INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA

INFORME DE ACTIVIDADES PROFESIONALES "SEGURIDAD EN TÉCNOLOGIAS DE LA INFORMACIÓN"

T É S I S

Q U E P A R A O B T E N E R E L T Í T U L O D E:
INGENIERO EN COMUNICACIONES Y ELECTRONICA

P R E S E N T A N

JOSÉ ANTONIO GUTIÉRREZ MORELOS.

ASESORES:
ING. ARMANDO MANCILLA LEÓN.
.

MÉXICO, D.F. 2013

INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELECTRICA

UNIDAD PROFESIONAL "ADOLFO LÓPEZ MATEOS"

REPORTE TÉCNICO

QUE PARA OBTENER EL TITULO DE: INGENIERIA EN COMUNICACIONES Y ELECTRÒNICA
POR LA OPCIÒN DE TITULACION: MEMORIA DE EXPERIENCIA PROFESIONAL
DEBERA (N) DESARROLLAR JOSE ANTONIO GUTIERREZ MORELOS

TEMA: SEGURIDAD EN TECNOLOGÌAS DE LA INFORMACIÒN

OBJETIVO DEL TEMA: DESARROLLO DE MEJORAS A LA INFRAESTRUCTURA DE SEGURIDAD DE TECNOLOGIAS DE LA INFORMACIÒN

PUNTOS A DESARROLLAR:

- SEGREGACIÒN DE FUNCIONES (ACCESS MANAGEMENT) PARA SISTEMA DE FACTURACIÒN.
- MIGRACIÒN DE ANTIVIRUS
- VAULT PASSWORD PARA USUARIOS PRIVILEGIADOS
- HARDENING EN MAIL FILTER TOOL (ANT SPAM) MEXICO

MÉXICO D.F., A 14 DE AGOSTO FRL 2013

A S E S O R E S

ING. ARMANDO MANCILLA LEÒN

ING. PATRICIA LORENA RAMIREZ RANGEL
JEFE DEL DEPARTAMENTO ACADÉMICO DE
INGENIERÍA EN COMUNICACIONES Y ELECTRÓNICA

INDICE

Página

OBJETIVOS GENERALES

El objetivo general de este informe de actividades profesionales es describir mi participación en el análisis y desarrollo de soluciones aplicando el conocimiento base adquirido en la escuela superior, es mostrar como de manera práctica y en el ambiente real se presentan problemas y se desarrolla un proyecto técnico y administrativo para dar una solución al mismo. Cómo el conocimiento académico se permea al uso de mejores prácticas en Tecnologías de la Información en la época del auge de la comunicación electrónica y los riesgos que implica, el desarrollo de soluciones en una de las ramas más atractivas y prácticamente novedosa como es el área de la Seguridad en Tecnologías de la Información que trabaja en reducir riesgo de pérdida de información, suplantación de identidad o daño dirigido.

Las bases académicas aumentan las posibilidades de resolver efectivamente cualquier problema en el ambiente laboral o dar una o más soluciones “ha doc”, según las necesidades del ambiente.

INTRODUCCION

Este informe muestra las actividades realizadas en el área de Entrega de Servicios Administrados en Tecnología e Información en el departamento de Seguridad Informática en la empresa Hewlett Packard, donde laboro desde Julio 2010 como Líder del área *Threat and Vulnerability Management* para Latinoamérica en la cuenta global de Nextel NII Holdings.

El informe se desarrolla de forma cronológica y muestra los problemas presentados en relación a Seguridad de la Información, muestra las actividades claves y cuidando la integridad y confidencialidad de las empresas el desarrollo y estrategia de solución, los logros obtenidos con los proyectos realizados, así como una visión futura como plan de mejora continúa.

En la cuenta global Nextel NII Holdings se realizaron los siguientes proyectos: Segregación de Funciones (Access Management) para sistema de Facturación, Migración de Antivirus, Vault Password para usuarios privilegiados, Hardening en Mail Filter Tool (Anti Spam) Mexico.

Todos los proyectos realizados se llevaron a cabo bajo las mejores prácticas de Tecnologías de la Información y para establecerse como modelo de servicio basado en metodología ITIL (Information Technology Infrastructure Library).

Los proyectos fueron diseñados e implementados por el equipo de trabajo asignado al mismo y liderados por un servidor.

TRAYECTORIA PROFESIONAL

Desde mi egreso en 2005 del Instituto Politécnico Nacional de la Escuela Superior de Ingeniería en Comunicaciones y Electrónica con Ingeniería en Comunicaciones y Electrónica con especialidad en Computación, mi trayectoria profesional siempre se ha estado orientada a la Seguridad de la Información, describo brevemente mi trayectoria a continuación:

√ En 2005 ingrese a laborar como Ingeniero de Soporte Nivel 2 en Grupo Scitum, empresa muy prestigiosa en Mexico en el área de la Seguridad de la Información como tester de herramientas de Seguridad, Firewall de segunda generación como Proventias, Antivirus Web Content Filter, Mail Filter, fue ahí donde descubrí que me apasionaba el área de Seguridad de la Información y comencé a reforzar los conocimientos adquiridos en la escuela superior con cursos y certificaciones como CCNA, Comptia, Unix, Oracle.

√ Ingrese 1 año después, en 2006 a la Telecom Iusacell de Mexico con el Puesto de Ingeniero en Seguridad de la Información para realizar hardening de Seguridad en sistemas de prevención de fraudes de llamadas en líneas celulares y SMS (Short Message Service), donde tuve que hacer ingeniería reversa y reingeniería para localizar todos los puntos vulnerables del sistema de prevención de fraudes, de esta forma aprendí mucho sobre el flujo de las llamadas CDR (Call Detail Record) y SMS, por ello el gerente de Aseguramiento de Ingresos me dio la oportunidad de realizar análisis de Fraudes en llamadas, SMS y MMS (Multimedia Messaging System) donde tuvimos grandes hallazgos de fraudes y remediación de los mismos, poco después me dieron el puesto de Experto en Análisis y Prevención de Fraudes.

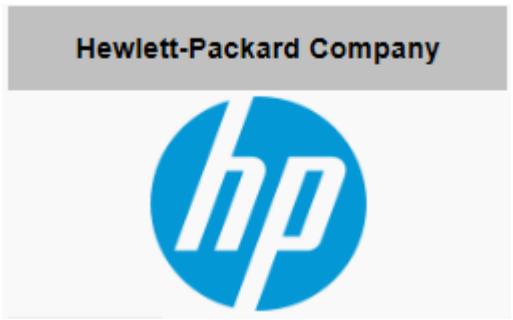
√ En 2008 Ingrese en la Telecom Nextel de Mexico como Coordinador de Seguridad de la Información, para llevar toda la operación de las consolas de Seguridad que Nextel había adquirido, propias (home made) y de herramientas formales de proveedores externos, aquí desarrolle capacidad de trabajo en equipo, niveles de servicio y desarrollo de micro proyectos para puesta en producción de mejoras a la operación y planes de mejora continua.

√ En 2010 por estrategia de Nextel Internacional NII Holdings, se realiza el Outsourcing de los Servicios de Tecnologías de la Información donde la empresa ganadora fue Hewlett Packard donde ingreso a laborar bajo un esquema global y participo en una selección interna para asignación de responsabilidades y me otorgan el puesto de Líder de la Torre de Servicio de Threat and Vulnerability Management para Latinoamérica siendo encargado de las operaciones de Seguridad Informática de USA, Mexico, Perú, Argentina, Chile y Brasil, teniendo la oportunidad de desarrollar proyecto clave para la mejora de operaciones en Seguridad Informática y reduciendo significativamente con ello los riesgos de seguridad que se tenían además del cerrar Issues de Auditoria, ya que al ser una empresa que cotiza en la bolsa de valores de USA se rige bajo auditoria Sarbanes-Oxley.

√ En 2013 me integro a apoyar dentro de Hewlett Packard a la cuenta Global Grupo Bimbo en el proyecto Go for Green de Endpoint Security, que significa realizar el análisis y recomendaciones para corrección del servicio de Antivirus.

EMPRESA DONDE SE DESARROLLO LAS ACTIVIDADES PROFESIONALES

Las actividades presentadas en este informe se realizaron en la empresa Hewlett-Packard, es una de las empresas de tecnologías de la información con mayor prestigio en el mundo, esta empresa es estadounidense con sede en Palo Alto, California, pero tiene presencia en los 5 continentes. El rol de la empresa es fabricar y comercializa hardware y software además de brindar servicios de asistencia relacionados con la informática. La compañía fue fundada en 1939 por William Hewlett y David Packard, y se dedicaba a la fabricación de instrumentos de medida electrónica y de laboratorio. Actualmente es la empresa líder en venta de computadoras personales e impresoras en el mundo, y recientemente está impulsando la entrega de servicios de administración de tecnología (Outsourcing).



http://www.hp.com/

DESARROLLO DE PROYECTOS

CAPÍTULO 1. Segregación de Funciones (Access Management) para sistema de Facturación.

1.1 Objetivo

El objetivo de este proyecto es remediar los problemas de seguridad respecto al área de Access Management del sistema de Facturación proponiendo un método efectivo para remediar los niveles de acceso como RBAC (Role Base Access Control) que contempla la segregación de funciones de todos los usuarios para acceso a la aplicación, el alcance es para usuarios finales como usuarios de aplicación y supervisar el hardening de Seguridad del Sistema Operativo, Base de Datos y Aplicación para cerrar los hallazgos de auditoria Sabanes-Oxley.

1.2 Responsabilidades y Organización del Proyecto

Para este proyecto nos correspondían las siguientes responsabilidades:

- √ Análisis y diseño de propuestas técnicas para solucionar la problemática presentada.
- √ Implementación.
- √ Validación de la implementación de correcciones por parte del proveedor del sistema de facturación en cuanto a seguridad de tecnologías de la información se refiere.
- √ Obtener evidencia fidedigna para cierre de hallazgos de auditoria.

El grupo de trabajo se conformaba por siguientes integrantes:

- **Analista de Base de Datos.** Responsable de análisis y manejo de los datos de todas las fuentes involucradas en el proyecto.

- **Analista de SO Unix.** Responsable de desarrollar scripts para manejo de información, validación de configuración de Sistema Operativo, análisis y desarrollo de procesos de manejo de información.

- **Analista de Seguridad de TI.** Responsable de validar los Base Line de Seguridad TI con apoyo de los analistas de SO y DB, orientando el análisis a el cumplimiento de seguridad TI.

- **Especialista en Seguridad TI y Líder Técnico (mi rol).** Responsable de toma de decisiones, análisis especializado y manejo de acuerdos con el proveedor del sistema de facturación para una implementación con todas las características de seguridad requeridas, manejo de cierre de hallazgos de auditoria y entregables a cliente final.

El desarrollo del proyecto se realizó en las siguientes etapas.

- Análisis del problema. En ésta etapa se identificaron los problemas y las necesidades de cliente, así como las dependencias para solucionarlos, se identificaron las responsabilidades de cada elemento u organización participante en el proyecto para determinar el alcance.

- Propuestas de solución. Se entregó una propuesta técnica de solución, las implicaciones, necesidades, y facilidades necesarias para el éxito del proyecto, en la propuesta se integraban tiempos de implementación, accesos, recursos humanos, prerrequisitos, así como la solución técnica a la problemática.

- Desarrollo de solución. En esta etapa se desarrolló/puesta en marcha de la solución propuesta, la información detallada está en el Capítulo 4 de este reporte.

- Evaluación de resultados y replanteamiento de estrategia y/o alcance. En esta etapa se identificaron problemas que no eran problema, problemas que no eran alcanzables para solucionar con las condiciones del ambiente y se tenía que realizar o implementar herramientas adicionales y hacer nueva inversión o vivir con el riesgo.

- Validación de resultado final. Realizar pruebas exhaustivas para comprobar qué la solución funcionaba y sin errores o bugs de sistemas, además de preparar la implementación a ambiente productivo minimizando las implicaciones operativas.

- Implementación en ambiente productivo. Puesta en producción con ventana de mantenimiento controlada y minimizando las implicaciones operativas.

- Etapa de estabilización. Etapa de utilización de usuarios finales y análisis de fallas o errores para corrección inmediata, monitoreo del correcto funcionamiento en cuanto a Seguridad de Tecnologías de la Información compete.

- Recolección de evidencia y cierre de hallazgos de auditoria. En esta etapa ya con el sistema de facturación estable se obtenía evidencia "dura" y se documentaba correctamente los hallazgos de auditoria para el cierre de los mismos.

1.3 Problema

A nivel global Nextel Internacional NII Holdings planeo la migración (subir) de versión del Sistema de Facturación con varios objetivos. Uno de los principales era estar preparado para facturación de servicios de datos (3G), otro de los principales era mejorar el control en sus procesos como facturación, crédito y cobranza, ventas, promociones, previniendo o corrigiendo fraudes, control de movimientos, manejo contable, etc. ya que con la versión que se tenía se tenían problemas de fraudes ya que se hacían promociones u ofertas no autorizadas y no se tenía registro del ejecutor, pérdida de ingresos por no facturación y no tener el registro del responsable, préstamo de usuarios para aplicación de pagos, promociones o condonaciones no autorizadas, usuarios genéricos para manejo de operaciones, las aplicaciones satelitales (aplicación para manejo de cartera vencida, DWH, etc.) tenían usuarios con altos privilegios y hacían escritura directa en la Base de Datos sin registro alguno y los usuarios y contraseñas eran conocidos por todos los integrantes de los grupos de soporte de sistemas, los usuarios tenían solo 3 niveles de acceso rompiendo el control de acceso "mínimos privilegios", estos problemas además de pérdidas monetarias eran hallazgos de auditoria externa Sarbanes-Oxley, dando mala calificación a una empresa ya que cotiza en la bolsa de valores de USA.

Dividiremos los problemas presentados en cuatro grandes rubros que son: la administración de usuarios, los roles asignados a los usuarios, la utilización de usuarios de aplicación (usuarios de altos privilegios) y las políticas de contraseñas (strong password); todos en

conjunto eran los grandes problemas de seguridad y los hallazgos detectados por auditoria externa (Sarbanes-Oxley). Las desviaciones presentadas eran las siguientes:

Administración de usuarios.

- No se contaba con nomenclatura de User ID.
- Existían usuarios con nombres genéricos que eran utilizados por varias personas.
- No se tenían identificados los usuarios utilizados para aplicaciones legadas al sistema de facturación que explotaban información de éste.

Roles asignados.

- No existían roles definidos.
- La asignación de permisos a un usuario era bajo demanda y solo con la autorización del jefe directo del solicitante se asignaban.
- Existían usuario con puesto menor y con grandes privilegios en la aplicación para hacer movimientos, (empleados de confianza).
- Existían usuarios con privilegios para gestionar cuentas por cobrar y cuentas por pagar.
- Existían usuarios con roles de cobranza asignados a usuarios de ventas.
- Existían usuario sin límite de crédito para abonos y/o condonaciones de deudas.

Usuarios de aplicación.

