - seguridad informática
        - gestión de riesgo operacional
        - certificación del aplicativo (con el que se conectaran al SPID)
        - riesgos adicionales (lavado de dinero)

- Actividades Realizadas: Colaboración y redacción, en los temas requisitos de seguridad informática, de la Circular Telefax 4/2016 denominada "Normas Internas de Operación del SPID" publicada en el Diario oficial de la Federación en marzo de 2016.
  Colaboración y redacción del Manual de Operación del SPID, principalmente en los temas de seguridad informática. En este manual se da detalle de los requisitos de incorporación y permanencia del SPID.
  De manera general los requerimientos de incorporación y permanencia son:
    - Contar con un área designada, responsable de la seguridad informática que verifique que la administración de la Infraestructura Tecnológica se lleva a cabo conforme a las políticas y procedimientos de seguridad informática establecidos.
    - Contar con una política escrita que deberá seguir sobre el fortalecimiento de la Infraestructura Tecnológica.
    - Contar con políticas que deberá seguir para un manejo seguro de la información electrónica.
    - Contar con políticas que deberá seguir para implementar mecanismos robustos y seguros de control de acceso a la Infraestructura Tecnológica.
    - Contar con políticas que deberá seguir para la gestión de una red de telecomunicaciones que permita la comunicación segura y eficiente con el Banco de México.

- Resultados: El resultado de este proyecto ha sido la puesta en marcha del Sistema de Pagos Interbancarios en Dólares a partir del 3 de abril de 2016 y actualmente se tienen operando 28 bancos.


*Figura 4. Diagrama de operación del sistema SPID.*

## Proyecto 8

- Fecha: 2010, 2012, 2015 y 2016

- Nombre: Fortalecimiento de los sistemas de pagos.

- Empresa: Banco de México

- Rol: Analista de Sistemas.

- Alcance del proyecto: Evaluar la seguridad de la infraestructura de cómputo, telecomunicaciones y de los componentes de software utilizados por los sistemas de pagos. Esta evaluación deberá ser hecha por un consultor externo, especializado en temas de seguridad informática.
  Debido a la importancia sistémica que han tomado los sistemas de pagos, ha sido necesario que la evaluación de los componentes (software y hardware) y no quede solo en la evaluación por parte del personal de El Banco, es de gran

importancia contar con la evaluación y opinión de un tercero experto en seguridad informática.

- Actividades Realizadas: Responsable de la Dirección de Sistemas de Pagos de dar seguimiento a las diferentes actividades realizadas por los consultores externos durante la evaluación de la seguridad de los sistemas de pagos.
  Atender las observaciones y hallazgos de la infraestructura de cómputo a mi cargo.

- Resultados del proyecto: Las diferentes evaluaciones por las que han pasado los sistemas de pagos, han servido para detectar debilidades en los sistemas de pagos.
  Estos hallazgos han ido decreciendo a través del tiempo, lo cual es un indicativo de que la seguridad informática en los sistemas de pago y en El Banco en general ha tomado una gran relevancia.

## Proyecto 9

- Fecha: 2015

- Nombre: Definición de políticas de seguridad y fortalecimiento de infraestructura de computo con sistema operativo Red Hat Enterprise Linux.

- Empresa: Banco de México

- Rol: Analista de Sistemas / Líder de proyecto.

- Alcance del proyecto: Definir políticas y procedimientos escritos que permitan tener una base para el fortalecimiento y aseguramiento de la infraestructura de cómputo. Estas políticas deberán cumplir con estándares internacionales y apegarse a las mejores prácticas publicadas por estos estándares.
  A pesar de que la infraestructura de cómputo se encontraba con un fortalecimiento adecuado, no se contaba con un procedimiento escrito que formalizara los esquemas de seguridad implementados en el sistema operativo y los servicios que estos ofrecen.

En este sentido, era necesario armar una política escrita que respaldara los esquemas implementados.

- Actividades Realizadas: Coordinar, desarrollar e implementar una política escrita que contempla todas las actividades que se realizan en los servidores para mantener los servicios y la operación segura.
  Coordinar e implantar herramientas que distribución libre para el monitoreo de los servidores de posibles intrusiones, comportamiento anómalo y validar la integridad de la información contenida en los servidores.
  Coordinar e implantar herramientas nativas del sistema operativo Red Hat Enterprise Linux para restringir y dar seguimiento a las actividades de los usuarios.
  Coordinar e implantar herramientas que permiten hacer pruebas de penetración y la identificación de vulnerabilidades en el sistema operativo

- Resultados del proyecto: La implementación de estas políticas ha permitido que las actividades de fortalecimiento estén respaldadas por un procedimiento escrito y en caso de una auditoria no se tengan observaciones.
  La utilización de herramientas de distribución libre ha permitido validar y fortalecer que los procedimientos implementados en la infraestructura de cómputo cumplan con los objetivos planteados.

## Proyecto 10

- Fecha: 2015 – Actualidad

- Nombre: Esquemas de supervisión a las instituciones financieras que se conectan con el SPID operados por Banco de México.

- Empresa: Banco de México

- Rol: Líder de especialidad.

- Alcance del proyecto: Supervisar y validar que las instituciones financieras que quieran conectarse y estén conectadas a la infraestructura en la que opera el SPID cumplan con los requisitos de seguridad definidos en la Circular

Telefax 4/2016 denominada “Normas Internas de Operación del SPID” publicada en el Diario oficial de la Federación en marzo de 2016

- Actividades realizadas: Revisión de los requisitos de seguridad informática de las instituciones interesadas en incorporase al SPID. Esto consiste en la revisión de elementos que envían las instituciones financieras que sirven como evidencia para incorporarse al SPID.
  Participación en los esquemas de supervisión de los requisitos de permanencia de las instituciones ya incorporadas al SPID. Esto consiste en hacer visitas a las instalaciones de las instituciones que ya se encuentran operando en el SPID y se valida que sigan cumpliendo los requisitos de seguridad informática.

- Resultados. Ha permitido conocer el nivel de seguridad informática con el que operan las instituciones financieras. Esto ha permitido que la operación del sistema SPID se lleve de una manera más segura.
  Actualmente se sigue colaborando con la revisión de requisitos de las instituciones financieras que están interesadas en incorporarse y se siguen realizando las visitas de supervisión a las instituciones que ya están operando en el SPID.


***Figura 5. Tarjeta de identificación como inspector por parte de Banco de México.***

# Capítulo III Definición de políticas de seguridad informática y fortalecimiento de infraestructura de cómputo con sistema operativo Red Hat Enterprise Linux

## 1. Descripción del proyecto.

El proyecto consistió en definir las políticas de seguridad informática y procedimientos que permitan el fortalecimiento de la infraestructura de cómputo, enfocándose en el fortalecimiento del sistema operativo y en este caso particular al sistema operativo Red Hat Enterprise Linux.

Una vez definidas, estas debieron de aplicarse a la infraestructura de cómputo siguiendo las mejores prácticas de seguridad informática emitidas por organismos como NIST, DSI, PCI, CIS, SANS y respetando las políticas internas de El Banco.

Posteriormente se debió validar y evaluar la infraestructura de cómputo con herramientas que permitan conocer el nivel de fortaleza con el que se cuenta e identificar posibles vulnerabilidades que pudieran representar un riesgo.

Por último, para las vulnerabilidades que fueron detectadas y que no pudieron ser mitigadas por la naturaleza de la operación de la infraestructura de cómputo, se implementaron controles compensatorios que ayudaron a reducir los riesgos que estas representaban.

## 2. Definición del problema.

A pesar de que la infraestructura de cómputo contaba con un nivel de fortalecimiento adecuado, no se contaban con las políticas y procedimientos escritos que avalaran y respaldaran que todos los controles que se tenían implementados para fortalecer y reducir los riesgos de un incidente de seguridad informática.

Los manuales y referencias para la configuración de estos controles son importantes, pero era necesario contar con una política de seguridad informática que formalizara y respaldara estos manuales y que indicara que esta es aplicada como parte del proceso de operación de la infraestructura de cómputo.

**¿Qué es una política?**

Una política está definida como: "Arte o traza con que se conduce un asunto o se emplean los medios para alcanzar un fin determinado"[1], esta definición es obtenida de la real academia española.

En informática está definida como: "La política de seguridad informática es un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de seguridad informática dentro de la misma, es decir, definen lo que está permitido y lo que está prohibido, permiten definir procedimientos y herramientas necesarias, expresan el consenso de los responsables y permiten adoptar un ambiente saludable en la organización"[2], esta definición es obtenida del sitio de laboratorio de seguridad informática y redes de la Facultad de Ingeniería de la UNAM.

En otras palabras, una política de seguridad informática define las reglas con las que se debe operar la tecnología y respalda los procedimientos aplicados para asegurar la operación de la tecnología.

## 3. Objetivo

Desarrollar una política y procedimientos que respalden que la infraestructura de cómputo a cargo de mi equipo de trabajo tiene el fortalecimiento adecuado para operar en una red de telecomunicaciones en la que interconecta con diferentes instituciones.

## 4. Análisis y proceso implementado.

[1] Definición de "política" http://dle.rae.es/?id=Ta2HMYR
[2] Definición de "políticas de seguridad" http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/DefinicionPolitica.php

Es importante mencionar, que la definición de políticas de seguridad informática y el fortalecimiento de la infraestructura de cómputo, no exentan que la infraestructura de cómputo quede libre de cualquier riesgo de seguridad informática. El objetivo de las políticas y los procedimientos de fortalecimiento y sobre todo los mecanismos implementados en la infraestructura de cómputo es reducir significativamente los riesgos ante algún incidente de seguridad informática.

A continuación, se enlistan los pasos que se siguieron para la elaboración de las políticas. Se parte del punto de que la problemática es que no se cuenta con una formalización de las configuraciones aplicadas.

**Paso 1: Alcance de las políticas.**

Para la definición de las políticas de seguridad informática y el fortalecimiento de la infraestructura de cómputo con sistema operativo Red Hat Enterprise Linux, fue necesario definir el alcance que se pretendía.

Alcance de las políticas.

- Infraestructura de cómputo a cargo de mi oficina.
    - Ambientes de operación (desarrollo, pruebas, pre-producción y producción).
- Fortalecimiento del sistema operativo Red Hat Enterprise Linux.
- Servicios de software contenidos en la infraestructura de cómputo.
    - Bases de datos.
    - Servidores web.
    - Servicios de propósito específico.
- Información contenida en los servidores.
    - Bitácoras del sistema operativo.
    - Bitácoras de la operación de los sistemas.

Aspectos que no cubren las políticas

- Infraestructura de telecomunicaciones.
- Seguridad perimetral.

- Infraestructura de cómputo que no está a cargo de mi oficina.

**Paso 2: Entender y considerar el negocio y operación de los sistemas**

Un punto importante para la definición de las políticas de seguridad informática, fue considerar y entender el negocio que opera en la infraestructura de cómputo que se pretendía fortalecer. De lo contrario, una política mal implementada podría derivar en la degradación de los servicios que se ejecutan o incluso derivar en una interrupción completa que podría tener consecuencias muy grandes.

Se consideraron las condiciones en las que opera esta infraestructura, es decir:

- Horarios de operación
    - Sistemas con operación diurna de lunes a viernes
    - Sistemas con operación nocturna de domingo a jueves.
    - Sistemas con operación 24 horas los 7 días de la semana.
- Entorno de operación
    - No se cuenta con acceso a Internet
    - Red privada con acceso restringido desde El Banco y con intercomunicación con otras instituciones
- Tipos de servicios ofrecidos
    - Web services
    - Base de datos
    - Servicios propietarios (protocolos propietarios)
- Tipo de información manejada por los servicios
    - Parte de la información confidencial y sensible es cifrada por las aplicaciones.
    - Manejo de certificados, que es considerara como información pública.
- Mecanismos de seguridad implementados en la infraestructura tecnológica adicional.
    - El acceso físico a centros de cómputo es controlado y con autorización puntual.
    - La infraestructura de telecomunicaciones, configurada y operando conforme a las mejores prácticas de seguridad.

- La infraestructura de cómputo de las instituciones que se comunican con los sistemas de pagos están fuera del alcance de El Banco, por lo que se asume que pueden ser un riesgo potencial.

En los casos donde se detectó un área de oportunidad en el negocio y operación de los sistemas, fue reportado y se propusieron controles compensatorios, dejando claro la posible afectación que podría verse reflejada en la operación.

Un ejemplo de esto, puede ser el envío de correos desde un cliente de operación, se detectó que las librerías que ocupaban para la conexión por Secure Shell tenían configurado algoritmos de cifrado débiles como DES y 3DES. En este caso se solicitó a los equipos de desarrollo que actualizaran las librerías de conexión para poder deshabilitar estos algoritmos en los servicios de Secure Shell de la infraestructura.

**Paso 3: Revisión de normas y estándares existentes.**

Fue necesario revisar la literatura y los diferentes estándares ya existentes relacionados con la seguridad informática. Esta revisión abarcó los estándares locales por los que es regido El Banco y los estándares con reconocimiento internacional. El tema de la seguridad informática no era algo nuevo y ya se tenía bastante información que consultar, lo que ayudó a tener un panorama más amplio y en consecuencia tener un mejor planteamiento de las políticas.

Entre los estándares internacionales que se revisaron y se tomaron en cuenta para la elaboración de las políticas se encuentran:

**NIST**

El NIST (por sus siglas en inglés National Institute of Standards and Technology), es un instituto del gobierno de los Estados Unidos que trabaja con la industria privada para promover normas, métricas y tecnología con el fin de realzar la productividad, facilitar el comercio y mejorar la calidad de vida.

Este instituto tiene un gran compendio de normas y métricas relacionadas con la seguridad informática, incluyendo los temas de reforzamiento de infraestructura de cómputo.


*Figura 6. Página web de NIST para consulta de normas y métricas en seguridad informática.*

## SANS

El SANS (por sus siglas en inglés SysAdmin Audit, Networking and Security Institute) es una de las organizaciones de mayor prestigio en seguridad de la información. Aunque se especializa en capacitación y asesorías en temas de seguridad informática, tiene un conjunto de guías de trabajo y referencias que promueven las mejores prácticas en seguridad de la información.