- No se tenían completamente identificados ni documentados los usuarios que utilizaban las aplicaciones legadas.
- Si algún administrador cambiaba la contraseña del usuario podía ser que otra aplicación se viera afectada.
- Si algún usuario era bloqueado por intentos de acceso fallido, varias aplicaciones eran afectadas.
- Los usuarios/contraseñas eran conocidos por todos los integrantes de soporte dando lugar a fraudes y pérdida de información.
- El proceso de cambio de contraseña era un proceso muy riesgoso por que no se tenía documentado cuantas aplicaciones y procesos estaban ligados a él.

Políticas de contraseña.

- Los usuarios no cumplían con políticas de contraseñas recomendadas:
  - Mínimo 8 caracteres.
  - Por lo menos una minúscula.
  - Por lo menos una letra mayúscula.
  - Mínimo un carácter especial.
  - Caducidad de contraseña a los 30 días.
  - Falta de logs para hacer el tracking de los movimientos.

Derivado de estas desviaciones de seguridad existían varios problemas como caídas de sistema por bloqueo o cambio de contraseña, lenta remediación ya que no se contaba con documentación, no se contaba con logs para realizar el análisis post mortem o análisis para identificar el origen de las solicitudes erróneas.

Las contraseñas eran altamente vulnerables al no existir políticas de contraseñas duras, existía conflicto de intereses al existir usuario con roles de autorizados y solicitante, no se tenía control en la asignación de permisos lo que derivaba en riesgo alto de cometer fraude o errores de operación por asignar permisos de altos privilegios a personas no calificadas, era muy difícil identificar la identidad de un usuario ya que los usuarios no tenían una nomenclatura definida.

A continuación se muestra una matriz de permisos asignados.

Tabla1. Tabla de roles asignados.

PRIVILEGIOS DE ACCESO								
NIVEL DE ACCESO	MODULO	LECTURA	ACTUALIZAR	BORRAR	INFORMES	MOSTRAR GASTOS/PRECIOS	ABONO	CARGO
1	DB	X	x	X	X	X		
	KV	X			X	X	NA	NA
2	DB,KV	X			X		NA	NA
3	DB,KV	X	x	X	X	X	0	0
	DB,KV	X	x	X	X	X	0	1600
	DB,KV	X	x	X	X	X	100000	100000
	DB,KV	X	x	X	X	X	10000	10000
	DB,KV	X	x	X	X	x	1500	1500
	DB,KV	X	x	X	X	x	1600	1600
	DB,KV	X	x	X	X	x	50000	50000
	DB,KV	X	x	X	X	x	500	500
4	DB	X	x	X	X	x		
	KV	X	x		X	x	200000	200000
5	DB	X			X	x		
	KV	X	x	X	X	x	0	0
6	DB	X			x	x		
	KV	X	x	X	x	x	1600	1600
7	DB	X			x	x	NA	NA
	KV	X			x	x	NA	NA
8	KV	X			x		NA	NA
9	KV	X	x	X	x	x	0	0
10	KV	X	x	X	x	x	1600	1600
11	KV	X	x	X	x	x	200000	200000
12	KV	X	x	X	x	x	50000	50000
13	KV	X	x	X	x	x	500	500

La *Tabla 1 de roles asignados* muestra lo genérico de los perfiles, el ~50 % de los perfiles tienen el mismo nivel de acceso, la única diferencia es el monto autorizado de abono y cargo.

No existen perfiles dedicados a aplicaciones satelitales ni segregación de funciones a los diferentes puestos operativos de las diferentes áreas de negocio.

1.4 Solución

Los problemas expuestos en el capítulo anterior se resolvieron con segregación de funciones de acceso al sistema de facturación, identificando las áreas operativas, dentro de las áreas operativas los roles por área (Perfiles) y el nivel de acceso que debían tener en los sistemas de facturación, estos niveles de acceso deberían estar autorizados a alto nivel de la empresa Dirección y Subdirección de cada área operativa para dar certidumbre de los que los niveles segregados corresponden a las políticas e intereses de la compañía.

La metodología utilizada para fue el modelo RBAC de sus siglas en Ingles *Role Base Access Control*.

RBAC es una familia de modelos de referencia en los permisos que están asociados con roles y los usuarios se asignan a roles apropiados, esto simplifica enormemente la gestión de permisos, los roles se crean para diversos trabajos o funciones en una organización y los usuarios se asignan a los roles en función de sus responsabilidades y calificaciones, los usuarios fácilmente pueden ser reasignados de una función a otra simplemente cambiando el rol de acceso, los roles pueden conceder nuevos permisos en la misma aplicación o nuevas aplicaciones y pueden ser revocados si es necesario.

Las restricciones son un aspecto importante en RBAC, que puede aplicarse a los componentes antes expuestos (usuarios, roles, permisos, sesiones), un ejemplo común es que un gerente de compras y el gerente de cuentas por pagar sea la misma persona, en esta metodología no se permite tener ambos funciones, ya que esto crea una posibilidad de cometer fraude. En resumen existen tres reglas básicas para la restricción:

A) Asignación. El sujeto puede ejecutar una función solo si el sujeto has sido elegido o seleccionado para esa función. El proceso de identificación y autenticación (por ejemplo inicio de sesión) no se considera una transacción. Todas las demás actividades que el usuario realiza en el sistema o aplicación sí son consideradas transacciones, por lo tanto todos los usuarios requieren algún rol activo.

B) Autorización. Los sujetos con rol activo debieron ser autorizados para tenerlo, esto asegura que el sujeto solo tiene el rol que debe tener activo y que fue autorizado.

C) Transacción. El sujeto puede ejecutar la transacción sólo si el sujeto es autorizado a través del proceso o autorizadores definidos, esto garantiza que el sujeto puede ejecutar solo las transacciones para las que fue autorizada.

Un propósito importante de RBAC es facilitar la administración del control de acceso y su revisión, de esta forma se simplifica el proceso de autorización y proporciona gran flexibilidad en hacer cumplir las políticas de seguridad específicas de la empresa y del mismo modo agiliza el proceso de gestión de la seguridad.

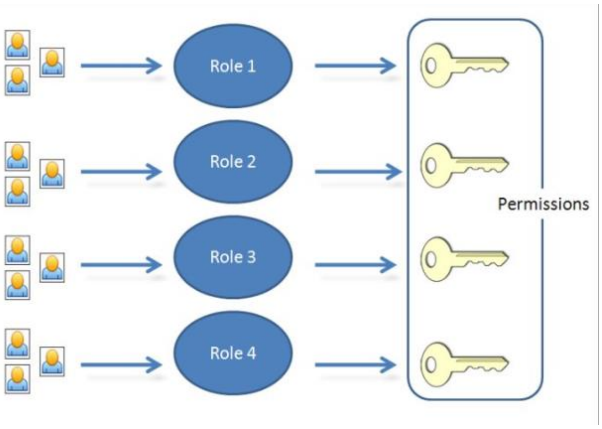


Fig1. Diagrama metodología RBAC.

Los pasos generales a seguir para desarrollar la metodología RBAC son los siguientes:

1. Identificar los procesos de negocio.
2. Determinar los requerimientos de control de acceso para cada operación.
3. Mapear los requerimientos y necesidades de acceso con los puestos operativos de los usuarios.
4. Formular reglas de decisión basado en las restricciones (block as default).
5. Definir los mecanismos de aseguramiento del control de acceso.

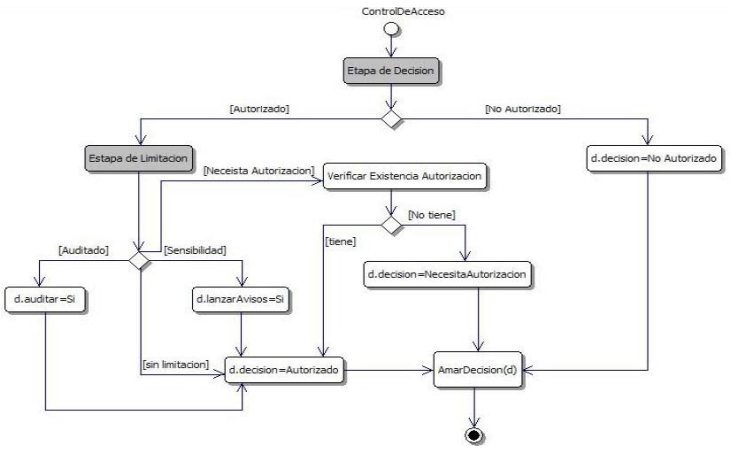


Fig2. Ejemplo de reglas de decisión.

El desarrollo de la solución se divide en los cuatro mismos rubros de problemas:

1) Administración de usuarios.
2) Roles asignados.
3) Usuarios de aplicación.
4) Políticas de contraseña.

Vamos a desarrollar cada tema, no necesariamente en orden cronológico y algunas dependen de otras como Roles asignados y Administración de usuarios.

Administración de usuarios.

La primera etapa para corregir los problemas de administración de usuarios fue realizar el análisis de los usuarios activos en el sistema, clasificarlos por área de negocio y confirmar con cada área de negocio la identidad de cada usuario y si debería seguir estando activo. Detallando las actividades sobre esta primera etapa, se sacó un extracto de usuarios existentes del sistema de facturación y se cruzó con diferentes fuentes de información para

identificar el área de negocio al que pertenecía como el Directorio Activo, aplicación de Recursos Humanos y fuentes de información de empresas terceras subcontratadas para call-center.

En la segunda etapa ya con la información clasificada, se convocó a reuniones con los líderes de las áreas de negocio, se solicitó un representante para el proyecto de Segregación de Funciones quien a su vez consultaría dentro de su área competente, se envió la información clasificada por área de negocio para que cada dueño de área de negocio identificara el personal perteneciente a cada área e identificara el rol operativo dentro del área de negocio, esta primer actividad nos dio un ~80% de efectividad, se describen los porcentajes y los escenarios encontrados en la siguiente *Tabla 2.*

Tabla2. Tabla de efectividad 1ra etapa

Efectividad		
	Activos	Para deshabilitar
Identificados	79.5%	0.50%
No identificados	20%	0.00%

Teníamos que trabajar en deshabilitar el ~0.5% porque eran usuarios que reconocieron las áreas de negocio que no laboraban más en la empresa o se habían cambiado de puesto y no necesitaban más el acceso, y en buscar el 20% restante que no habían sido identificados.

La segunda actividad fue enviar a todas las áreas de negocio el ~20% de usuarios sin identificar para que cada una hiciera el análisis dentro de cada área de negocio.

Se pudo identificar ~10% más, que eran usuarios que se habían cambiado de área de negocio, de este ~10% el ~8% eran usuarios activos y el ~2% eran usuarios que deberían ser deshabilitados del sistema de facturación, por los motivos antes mencionados.

Del ~10'% restante por identificar se validó con el área de IT e identificaron ~3%, el ~7% restante que no se localizó se programaron RFC (Request for Change) para deshabilitarlos de manera controlada y con un periodo de monitoreo de no tuviera impacto.

Una vez identificados los usuarios User ID con la persona física y área de negocio a quien pertenecía así como todos los datos de organigrama (puesto operativo y reporte directo) se procedió al cambio de User ID (identificador de usuario) conservando la misma contraseña, el User ID se otorgó con la nomenclatura siguiente:

Prefijo: NMI (Nextel Mexico Interno) o NME (Nextel Mexico Externo)
Dígitos: 6 dígitos que eran el número de empleado en caso de interno y número consecutivo en case de externo.

USERID: NMI000001 | NME000001

Se publicó el procedimiento para crear usuarios en el sistema de facturación y a partir de la fecha de publicación se tomaba la nomenclatura propuesta.

Roles asignados.

El siguiente paso era verificar el Rol Operativo de cada usuario la tarea más ardua en este proceso, primero se realizó el match de puesto de RH vs el puesto operativo para el Sistema de Facturación de ahí se obtuvo la base para construir los perfiles existían y que deberían existir, combinando la realidad operativa versus el puesto de Recursos Humanos.

El proceso a seguir fue el siguiente:

Se establecieron los Roles por cada área de negocio, diseñado a bajo nivel por gente experta en operaciones y con las funciones que en esa actualidad se desempeñaban. Cada área de negocio con el representante como líder entrego a Seguridad IT las funciones que desempeñaban cada sub área, entrego los procedimientos operativos actualizados.

El área de Seguridad TI moderó y moduló patrones de funciones basados en actividades de negocio directamente aplicados en el sistema de facturación haciendo referencia con los puestos operativos existentes, metodología RBAC. A continuación se presenta un ejemplo.

Tabla3. Tabla de Puestos Operativos vs Actividades realizadas.

Nombre del Perfil	Descripción del Perfil	Área	Proceso	Nivel de Acceso	Permisos	Montos
Analista Aplicación de Pagos	Responsable de la aplicación de los diferentes medios de pago, realizar reversos y reclasificaciones de pagos	Crédito y Cobranza	P5 – Aplicaciones de Cobranzas P6 – Manejo de Incidentes P7 – Reversos P8 – Cheques devueltos	Lectura y escritura	Aplicación de Pagos Reclasificaciones Reversos	OCC y ajustes – 0

Analista Aplicación de Pagos	Responsable de la aplicación de los diferentes medios de pago, realizar reversos y reclasificaciones de pagos	Crédito y Cobranza	P5 – Aplicaciones de Cobranzas P6 – Manejo de Incidentes P7 – Reversos P8 – Cheques devueltos	Lectura	Validación de datos	N/A
Analista Aplicación de Pagos	Responsable de la aplicación de los diferentes medios de pago, realizar reversos y reclasificaciones de pagos	Crédito y Cobranza	P5 – Aplicaciones de Cobranzas P6 – Manejo de Incidentes P7 – Reversos P8 – Cheques devueltos	Escritura	Aplicación de OCCs y ajustes	OCC y ajustes – 0
Supervisor Aplicación de Pagos	Responsable de la aplicación de los diferentes medios de pago, realizar reversos y reclasificaciones de pagos	Crédito y Cobranza	P5 – Aplicaciones de Cobranzas P6 – Manejo de Incidentes P7 – Reversos P8 – Cheques devueltos	Lectura y escritura	Aplicación de Pagos Reclasificaciones Reversos	OCC y ajustes <=10,000
Supervisor Aplicación de Pagos	Responsable de la aplicación de los diferentes medios de pago, realizar reversos y reclasificaciones de pagos	Crédito y Cobranza	P5 – Aplicaciones de Cobranzas P6 – Manejo de Incidentes P7 – Reversos P8 – Cheques devueltos	Lectura	Validación de datos	N/A
Supervisor Aplicación de Pagos	Responsable de la aplicación de los diferentes medios de pago, realizar reversos y reclasificaciones de pagos	Crédito y Cobranza	P5 – Aplicaciones de Cobranzas P6 – Manejo de Incidentes P7 – Reversos P8 – Cheques devueltos	Escritura	Aplicación de OCCs y ajustes	OCC y ajustes <=10,000

Coordinador Aplicación de Pagos	Responsable de la aplicación de los diferentes medios de pago, realizar reversos y reclasificaciones de pagos	Crédito y Cobranza	P5 – Aplicaciones de Cobranzas P6 – Manejo de Incidentes P7 – Reversos P8 – Cheques devueltos	Lectura y escritura	Aplicación de Pagos Reclasificaciones Reversos	OCC y ajustes <=50,000
Coordinador Aplicación de Pagos	Responsable de la aplicación de los diferentes medios de pago, realizar reversos y reclasificaciones de pagos	Crédito y Cobranza	P5 – Aplicaciones de Cobranzas P6 – Manejo de Incidentes P7 – Reversos P8 – Cheques devueltos	Lectura	Validación de datos	OCC y ajustes <=50,000
Coordinador Aplicación de Pagos	Responsable de la aplicación de los diferentes medios de pago, realizar reversos y reclasificaciones de pagos	Crédito y Cobranza	P5 – Aplicaciones de Cobranzas P6 – Manejo de Incidentes P7 – Reversos P8 – Cheques devueltos	Escritura	Aplicación de OCCs y ajustes	OCC y ajustes <=50,000
Gerente Aplicación de Pagos	Responsable de la aplicación de los diferentes medios de pago, realizar reversos y reclasificaciones de pagos	Crédito y Cobranza	P5 – Aplicaciones de Cobranzas P6 – Manejo de Incidentes P7 – Reversos P8 – Cheques devueltos	Lectura y escritura	Aplicación de Pagos Reclasificaciones Reversos	OCC y ajustes <=200,000
Gerente Aplicación de Pagos	Responsable de la aplicación de los diferentes medios de pago, realizar reversos y reclasificaciones de pagos	Crédito y Cobranza	P5 – Aplicaciones de Cobranzas P6 – Manejo de Incidentes P7 – Reversos P8 – Cheques devueltos	Lectura	Validación de datos	N/A

Gerente Aplicación de Pagos	Responsable de la aplicación de los diferentes medios de pago, realizar reversos y reclasificaciones de pagos	Crédito y Cobranza	P5 – Aplicaciones de Cobranzas P6 – Manejo de Incidentes P7 – Reversos P8 – Cheques devueltos	Escritura	Aplicación de OCCs y ajustes	OCC y ajustes <=200,000

Seguridad TI realizó la matriz de correspondencia de Puesto Operativo vs Actividades realizadas basado estadísticamente en mayorías de coincidencias, es decir si él Gerente de Aplicación de Pagos realizaba A, B y C y uno realizaba A, B, C y D, el rol para Gerente de Aplicación de Pagos es sobre las actividades A.B y C, la actividad D debería ser asignada a otro rol o bien el rol de Gerente de Aplicación de Pagos debería tener las actividades de A, B, C y D.

Seguridad TI fue responsable de entregar la matriz modulada y los responsables de cada área de negocio debería validarlo y definir roles únicos, una vez establecidos los roles únicos se entregó a la dirección de cada área de negocio para su aprobación.

Con la aprobación de la dirección de cada área de negocio se designaron grupos de trabajo para validar cada perfil en un ambiente de pruebas UAT (Quality Assurance Test).

El procedimiento de creación de cada perfil se realizó mediante el método de burbuja ya que como eran perfiles a-doc., se tenía que configurar y validar permiso por permiso manualmente, los módulos de acceso en general eran los siguientes:

Tabla4. Tabla de Módulos de acceso Sistema de Facturación

MODULOS ONLINE		
ER.EXE	Local EIR Administration	ER
MI.EXE	Motivation & Incentives	MI
PA.EXE	Profile Administration	PA
RA.EXE	Resource Administration	RA
SY.EXE	System Administration	SY
TA.EXE	Taxation Administration	TA
TR.EXE	Translation Administration	TR
DB.EXE	Accounts Receivable	AR
ES.EXE	External Interfaces	EI
HB.EXE	General Ledger	GL
MP.EXE	Product Center	PX
RM.EXE	Report Manager	RM
SP.EXE	Reference Data	RD
MODULOS WEB		
CUSTOMER CENTER		CX
Provisioning GUI Extension		PGX
Partner CX		Partner CX

Pero los permisos se deberían otorgar de forma mucho más granular como se muestra en la *Tabla3. Tabla de Puestos Operativos vs Actividades realizadas,* para lo que se debió realizar el análisis de Access Right que otorgaban los permisos específicos de cada módulo a cada rol creado, por ejemplo para el rol Analista Aplicación de Pagos requería acceso de Lectura y Escritura a las actividades: Aplicación de Pagos Reclasificaciones y Reversos estas actividades se realizaban en el módulo WEB Customer Center (CX), pero también muchas más actividades, por lo que se debió identificar específicamente cada Access Right para otorgarlo y no más permisos porque era un riesgo; el mismo que queríamos mitigar y no menos permisos porque el rol no sería funcional.

Ejemplo de creación de rol.

En la tabla de la Base de Datos relacional llamada **useraccess**, se insertan los Access Right y el nivel de acceso de cada permiso, es decir de lectura o de escritura, la estructura de la tabla era la siguiente:

Useraccess
Username, modulename, uaperm, entdate, moddate, modified, rec_version, expiration_date
Donde los campos:
Username = ID del Rol
Modulename = Access Rigth, permiso en el modulo
Uaperm = Nivel d acceso, lectura o escritura
Entdate = fecha de asignación
Moddate = Campo Nulo
Modified= Campo Nulo
rec_version = Asignación 0
expiration_date = Campo Nulo

Pero la estructura de Access Right específicamente el campo **modulename** tiene una estructura de herencia, es decir un Access Right puede tener asociados varios Access Right que al asignarlo se asignan en automático los asociados, por ejemplo el Access Rigth = CMSFR tiene implícitos los Access Rigth CMSFRS y CMSFPCR lo que implica que si solo queremos asignar CMSFR deberíamos poner en el campo de Uaperm = 0 en los Access Rigth CMSFRS y CMSFPCR para que no tuvieran efecto, se muestra la asignación:

Username	modulename	uaperm	entdate	moddate	modified	rec_version	expiration_date
PRADMVTA	CMSFR	2147483647	SYSDATE	NULL	NULL	0	NULL
PRADMVTA	CMSFPCR	0	SYSDATE	NULL	NULL	0	NULL
PRADMVTA	CMSFRS	0	SYSDATE	NULL	NULL	0	NULL

Tabla5. Tabla muestra de asignación de permisos (Access Rigth)

La asignación de los Access Rigth correctos es con el método de ordenamiento de burbuja hasta localizar los permisos que deben asignarse de forma correcta.

De esta forma se construyó la matriz final de roles versus puesto operativo.

a) Usuarios de aplicación.

El tema de usuarios de aplicación se realizó desde cero ya que existían usuarios compartidos y con privilegios altos que eran del conocimiento de los grupos de soporte, por lo que se decidió por la opción de crear usuarios por aplicación y con el nivel de accesos adecuado.

En el sistema de facturación existe un módulo de conexión API donde se puede ejecutar comandos vía comando ya que el sistema de facturación radica en un sistema operativo HP-UX, el proceso de asignación de permisos se llevó a cabo en 3 etapas, la primera etapa fue la solicitud por escrito de cada administrados de sistema legado de los permisos requeridos,

la segunda etapa fue de validación con expertos de operación de áreas de negocio para confirmar que los permisos solicitados sean los necesarios para que la aplicación legada funcionara y la tercera y última etapa fue la de autorización de las direcciones de las áreas de negocio y de IT.

Cuando los usuarios solicitados y los permisos autorizados estuvieron listos, se realizó un UAT para garantizar el correcto funcionamiento de la aplicación legada corriendo una serie de pruebas que englobara todas las funciones que debería hacer la aplicación legada.

Como proceso de control de Seguridad TI una vez confirmada la finalización de las pruebas se revisaron los logs y se descartó que todos y cada uno de los permisos asignados fueran utilizados durante las pruebas, si existían permisos no utilizados, éstos eran eliminados del usuario para administración de la aplicación legada.

Las contraseñas de los usuarios de aplicación se ingresaron a esquema de sobre de emergencia partiéndola en dos partes, la primera de ellas la ingresaba el administrador de la aplicación y la segunda parte fue ingresada por el administrador del sistema operativo, minimizando de esta forma que las contraseñas sean comprometidas.

Por otro lado se validó en el código Hardcode de la API que la contraseña ingresada estuviera encriptado para que no fuera expuesta.

b) Políticas de contraseña.

Las políticas de contraseña fueron implementadas en el sistema y validadas por el equipo de Seguridad TI, las políticas revisadas fueron:

1. **Mínima longitud:**

   Una contraseña debe de contener como mínimo 8 caracteres.

2. **Bloqueo por inactividad.**

   Una cuenta debe de bloquearse después de 30 días inactividad del usuario.

3. **Baja por inactividad.**

   Una cuenta debe ser dada de baja después de 60 días de inactividad del usuario.

4. **Periodo de vida**

   Una contraseña debe de ser cambiada al cumplirse 30 días de su última asignación.

5. **Intentos fallidos**

   Las cuentas deben de ser bloqueadas si escribe en 3 ocasiones la contraseña de manera equivocada.

6. **Historial de contraseña**

   Una contraseña no puede ser repetida en un periodo menor a 360 días.

7. **Restricción de login**

   Una contraseña no puede ser igual al login.

8. **Repetición de carácter.**

   No se bebe de contener caracteres repetidos.

9. **Mínimo número de caracteres numéricos.**

   Una contraseña debe tener por lo menos un número.

10. **Número mínimo de letras.**

    Una contraseña debe de contener por lo menos una letra en su conformación. La aplicación cumple con este requerimiento al no permitir asignar una contraseña sin números.

11. **Encripción**

    La contraseña deberá estar encriptado.

12. First Time Use (FTU)

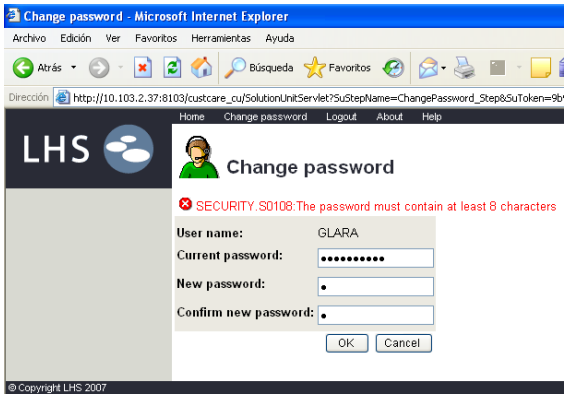
Cuando un usuario acceda al sistema después de haber sido creado o cada vez que un administrador restablezca su contraseña, se deberá solicitar el cambio de contraseña

13. Timeouts.

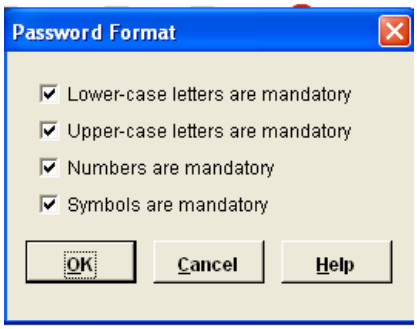
Después de un periodo de inactividad de 30 min

Algunos resultados de las pruebas se mencionan a continuación:

Mínima longitud:



Número mínimo de letras.



Este rubro quedo cubierto y validado, cerrando el *Issue* de auditoría.

1.5 Conclusiones

El objetivo fue cumplido según el alcance original y el proceso administrativo validado mostrando la efectividad para la forma de trabajar culturalmente hablando del cliente final, y las configuraciones y procedimientos técnicos se desarrollaron según el acuerdo administrativo.

El siguiente paso para mejorar el proceso de segregación de funciones del sistema de facturación y la operación de Access Management en general es implementar una herramienta de Identity Managaget (IDM) ligado al sistema de Recursos Humanos para que sea completamente automática el alta y baja de usuarios y la asignación de sus accesos basado en su rol, puesto o perfil.

CAPÍTULO 2. Migración de Antivirus

2.1 Objetivo

El cliente solicitó realizar el reemplazo de la herramienta de Antivirus ya que presentaba varios problemas técnicos y administrativos, el objetivo fue diseñar la nueva arquitectura y realizar el reemplazo con la menor afectación posible a los usuarios finales, no afectación a la operación.

2.2 Responsabilidades y Organización del Proyecto

Para este proyecto nos correspondían las siguientes responsabilidades:

- √ Análisis y diseño de nueva arquitectura de Antivirus, así como diseño de la estrategia de migración.
- √ Implementación.
- √ Validación de la implementación, garantizar que el 100% de los equipos (Servidores y computadoras) fueron migradas.
- √ Apagar la vieja infraestructura de Antivirus.

El grupo de trabajo se conformaba por siguientes integrantes:

- **Analista de Red.** Responsable de análisis de ancho de banda, monitoreo de red durante la migración e implementación controles de calidad de servicio (asignación de ancho de banda por prioridades).

- **Responsables de Aplicaciones montadas en Servidores con Windows.** Los responsables de cada aplicación debería validar durante el cambió de Antivirus y

posterior al mismo el correcto funcionamiento, así como monitorear que no hubiera afectación posterior con la aplicación.

- **Administrador de Sistema Operativo Windows Server.** Responsable de validar el correcto funcionamiento del sistema operativo durante la migración y posterior a la misma y monitorear que no hubiera afectación pro el cambio de antivirus.

- **2 Analistas de Seguridad de TI.** Responsables de realizar la migración de Antivirus y administración de las consolas.

- **Especialista en Seguridad TI y Líder Técnico (mi rol).** Responsable de diseño de arquitectura y diseño de estrategia de migración, toma de decisiones, análisis especializado y manejo de acuerdos con el cliente y para guiar el desarrollo del proyecto buscando minimizar los riesgos y no afectar la operación diaria.

El desarrollo del proyecto se realizó en las siguientes etapas.

- Análisis del problema. En particular ésta etapa ya no se debía realizar nada, porque la decisión estaba tomada, quitar el Antivirus viejo y poner el nuevo software.

- Propuestas de solución. Se entregó una propuesta técnica de solución, las implicaciones, necesidades, riesgos, prerrequisitos, y el diseño de la arquitectura nueva.

- Desarrollo de solución. En esta etapa se desarrolló la solución propuesta, la información detallada está en el Capítulo 4 de este reporte.

- Evaluación de resultados y replanteamiento de estrategia y/o alcance. En esta etapa se identificaron problemas que no eran problema, problemas potenciales y toma de decisión de no llevar a cabo, por ejemplo el encendido del IPS local ya que no había un estudio de comportamiento de tráfico de red de las aplicaciones y problemas que se resolvieron reconsiderando la estrategia de distribución por conocimiento adquirido.

- Validación de resultado final. En esta etapa se realizó un cotejo de varias fuentes (antivirus viejo, nuevo antivirus, inventario de equipos, inventario de Servidores, Directorio Activo) para garantizar que todos los dispositivos fueron migrados.

- Etapa de estabilización. En esta etapa se presentaron usuarios finales con dudas, computadoras con virus que el viejo antivirus no detectaba, servidores que debieron ser modificados en sus políticas de escaneo porque afectaba el performance.