*Figura 7. Página web de SANS para consulta de estándares y mejores prácticas en seguridad informática.*

## DISA

Es una agencia de seguridad de los Estados Unidos de América especializada en seguridad de la información. La principal aportación de esta agencia es la publicación de guías de trabajo, publicaciones de investigaciones, listas de verificación, todas con el objetivo de promover la seguridad de información.

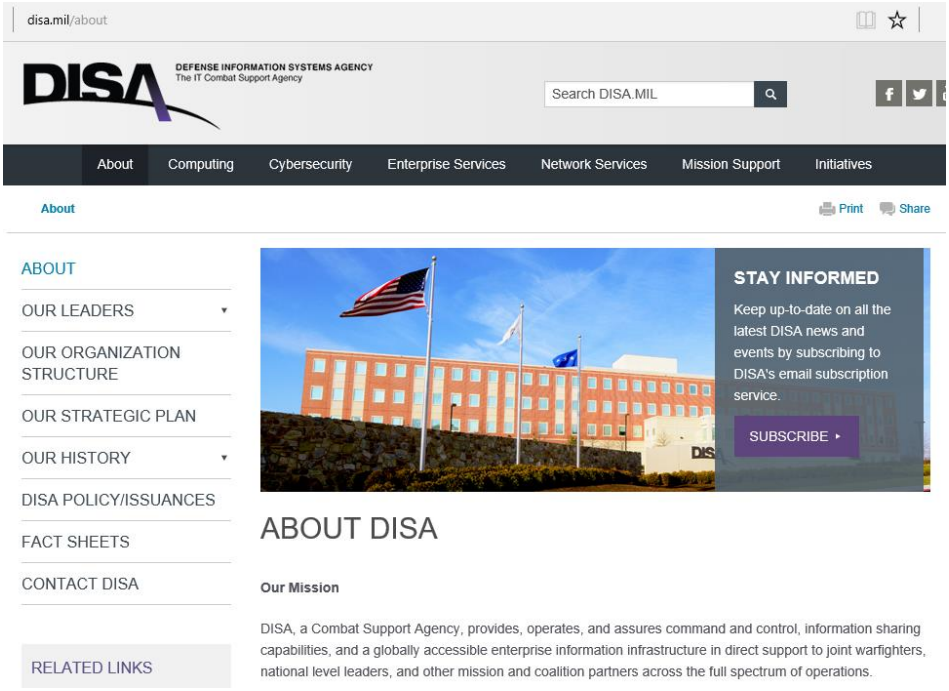



*Figura 8. Página web de DISA para consulta de guías y mejores prácticas en seguridad informática.*

## PCI

El PCI Security Standards Council es un foro internacional abierto destinado a la formulación, la mejora, el almacenamiento, la difusión y la aplicación permanente de las normas de seguridad para la protección de datos de cuentas bancarias.

La misión del PCI Security Standards Council es aumentar la seguridad de los datos de cuentas de pago mediante la promoción de la educación y el conocimiento sobre las Normas de seguridad de la PCI (Payment Cards Industry). Las empresas fundadoras de esta organización son American Express, Discover Financial Services, JCB International, MasterCard y Visa Inc.

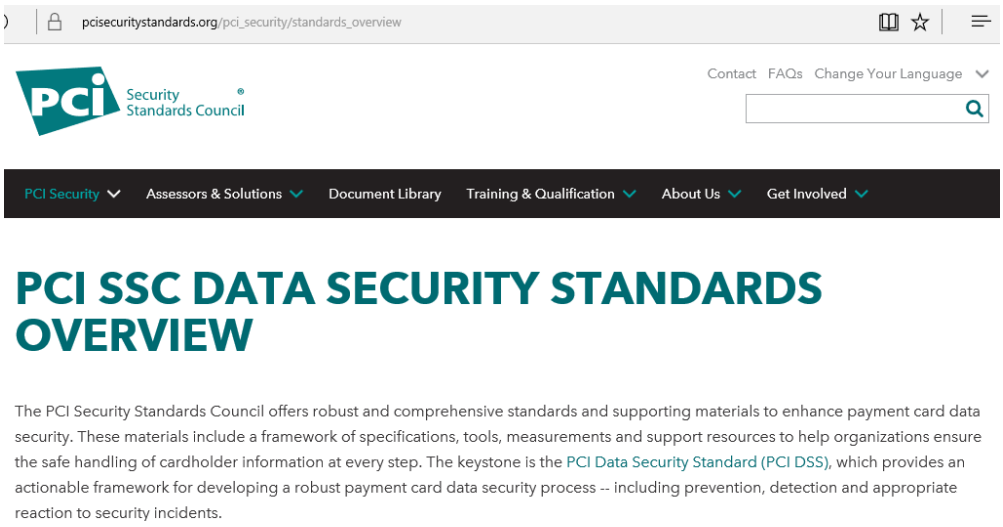



*Figura 9. Página web de PCI para consulta de estándares de seguridad para el manejo de información sensible y crítica.*

## CIS

El CIS (por sus siglas en inglés, Center for Internet Security) es una organización dedicada a aportar mejoras en la seguridad informática. Utilizando su experiencia en la industria y en las entidades gubernamentales enfrenta los retos de seguridad informática ayudando a organizaciones en la implementación de las mejores prácticas para que estén preparadas para un posible ataque.

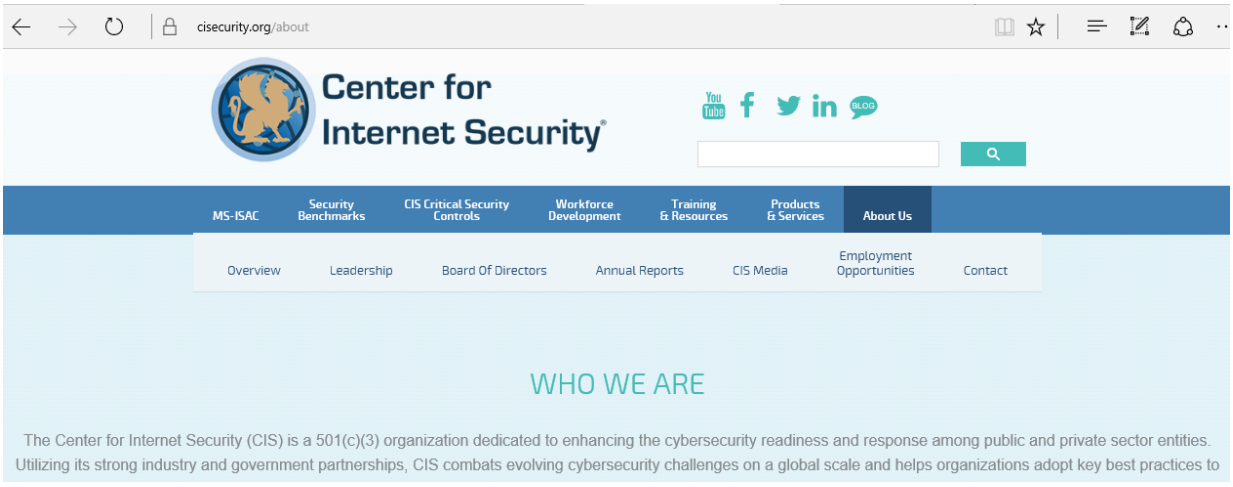



*Figura 10. Página web de CSI para consulta de guías y mejores prácticas de seguridad informática.*

**Paso 4: Definición de las políticas de seguridad informática.**

Una vez completados los pasos anteriores, se pudo proceder a la definición de las políticas, las cuales describen de manera general los procedimientos para tener una infraestructura de cómputo con controles que permitan mitigar los riesgos de seguridad informática y que al mismo tiempo respeten el negocio y la operación de la institución.

Estas políticas fueron revisadas y autorizadas por mis jefes inmediatos. Si esta tarea sólo se dejara a los administradores de la infraestructura se puede caer en omisiones por parte en los procedimientos definidos y siempre es bueno tener una segunda opinión.

En términos generales las políticas de seguridad informática que respaldan el fortalecimiento de la infraestructura de cómputo con sistema operativo Red Hat Enterprise Linux quedaron descritas de la siguiente manera:

a) Procedimientos escritos que describan sobre el fortalecimiento de la infraestructura de cómputo.
b) Procedimientos escritos que describan sobre el manejo seguro de la información.
c) Procedimientos escritos que describan sobre la implementación de mecanismos robustos y seguros de acceso a la infraestructura de cómputo.
d) Procedimientos escritos que regulen las conexiones a los puertos de servicio que se ejecutan en la infraestructura de cómputo.
e) Procedimientos escritos que describan sobre la continuidad de la operación ante la falla de la infraestructura de cómputo.

Es importante mencionar que las políticas que se plantearon no son copias fieles a los estándares internacionales, esto debido a que se debe considerar las condiciones de la operación. Un ejemplo de esto puede ser:

Algunas prácticas sugieren que la red se encuentre cifrada, lo cual baja significativamente la posibilidad de que un usuario mal intencionado pueda robarse información desde la red. Suponiendo que las comunicaciones fueran cifradas desde los dispositivos de telecomunicaciones, ante algún incidente operativo que requiera que el personal que administra las telecomunicaciones deba monitorear la red, debe deshabilitar el cifrado para poder realizar el monitoreo y hacer esto significa una posible afectación en la operación de los sistemas. Por eso es importante evaluar la seguridad contra el buen funcionamiento de la operación, en este caso, una posible solución podría ser que las aplicaciones cifren la información sensible.

En el numeral 5 de este capítulo, página 35, se da mayor detalle sobre estas políticas.

**Paso 5: Implementación de las políticas de seguridad informática.**

La implementación de las políticas de seguridad informática consistió en realizar las configuraciones y aplicar los controles compensatorios en la infraestructura de cómputo.

Estas configuraciones tuvieron que hacerse considerando los esquemas de la operación de los sistemas esto con el objetivo de que no se tengan contratiempos en la operación.

Esta implementación se documentó y es conocida como Instructivos de Fortalecimiento de Infraestructura de cómputo. Fue importante que estos documentos se catalogaran como de acceso restringido ya que solo podrán tener acceso a estos los responsables de la infraestructura.

En el numeral 6 de este capítulo, página 47, se dará mayor detalle sobre estas implementaciones.

**Paso 6: Validación de los procedimientos implementados en la infraestructura de cómputo.**

Para tener una mayor certeza de la eficiencia y eficacia de los procedimientos implementados, fue necesario validarlos.

La validación fue por medio de herramientas automatizadas especializadas en pruebas de penetración. Para esta validación fueron utilizadas dos herramientas de ámbito comercial y una distribución de Red Hat Enterprise Linux conocida como “Kali” especializada en temas de seguridad. Es importante mencionar que esta validación se puede hacer con las versiones gratuitas de estas herramientas.

En el numeral 7 de este capítulo, página 48, se dará más detalle sobre esta validación.

## Diagrama general del proceso

Es importante comentar que este proceso definido podrá ser aplicado para nueva infraestructura que se incorpore a la operación de los sistemas de pagos.

A manera de diagrama de flujo el proceso quedó representado de la siguiente manera.

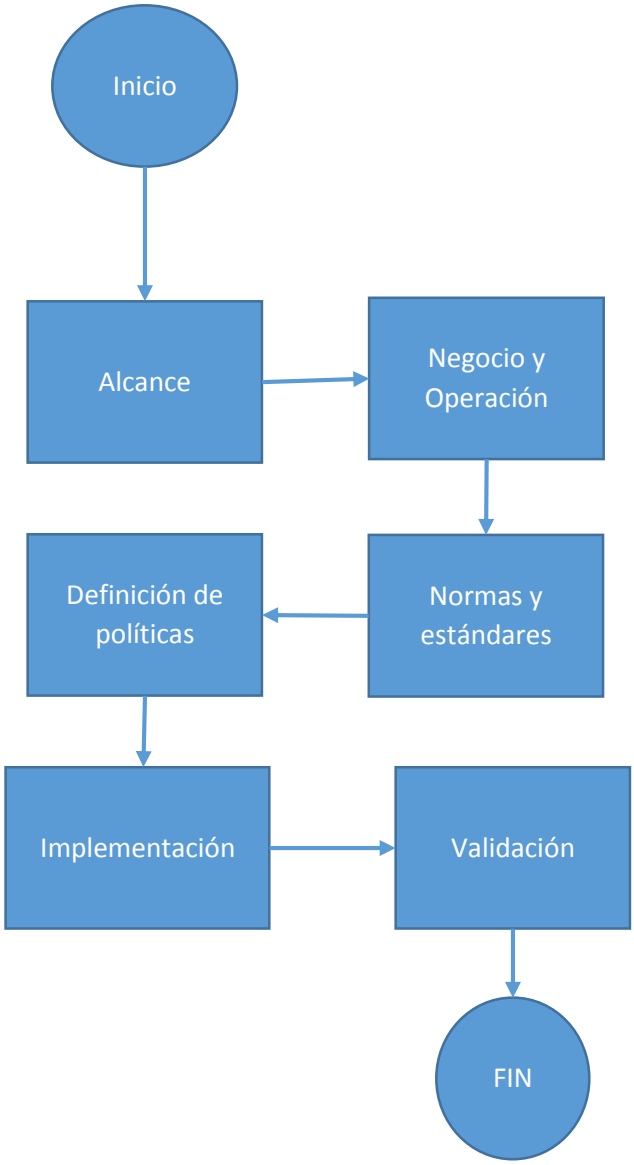



***Figura 11. Diagrama de proceso de implementación de Políticas de seguridad informática.***

## 5. Definición de políticas de seguridad informática.

### ¿Por qué es importante contar con una política de seguridad informática?

Las políticas de seguridad informática son la base para poder respaldar los procedimientos que se tienen implementados en materia de seguridad informática.

En primer lugar, las políticas escritas son un mecanismo para obligar a seguir los procedimientos definidos y, en segundo lugar, como medios para transparentar las actividades en temas de seguridad informática que se realizan ante un tercero, como puede ser un proceso de auditoría ya sea externo o interno a El Banco.