- Etapa de apagado de vieja infraestructura de Antivirus. En esta etapa con la garantía de que el 100% de equipos y servidores habían sido migrados a la nueva herramienta, se apaga y se entrega al cliente la infraestructura y se liberan licencias de la vieja herramienta de Antivirus.

2.3 Problema

En Nextel Mexico existía un Antivirus con mala reputación ya que es una herramienta con pobre nivel de administración, por ello se presentaban continuamente problemas de virus ya que el motor de análisis del antivirus solo permitía neutralizar o vacunar un virus a la vez, siendo que si se ingresaba una memoria USB infectada con más de 1 virus en algún equipo, el Antivirus eliminaba el primer virus localizado mientras el segundo o los que estuvieran

alojados en la memoria contaminaban la computadora e inclusive la red si la computadora tenia recursos compartidos con permisos de lectura/escritura a todo el dominio y se convertía en una problema grabé de infección, en muchas ocasiones existían infecciones masivas en las áreas de call center, en algún momento el cliente solicito enviar un Full Scan para eliminar el malware en los equipos de la red y se convirtió en un problema porque al activarse el Full Scan las computadoras que analizaban recursos compartidos como File Shares, adjuntado como Map Network Drive colapso los File Share ya que todos los equipos escaneaban simultáneamente el mismo recurso compartido, la herramienta tampoco tenía como detener en automático el Full Scan y si se reiniciaban los equipos solo iniciaba de nuevo el Scan, se tuvo que hacer un workaround para detener el Full Scan en los equipos con los Share configurados.

A continuación se muestra el Cuadrante mágico de Gartner para herramientas de Endpoint Security como referencia.

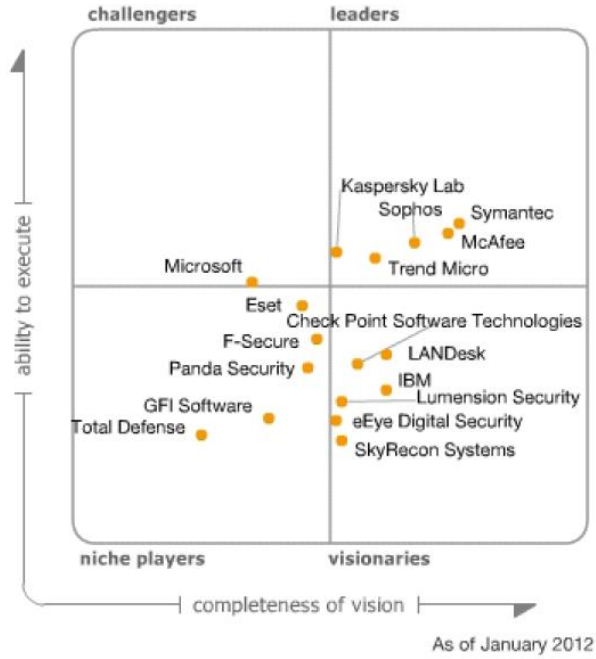


Fig 3. Cuadrante Magico de Garthner para Antivirus

En la empresa existían constantes infecciones graves de malware en los equipos de las diferentes áreas de negocio, derivado del mal funcionamiento de la herramienta de Antivirus, el antivirus no contaba con herramientas administrativas efectivas, en una ocasión por una infección que había afectado durante 2 semanas continuas, de un virus llamado Confiker.C se propagaba así mismo y el comportamiento era que leía el LDAP (***L****ightweight* ***D****irectory* ***A****ccess* ***P****rotocol*) que en este caso era el Directorio Activo montado en Microsoft y comenzaba a hacer intentos de acceso, lo que provocaba bloqueo de cuentas de usuarios finales y cuentas de aplicación usuarios de API (Aplicación) como correo Electrónico, Intranet, etc., lo que provocaba caída de servicios primordiales como correo electrónico y acceso a aplicaciones.

Como muestra de las fallas de la herramienta de Antivirus la consola principal tenía una deficiencia de mostrar porcentajes de equipos administrados, es decir en este ejemplo se muestra un 87% de equipos sin problemas, el 8% de computadoras que no reportan y el 2% de computadoras que reportan con problemas críticos, si se suman estos porcentajes 87+8+2 da un total del 97%, faltando un 3% que no reporta, el proveedor confirma que ese 3% faltantes son equipos que tienen problemas menores. Como se muestra en el Dashboard es un problema no crítico porque es informativo pero no es admisible en una herramienta tan importante para la protección de Seguridad TI, y no da certeza del correcto funcionamiento en general.

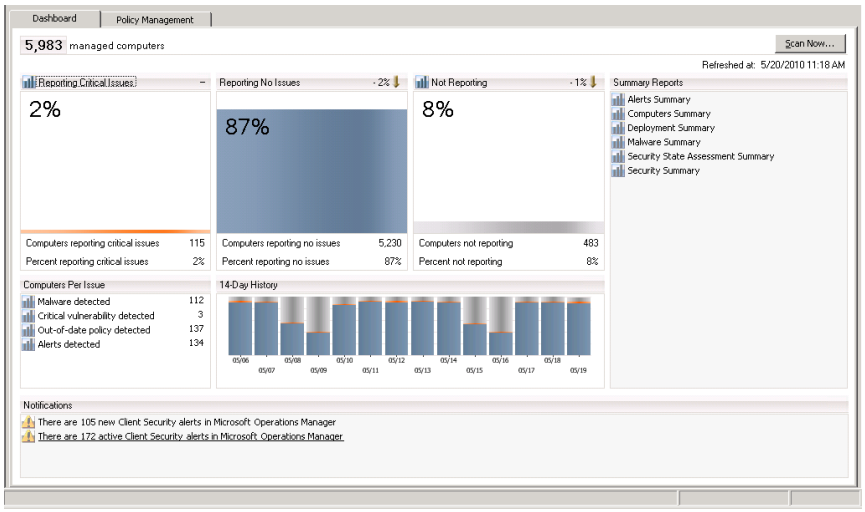


Fig4. Dashboard Antivirus

Otro de los problemas por el cual se tomó la decisión de cambiar la herramienta sucedió cuando el cliente solicito realizar un Full Scan a todos los equipos de la empresa, pese a que se recomendaba ampliamente no ejecutarlo el cliente asumió el riesgo y las consecuencias fueron 5 horas fuera de operación de alrededor del 30% de los equipos, el motivo se explica detalladamente a continuación:

- La herramienta de Antivirus programa los Full Scan mediante una tarea programada re-ejecutable si se interrumpe al apagar el equipo o al deshabilitar el proceso que ejecuta la actividad.

- El Full Scan se programa bajo un Indexado creado de las unidades lógicas del equipo, por lo que demoraba según el volumen de información existente.

- Los recursos compartidos de File Server asignados como unidad lógica provoco el escaneo simultaneo de los File Server configurados en las diferentes equipos, es decir al mismo

tiempo un alto número de equipos escaneaba el mismo servidor, lo que colapso los recursos de los File Server y los equipos que estaban realizando el escaneo, ya que la información en los File Server es dinámica y se ciclo el escaneo.

Al final se desarrolló e implementó un workaround para recuperar los File Server y los equipos involucrados, éste consistió en enviar vía script el borrado de los registros de la tarea programada y el Kill Task del proceso de antivirus, dejando los equipos sin protección Antivirus hasta que se envió el script para restablecer los servicios.

Esta fue la causa de peso para toma de decisión de cambiar la herramienta de Antivirus.

2.4 Solución

En HP se tenía en ese momento un convenio con Symantec por lo que se ofreció como herramienta para sustituir el antivirus que se tenía implementado y el cliente acepto.

La arquitectura fue diseñada tomando en cuenta la topología de red, se describe a continuación.

Existen la oficina central donde se encontraba el centro de cómputo principal (Site = Sculpture in the Environment) la oficina de gobierno donde se encuentra personal VIP, y 5 regiones principales, Tecnoparque, Monterrey, Guadalajara, Tijuana, Veracruz, entre las regiones existía un enlace limitado red WAN y dentro de cada regios red LAN existía un enlace de 100Mbps.

Con estas características de red, se definió una consola principal en el centro de datos principal y GUP = Group Update Provider, el GUP es una configuración que sirve como punto de distribución para actualización de firmas de antivirus y políticas esto en el flujo de la consola principal hacia los GUP y de los GUP a los equipos finales y en flujo inverso se envían los logs de estado de salud de los equipos, de esta forma solo había un solo punto de contacto entre la consola principal y las regiones.

El tráfico en WAN es mínimo, se muestran el promedio de consumo en la siguiente tabla.

FORMULA

Content type	Size of Package
Heartbeat	2 KB/s to 3 KB/s per heartbeat.
Policies	20 KB to 80 KB.
IPS Signature Updates	50 KB and 100 KB
AV Signatures	50 KB to 100 KB (daily)
Logs	10 KB

Concurrent Connections X Average Content Size ÷ Available Bandwidth = Content Distribution

Análisis

1 Workstation		**KB**
Heartbeat cada 5 minutos en 8 horas laborales		96
Policies 1 por día		50
AV Signatures		100
Logs		10
Total Ancho de Banda Consumido ()	~	**256**

Argentina	
Numero de Workstation	176
Numero de Enlaces	28
Ideal Wkt x Enlace	6
BW x Enlace	1609 ~ 1.7 MB x día

Tabla6. Tabla de consumo de Ancho de Banda

Al final la arquitectura de la nueva herramienta de antivirus quedo con una consola principal y GUP en las regiones, se muestra a continuación.

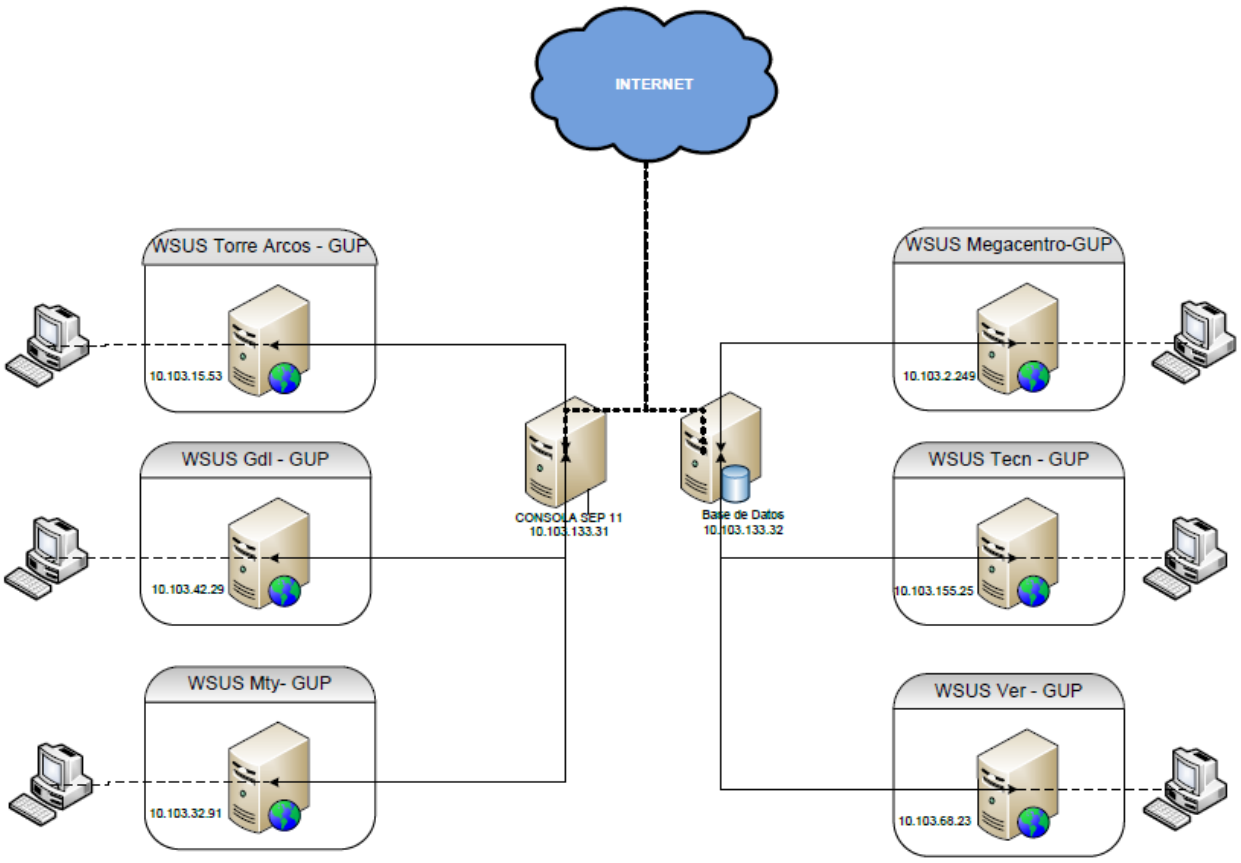


Fig5. Arquitectura de Antivirus

Una vez diseñada e implementada la arquitectura de la nueva herramienta de Antivirus el siguiente paso era la planeación de migración.

La migración debería considerar como principal punto la correcta sincronización entre desinstalar en antiguo antivirus e instalar el nuevo y que el tiempo entre esa actividad sea la mínima posible ya que los equipos estarían sin antivirus durante ese periodo de tiempo y por ningún motivo pueden convivir ambos antivirus en un equipo porque los engines de escaneo degradan considerablemente el rendimiento del equipo.

Otro punto a considerar es él nuevo antivirus tiene un Firewall integrado, esto es un problema para los equipos que utilizan comunicación por voz sobre la red LAN (VOIP), porque en la instalación se pierde comunicación durante unos segundos ya que el Firewall se agrega al driver de la tarjeta de red (NOC), lo que para cualquier usuario normal es imperceptible pero para el área de call-center es un impacto alto la interrupción de la comunicación porque se pierde la llamada en proceso.

Teniendo en consideración los puntos mencionados se desarrolló la estrategia de distribución que se describe a continuación.

El despliegue para equipos personales se realizó en 3 etapas:

- Primer Etapa: a traves de la herramienta de software de distribución.

  Objetivo a alcanzar: 80% de total.

  1 Ola: 500 Computadoras (Duración: 1 día)

  - Megacentro: 150 Workstations
  - Torre Arcos : 100 Workstations
  - Tecnoparque :150 Workstations
  - Regionales: 100 Workstations

2 Ola: 1000 Computadoras en Megacentro (Duración: 1 día)
3 Ola: 1000 Computadoras en Torre Arcos (Duración: 1 día)
4 Ola: 1000 Computadoras en Tecnoparque (Duración: 1 día)
5 Ola: 1000 Computadoras en Regionales (Duración: 1 día)
6 Ola: 1000 Computadoras en Regionales (Duración: 1 día)
7 Ola: 1000 Computadoras en Regionales (Duración: 1 día)

Para esta estrategia de distribución se tenían listos pre-requisitos:

- Comunicados masivos a los usuarios para que dejaran los equipos encendidos.

- Se discriminaron los equipos de Call-center, no se intervendrían durante esta distribución.

- Segunda Etapa: Reenviar la instalación a los equipos que por alguna razón no se instaló (apagado, problema de distribución, etc.) en olas de 100 equipos y con comunicados directos.

  - Iniciar la instalación manual del 5% de los equipos de Call-center de forma diurna y cuando no se tuviera llamada en proceso.

  Objetivo a alcanzar: 15% de total.

Tercera Etapa: Instalación Manual, de los equipos que no fueron alcanzados por ninguna de las holas anteriores.

Objetivo a alcanzar: 5% de total.

El gran total se completaba con las tres etapas de la estrategia de distribución, en paralelo se llevaba un control de calidad de equipos migrados, equipos con 2 antivirus y equipos sin antivirus los cuales eran remediados con alta prioridad con apoyo de la herramienta de distribución de software, el equipo de soporte en campo e incluso localizando a los usuarios finales vía telefónica para hacer la remediación inmediata, el porcentaje entre para los problemas con dos antivirus instalados o ninguno de ellos sumo el ~1% del total de los equipos.

El Plan de migración total en etapas fue seguido en el siguiente cronograma.

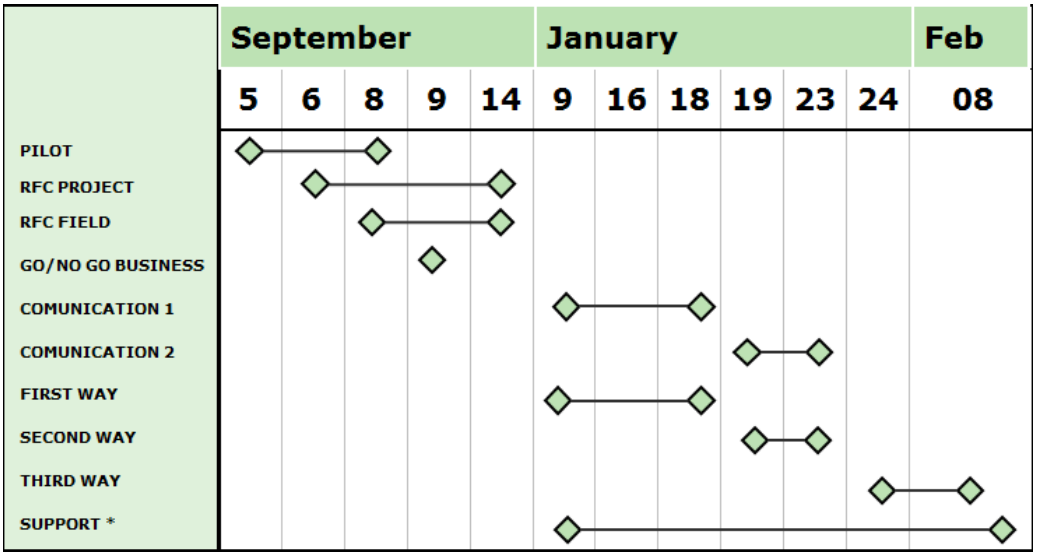


Fig6. Cronograma de proyecto de distribución nuevo AV

La *Fig6. Cronograma de proyecto de distribución nuevo AV* muestra las etapas de desarrollo del proyecto, comenzando en el mes de Septiembre con pruebas piloto, solicitud de *Request for Change RFC,* la toma de decisión de ejecución por las áreas de negocio, la comunicación a los empleados y las etapas de despliegue que se explicaron anteriormente.

La etapa final de este proyecto era implementar el control de los equipos que se ingresaban a la red y deberían tener el antivirus instalado, para lo que se implementó en 2 sentidos, de forma administrativa se desarrolló un procedimiento de ingreso de equipo nuevo a la red donde incluía explícitamente el software antivirus y los responsables de la actividad, y de forma técnica se desarrolló un LogOn Script implementado en el Directorio Activo que validaba los servicios del Antivirus al momento de hacer log In en la red y si no encontraba los servicios ejecutaba la instalación del software, también se reforzó con una análisis mensual de cotejar las fuentes de información del dominio versus la consola de Antivirus los faltantes se corregían o identificaban plenamente como equipo de terceros es decir de invitados (guest).

Para diseñar el proceso de migración de Antivirus en Servidores se clasificaron los servidores en nivel de criticidad, los tres niveles de criticidad eran Low, Medium and High, la clasificación la realizo la gerencia y dirección de TI junto con los niveles operativos, determinando un número máximo de 10 servidores para migrar por noche para criticidad Low, 5 servidores por noche para criticidad Medium y 1 servidor por noche para criticidad High.

Para la migración de un servidor se contempla las siguientes actividades:

- Desinstalar el Antivirus anterior.
- Reiniciar el servidor.
- Instalar Antivirus nuevo.
- Reiniciar el Servidor.
- Validar la funcionalidad del servidor.
- Validar la correcta instalación del Antivirus.

Y se requería el siguiente personal de apoyo por ventana de mantenimiento:

- Administrador de Servidores
- Administración de API, aplicación que corriera en el servidor.
- Administrador de Antivirus
- Ingeniero de Soporte en Sitio para apoyo local.

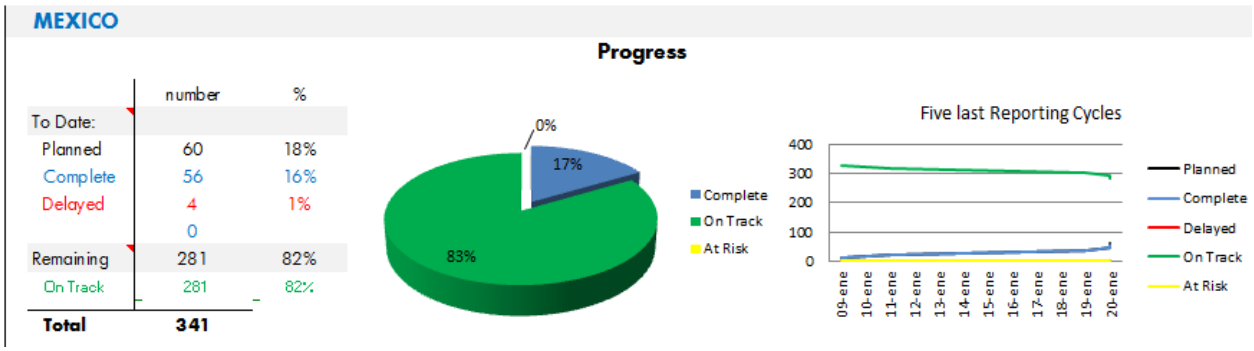


Fig7. Muestra de cifras de control (referencia).

Una vez completada la migración de deshabilito la infraestructura del anterior Antivirus y se entregó para re uso o upgrade.

2.5 Conclusiones

Se realizó la migración satisfactoriamente con el mínimo de incidentes y los reportes de virus e infecciones redujeron considerablemente.

La mejora pendiente en la herramienta de Antivirus es utilizar por completo las herramientas que contiene, el Device Control Module, que funcionaria para no permitir el ingreso de

dispositivos de almacenamiento no permitido, con ello se tendría más menos contaminación vía dispositivos de almacenamiento y se prevendría fuga de información.

La otra herramienta que se podría utilizar es el IPS local, con esto se podría mitigar los ataques de red de computadoras comprometidas así como un control de los recursos compartidos.

No olvidemos que para proteger equipos de ataques ya no es suficiente con un software Antivirus, son necesarias herramientas complementarias que aporten a la diminución de los riesgos.

CAPÍTULO 3. Vault Password para usuarios con altos privilegios

3.1 Objetivo

El objetivo de este proyecto es hacer la evaluación técnica de las herramientas del mercado e implementarla en el ambiente para obtener la automatización del uso de usuarios de emergencia, también llamado usuarios con altos privilegios.

3.2 Responsabilidades y Organización del Proyecto

Para este proyecto nos correspondían las siguientes responsabilidades:

- √ Evaluación de herramientas similares para entregar los resultados de sus competencias técnicas, matriz de ventajas y desventajas.
- √ Implementación de la herramienta elegida por el cliente.
- √ Cambio del proceso para solicitud de contraseñas de usuarios con altos privilegios.
- √ Entrenamiento a áreas de soporte quienes utilizan usuarios con altos privilegios.
- √ Documentación preparatoria para Auditoria Sarbanes-Oxley.

El grupo de trabajo se conformaba por siguientes integrantes:

- ❖ **Analista de Administración de Usuarios.** Responsable de alta, baja de usuarios, restablecer contraseña y asignación de perfil.

- ❖ **Analista de Seguridad de TI.** Responsable de realizar las pruebas de seguridad, creación de perfiles y asignación en la herramienta de control automático.

- **Especialista en Seguridad TI y Líder Técnico (mi rol).** Responsable de toma de decisiones, análisis especializado y realización de matriz de pruebas de las herramientas competidoras e implementación.

El desarrollo del proyecto se realizó en las siguientes etapas.

- Análisis del problema. En ésta etapa se identificaron los problemas y las necesidades de cliente, así como las dependencias para solucionarlos, se identificaron las responsabilidades de cada elemento u organización participante en el proyecto para determinar el alcance.

- Propuestas de solución. Se entregó una propuesta técnica de solución, basado en pruebas de seguridad y funcionalidad de las herramientas competidoras.

- Desarrollo de solución. En esta etapa se desarrolló/puesta en marcha de la solución propuesta, la información detallada está en el Capítulo 4 de este reporte.

- Evaluación de resultados y replanteamiento de estrategia y/o alcance. Para la implementación de esta herramienta no hubo variaciones en la implementación.

- Implementación en ambiente productivo. Puesta en producción con ventana de mantenimiento controlada y minimizando las implicaciones operativas.

- Etapa de estabilización. Etapa de utilización de usuarios finales y análisis de fallas, manejo de problemas para solución inmediata.

- Recolección de evidencia para auditoria. En esta etapa ya con el sistema estable se obtenía evidencia “dura” y se documentaba correctamente para exponer a auditoria y diera la validación de un proceso adecuado.

3.3 Problema

Vault Password es un concepto que significa, administrar los usuarios y contraseñas de cuentas de acceso con altos privilegios a los diferentes sistemas y plataformas como ‘root’ en Unix, ‘Oracle’ en Base de datos Oracle, ‘sa’ en Base de datos SQL Server, ‘Adminitrator’ en Controladores de Dominio basados en arquitectura Microsoft y toda cuenta administradora de un sistema, aplicación, plataforma o arquitectura, que por seguridad de la información deba estar resguardada, monitoreada y controlada en actividades para evitar mal uso de las mismas.

Los problemas presentados por el mal manejo de usuarios privilegiados eran los siguientes:

- ✓ Hallazgos de Auditoria Externa Sarbanes-Oxley por el control deficiente.
- ✓ Movimientos realizados sin autorización y/o control que derivaban en caídas de sistemas, fallas en aplicaciones.
- ✓ Uso indebido de creación de Planes tarifarios, registros contables y/o fraudes, sin tener los elementos para deslindar responsabilidades ya que el usuario/contraseña era conocido por los integrantes de soporte.

- ✓ El control que se tenía sobre usuarios de emergencia era manual, por lo que presentaba fallas humanas, riesgos altos en robo de las contraseñas, gastos de papelería y almacenamiento de evidencia física de los sobres que contenían las contraseñas, y deficiencias operativas.

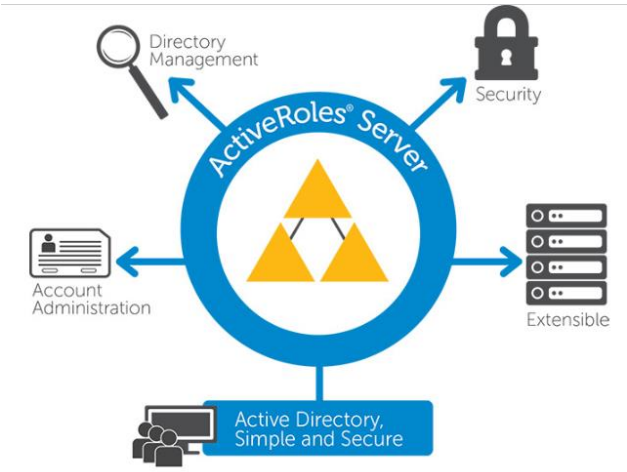


Fig8. Flujo de Vault Password

En Nextel México existía el esquema de sobres de emergencia operado manualmente lo que tenía varias puntos de mejora como eficiencia en operación, errores de asignación de contraseña, pero él mayor problema era la recopilación y entrega de evidencia para las diferentes auditorias que se ejecutaban durante el año, auditoria interna y auditoria externa, y por último pero no menos importante los grandes huecos de seguridad que se presentaban al mantener el proceso manual.

Por lo que se le propuso al cliente comprar una herramienta dedicada para el manejo de contraseñas de usuarios privilegiados A lo que el cliente accedió y solicito a HP realizar una recomendación.

3.4 Solución

Se realizó el procedimiento de RFP (Request for Proposal) y se identificaron dos herramientas que tenían los requerimientos del cliente y se procedido a realizar las pruebas de funcionalidad correspondientes, mismas que se muestran en una matriz para que el cliente pudiera decidir en cuanto a requerimientos técnicos la más competente para sus necesidades. A continuación se muestra la *Fig9. Cuadro comparativo* la matriz de resultados de las pruebas realizadas a as dos herramientas que concursaron.