### ¿Cuál es la información que debe llevar una política?

Considerando que las políticas pueden ser auditadas y en un momento dado consultadas por terceros ajenos a El Banco, la política no debía contener el detalle técnico con valores sensibles que en algún momento dado pueden ser aprovechados por un usuario mal intencionado y en un supuesto poder sacar ventaja de esos datos para intentar vulnerar la infraestructura de cómputo. Algunos ejemplos de estos datos son: longitudes de contraseñas, puertos de operación de servicios, versión de kernel del sistema operativo, ciclo de actualizaciones y atención vulnerabilidades, etc.

Las políticas solo debían tener información general que explique los tipos de controles que son implementados.

En casos donde es necesario incluir todo el detalle en las políticas, se recomienda tener dos versiones: una versión restringida que solo esté al alcance de la institución y otra versión pública que en algún momento pueda ser compartida, esto siempre indicando que se tiene otra con el detalle técnico.

Otro motivo por el cual no fue recomendable incluir el detalle en las políticas, era por facilidad de administración y actualización. Normalmente las políticas deben de ser revisadas y aprobadas por unidades administrativas de auditoría, lo que implica que cualquier modificación a la política debe ser llevada nuevamente para su revisión y aprobación, en la mayoría de los casos estos procesos son lentos y requiere

la inversión de muchas horas de trabajo. Por lo que se optó por hacer referencia a Anexos u otros documentos que no formen parte de la política y que cualquier actualización y/o modificación sea prácticamente transparente.

**Políticas de seguridad informática definidas para el fortalecimiento de la infraestructura tecnológica.**

Para el caso de la infraestructura tecnológica que está a mi cargo se enunciaron los siguientes incisos, los cuales engloban los diferentes aspectos que pretenden cubrir las políticas de seguridad informática.

a) Procedimientos escritos que describan sobre el fortalecimiento de la infraestructura de cómputo.
b) Procedimientos escritos que describan sobre el manejo seguro de la información.
c) Procedimientos escritos que describan sobre la implementación de mecanismos robustos y seguros de acceso de control de acceso a la infraestructura de cómputo.
d) Procedimientos escritos que regulen las conexiones a los puertos de servicio que se ejecutan en la infraestructura de cómputo.
e) Procedimientos escritos que describan sobre la continuidad de la operación ante la falla de la infraestructura de cómputo.

Es importante mencionar que estas políticas y procedimientos debieron ser aplicadas a todos los ambientes de operación, es decir, a los ambientes de: desarrollo, pruebas, pre-producción y producción.

A continuación, se detalla cada uno de los procedimientos.

**a) Procedimientos escritos que describan sobre el fortalecimiento de la infraestructura de cómputo.**

i. Procedimiento sobre las características de instalación de un servidor con sistema operativo Red Hat Enterprise Linux.
    1. El sistema operativo deberá ser instalado con una instalación tipo Base, es decir, sin ambiente gráfico, aplicaciones y sin ningún tipo de servicio que permita su conexión.

2. El acceso con el usuario “root”, ya sea local o remotamente, será deshabilitado y éste se mantendrá así durante toda la operación del servidor.
3. El único servicio para conexión remota que tendrá habilitado para la configuración inicial será el servicio de “Secure Shell” y la autenticación será únicamente por de llave pública.

ii. Procedimientos para prescindir de protocolos de comunicación y servicios de cómputo que no sean necesarios para la operación de los sistemas y el buen funcionamiento de la infraestructura de cómputo.
    1. Todos los servicios que son instalados por “default” y que no son necesarios para el buen funcionamiento del servidor deberán ser desinstalados o, de no ser posible, deshabilitados.
    2. Los servicios y protocolos que sean necesarios para la operación, deberán ser solicitados por medio de correo electrónico a los administradores de la infraestructura con copia a los responsables, indicando el tipo de servicio, una pequeña descripción de su uso e indicará, si fuera el caso, los clientes y direcciones IP de los mismos que se conectaran a los servicios solicitados.
    3. En caso de ser necesario habilitar alguno de los protocolos de comunicación considerados como “inseguros” o que transfieren la información en texto claro, el administrador deberá validar con el usuario que no se tengan algún otro tipo de medio de conexión para cubrir la operación. De no tener alternativas se deberán de aplicar controles compensatorios para mitigar los riesgos que resultan de usar protocolos inseguros.

iii. Procedimientos que contemplen mecanismos para el seguimiento de las actualizaciones y parches del sistema operativo e infraestructura de software.
    1. Se deberá de ejecutar periódicamente un escaneo con diferentes herramientas para detectar las posibles vulnerabilidades en la

infraestructura de cómputo derivadas de la falta de actualización y de aplicación de parches.

2. El escaneo de vulnerabilidades deberá ser realizada por la unidad administrativa encargada de la seguridad informática de El Banco.
3. Las vulnerabilidades serán categorizadas de la siguiente manera: Bajas, Medias y Altas. Esta categorización deberá hacerse considerando los criterios descritos en "Instructivos de fortalecimiento de Infraestructura de Cómputo".
4. La prioridad en la atención de las vulnerabilidades deberá ser dando prioridad a las que representen mayor riesgo y la atención deberá ser de acuerdo a los tiempos definidos en los "Instructivos de fortalecimiento de Infraestructura de Cómputo".
5. La atención de las vulnerabilidades deberá seguir el proceso de desarrollo, es decir, primero deberá validarse su buen funcionamiento en los ambientes de desarrollo y pruebas, siguiendo por pre-producción y por último en producción.
6. En caso de que la atención de alguna de las vulnerabilidades derive en una modificación a las aplicaciones y/o sistemas, esta atención deberá ser calendarizada considerando los tiempos que se lleven las modificaciones a los sistemas y servicios.
7. En caso de que una vulnerabilidad detectada represente un gran riesgo a la operación y a la seguridad de los sistemas, se deberá de acordar con las áreas de control y operación la aplicación de las correcciones en el inmediato plazo sin la validación completa de los sistemas.
8. En caso de que una vulnerabilidad considerada con un riesgo alto no pueda ser atendida en el inmediato plazo, se deberán aplicar controles compensatorios y monitorear la infraestructura de cómputo.

iv. Procedimiento de monitoreo y registro de recursos de la infraestructura de cómputo.

1. En este procedimiento quedarán excluidos los eventos relacionados con la seguridad informática.

2. Se deberá tener un monitoreo constante de los recursos (CPU, disco duro), éste debe ser capaz de enviar alarmas para avisar sobre el estado de la infraestructura.
3. Se deberá definir y configurar los umbrales en los cuales el monitoreo dará aviso a los administradores antes de que los recursos lleguen al límite de su capacidad. Los umbrales deberán estar definidos en "Instructivos de fortalecimiento de Infraestructura de Cómputo"
4. Se deberá dar seguimiento y atención a las alarmas generadas por los monitores de los recursos.
5. Se deberán registrar los eventos ocurridos y dar solución definitiva a la causa raíz del evento o en caso de no ser posible, implementar controles compensatorios para que no se generen estos eventos.

v. Procedimiento para fortalecer la configuración del sistema operativo conforme las mejores prácticas internacionales de seguridad y administración.
    1. Se deberá elaborar una guía que permita implementar y documentar las mejores prácticas de seguridad y administración aplicadas en el sistema operativo. La guía deberá estar documentada en "Instructivos de fortalecimiento de Infraestructura de Cómputo"
    2. Se deberán seguir y tomar como referencia las guías de configuración publicadas por organizaciones con reconocimiento internacional que sean vigentes al momento de aplicarlas.
    3. Se deberán considerar las recomendaciones y guías emitidas por el proveedor del sistema operativo.
    4. Se deberán de evaluar y validar los controles y configuraciones implementadas a través de herramientas y/o mecanismos automatizados.
    5. Las vulnerabilidades detectadas deberán ser atendidas conforme a lo establecido en los "Instructivos de fortalecimiento de Infraestructura de Cómputo".
    6. Las guías deben ser revisadas y actualizadas al menos una vez al año.

7. Cualquier requerimiento nuevo en la infraestructura de cómputo que derive en una nueva configuración y/o control deberá ser documentada en las guías.

vi. Procedimientos para fortalecer servicios ofrecidos por la infraestructura de cómputo

1. Se deberá elaborar una guía que permita implementar y documentar las mejores prácticas de seguridad a los servicios ofrecidos por la infraestructura. La guía deberá estar documentada en los "Instructivos de fortalecimiento de Infraestructura de Cómputo".
2. Se deberán seguir y tomar como referencia las guías de configuración publicadas por organizaciones con reconocimiento internacional que sean vigentes al momento de aplicarlas.
3. Se deberán considerar las recomendaciones y guías emitidas por los proveedores de los servicios.
4. En la medida de lo posible, se deberán de evaluar y validar los controles y configuraciones implementadas a través de herramientas y/o mecanismos automatizados.
5. Las vulnerabilidades detectadas deberán ser atendidas conforme a lo establecido en los "Instructivos de fortalecimiento de Infraestructura de Cómputo".
6. Las guías deben ser revisadas y actualizadas al menos una vez al año.
7. Cualquier servicio y/o aplicación nueva en la infraestructura de cómputo deberá ser documentada en las guías.

vii. Procedimiento que permita la detección y gestión de incidentes de seguridad informática en la infraestructura de cómputo.

1. Se deberá contar con herramientas y/o mecanismos que permitan detectar eventos de seguridad informático en la infraestructura de cómputo.
2. Los eventos que deben ser monitoreados son:

a) Escaneo de puertos.
b) Intento de intrusiones.
c) Integridad de archivos del sistema operativo.
d) Registro de actividades de los usuarios en la infraestructura de cómputo.

3. Cualquier evento anómalo detectado en la infraestructura debe ser documentado e informado al área de seguridad informática de El Banco.
4. Se dará seguimiento a cualquier evento relacionado a un incidente informático, teniendo un registro del evento con la siguiente información:
    a) Hora de inicio del incidente
    b) Infraestructura, servicios y sistemas afectados por el incidente
    c) Personal que atendió el incidente
    d) Los controles aplicados para la contención del incidente
    e) Hora del fin del incidente
    f) Si aplica, las acciones correctivas para evitar este tipo de incidentes
5. En caso de un incidente informático, se deberán tomar y documentar las acciones necesarias para la contención del incidente, estas acciones dependerán del tipo de incidente que se presente.
6. En caso de un incidente, se deberá obtener una imagen de la infraestructura afectada y resguardada para un análisis exhaustivo, si así lo requiriera.

viii. Procedimiento para evaluar la infraestructura de cómputo a través de procesos automatizados que incluyan la realización de pruebas de penetración.

1. Se deberá de hacer una evaluación periódica de la infraestructura de cómputo para detectar vulnerabilidades derivadas de omisiones y deficiencias en las configuraciones del sistema operativo e infraestructura de software.
2. La evaluación de vulnerabilidades deberá ser realizada con el apoyo de la unidad administrativa encargada de la seguridad informática de El Banco.

3. Las vulnerabilidades detectadas serán categorizadas de la siguiente manera: Bajas, Medias y altas. Esta categorización deberá hacerse considerando los criterios descritos en "Instructivos de fortalecimiento de Infraestructura de Cómputo".
4. La prioridad en la atención deberá ser atendiendo en primer lugar a las que representen mayor riesgo y la atención deberá ser conforme a los tiempos definidos "Instructivos de fortalecimiento de Infraestructura de Cómputo".
5. La atención de las vulnerabilidades deberá seguir el proceso de desarrollo, es decir, primero deberá validarse su buen funcionamiento en los ambientes de desarrollo y pruebas, siguiendo por pre-producción y por último en producción.
6. En caso de que la atención de alguna de las vulnerabilidades derive en una modificación a las aplicaciones y sistemas, esta atención deberá ser calendarizada considerando los tiempos que se lleven las modificaciones a los sistemas y servicios.
7. En caso de que una vulnerabilidad detectada represente un gran riesgo a la operación y a la seguridad de los sistemas, se deberá de acordar con las áreas de control y operación la aplicación de las correcciones en el inmediato plazo sin la validación completa de los sistemas.
8. En caso de que una vulnerabilidad considerada como "alta" no pueda ser atendida en el inmediato plazo, se deberán aplicar controles compensatorios y monitorear la infraestructura de cómputo.

**b) Procedimientos escritos que describan sobre el manejo seguro de la información.**

i. Procedimientos que restrinjan el acceso a los puertos físicos de conexión y dispositivos periféricos.

1. El sistema operativo deberá ser configurado para que los puertos físicos de conexión y dispositivos periféricos solo sean accedidos con el usuario "root".

2. Si la operación de los sistemas requiriera tener acceso a un puerto de conexión o un dispositivo periférico, deberá ser validado con los administradores, los operadores y los responsables de la operación.
3. Cualquier permiso de acceso a un puerto de conexión o un dispositivo periférico deberá ser puntual y monitoreado.

ii. Procedimientos para el resguardo de información histórica de la infraestructura de cómputo.

1. La información contenida en la infraestructura de cómputo deberá ser respaldada diariamente.
2. Los respaldos deben de ser realizados cuando el nivel de operación de los sistemas sea el más bajo.
3. La información deberá ser resguardadas conforme a lo descrito en los "Instructivos de fortalecimiento de Infraestructura de Cómputo".

**c) Procedimientos escritos que describan sobre la implementación de mecanismos robustos y seguros de acceso a la infraestructura de cómputo.**

i. Procedimiento para el acceso a la infraestructura de cómputo.

1. El acceso a la infraestructura de cómputo solo será utilizando al menos usuario y contraseña como autenticación por medio del protocolo de comunicación "Secure Shell".
2. Aquellos equipos que su operación lo permitan, la autenticación será por medio de llave pública utilizando el protocolo de comunicación "Secure Shell".
3. La creación de una cuenta deberá ser solicitada por medio de correo electrónico indicando el "login" de la cuenta, el propósito de la cuenta, el responsable de la cuenta y el servidor donde debe ser creada.

4. Las cuentas para sistemas y servicios solo podrán ser solicitadas por el equipo responsable de la implantación de los sistemas.
5. Las cuentas personales serán creadas conforme a lo establecido en los "Instructivos de fortalecimiento de Infraestructura de Cómputo".
6. La baja de una cuenta deberá ser solicitada por medio de una solicitud por correo electrónico.

ii. Procedimiento que aseguren una gestión de contraseñas segura.

1. Las contraseñas de los usuarios deberán ser guardadas con un algoritmo de digestión robusto y vigente.
2. Las contraseñas deberán contar valores robustos y vigentes en los siguientes atributos:
    a) longitud de caracteres.
    b) deberán estar compuesta por:
        - caracteres especiales
        - dígitos
        - mayúsculas
        - minúsculas
    c) reutilización de contraseñas.
    d) si la operación lo permite, deberán ser cambiadas periódicamente.
    e) la cuenta debe ser bloqueada al tener intentos de acceso no exitosos.
3. Todos los atributos deberán ser configurados conforme a lo descrito en los "Instructivos de fortalecimiento de Infraestructura de Cómputo".

**d) Procedimientos escritos que regulen las conexiones a los puertos de servicio que se ejecutan en la infraestructura de cómputo.**

i. Procedimiento que gestione las conexiones inactivas.

1. Las conexiones que estén inactivas deberán ser desconectadas conforme a lo establecido en los “Instructivos de fortalecimiento de Infraestructura de Cómputo”

ii. Procedimiento que restringa la conectividad en la infraestructura de cómputo.

1. La infraestructura de cómputo no deberá contar con acceso a internet.

    a) Esto deberá ser validado con la unidad administrativa encargada de supervisar y administrar las telecomunicaciones de El Banco.

2. La infraestructura de cómputo deberá de contar con un firewall de software personalizado.

    b) El firewall solo filtrará las conexiones de entrada al servidor.
    c) Para el caso de infraestructura de cómputo en regiones de la DMZ, las conexiones de salida también serán controladas por el firewall.
    d) La apertura de puertos deberá ser solicitada por medio de correo electrónico a los administradores con copia a los responsables de los sistemas, indicando los siguientes datos:
        - Dirección IP del servidor.
        - Dirección(es) IP de los clientes.
        - Puerto(s) solicitados para su apertura.
        - Para equipos en regiones de la DMZ, puertos de los servidores destinos.

3. Se deberá contar con un registro de todos los puertos de comunicación operando en la infraestructura y una relación indicando a que servicio está relacionado.

**e) Procedimientos escritos que describan sobre la operación en la infraestructura de cómputo de respaldo o contingencia**

i. Procedimiento para cambio de servidor.

1. Contar con una guía que describa todo el procedimiento para realizar el cambio de servidor, esta guía deberá estar descrita en los "Instructivos de fortalecimiento de Infraestructura de Cómputo".
2. La guía debe ser revisada y, si se requiriera, actualizada al menos cada 6 meses.
3. Los esquemas de cambio de servidor deben ser probados al menos una vez al año.
4. Los esquemas de cambio de servidor deben de considerar el buen funcionamiento de todos los servicios que son ejecutados en la infraestructura de cómputo.
5. Los esquemas de contingencia deben ser aplicados únicamente a la infraestructura de cómputo de los ambientes de pre-producción y producción.

Para la definición de las políticas se debió tener constante comunicación con los administradores de la infraestructura de telecomunicaciones y de las otras infraestructuras con las que se opera, y de ser necesario, hacer los ajustes necesarios conforme a la operación de sus infraestructuras.

## 6. Implementación de las políticas de seguridad.

La implementación de las políticas de seguridad consistió en realizar las configuraciones y aplicar los controles a la infraestructura de cómputo con el objetivo de mitigar los riesgos.

Fue importante que las configuraciones aplicadas consideraran la operación de los sistemas, porque de lo contrario una mala configuración afectaría la operación y las consecuencias pudieron ser muy graves.

Un ejemplo de esto sería:

Se puede tener un script que ejecute una tarea en un servidor remoto por medio de "Secure Shell" y este ejecute un proceso de validación de firmas electrónicas para posteriormente seguir con el flujo de sus actividades, pero este proceso de validación de firmas puede llevarse un par de horas lo cual se vería reflejado como dos horas de inactividad por la conexión de "Secure Shell". Si, por ejemplo, se tiene una política de desconexión por inactividad de 30 minutos, el proceso descrito anteriormente podría verse afectado y en consecuencia se tendría una afectación en la operación.

Otro punto importante de la implementación de las políticas de seguridad, es que debieron ser validadas en los ambientes previos al de producción, poniendo mayor énfasis en el ambiente pre-productivo, que es un ambiente con operación similar al de producción, pero con datos ficticios. Dado que las pruebas y validaciones de las políticas implementadas en los ambientes pre-productivos resultaron exitosas, la operación no resultó afectada.

Un escenario ideal es que estas políticas hubieran sido implementadas antes de que la infraestructura fuera utilizada para la operación, pero esto solo hubiera sido posible si se integrara infraestructura de cómputo nueva a la operación.

En el Anexo A, se muestran a modo de ejemplo como fueron implementadas algunos controles descritos en las políticas.

## 7. Validación de los procedimientos implementados en la infraestructura de cómputo.

Para tener la certeza de que los controles implementados en la infraestructura de cómputo cumplieran su objetivo de fortalecer y disminuir los riesgos de un incidente de seguridad, era necesario validarlos.

La validación se hizo por medio de varias herramientas automatizadas especializadas en pruebas de penetración. Para esta validación fueron utilizadas dos herramientas de ámbito comercial y una distribución de GNU/Linux conocida como "Kali" diseñada para evaluar aspectos de seguridad.

Las herramientas de ámbito comercial utilizadas fueron: “Nessus” y “Rapid7 Nexpose”. Es importante mencionar que ambas herramientas tienen versiones gratuitas para su utilización y las limitantes van en sentido del número de servidores que pueden ser escaneados y en algunos casos cuentan con plugins para con base al análisis dar una puntuación indicando el nivel de riesgo con el que cuenta la infraestructura.

**Proceso de validación de la infraestructura de cómputo.**

La validación del fortalecimiento de la infraestructura de cómputo se realizó por parte de dos unidades administrativas diferentes, por un lado, mi equipo de trabajo encargado de administrar la infraestructura de cómputo y la segunda se hizo por la unidad administrativa encargada de la seguridad informática de El Banco.

Fue muy importante que la evaluación de la infraestructura fuera hecha por un tercero ajeno a mi unidad administrativa. La importancia radica en:

- Al tener un tercero en la evaluación, yo como responsable de la infraestructura de cómputo dejo de ser juez y parte en la seguridad informática, es decir, somos responsables de mantener la infraestructura de cómputo segura, pero la evaluación y visto bueno de que se cuenta con una infraestructura de cómputo fortalecida me la da un tercero.

Esta mecánica de trabajo ayuda bastante, en el sentido de que como administrador de la infraestructura puedo omitir u obviar puntos que pueden convertirse más adelante en un posible vector de ataque.

**Sobre el tipo de evaluación y pruebas.**

Considerando que el fortalecimiento de la infraestructura de cómputo incluye el reforzamiento del perímetro (puertos y conexiones) y el interior de la infraestructura de cómputo, las pruebas debieron hacerse en el mismo sentido.

Para las pruebas perimetrales, las herramientas no contaban con ningún tipo de acceso al sistema operativo y solo validaron lo que pudieran encontrar desde la red. A este tipo de pruebas normalmente se le conocen como pruebas de caja negra, es decir, se evalúa el sistema solo con la información que puede obtener la herramienta por si sola.

Para las pruebas internas, se generó un usuario con privilegios mínimos para que las herramientas tuvieran acceso al sistema operativo y pudieran evaluar la infraestructura con privilegios mínimos. A este tipo de pruebas normalmente se le conocen como pruebas de caja gris, es decir, se evalúa el sistema solo con la información que puede obtener con un usuario con privilegios mínimos.

Por último, se realizó una prueba interna en la que las herramientas contaron con un usuario con privilegios de administrador y así pudieran evaluar de una manera minuciosa la configuración interna de la infraestructura de cómputo. Esta prueba es de suma importancia ya que validó parámetros que como administrador omití en la configuración. A este tipo de pruebas normalmente se le conocen como pruebas de caja blanca, es decir, se evalúa el sistema con la información que puede obtener con un usuario con privilegios de administrador.

Las primeras dos pruebas fueron realizadas por mi equipo de trabajo y la unidad administrativa responsable de la seguridad informática de El Banco y la tercera prueba solo fue realizada por mi equipo de trabajo, esto por motivos de seguridad y deslinde de responsabilidades por el uso de una cuenta con privilegios de administrador.

En el Anexo B se muestran algunos ejemplos de este tipo de pruebas con herramientas de penetración y que tipo de información puede ser verificada.

# Capítulo IV Resultados.

Los resultados de la instrumentación de este proyecto han servido para darle formalización a los esquemas de seguridad implementados en la infraestructura de cómputo a mi cargo.

La metodología implementada permitió que las políticas de seguridad informática fortalecieran la infraestructura de cómputo, pero considerando y respetando la operación de los sistemas.

El proyecto ayudó a detectar algunas áreas de oportunidad que se tenían en la infraestructura de cómputo que eran obviadas por mi parte, algunos temas sencillos e irrelevantes que no representaban un potencial riesgo y otros que bajo ciertas condiciones hubieran podido llegar a ser explotados por usuarios mal intencionados.

Esto fue gracias al seguimiento de los estándares internacionales como NIST, SANS y guías de buenas prácticas como CIS, DISA; complementado con el uso de herramientas automatizadas para la detección de vulnerabilidades.

Uno de los principales problemas que logramos resolver, fue poder separar los procedimientos generales de los manuales con la implementación técnica. Esto ayudará a que los procesos de auditoría sean más ágiles y que en caso de auditorías, sobre todo externas, como puede ser la Auditoría Superior de la Federación, puedan conocer los procedimientos sin tener acceso al detalle técnico de las implementaciones.

Por último, estos procedimientos serán aplicados a toda nueva infraestructura que llegue y se incorpore a la operación de infraestructura que está a cargo de mi equipo de trabajo.

# Capítulo V Conclusiones.

Mi ingreso a la Facultad de Ingeniería fue en el ciclo escolar 1999 - 2000, en un momento muy relevante para la Universidad, se gestaba un movimiento estudiantil que peleaba por el derecho de una educación superior gratuita y accesible a todos.

Más allá de estar a favor o en contra de alguno de los actores de este evento, sin duda, debo agradecer que la Universidad y en particular a la Facultad de Ingeniería que a pesar de las condiciones en las que se debían de llevar las actividades, siempre me dio la oportunidad, medios, enseñanzas, derrotas y aprendizajes para prepararme y desarrollarme como el profesionista que soy actualmente.

Gracias a la formación académica que recibí en la Facultad de Ingeniería no fue difícil encontrar un primer trabajo a finales de 2004 en una empresa transnacional en la cual experimenté mis primeras experiencias laborales por un periodo de 7 meses.

Fue hasta mediados de 2005 que, nuevamente gracias a la formación académica que recibí en la Facultad, pude entrar a laborar en Banco de México y es aquí donde se ha desarrollado prácticamente toda mi trayectoria profesional. Durante mi estancia en el banco he participado en diferentes proyectos, algunos muy localizados en El Banco y otros con impacto nacional como los temas de firma electrónica y las regulaciones de los participantes en el sistema financiero.

El proyecto que describo en este informe, es para mí uno de los más significativos e importantes, esto debido a que es uno de los proyectos que salió como una iniciativa de mi parte y fue coordinado y desarrollado en su totalidad por mi equipo de trabajo. Esto me permitió aplicar una de las principales enseñanzas durante mi formación como ingeniero, que es, identificar un problema, analizarlo, plantear soluciones y solucionarlo.

Algunas actividades que el proyecto me permitió realizar fue:

- Coordinar un equipo de trabajo.
- Aplicar conocimientos elementales de ingeniería, como fue el planteamiento y solución de un problema.
- Trabajo en equipo.
- Desarrollar habilidades técnicas en seguridad informática.
- Compartir conocimientos con personal con menor experiencia.

- Conocer y entender más la operación de los sistemas de pagos operados por El Banco.
- Aceptar y reconocer errores.

Es muy gratificante para mí el poder estar desarrollando mi carrera profesional en una institución medular para el país como es Banco de México y colaborar en proyectos tan relevantes como los sistemas de pagos.

Por último, es importante mencionar que mi desarrollo profesional actual es en gran medida gracias a la formación académica por parte de la Facultad de Ingeniería, los conocimientos y experiencias adquiridos en mi participación como becario del Programa de Tecnología en Cómputo (PROTECO) y actividades realizadas en el laboratorio de Cómputo.