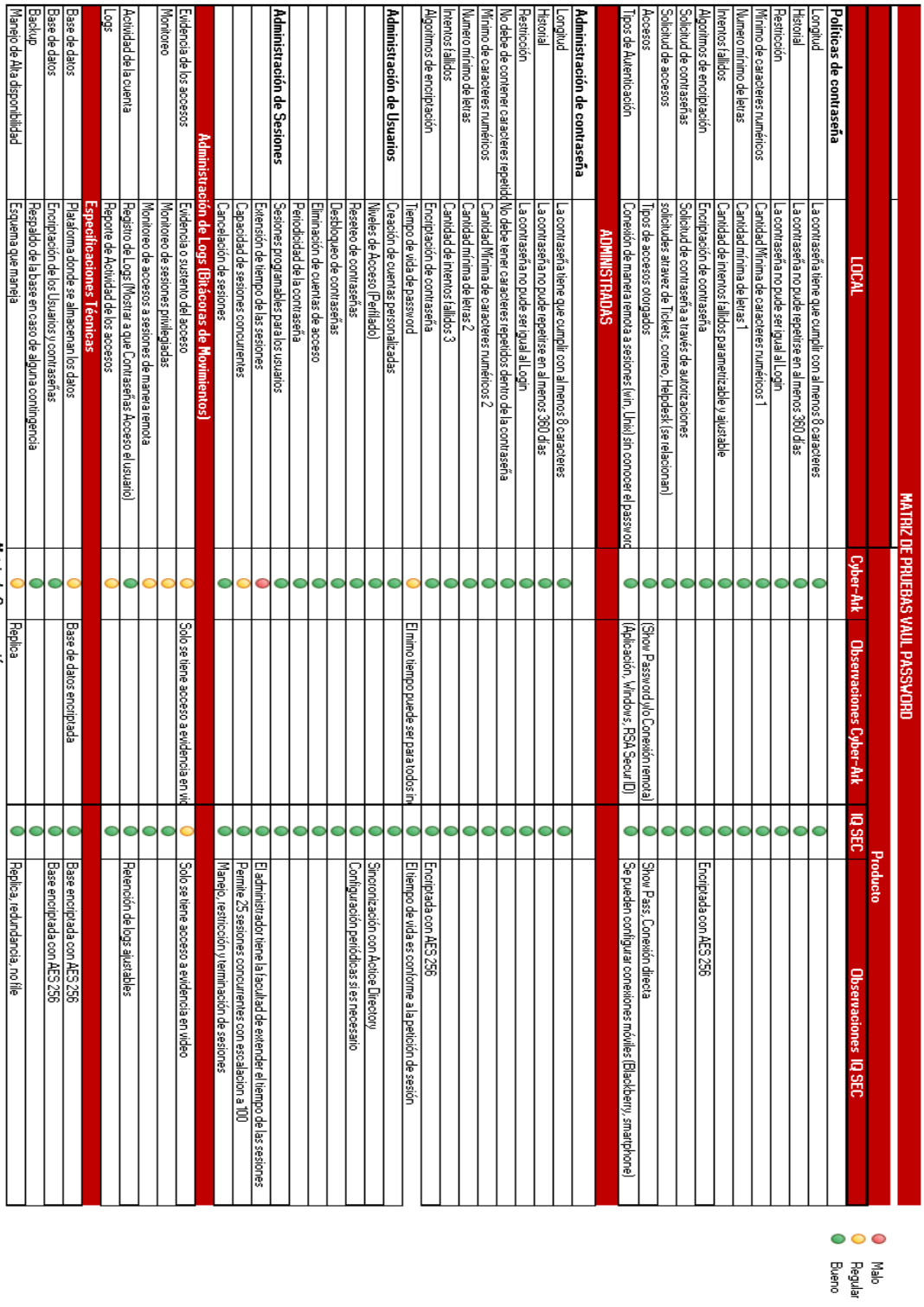


Fig9. Cuadro comparativo

El cliente decidió el que más le convenía según habilidades técnicas y recursos financieros y se trabajó en el plan de migración a la nueva herramienta en dos etapas migración de usuarios en equipos NO Productivos, como sigue:

Task Name	Duration	% Complete
Puesta en producción de vault password para equipos no productivos	**33 days?**	**100%**
Inventario de Sobres de Emergencia de equipos no productivos	1 day	100%
Lista de excepciones	1 day	100%
Creacion de usuarios aplicativos	5 days?	100%
Preparación del Sudo (Unix)	4 days?	100%
Probar las cuentas funcionales en la herramienta de vault password	1 day?	100%
Levantar el RFC para la implementación en equipos no productivos	1 day?	100%
Solicitud para agregar las 3 IP´s del eDMZ al DNS interno y la búsqueda sea por nombre de URL	1 day?	100%
Enviar el calendario del la puesta en produccion	1 day?	100%
Implementación de la herramienta	**8 days**	**100%**
Lote 1 Configurar 26 cuentas de sobres de emergencia	**1 day**	**100%**
Lote 2 Configurar 25 cuentas de sobres de emergencia	**1 day**	**100%**
Lote 3 Configurar 24 cuentas de sobres de emergencia	**1 day**	**100%**
Lote 4 Configurar 19 cuentas de sobres de emergencia	**1 day**	**100%**
Lote 5 Configurar 24 cuentas de sobres de emergencia	**1 day**	**100%**
Lote 6 Configurar 24 cuentas de sobres de emergencia	**1 day**	**100%**
Lote 7 Configurar 25 cuentas de sobres de emergencia	**1 day**	**100%**
Lote 8 Configurar 16 cuentas de sobres de emergencia	**1 day**	**100%**

Una vez migrados todos los usuarios de equipos no productivos se procedió diseñar los flujos de autorización al solicitar un usuario integrado en esquema de sobre de emergencia, ya que cambiaría el flujo, no el proceso de autorización ni los autorizadores.

Los puntos clave que se modificaron fue la validación manual de una solicitud de sobre de emergencia la realizaba personal de SYSOPS cotejando que el solicitante tuviera autorización para solicitar la contraseña, ahora la validación se realizaría de forma automática.

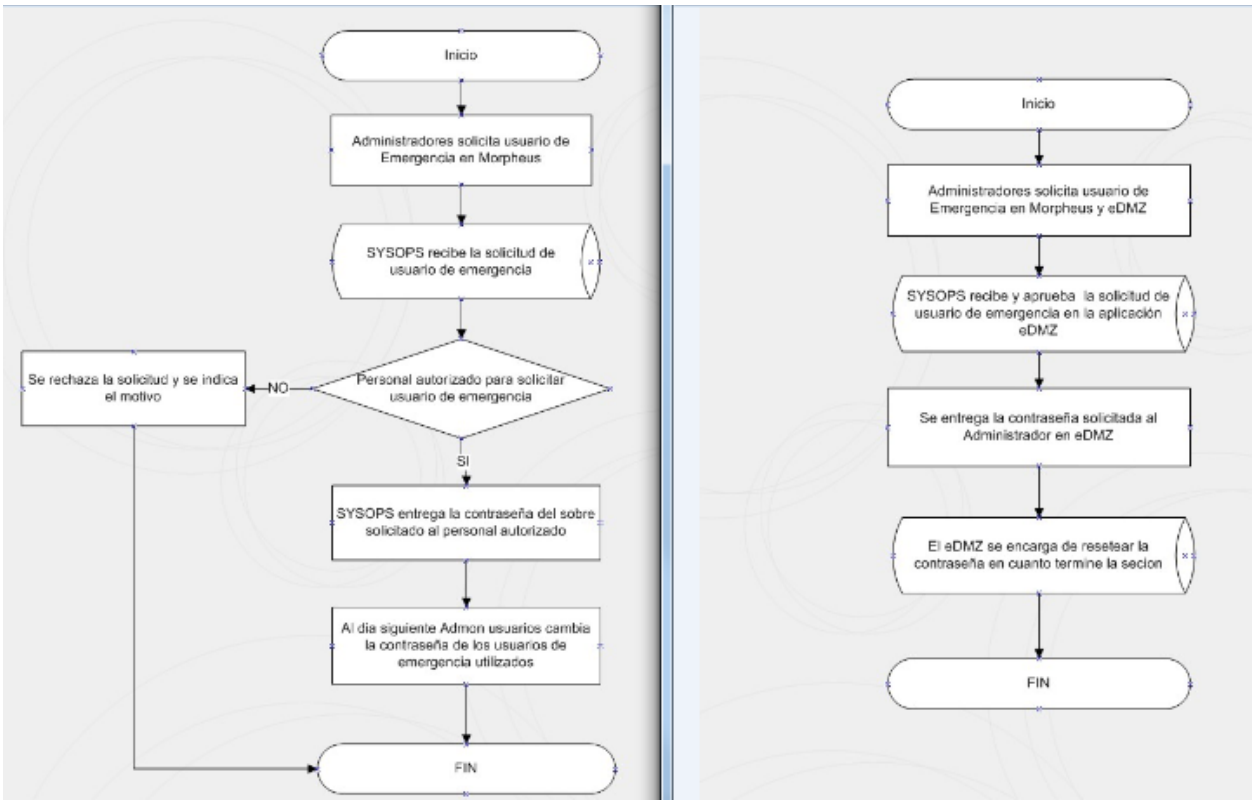


Fig 10.Diagrama de flujo anterior y con la herramienta

El siguiente paso fue hacer sesiones de entrenamiento de la herramienta para todo el personal que participaría en el proceso:

- Sysops.- Personal que coteja la solicitud, abre el sobre físico y entrega de la contraseña.

- Áreas de Soporte.- Administradores de Bases de Datos, sistemas operáticos Unix, HP-UX, Solaris, Linux, Windows.

- Administración de Usuarios.- Área de gobierno de los usuarios que viven en esquema de sobres de emergencia.

- Auditoria.- Área que audita las actividades y verifica el cumplimiento del proceso.

Se realizó la ejecución del plan de integración para usuarios privilegiados de servidores Productivos, en el mismo esquema de integración.

Se consideró en el plan de migración lo siguiente:

- Notificación diaria a las áreas involucradas del avance del proyecto, por si requerían una contraseña supieran si estaba en el esquema viejo o en la nueva herramienta.

- La migración debería ser de aplicaciones completas, es decir si una aplicación X manejaba 2 Bases de datos y 4 servidores todos deberían ser migrados en una misma noche para mejor control y evitar confusión entre las áreas operadoras.

Task Name	Duration
Puesta en producción de vault password para equipos Productivos	**33 days**
Inventario de Sobres de Emergencia de equipos no productivos	1 day
Lista de excepciones	1 day
Creacion de usuarios aplicativos	5 days
Preparación del Sudo (Unix)	4 days
Probar las cuentas funcionales en la herramienta de vault password	1 day
Levantar el RFC para la implementación en equipos no productivos	1 day
Solicitud para agregar las 3 IP´s del eDMZ al DNS interno y la búsqueda sea por nombre de URL y no por IP	1 day
Enviar el calendario del la puesta en produccion	1 day
Implementación de la herramienta	**8 days**
Lote 1 Configurar 20 cuentas de sobres de emergencia	**1 day**
Lote 2 Configurar 20 cuentas de sobres de emergencia	**1 day**
Lote 3 Configurar 20 cuentas de sobres de emergencia	**1 day**
Lote 4 Configurar 20 cuentas de sobres de emergencia	**1 day**
Lote 5 Configurar 20 cuentas de sobres de emergencia	**1 day**
Lote 6 Configurar 10 cuentas de sobres de emergencia	**1 day**
Lote 7 Configurar 12 cuentas de sobres de emergencia	**1 day**
Lote 8 Configurar 12 cuentas de sobres de emergencia	**1 day**

Cronograma de proyecto de Vault Password para usuarios Privilegiados.

Se cambió el procedimiento de solicitud de sobres de emergencia y se creó un usuario con rol de auditor, el cual es entregado a los recursos humanos encargados de la gestión de auditoria, cabe mencionar que nunca más se ha realizado ningún hallazgo.

3.5: Conclusiones

La herramienta superó las expectativas, después de la implementación no se presentó problemas mayores con la entrega y uso de las contraseñas, además de que para auditoria fue la solución ideal al quitar la gestión manual.

La siguiente etapa de mejora para herramienta de control de contraseñas de usuarios privilegiados es implementar contraseñas de API, la herramienta maneja un concepto de variables funciona para asignar en código duro (hardcode) la variable y la contraseña sea cambiada y sincronizada periódicamente, de esta forma ningún administrador tendría la contraseña y se garantiza confidencialidad del usuario.

Otro modulo que podría implementarse para aplicaciones de riesgo alto es la apertura de sesión y no entrega de contraseña, esta funciona con el mismo flujo, solo que en vez de entregar la contraseña abre una terminal hacia el servidor solicitado, con acceso (log in) con el usuario de administración lo que permite grabar las sesiones y perfilar a nivel comando lo que está permitido o no, no obstante que el administrador ingrese con una cuenta de altos privilegios se debe prevenir comando irreversibles.

CAPÍTULO 4. Hardening en Mail Filter Tool (Ant spam) Mexico

4.1 Objetivo

El objetivo de este proyecto es implementar mejoras de diseño y arquitectura para reducir al mínimo el riesgo de ataque de Spam y Spoofing.

4.2 Responsabilidades y Organización del Proyecto

Para este proyecto nos correspondían las siguientes responsabilidades:

- √ Valoración de la arquitectura y políticas implementadas de la herramienta Antispam.
- √ Propuesta de solución para robustecer las Seguridad y disminuir los problemas presentados por Spam y Spoofing.
- √ Implementación.

El grupo de trabajo se conformaba por siguientes integrantes:

- **Administrador de DNS.** Responsable de implementar las adecuaciones a las en el DNS primario.

- **Administrador de red.** Responsable de implementar las adecuaciones en cuanto a elementos de red se refiere.

- **Analista de Seguridad de TI.** Responsable de implementar las adecuaciones a las políticas de seguridad de la herramienta Antispam.

- **Especialista en Seguridad TI y Líder Técnico (mi rol).** Responsable realizar la validación y propuestas de remediación para el endurecimiento (hardening) de la seguridad en la herramienta Antispam, liderar y validar las modificaciones.

El desarrollo del proyecto se realizó en las siguientes etapas.

- Análisis del problema. En ésta etapa se identificaron los problemas, se identificaron los motivos tanto administrativos como manejo de políticas, proceso de administración de incidentes, awareness program (proceso de concientización) y técnicos como arquitectura, diseño, políticas., logs habilitados.

- Propuestas de solución. Se entregó una propuesta técnica de solución, y una propuesta administrativa como proceso de manejo de incidentes, se mostró los motivos más críticos de los problemas presentados y la remediación.

- Desarrollo de solución. En esta etapa se desarrolló/puesta en marcha de la solución propuesta, la información detallada está en el Capítulo 4 de este reporte.

- Evaluación de resultados y replanteamiento de estrategia y/o alcance. Se obtuvieron métricas para poder evaluar la disminución de incidentes relacionados con la solución.

- Validación de resultado final. Realizar pruebas exhaustivas para comprobar que solución funcionaba y sin errores o bugs de sistemas y preparar la implementación a ambiente productivo minimizando las implicaciones operativas.

- Implementación en ambiente productivo. Puesta en producción con ventana de mantenimiento controlada y minimizando las implicaciones operativas.

- Etapa de estabilización. Ésta etapa se limitaba a recibir y atender de forma personalizada los incidentes reportados por Spam.

4.3 Problema

La herramienta de Mail Filter implementada en Nextel Mexico, tenía las configuraciones por default tanto en la configuración de filtrado de correo reglas de bloqueo, heurística, niveles de seguridad, es decir las configuraciones de la herramienta (Settings), así como en la arquitectura implementada a nivel red que era poco segura y sin tolerancia a fallas (no en Alta disponibilidad).

Lo que se realizó derivaba en muchos problemas de operación afectando el 60% de los usuarios finales en las diferentes área donde es imprescindible el servicio de correo como Crédito y Cobranza, atención a clientes, paquetería y entrega, Tecnología e Infraestructura (Sistemas), mercadotecnia, entre las más afectadas.

Describo algunos de los mayores problemas presentados:

Ataques de Suplantación de Identidad (Spoofing), y el comportamiento era que él enviaba correos masivos de contenido dudoso a dominios externos como @hotmail.com, @yahoo.com, @gmail.com, identificándose con el dominio de la empresa en cuestión, lo que provocaba es que se diera mala reputación a la IP y se bloqueara por las herramientas de seguridad de los dominios terceros, herramientas como IPS, Mail Filter, Firewall, IDS.

Fuga de Información, al existir cuentas de correos "genéricos" SMTP ID, y con permisos delegados a muchas personas de una o varias áreas de trabajo, era imposible identificar quien enviaba el correo pero también tampoco era visible el contenido del mismo, ya que solo se tenía el registro SMTP logs.