# REFERENCIAS


1. Banco de México. http://www.banxico.org.mx/
2. Banco de México, IES http://www.banxico.org.mx/sistemas-de-pago/servicios/firma- electronica/firma-electronica.html
3. Banco de México, SPEI. http://www.banxico.org.mx/sistemas-de-pago/servicios/sistema-de-pagos-electronicos-interbancarios-spei/sistema-pagos-electronicos-in.html
4. Banco de México, SPID. http://www.banxico.org.mx/sistemas-de-pago/servicios/sistema-de-pagos-interbancarios-en-dolares-spid/sistema-pagos-interbancarios-.html
5. Ley de Firma Electrónica Avanzada. http://www.diputados.gob.mx/LeyesBiblio/pdf/LFEA.pdf
6. Reglamento de Ley de Firma Electrónica Avanzada. http://dof.gob.mx/nota_detalle.php?codigo=5337860&fecha=21/03/2014
7. Circular 4/2016 dirigida a los participantes en el SPID, relativa a las Reglas del Sistema de Pagos Interbancarios en Dólares (SPID) http://dof.gob.mx/nota_detalle.php?codigo=5429649&fecha=11/03/2016
8. Red Hat. https://www.redhat.com/es
9. NIST. http://www.nist.gov/
10. SANS. https://www.sans.org/
11. DISA. http://www.disa.mil/About/Legal-and-Regulatory/Security-and-Privacy
12. PCI. https://www.pcisecuritystandards.org/
13. CIS. https://benchmarks.cisecurity.org/
14. Real academia española. http://www.rae.es/
15. Seguridad informática. http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/DefinicionPolitica.php
16. Linux check list. SANS. https://www.sans.org/media/score/checklists/linuxchecklist.pdf
17. Infrastructure security step by step. https://www.sans.org/reading-room/whitepapers/basics/infrastructure-security-step-step-430
18. CIS Red Hat Enterprise Linux 7 Benchmark, CIS. https://benchmarks.cisecurity.org/tools2/linux/CIS_Red_Hat_Enterprise_Linux_7_Benchmark_v1.1.0.pdf

**19.** PCI Data Security Standard. https://www.pcisecuritystandards.org/documents/PCI_DSS_v3_DESV.pdf
**20.** PCD DSS Quick Reference Guide. https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_1.pdf
**21.** Kali. https://www.kali.org/
**22.** Nessus. http://www.tenable.com/products/nessus-vulnerability-scanner
**23.** Rapid7 Nexpose. https://www.rapid7.com/products/nexpose/

# GLOSARIO

- **Accenture.** Es una empresa multinacional dedicada a la prestación de servicios de consultoría, servicios tecnológicos y de contratación de terceros.
- **3DES.** Algoritmo de cifrado de información que hoy en día es considerado inseguro.
- **Certificado Digital.** el mensaje de datos o registro que confirme el vínculo entre un firmante y la clave privada
- **DES.** Algoritmo de cifrado de información que hoy en día es considerado inseguro.
- **default.** Configuración que traen los componentes de software cuando son instalados.
- **Firma electrónica Avanzada.** El conjunto de datos y caracteres que permite la identificación del firmante, que ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual produce los mismos efectos jurídicos que la firma autógrafa;
- **Kali.** Distribución de Linux avanzada para pruebas de penetración y auditorías de seguridad.
- **Ley de firma electrónica Avanzada.** Ley que regula el uso de la firma electrónica avanzada y la expedición de certificados digitales a personas físicas, los servicios relacionados con la firma electrónica avanzada, y la homologación de la firma electrónica avanzada con las firmas electrónicas avanzadas reguladas por otros ordenamientos legales, en los términos establecidos en esta Ley.
- **Linux.** Es un sistema operativo de distribución libre y código abierto, el cual tienes las características de ser multitarea y multiusuario.
- **MAC ADDRESS.** Identificador único de 48 bits que corresponde de forma única a un dispositivo de red.
- **Nessus.** Programa especializado en escaneo de vulnerabilidades y pruebas de penetración en infraestructura tecnológica (software, cómputo, telecomunicaciones) que permite evaluar y auditar la seguridad informática de la infraestructura.

- **Oracle.** Es un sistema administrador de base de datos tipo objeto – relacional (ORDBMS, por sus siglas en inglés Object-Relational Data Base Management System) desarrollado por la corporación Oracle
- **PostgreSql.** Es un sistema administrador de base de datos tipo objeto – relacional (ORDBMS, por sus siglas en inglés Object-Relational Data Base Management System) de código abierto y distribución libre.
- **Pro C.** Es un lenguaje embebido de SQL implementado por Oracle. Pro C utiliza el lenguaje C/C++ como parte de su programación.
- **Rapid7 Nexpose.** Programa que evalúa los riesgos de la infraestructura tecnológica (software, cómputo, telecomunicaciones) que permite la administración del ciclo de vida de las vulnerabilidades, incluyendo el descubrimiento, detección, verificación, clasificación de riesgos, análisis de impactos y mitigación
- **Red Hat.** Es la compañía responsable de la distribución del sistema operativo Red Hat Enterprise Linux.
- **Reglamento de la Ley de Firma Electrónica Avanzada**. establecer las normas reglamentarias para el uso de la Firma Electrónica Avanzada; los servicios relacionados con ésta, así como su homologación con otras firmas electrónicas avanzadas, en cumplimiento de la Ley.
- **root.** Es el nombre que identifica a la cuenta con privilegios de administrador en los sistemas operativos de tipo UNIX y Linux.
- **SAT.** Servicio de Administración Tributaria. Organismo responsable de la recaudación de impuestos en México y entidad responsable de emitir la Firma Electrónica Avanzada.
- **Secure Shell.** Protocolo de comunicación considerado como un protocolo seguro de conexión que implementa cifrado en sus autenticaciones y transferencia de archivos.
- **Solaris.** Solaris es un sistema operativo desarrollado por Sun Microsystems que tiene la certificación como una versión de UNIX, dentro de sus características están que es multiusuario, multitarea y aunque Solaris en sí mismo aún es software propietario, la parte principal del sistema operativo se ha liberado como un proyecto de software libre denominado OpenSolaris.
- **Sybase Adaptive Server.** Es un sistema administrador de base de datos relacional (RDBMS, por sus siglas en inglés Relational Data Base Management System) desarrollado por la corporación Sybase.

- **Tablas ARP.** son tablas que almacenan direcciones IP y direcciones MAC asociándolas entre sí.
- **web services.** Es un conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones.

# ANEXO A: Ejemplo de controles de seguridad informática implementados en servidores Red Hat Enterprise Linux.

En el siguiente anexo se enlistarán algunos ejemplos de implementaciones que permitieron hacer un endurecimiento adecuado de la infraestructura.

## 1. Inhabilitación del usuario “root” para que pueda hacer login.

Para evitar que el usuario root haga login en un servidor con sistema operativo Red Hat Enterprise Linux se pueden implementar los siguientes controles.

### a) Inhabilitación por archivo de configuración sercuretty.

En el archivo /etc/securetty se deben comentar todos los tipos de accesos. El archivo debería verse de la siguiente manera:

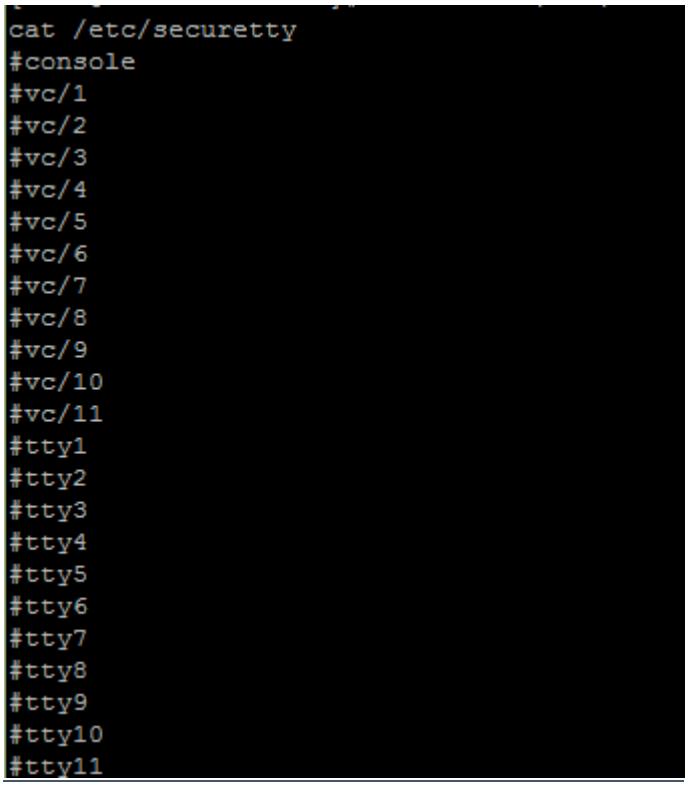



*Figura 13. Archivo de configuración /etc/securetty inhabilitando el acceso con root.*

### a) Inhabilitación por nologin en /etc/passwd.

En el archivo /etc/passwd se debe modificar para que root ejecute como “shell” el comando /sbin/nologin. El archivo debería verse de la siguiente manera:

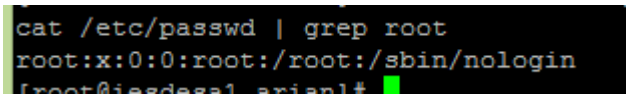



*Figura 14. Archivo de configuración /etc/passwd inhabilitando el acceso con root.*

## 2. Habilitación de usuarios para poder realizar tareas de administración en /etc/sudoers.

Para poder realizar las tareas de administración del servidor, es necesario que el usuario del administrador cuente con privilegios de administración. Para este proceso se propone utilizar la utilería sudo.

Para esto fue necesario hacer la configuración en el archivo /etc/sudoers donde definimos los comandos “Cmnd_Alias” que queremos ejecutar con privilegios de administrador, los usuarios “User_Alias” que tiene estos privilegios y forzamos “ALL= PASSWD: a que los usuarios tecleen el password cuando quieran ejecutar los comando definidos. Un ejemplo de archivo podría ser:

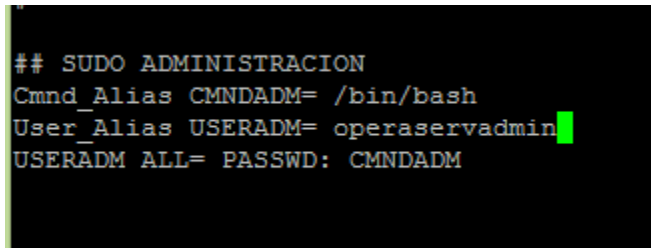



*Figura 15. Archivo de configuración /etc/sudoers dando permisos al usuario operaservadmin para ejecutar /bin/bash con privilegios de root.*

## 3. Inhabilitación de procesos, servicios y protocolos de comunicación no necesarios para la operación del servidor.

Cuando un servidor es instalado normalmente se instalan servicios y paquetes que no son necesarios para su operación.

Un ejemplo de un servidor instalado por default se podría ver así, con alrededor de 58 servicios configurados y 1088 paquetes instalados.

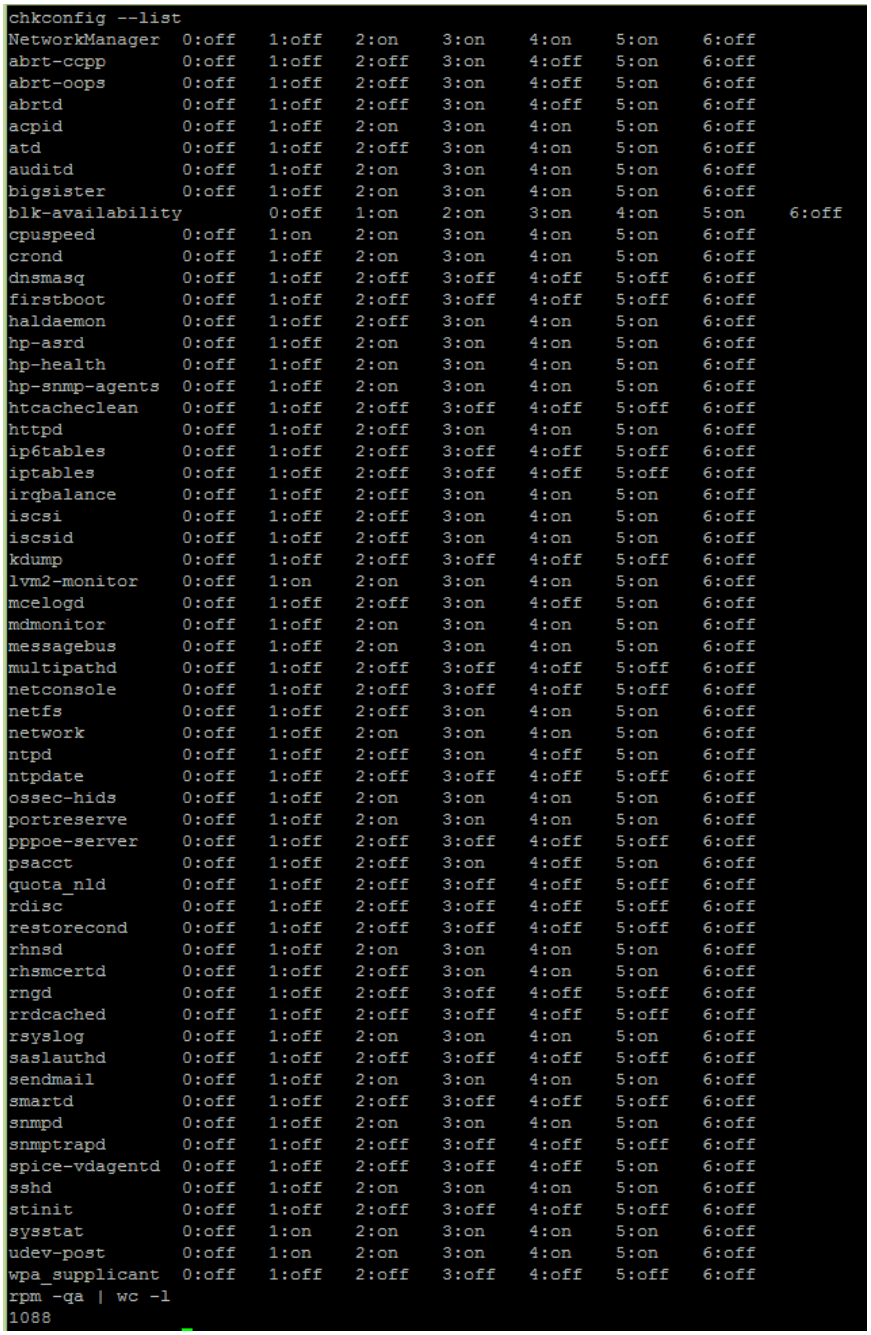



***Figura 16. Listado de servicios y total de paquetes instalados en un servidor con instalación por default.***

Después de hacer una revisión de servicios y de paquetes no necesarios para la operación del servidor podría verse así. Un total de 24 servicios configurados con 269 paquetes instalados.

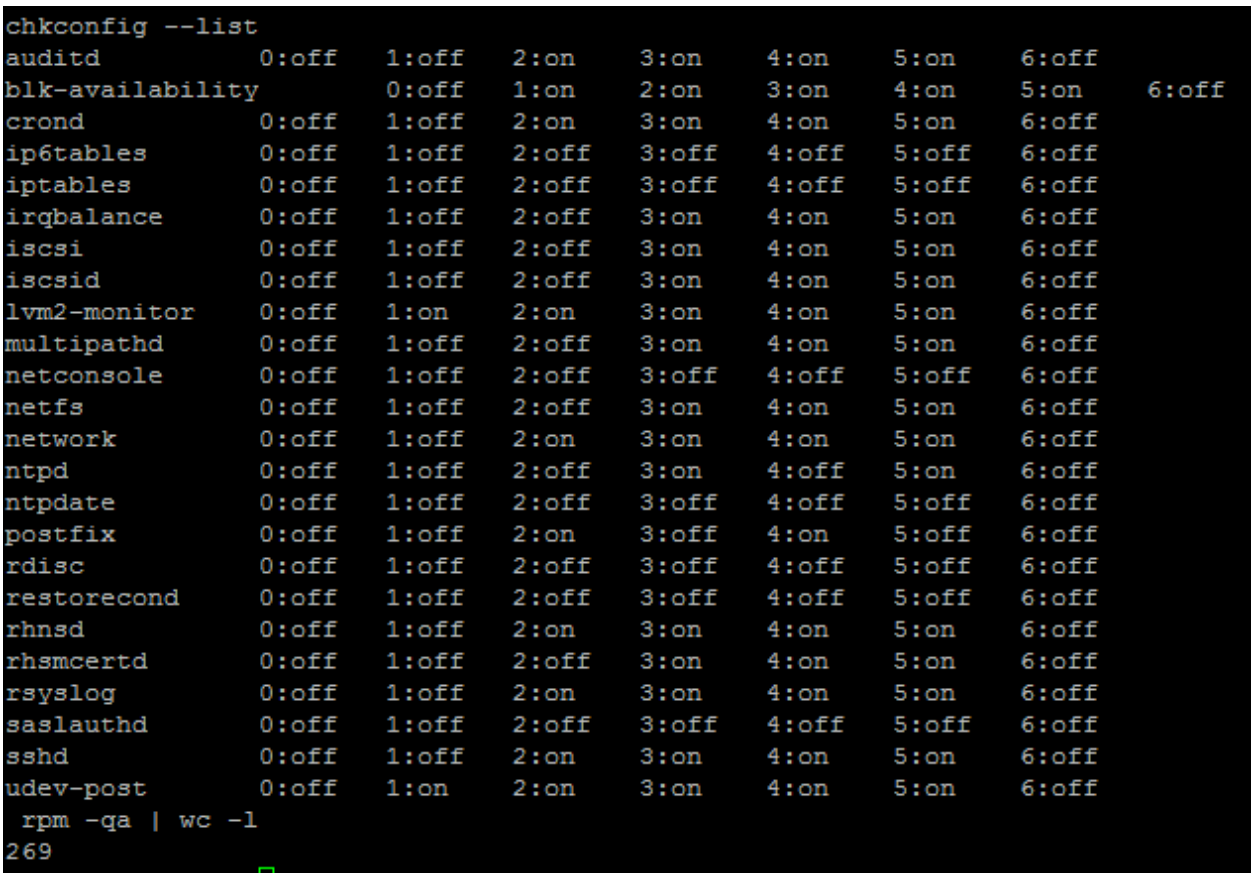



***Figura 17. Listado de servicios y total de paquetes instalados en un servidor con la revisión de procesos, servicios y protocolos de comunicación no necesarios para la operación del servidor.***

Para poder llegar al punto de reducir servicios y aplicaciones instaladas en el servidor, es recomendable seguir estos pasos.

- Hacer una instalación del sistema operativo Base
- Evaluar los servicios que se están ejecutando y en primera instancia desinstalar los servicios no necesarios y si por cuestiones de dependencias con otros paquetes no pueden ser desinstalados, proceder a desactivarlos.
- Desinstalación de paquetería no necesaria para la operación.

## 4. Gestión de contraseñas seguras.

Para tener una configuración de contraseñas robustas en el sistema operativo, puede realizarse por medio del módulo de "PAM" (plugable authentication module) que permite, entre otras configuraciones, configurar atributos de las contraseñas:

a) longitud de caracteres.
b) deberán estar compuesta por:
- caracteres especiales
- dígitos
- mayúsculas
- minúsculas

c) reutilización de contraseñas.
d) si la operación lo permite, deberán ser cambiadas periódicamente.
e) la cuenta debe ser bloqueada al tener intentos de acceso no exitosos.

Para los incisos a), b) es necesario utilizar módulo pam_cracklib.so

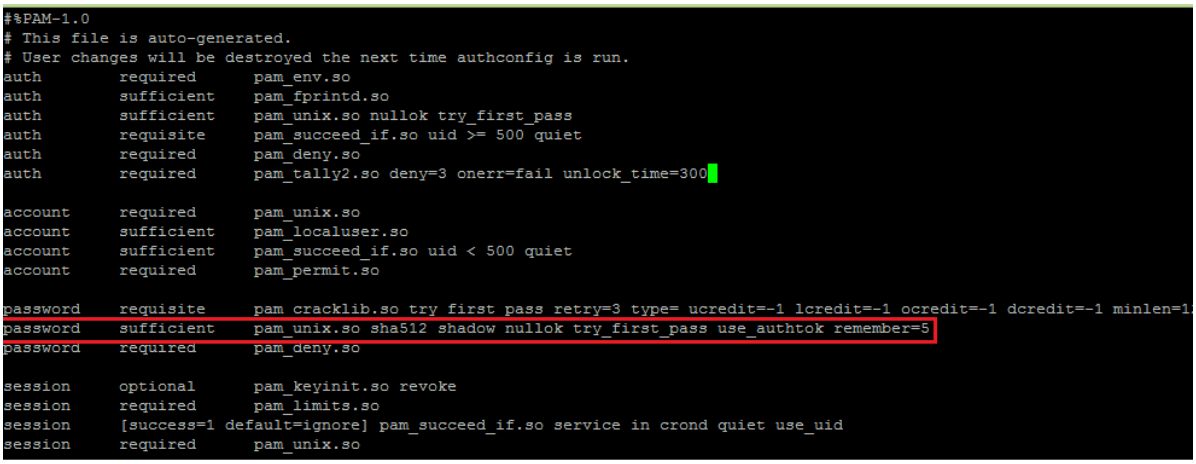
- minlen → longitud mínima
- ocredit → caracteres especiales
- dcredit → dígitos
- ucredit → mayúsculas
- lcredit → minúsculas

```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        sufficient    pam_fprintd.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 500 quiet
auth        required      pam_deny.so
auth        required      pam_tally2.so deny=3 onerr=fail unlock_time=300

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 500 quiet
account     required      pam_permit.so

password    requisite     pam_cracklib.so try_first_pass retry=3 type= ucredit=-1 lcredit=-1 ocredit=-1 dcredit=-1 minlen=1
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok remember=5
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
```

*Figura 18. Configuración del archivo /etc/pam.d/system-auth para la configuración de incisos a) y b)*

Para los incisos c) es necesario utilizar el módulo pam_unix.so

- remember → número de contraseñas que recordara el sistema operativo.

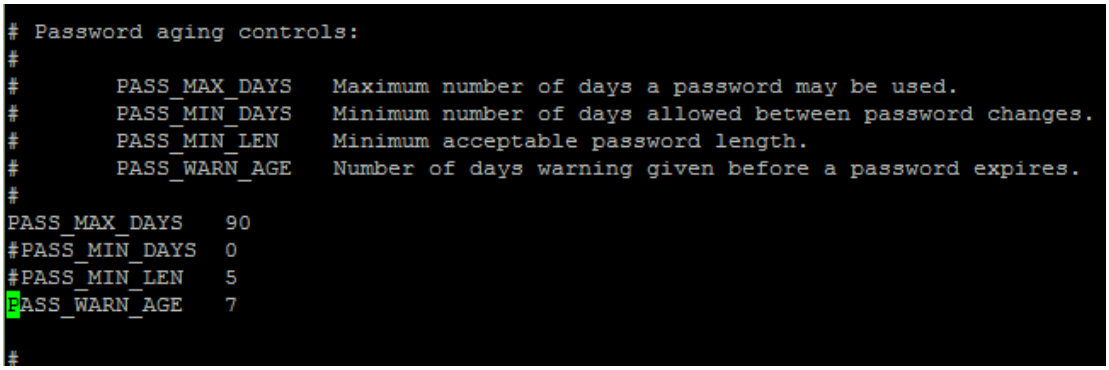


```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        sufficient    pam_fprintd.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 500 quiet
auth        required      pam_deny.so
auth        required      pam_tally2.so deny=3 onerr=fail unlock_time=300

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 500 quiet
account     required      pam_permit.so

password    requisite     pam_cracklib.so try_first_pass retry=3 type= ucredit=-1 lcredit=-1 ocredit=-1 dcredit=-1 minlen=1
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok remember=5
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
```

*Figura 19. Configuración del archivo /etc/pam.d/system-auth para la configuración del inciso c)*

Para el inciso d) es necesario configurar utilizar el archivo /etc/login.defs

- PASS_MAX_DAYS → número de días en que la contraseña deberá ser cambiada.



```
# Password aging controls:
#
#        PASS_MAX_DAYS   Maximum number of days a password may be used.
#        PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#        PASS_MIN_LEN    Minimum acceptable password length.
#        PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS   90
#PASS_MIN_DAYS  0
#PASS_MIN_LEN   5
PASS_WARN_AGE   7

#
```

*Figura 20. Configuración del archivo /etc/login.defs para la configuración del inciso d)*

Para el inciso e) es necesario configurar el módulo pam_tally2.so

- deny → número de intentos para bloquear la cuenta.
- unlock_time → tiempo de bloqueo de la cuenta por intentos fallidos.

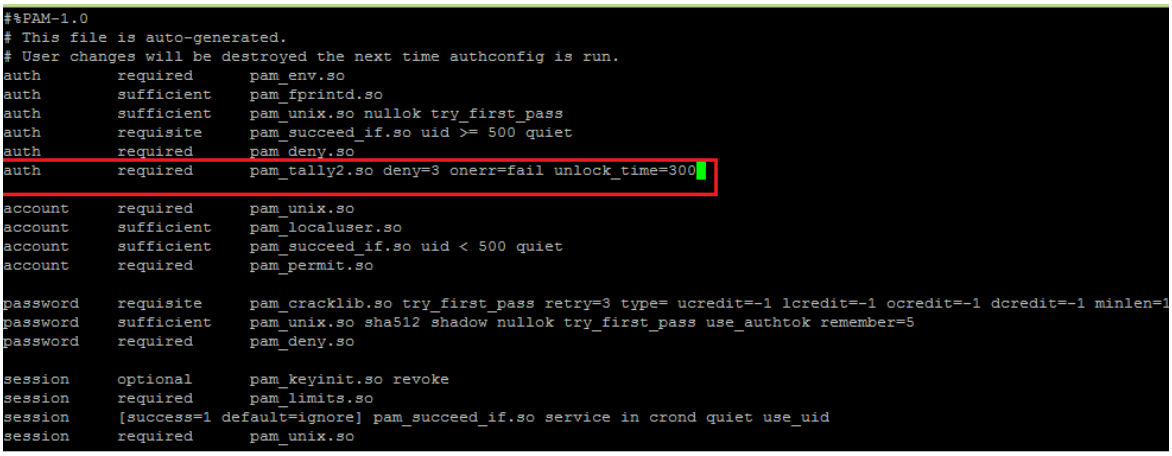



*Figura 21. Configuración del archivo /etc/pam.d/system-auth para la configuración del inciso e)*

## 5. Herramienta para la detección de intentos de intrusión, modificación de archivo (integridad) y monitoreo de bitácoras.

### a) Herramientas de monitoreo.

Para mantener la seguridad del servidor, fue necesario de auxiliarse de herramientas que permitan tener un monitoreo constante del servidor. Los elementos que se desean monitorear son los siguientes.

a) Escaneo de puertos.
b) Intento de intrusiones.
c) Integridad de archivos del sistema operativo.
d) Registro de actividades de los usuarios en la infraestructura de cómputo.

Para esta actividad se tienen herramientas comerciales que dan muy buenos resultados como:

- Tripwire. Herramienta especializada en el monitoreo de la integridad de archivos https://www.tripwire.com.

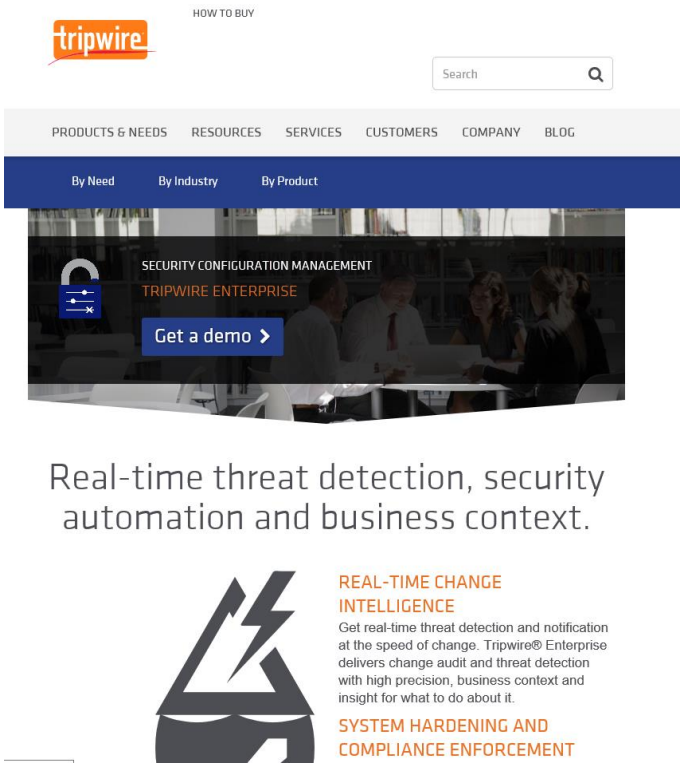



***Figura 22. Sitio de internet de Tripwire***

- Palo Alto. Herramienta especializada en monitoreo de red y detección de intrusos. https://www.paloaltonetworks.com/

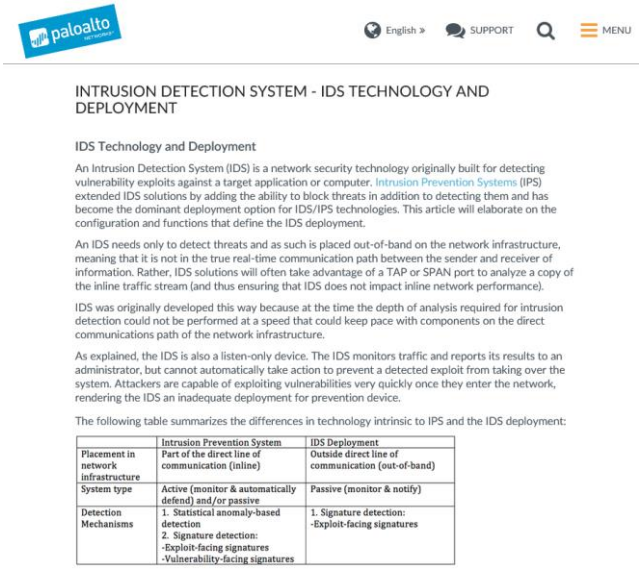



***Figura 23. Sitio de internet de paloalto***

Sin embargo, estas herramientas tienen un gran costo y en ocasiones solo son alcanzables por empresas con un gran presupuesto.