No se detectaban y no se tenía registro de correos de desprestigio de personal, nepotismo, agresiones, amenazas, spam generado por el propio personal y muy poca efectividad de detención y detención de correo malicioso.

Ejemplo:

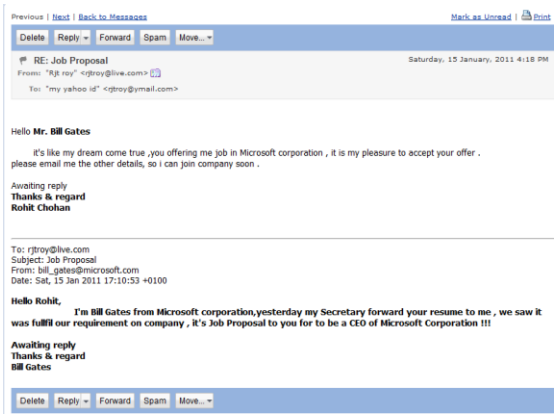


Fig11. Ejemplo de Spoofing

Se tenían recurrentes problemas de Spam y Spoofing, correo con malware, y palabras altisonantes por la mala configuración de las políticas de bloqueo y la arquitectura de la herramienta de Antispam, constante bloqueos de la IP públicas por mala reputación y mal comportamiento de correo.

Aquí se muestran diversos ejemplos de correos Spam que se recibían:

-----Mensaje original-----
De: esp_dl@groups.hp.com [mailto:esp_dl@groups.hp.com] Enviado el: Lunes, 09 de Julio de 2012 10:21 a.m.
Para: Mail Filter
Asunto: Spam: Your new password has been reset.

Dear SEGUTIDAD,

Your HP Passport password has been reset. It can be used to login to Enterprise Service Portal. HP Passport is a single login service from HP.com.

Choose New Password
This link is time sensitive and will expire.

If you click the link and do not see the "Reset Password" page, it may be because your browser is set to not accept Third Party Cookies* or some other technical reason. If this is the case, paste the URL below into the address line in your browser.

https://am-p.serviceportal.hp.com/smp/A/ChoosePassword.aspx?lang=en-US&guid=GZMFJ5GSHILNHCPW3CJHNR412JASDJCS

Respectfully,

The HP Passport Support Team

*For instructions on how to accept Third Party Cookies on your Internet browser, please use the help button on your browser.

De: Purificadores de Aire IQAir [mailto:16feb2012@rsd.com.mx]
Enviado el: jueves, 16 de febrero de 2012 01:58 p.m.
Para: Chan Leo, Jose
Asunto: Spam: Con IQAir Protege a tu familia de la gripe e influenza.

Elimine la gripa e influenza de su casa y oficina.
Limpie areas de mucho trafico o con mucho personal.
Reduzca los contagios.

Si este es su caso, usted necesita un purificador de aire SUIZO llamado *IQAir.*

Elimina Contaminacion, Virus, Bacterias, Ozono, Smog.
Equipo aprobado por la FDA para tratamiento gripe, influenza (SARS, A/H1N1).

Así como bloqueo de dominio de Nextel hacia dominios externos.

```
Reporting-MTA: dns;MAILHOST.nextel.com.mx
Received-From-MTA: dns;mxtla1w3pmr01.nextelmx.net
Arrival-Date: Tue, 13 Sep 2012 14:45:19 +0000

Final-Recipient: rfc822;radvil@prodigy.net.mx
Action: failed
Status: 5.0.0
Diagnostic-Code: smtp;550 #5.1.0 Address rejected radvil@prodigy.net.mx
Remote-MTA: dns;-
.
```

Fig 12. Log Error

Errores Publicados por Hotmail para problemas de Spam.

Why are the emails sent to Hotmail rejected for policy reasons?

The mails that I or my domain users sent to Hotmail are rejected for policy reasons.

Error Codes:

550 SC-001 Mail rejected by Hotmail for policy reasons. Reasons for rejection may be related to content with spam-like characteristics or IP/domain reputation. If you are not an e-mail/network admin please contact your E-mail/Internet Service Provider for help.

550 SC-002 Mail rejected by Hotmail for policy reasons. The mail server IP connecting to Hotmail has exhibited namespace mining behavior. If you are not an e-mail/network admin please contact your E-mail/Internet Service Provider for help.

550 SC-003 Mail rejected by Hotmail for policy reasons. Your IP address appears to be an open proxy/relay. If you are not an e-mail/network admin please contact your E-mail/Internet Service Provider for help.

550 SC-004 Mail rejected by Hotmail for policy reasons. A block has been placed against your IP address because we have received complaints concerning mail coming from that IP address. We recommend enrolling in our Junk E-Mail Reporting Program (JMRP), a free program intended to help senders remove unwanted recipients from their e-mail list. If you are not an e-mail/network admin please contact your E-mail/Internet Service Provider for help.

4.4 Solución

Para la solución de este problema de trabajo en dos sentidos correcciones Locales y correcciones no locales.

Correcciones Locales,

- ✓ Se crearon diccionarios de malas palabras en idioma inglés y en idioma español, se crearon diferentes políticas de contenido donde se agregaron los diccionarios.
    - Subject, toda coincidencia con las palabras de los diccionarios en el asunto se enviara el correo a cuarentena.
    - Body, toda coincidencia con las palabras de los diccionarios en el cuerpo del correo se enviara a cuarentena
- ✓ Se crearon diccionarios de Dominios y Remitentes para ser bloqueados (black list).
- ✓ Se elevó el nivel de heurística para el bloqueo de correos sospechosos.

Lo anterior se logró con un análisis de patrones (análisis de comportamiento), que se describe a continuación.

a) Primero se habilitaron los Logs de Message Tracking a su máximo nivel de detalle, estos logs son los registros que procesa la herramienta de Antispam para un correo que es recibido y entregado, así como su status (Delivered, Fail, Delay, etc.)

b) También se habilitaron los logs en los conectores de salida y entrada, es decir, los logs SMTP de la comunicación de la herramienta Antispam con otros servidores de correo.

El análisis con los logs habilitados en el flujo de correos desde Internet hacia cuentas de dominio Internas, en volumen y contenido, es decir, cuantos correos eran recibidos desde un mismo dominio y el mismo Asunto, si existía un numero alto de correos con el mismo contenido se clasificaba como posible Spam, y se ingresaban los patrones de palabras o contenido en los diccionarios.

Estos correos se mantenían por quince días y si no se recibía queja de los usuarios finales por no recibir el correo se eliminaban.

Implementamos algunos criterios para colocar como correos no deseados de manera inmediata, a continuación una tabla de valores y toda decisión para agregar correos dudosos como Spam o no hacerlo.

Comportamiento	Decisión
Numero de correos mayor a 50 durante 24 horas, mismo Asunto y mismo remitente.	Se ponía en cuarentena y se esperaban quince días para catalogarlo como Spam si nadie reclamaba la no recepción.
Numero de correos mayor a 50 durante 24 horas, mismo asunto y mismo remitente, se repite en las siguientes 24 horas o las siguientes 48 horas, diferentes destinatarios.	Se ponía en cuarentena y se esperaban quince días para catalogarlo como Spam si nadie reclamaba la no recepción.
Numero de correos mayor a 50 durante 24	Se catalogaba como Spam.

horas, mismo asunto y mismo remitente, se repite en las siguientes 24 horas o las siguientes 48 horas, mismos destinatarios.	
Numero de correos mayores a 50 durante 24 horas, diferente asunto mismo remitente.	Se ponía en cuarentena y se esperaban quince días para catalogarlo como Spam si nadie reclamaba la no recepción.
Numero de correos mayores a 50 durante 24 horas, diferente asunto diferente remitente.	Correo valido.
Numero de correos recibidos mayores a 200 mismo remitente o dominio remitente en 24 horas.	Se catalogaba como Spam
Correos de Publicidad	Se catalogaba como Spam

Tabla7. Tabla de decisión para Spam

El análisis con los logs habilitados en el flujo de correos desde cuentas de dominio Interna hacia Internet, se revisaba patrones de comportamiento, y si existía mal uso de los recursos de la empresa como motivos personales o recreacionales, se pasaba el reporte a recursos humanos para que tomara medidas.

En este análisis se identificó un comportamiento de Spoofing que provocaba constante bloqueos de los dominios externos hacia el dominio de Nextel Mexico.

El comportamiento se describe a continuación:

Flujo.

1. Un tercero (fuera de la red de Nextel) enviaba correos a Nextel Mexico con dominio remitente de Hotmail.
2. Los destinatarios cuentas de correo de Nextel no existían y los rechazaba con un NDR (Non Delivery Record).

3. El remitente tampoco existía y el dominio Hotmail bloqueaba la IP pública debido a un comportamiento de ataque de Minería.

Los logs se muestran a continuación.

```
2,Externo,08CD0D207431D1F9,12,192.168.120.55:2455,65.55.92.168:25,<,250 XB,
2,Externo,08CD0D207431D1F9,13,192.168.120.55:2455,65.55.92.168:25,*,8697814,sending message
2,Externo,08CD0D207431D1F9,14,192.168.120.55:2455,65.55.92.168:25,>,MAIL FROM:<myrna.lopezz@nextel.com.mx> SIZE=75995 AUTH=<>,
2,Externo,08CD0D207431D1F9,15,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<loveboa@hotmail.com>,
2,Externo,08CD0D207431D1F9,16,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<leokaotik@hotmail.com>,
2,Externo,08CD0D207431D1F9,17,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<lopezvelardegerardo@hotmail.com>,
2,Externo,08CD0D207431D1F9,18,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<lodh6303@hotmail.com>,
2,Externo,08CD0D207431D1F9,19,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<leticialopa@hotmail.com>,
2,Externo,08CD0D207431D1F9,20,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<lclogisticainternacional@hotmail.com>,
2,Externo,08CD0D207431D1F9,21,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<LOBOURS@HOTMAIL.COM>,
2,Externo,08CD0D207431D1F9,22,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<lamsyco01@hotmail.com>,
2,Externo,08CD0D207431D1F9,23,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<luisonojeda@hotmail.com>,
2,Externo,08CD0D207431D1F9,24,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<leonavila2@hotmail.com>,
2,Externo,08CD0D207431D1F9,25,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<mjlz99@hotmail.com>,
2,Externo,08CD0D207431D1F9,26,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<ma_eugenia_s@hotmail.com>,
2,Externo,08CD0D207431D1F9,27,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<mabru70@hotmail.com>,
2,Externo,08CD0D207431D1F9,28,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<mafelix3@hotmail.com>,
2,Externo,08CD0D207431D1F9,29,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<mariednac@hotmail.com>,
2,Externo,08CD0D207431D1F9,30,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<marisagarcial@hotmail.com>,
2,Externo,08CD0D207431D1F9,31,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<mauhiz@hotmail.com>,
2,Externo,08CD0D207431D1F9,32,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<mayko68@hotmail.com>,
2,Externo,08CD0D207431D1F9,33,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<mabm_62@hotmail.com>,
2,Externo,08CD0D207431D1F9,34,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<marceladefelix@hotmail.com>,
2,Externo,08CD0D207431D1F9,35,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<magnoliarangel@hotmail.com>,
2,Externo,08CD0D207431D1F9,36,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<mehb1@hotmail.com>,
2,Externo,08CD0D207431D1F9,37,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<jclo_23@hotmail.com>,
2,Externo,08CD0D207431D1F9,38,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<jquintanillaj@hotmail.com>,
2,Externo,08CD0D207431D1F9,39,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<jorgeolea74@hotmail.com>,
2,Externo,08CD0D207431D1F9,40,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<jmcholo@hotmail.com>,
2,Externo,08CD0D207431D1F9,41,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<jorgillo_07@hotmail.com>,
2,Externo,08CD0D207431D1F9,42,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<javiertorres425@hotmail.com>,
2,Externo,08CD0D207431D1F9,43,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<javier_blancarte@hotmail.com>,
2,Externo,08CD0D207431D1F9,44,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<juliegutz@hotmail.com>,
2,Externo,08CD0D207431D1F9,45,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<jaimeariel69@hotmail.com>,
2,Externo,08CD0D207431D1F9,46,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<jhsv79@hotmail.com>,
2,Externo,08CD0D207431D1F9,47,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<louvalag@hotmail.com>,
2,Externo,08CD0D207431D1F9,48,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<lorenaservin@hotmail.com>,
2,Externo,08CD0D207431D1F9,49,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<laurisparedes@hotmail.com>,
2,Externo,08CD0D207431D1F9,50,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<liliahall@hotmail.com>,
2,Externo,08CD0D207431D1F9,51,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<lic_sandramoreno@hotmail.com>,
2,Externo,08CD0D207431D1F9,52,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<luzvalen@hotmail.com>,
2,Externo,08CD0D207431D1F9,53,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<karynicha82@hotmail.com>,
2,Externo,08CD0D207431D1F9,54,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<KARLALIZARRAGA5@HOTMAIL.COM>,
2,Externo,08CD0D207431D1F9,55,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<lclopezpadilla@hotmail.com>,
2,Externo,08CD0D207431D1F9,56,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<luisguevara02@hotmail.com>,
2,Externo,08CD0D207431D1F9,57,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<wera_fg@hotmail.com>,
2,Externo,08CD0D207431D1F9,58,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<panchowillis@hotmail.com>,
2,Externo,08CD0D207431D1F9,59,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<patricia_badilla_alvarez@hotmail.com>,
2,Externo,08CD0D207431D1F9,60,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<plagas@hotmail.com>,
2,Externo,08CD0D207431D1F9,61,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<quezadag@hotmail.com>,
2,Externo,08CD0D207431D1F9,62,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<quiquevazquez@hotmail.com>,
2,Externo,08CD0D207431D1F9,63,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<qesp_noroeste@hotmail.com>,
2,Externo,08CD0D207431D1F9,64,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<patytrevi@hotmail.com>,
2,Externo,08CD0D207431D1F9,65,192.168.120.55:2455,65.55.92.168:25,>,RCPT TO:<purasantaobson@hotmail.com>,
```

Fig13. Logs SMTP

Y después del bloqueo de Hotmail era el siguiente:

lulupollito@hotmail.com
bay0-mc3-f5.Bay0.hotmail.com #550 SC-002 Unfortunately, messages from 201.130.47.13 weren't sent. Please contact your Internet service provider since part of their network is on our block list. You can also refer your provider to http://mail.live.com/mail/troubleshooting.aspx#errors. ##

Este ataque no se podía identificar desde origen externo e incluso interno, y se bloqueaban las IPs vía el Firewall pero no era la remediación de raíz, por lo que se realizaron mejoras en la infraestructura (correcciones no locales).

Correcciones no locales o de arquitectura.