Aunque El Banco cuenta con herramientas empresariales de esta categoría, durante la implementación del proyecto se evaluaron herramientas de distribución gratuita que pudieran cubrir los requerimientos planteados.

La herramienta evaluada fue OSSEC (http://ossec.github.io/), que es una herramienta especializada en la detección de intrusos de host. En este caso el monitoreo de la red está a cargo de la unidad administrativa responsable de las telecomunicaciones de El Banco y por lo tanto no estuvieron en el alcance de las políticas.

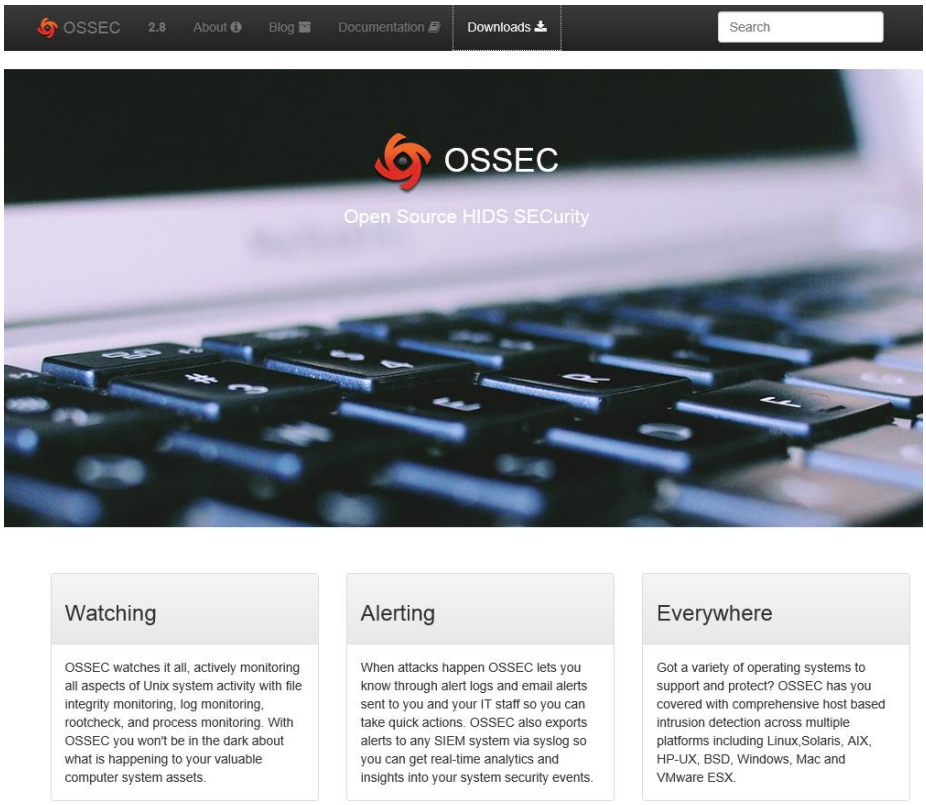



***Figura 24. Sitio de internet de OSSEC***

Esta herramienta permite el monitoreo de:

- logs.

- integridad de archivos.
- procesos en ejecución.
- rootkits.

Por lo que permite cubrir parte de los requerimientos planteados.

a) Escaneo de puertos.
b) Intento de intrusiones.
c) Integridad de archivos del sistema operativo.

Todas las actividades monitoreadas son reportadas a los administradores por medio de correos electrónicos, en los cuales viene el detalle de las alertas.

La herramienta debe de configurarse de acuerdo a las condiciones de la operación, porque de lo contrario generará muchas alarmas consideradas como falsos positivos.

Para cubrir el requerimiento d) relacionado con el "Registro de actividades de los usuarios en la infraestructura de cómputo" se puede realizar por medio de la utilería "psacct" de Red Hat Enterprise Linux que forma parte de la distribución de Red Hat, la cual permite, monitorear las actividades de los usuarios.

## b) Ejemplos de monitoreo con OSSEC.

- Notificación de escaneo del servidor.

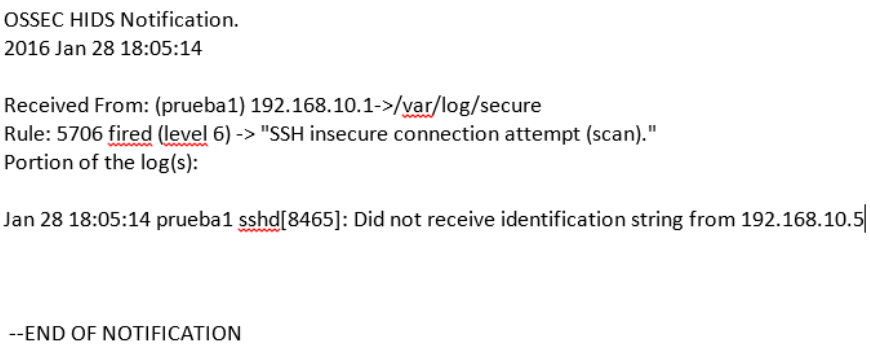



*Figura 25. Ejemplo de correo de escaneo de un servidor.*

- Notificación de intrusión desde el web a un directorio sin permisos.

OSSEC HIDS Notification.
2016 Jan 29 13:09:04

Received From: pruebas2->/etc/httpd/logs/error_log
Rule: 30105 fired (level 5) -> "Attempt to access forbidden file or directory."
Portion of the log(s):

[Fri Jan 29 13:09:04 2016] [error] [client 192.168.12.3] client denied by server configuration: /var/www/web/

--END OF NOTIFICATION

***Figura 26. Ejemplo de correo de cambio detectando la intrusión a un repositorio sin permisos en el servidor.***

- Notificación de integridad de archivos.

OSSEC HIDS Notification.
2016 Jan 29 14:35:39

Received From: (pruebas2) 192.168.10.3->syscheck
Rule: 550 fired (level 7) -> "Integrity checksum changed."
Portion of the log(s):

Integrity checksum changed for: '/usr/bin/x86_64-redhat-linux-c++'
Size changed from '267904' to '271368'
Old md5sum was: '8aa1f4a5a02adcc9d1b990606a423dc3'
New md5sum is : '3c74b435733b21d6f0ea873226b52c1d'
Old sha1sum was: 'eb8c83093084b6bdfd8ce92b96f705f7f1df5ac4'
New sha1sum is : '719af0e4e5e56fe1a697f50ffce718a058213d08'

--END OF NOTIFICATION

***Figura 27. Ejemplo de correo de cambio de un archivo en el servidor.***

## c) Ejemplos de monitoreo con OSSEC.

- Lista de comandos del usuario arian.

```
lastcomm arian
passwd           S     arian    pts/11     0.00 secs Tue May 31 23:36
ls                     arian    pts/11     0.00 secs Tue May 31 23:36
ls                     arian    pts/11     0.00 secs Tue May 31 23:36
ls                     arian    pts/11     0.00 secs Tue May 31 23:36
bash              F    arian    pts/12     0.00 secs Tue May 31 23:33
id                     arian    pts/12     0.00 secs Tue May 31 23:33
grep                   arian    pts/12     0.00 secs Tue May 31 23:33
bash              F    arian    pts/12     0.00 secs Tue May 31 23:33
bash              F    arian    pts/12     0.00 secs Tue May 31 23:33
uname                  arian    pts/12     0.00 secs Tue May 31 23:33
grep                   arian    pts/12     0.00 secs Tue May 31 23:33
grep                   arian    pts/12     0.00 secs Tue May 31 23:33
bash              F    arian    pts/12     0.00 secs Tue May 31 23:33
dircolors              arian    pts/12     0.00 secs Tue May 31 23:33
bash              F    arian    pts/12     0.00 secs Tue May 31 23:33
tput                   arian    pts/12     0.00 secs Tue May 31 23:33
tty                    arian    pts/12     0.00 secs Tue May 31 23:33
bash              F    arian    pts/12     0.00 secs Tue May 31 23:33
id                     arian    pts/12     0.00 secs Tue May 31 23:33
bash              F    arian    pts/12     0.00 secs Tue May 31 23:33
id                     arian    pts/12     0.00 secs Tue May 31 23:33
bash              F    arian    pts/12     0.00 secs Tue May 31 23:33
hostname               arian    pts/12     0.00 secs Tue May 31 23:33
bash              F    arian    pts/12     0.00 secs Tue May 31 23:33
id                     arian    pts/12     0.00 secs Tue May 31 23:33
bash              F    arian    pts/11     0.00 secs Tue May 31 21:16
id                     arian    pts/11     0.00 secs Tue May 31 21:16
grep                   arian    pts/11     0.00 secs Tue May 31 21:16
```

*Figura 28. Ejemplo de lista de comandos ejecutados por el usuario arian.*

- Lista de comandos de usuarios arian, root, moniserv, sshd

```
bash              F    arian    pts/1      0.00 secs Tue May 31 23:39
hostname               arian    pts/1      0.00 secs Tue May 31 23:39
bash              F    arian    pts/1      0.00 secs Tue May 31 23:39
id                     arian    pts/1      0.00 secs Tue May 31 23:39
sshd              SF   sshd     __         0.00 secs Tue May 31 23:39
splunk-optimize   S    root     __         0.00 secs Tue May 31 23:39
splunk-optimize   S    root     __         0.00 secs Tue May 31 23:39
splunk-optimize   S    root     __         0.00 secs Tue May 31 23:39
sendmail          SF   root     __         0.00 secs Tue May 31 23:39
procmail          S    root     __         0.00 secs Tue May 31 23:39
crond             SF   moniServ __         0.00 secs Tue May 31 23:39
sendmail          SF   root     __         0.02 secs Tue May 31 23:39
sendmail               moniServ __         0.01 secs Tue May 31 23:39
logrotate              moniServ __         0.00 secs Tue May 31 23:39
```

*Figura 29. Ejemplo de lista de comandos ejecutados por el usuario arian, root, sshd, moniServ.*

# ANEXO B: Ejemplo de herramientas de detección de vulnerabilidades en la infraestructura de cómputo.

En el siguiente anexo se enlistarán algunos ejemplos de una la herramienta "Nessus" y "Rapid7 Nexpose" para la validación del fortalecimiento de la infraestructura de cómputo.

## a) Herramientas para pruebas de penetración.

Para validar el fortalecimiento de los servidores con infraestructura Red Hat Enterprise Linux, fue necesario de auxiliarse de herramientas que permitan realizar pruebas de penetración a la infraestructura de cómputo y pueda detectar vulnerabilidades como:

a) falta de actualizaciones.
b) omisiones en la configuración.
c) archivos que pudieran representar un riesgo.

Es muy importante que estas actividades se realicen por medio de un tercero que no esté involucrado directamente en la administración de la infraestructura, pero es necesario que el administrador de la infraestructura revise los resultados para descartar cualquier falso positivo o detallar los controles compensatorios implementados.

Para esta actividad se propone el uso de las siguientes herramientas:

- Nessus. Herramienta especializada en descubrimiento de vulnerabilidades la cual, en su versión comercial, pueden cargarse módulos que verifican puntos ya pre-establecidos en guías de fortalecimiento para el sistema operativo Red Hat Enterprise Linux. http://www.tenable.com/products/nessus-vulnerability-scanner

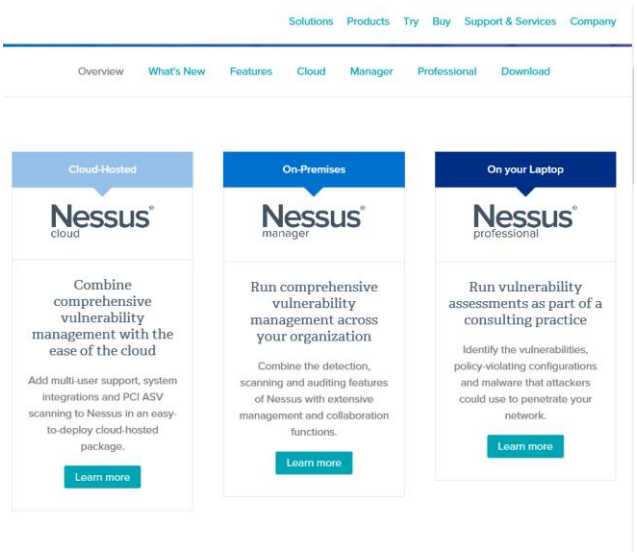



***Figura 30. Sitio de internet de Nessus.***

- Rapid7 Nexpose. Herramienta especializada en pruebas de penetración la cual tiene la característica de que evaluar los riesgos de la infraestructura tecnológica (software, cómputo, telecomunicaciones) y permite la administración del ciclo de vida de las vulnerabilidades, incluyendo el descubrimiento, detección, verificación, clasificación de riesgos, análisis de impactos y mitigación. https://www.rapid7.com/

*Figura 31. Sitio de internet de Rapid7 Nexpose.*

## b) Ejemplos de evaluación de vulnerabilidades con Nessus.

La herramienta te permite agrupar los servidores para obtener un reporte gráfico de cuál es el estatus de los servidores.

Como se comentó la herramienta, al menos para la versión gratuita, está especializada en la detección de vulnerabilidades por falta de actualizaciones y/o parches.

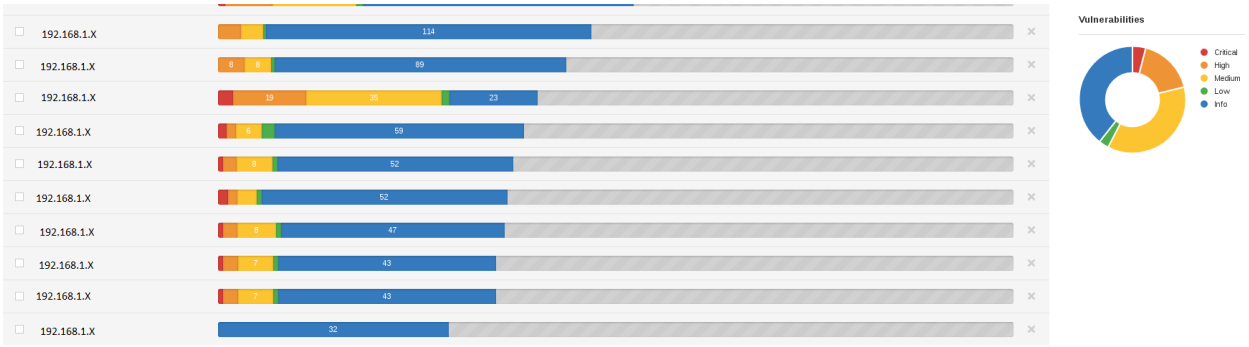



*Figura 32. Ejemplo de reporte de vulnerabilidades detectas con Nessus a un grupo de servidores.*

Los colores indican el nivel de criticidad de la vulnerabilidad.

- Rojo: Crítica
- Naranja: Alta
- Amarilla: Media
- Verde: Baja
- Azul: Informativo

Es necesario que los resultados sean analizados y validados. Se deben descartar falsos positivos y ajustar la criticidad de las vulnerabilidades considerando las condiciones de operación y funcionamiento del servidor.

La herramienta da detalle sobre las vulnerabilidades detectadas indicando la clave de la vulnerabilidad, una descripción detallada de la vulnerabilidad y una propuesta para mitigar la vulnerabilidad.

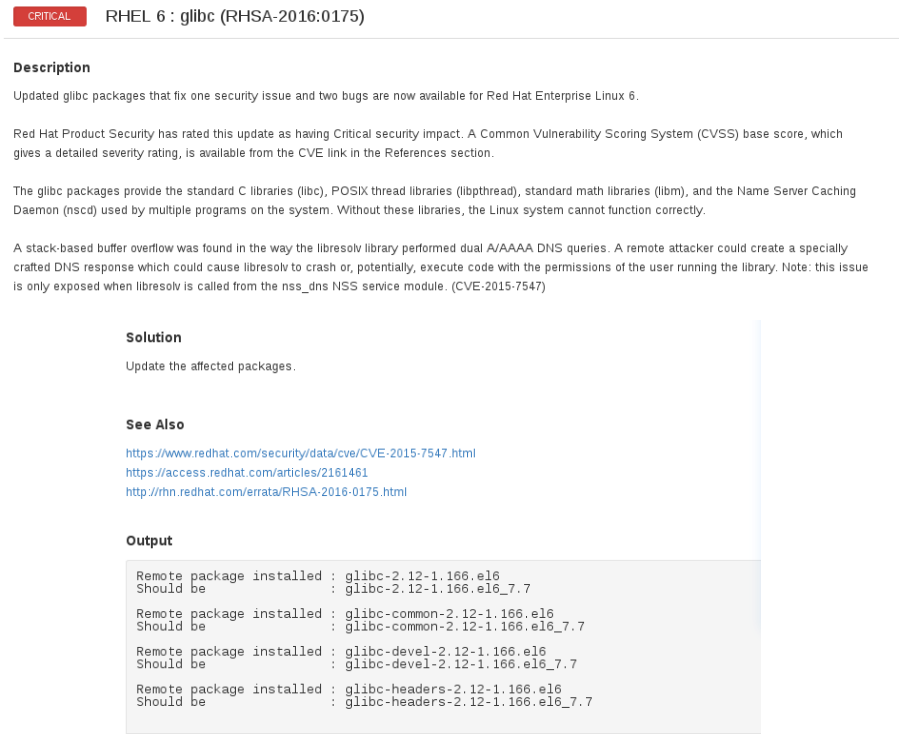



***Figura 33. Ejemplo de vulnerabilidad detectas con Nessus en las librerías de glibc y la solución propuesta.***

Cómo se puede ver, esta herramienta puede auxiliarnos en la detección y atención de vulnerabilidades, sobretodo en vulnerabilidades derivadas de la falta de actualización de parches.

### c) Ejemplos de evaluación de vulnerabilidades con Rapid7 Nexpose.

La herramienta, aún en su versión gratuita, es una excelente opción para la detección y seguimiento de vulnerabilidades.

La herramienta permite agrupar los servidores que son analizados para generar reportes con los resultados de los escaneos.

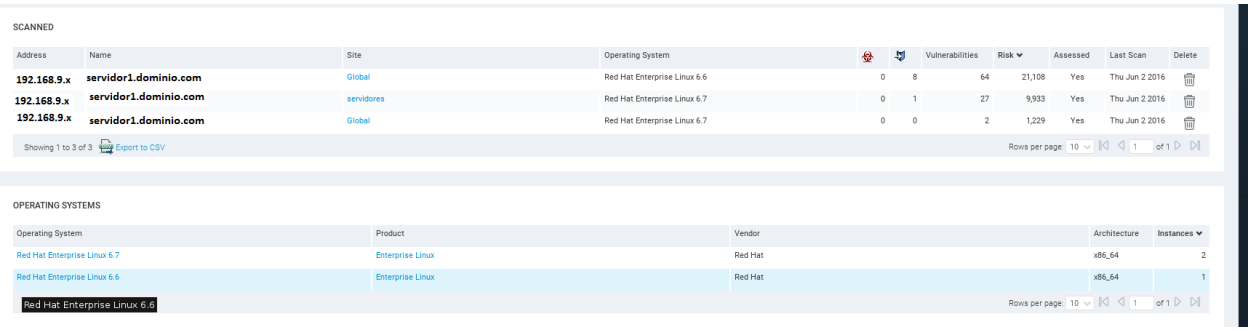



***Figura 34. Ejemplo de reporte de vulnerabilidades detectadas con Nexpose***

Una ventaja de esta herramienta, en su versión gratuita, es que verifica configuraciones del sistema operativo e identifica aquellas que representan un riesgo de seguridad informática.

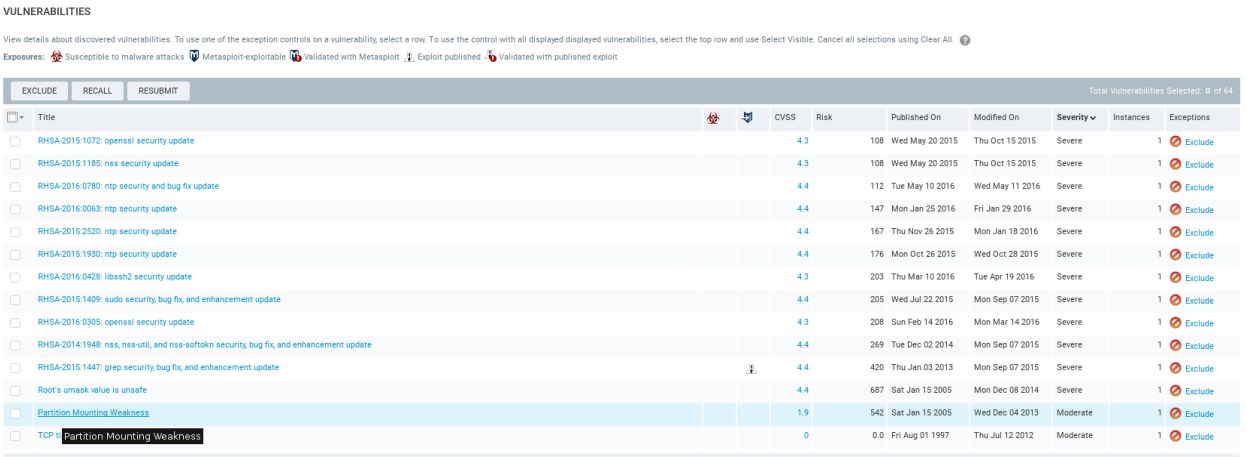



***Figura 35. Ejemplo de diferentes (falta de parches y configuraciones) vulnerabilidades encontradas por Nexpose.***

Esta herramienta puede ser integrada con la herramienta Metasploit, con la cual se podrían explotar las vulnerabilidades para tener un mejor entendimiento de los riesgos que representan.

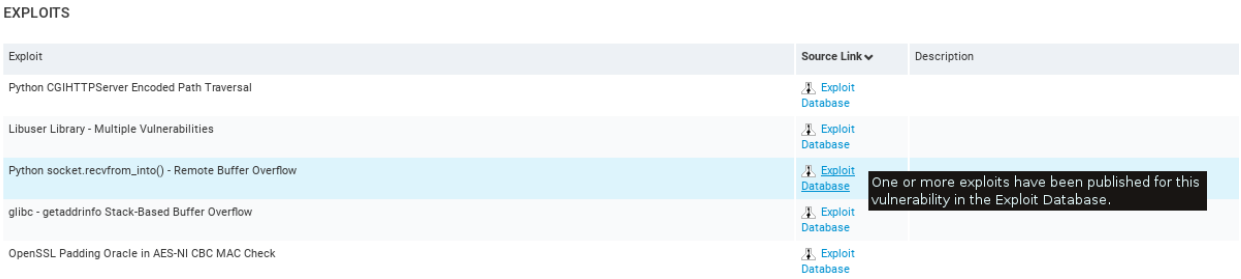
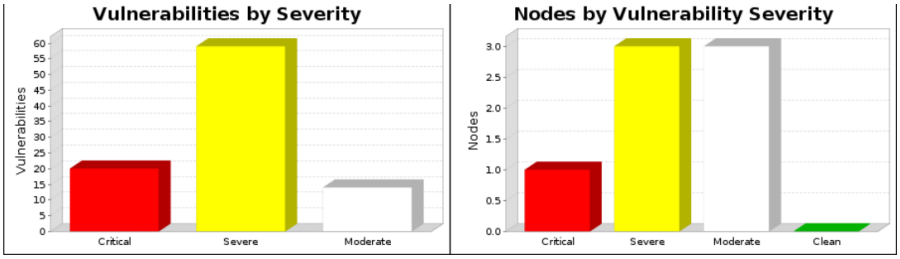
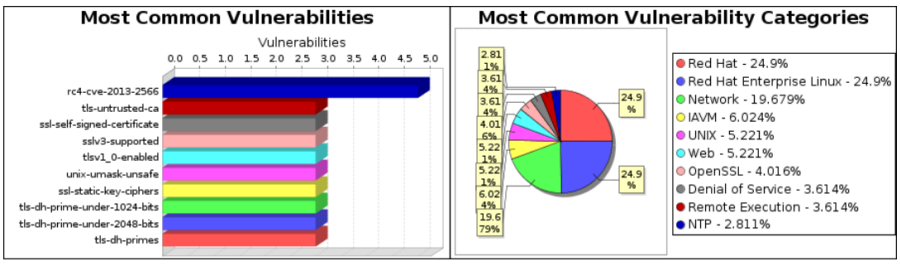



***Figura 36. Ejemplo de vulnerabilidades detectadas con Nexpose que puede ser explotada por Metasploit.***

Por último, la herramienta tiene un módulo de administración de vulnerabilidades que permite de una manera fácil y eficiente darle seguimiento a las vulnerabilidades desde su detección hasta que son atendidas. Algo interesante de este módulo es que permite medir y graficar el riesgo con el que cuenta la infraestructura. La herramienta tiene la capacidad de generar reportes ejecutivos

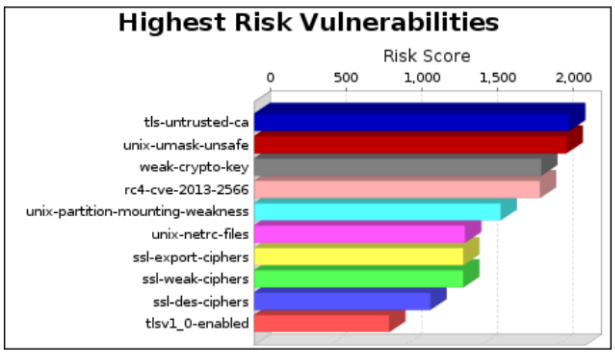



There were 93 vulnerabilities found during this scan. Of these, 20 were critical vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 59 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 14 moderate vulnerabilities discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities. Critical vulnerabilities were found to exist on 1 of the systems, making them most susceptible to attack. 3 systems were found to have severe vulnerabilities. Moderate vulnerabilities were found on 3 systems. No systems were free of vulnerabilities.




There were 5 occurrences of the rc4-cve-2013-2566 vulnerability, making it the most common vulnerability. There were 62 vulnerability

***Figura 37. Ejemplo de reporte ejecutivo de vulnerabilidades detectadas por Nexpose.***




The tls-untrusted-ca vulnerability poses the highest risk to the organization with a risk score of 2,077. Risk scores are based on the types and numbers of vulnerabilities on affected assets.
One operating system was identified during this scan.
There were 5 services found to be running during this scan.

***Figura 38. Ejemplo de reporte ejecutivo de los riesgos conforme a las vulnerabilidades detectadas por Nexpose.***