Se realizaron varias mejoras a la infraestructura de Antispam, se listan a continuación:

- ✓ Se configuro un NAT estático (uno a uno) con la IP Publica y la IP de la DMZ.
- ✓ Se bloqueó por completo el protocolo SMTP a través del Firewall exceptuando el Antispam y las herramientas de envío de factura electrónica (paperless).
- ✓ Se bloqueó por Firewall el puerto 25 y protocolo SMTP desde la intranet hacia la DMZ, exceptuando las IPs con servicio de correo.
- ✓ Se creó el registro SPF y se publicó en los DNS externos.
- ✓ Se eliminó autenticación anónima y se sincronizo con el Controlador de Dominio.
- ✓ Se depuro las IPs con privilegio de enviar correo (Relay) a través de la herramienta Antispam y se implementó proceso de control periódico para ellas.
- ✓ Se dio de alta el servicio Smart Network Data Services de Hotmail para monitorear el comportamiento del envío de correo desde el dominio de Nextel.

Se configuro un NAT estático (uno a uno) con la IP Publica y la IP de la DMZ.

La IP Privada de la DMZ con la IP publica no tenía un Nat (Network addess Traslation), dedicado, así que se configuro en el Firewall, lo que garantizaba que solo la IP publica podía ser usada por la IP Privada asignada a la herramienta Antispam.

Las mejoras que esta actividad traía consigo es que ningún servidor podía enviar información a través de la IP pública que no fuera autorizada y toda la información enviada a desde internet debería ser analizada por el Antispam.

Se bloqueó por completo el protocolo SMTP a través del Firewall exceptuando el Antispam y las herramientas de envío de factura electrónica (paperless).

Se identificaron los recursos que estrictamente tenían por funcionalidad enviar correo desde el dominio de Nextel hacia Internet, y se localizaron las aplicaciones de envío de factura electrónica, que tienen su propia IP Publica y como son aplicaciones dedicadas tienen heurística y comportamientos para no caer en mala reputación.

Se comunicó a todo el personal de áreas de soporte que deberían justificar y dirigir sus correos a través de la herramienta Antispam, lo que demoró un mes aproximadamente ya que todas las aplicaciones que enviaban correo SMTP eran de alertas de los sistemas o métricas de ventas y algunas de ellas estaban configuradas en código duro (hardcode), así que se tenía que cambiar el flujo hacia el Antispam y no hacia Internet directamente, la gran mayoría enviaba trafico SMTP a través del puerto 80 y regresaba el correo ya que las alertas estaban dirigidas a sus cuentas de correo, hubo pocas que tenían permisos para enviar directamente hacia Internet con sus propios recursos.

Se bloqueó por Firewall el puerto 25 y protocolo SMTP desde la intranet hacia la DMZ, exceptuando las IPs con servicio de correo.

Se configuró una regla de bloqueo explícito desde la intranet hacia la IP del Antispam en la DMZ, haciendo excepciones con previa autorización de la dirección de TI, esta actividad elimino por completo cualquier anomalía de inyección de correo por otro medio que no fuera el Antispam, quedando éste como único elemento para realizar el envío de correo hacia Internet.

Las tres medidas anteriores deja la nueva infraestructura del Antispam.

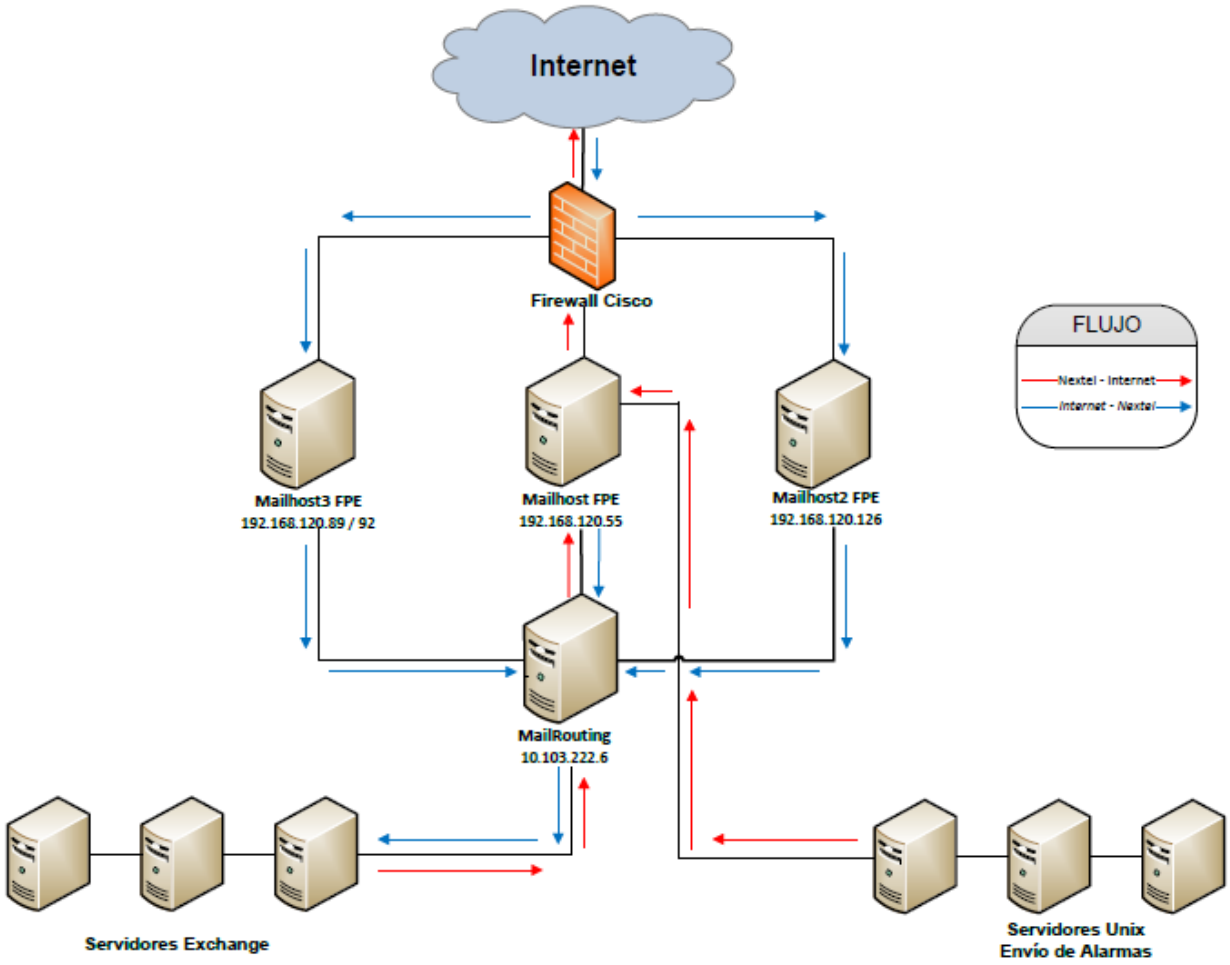


Fig14.Diagrama Antispam

Se creó el registro SPF y se publicó en los DNS externos.

Una vez identificado los elementos autónomos que deberían enviar correo y la herramienta Antispam se procedió a publicar el registro SPF en los DNS externos.

El registro SPF funciona de la siguiente manera.

Como se explicaba anteriormente, se utiliza para evitar el envío de correos suplantando identidades. El sistema se fundamenta en que en los registros SPF se introduce la información de las máquinas, redes, dominios, etc. Desde donde se autoriza a realizar envió de correos, en el momento en que se intenta enviar un correo se consulta este registro para compararlo con la IP desde donde se está enviando para ver si es autorizada, algo así como un registro “MX inverso”. El proceso sigue los siguientes pasos:

1. El emisor o remitente envía el correo.
2. El mensaje llega al servidor de correo entrante del destinatario o receiver, el cual llama a su Sender ID Framework (SIDF).
3. El SIDF consulta el registro SPF del dominio que el emisor está utilizando para enviar el correo y determina si debe pasar o no.
4. Al final si el correo no es devuelto se le pasa a los filtros de reputación para que lo clasifiquen como le corresponda.
5. Se entrega el correo al destinatario.

Gráficamente.

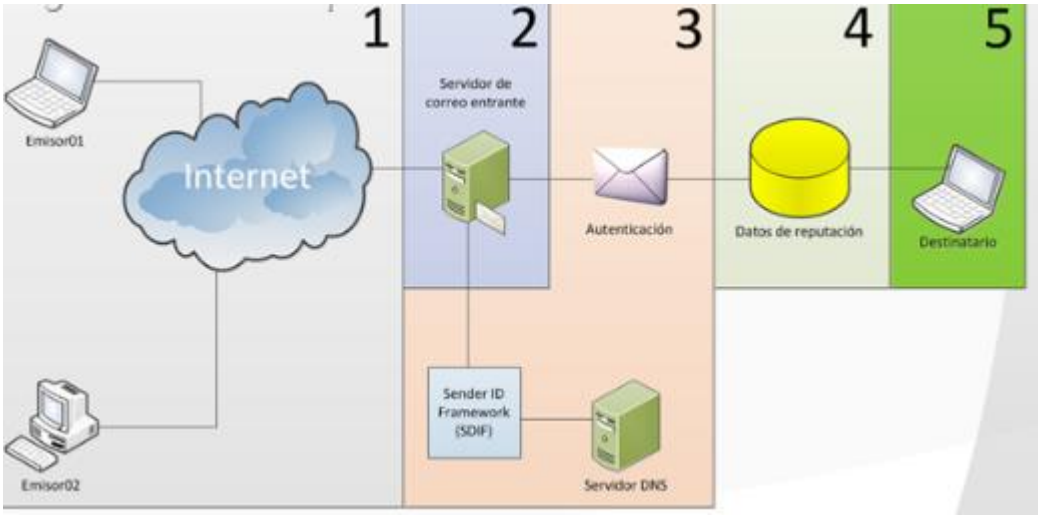


Fig15.Grafica de flujo de validación SPF

El registro SPF tiene la siguiente sintaxis.

v=spf1 ip4:192.168.0.1/16 –all

Que quiere decir que todas las IPs están permitidas en el rango de 192.168.0.1 y 192.168.255.255

Es decir si el receptor valido el flujo de correo desde una IP anterior quiere decir que es correcto el envío.

Analicemos el registro SPF de Nextel de Mexico que ahora tiene publicado.

v=spf1 a ptr a:info.nextel.com.mx ip4:201.130.47.31 ip4:201.130.47.17 ip4:201.130.47.39 ip4:201.130.47.14 ip4:201.130.47.89 mx:mailhost3.nextel.com.mx mx:mailhost2.nextel.com.mx mx:mailhost.nextel.com.mx include:_spf.google.com ~all

Esto quiere decir que el receptor tiene que validar solo las IPs permitidas que son:

+	ip4	201.130.47.31	Pass	Match if IP is in the given range
+	ip4	201.130.47.17	Pass	Match if IP is in the given range
+	ip4	201.130.47.39	Pass	Match if IP is in the given range
+	ip4	201.130.47.14	Pass	Match if IP is in the given range
+	ip4	201.130.47.89	Pass	Match if IP is in the given range

IPs válidas para enviar trafico SMTP

Además deben validar que cuadre con el registro MX en el DNS.

+	mx	mailhost3.nextel.com.mx	Pass	Match if IP is one of the MX hosts for given domain name
+	mx	mailhost2.nextel.com.mx	Pass	Match if IP is one of the MX hosts for given domain name
+	mx	mailhost.nextel.com.mx	Pass	Match if IP is one of the MX hosts for given domain name

Registro MX

Y que incluya también el registro SPF del dominio Google.

+	include	_spf.google.com	Pass	The specified domain is searched for an 'allow'.

Redireccionamiento a Registro SPF de Google

El beneficio de esta configuración es certificar la autenticidad del dominio que origina el correo.

Se eliminó autenticación anónima y se sincronizo con el Controlador de Dominio.

Se tenía autenticación anónima para poder conectarse y enviar correo a través de Antispam y se implementó autenticación explicita que valida las credenciales con el Controlador de Dominio y en caso de no coincidir se rechaza la solicitud de correo, en caso de coincidir se procesa.

La ventaja es tener un parámetro más de seguridad, “algo que sabes” que es la contraseña, no mitiga el riesgo de que la contraseña sea compartida o comprometida pero minimiza la posibilidad.

Se depuro las IPs con privilegio de enviar correo (Relay) a través de la herramienta Antispam y se implementó proceso de control periódico para ellas.

Se realizó mantenimiento de muchas IPs que ya no tenían flujo de correo y se identificó plenamente los responsables de las IPs que tenían permisos para enviar correo por medio de relay, lo que permitió mejorar el control de acceso a envío de correo y con ello una reacción más efectiva.

Se dio de alta el servicio Smart Network Data Services de Hotmail para monitorear el comportamiento del envío de correo desde el dominio de Nextel.

Se habilitó el servicio de SNDS de Hotmail que es una herramienta de apoyo para validar el comportamiento de correo enviado al dominio Hotmail.

The date and times in the displayed data below are rendered into your preferred timezone:
(GMT-06:00) Guadalajara, Mexico City, Monterrey - New (edit)

Activity period [?]	RCPT commands [?]	DATA commands [?]	Message recipients [?]	Filter result [?]	Complaint rate [?]	Trap message period [?]	Trap hits [?]	Sample HELO [?]	Sample MAIL FRO
Total: 80 days	3,747,671	300,915	402,239	0 red days	< 0.1%		34	1 distinct values	65 distinct values
3/29/2011 7:00 AM - 3/30/2011 1:00 AM	167372	2584	3619		< 0.1%	3/29/2011 10:28 AM - 3/29/2011 10:28 AM	1	MAILHOST.nextel.com.mx	ana.zamorano@next
3/23/2011 1:00 AM - 3/24/2011 1:00 AM	254013	5187	6595		< 0.1%		0	MAILHOST.nextel.com.mx	reyna.navarro@next

Fig16. Muestra de comportamiento de correo hacia Hotmail

Donde tiene algunos parámetros a evaluar para considerar un problema en el comportamiento.

Por ejemplo si el campo Filter Result está en verde quiere decir que el comportamiento de flujo de correo es normal, si esta en rojo quiere decir que hay un comportamiento de Spam, si esta en amarillo hay un riesgo de comportamiento de Spam.

Result	Example	Verdict percentage
Green		Spam < 10%
Yellow		10% < spam < 90%
Red		Spam > 90%

Tabla8. Tabla de criterio de Hotmail para catalogar como Spam

Esta herramienta ayuda a monitorear el comportamiento del flujo de correo hacia el dominio Hotmail que va de ~60 a 70 % del total de correos.

5.5 Conclusiones

Al final del proyecto se redujo considerablemente los problemas de Spam y los constantes bloqueos de la IP Publica por mala reputación, el objetivo fue alcanzado.

La mejora es implementar un esquema de HA (High Availability) alta disponibilidad, ya que si alguno de las cajas de Antispam falla, se tiene que direccionar de forma manual el flujo de correo.

Se recomienda implementar una herramienta más robusta que tenga módulo de auto servicio (self-service) para que los usuarios puedan permitir o negar los correos que esperan o no recibir.

CONCLUSIONES GENERALES

La profesión de Ingeniería requiere disciplina, dedicación, constante preparación y debe adecuarse al ambiente, según los intereses de la empresa o sociedad donde se desarrolla e incluso el presupuesto para la misma, no obstante el resultado será directamente proporcional al esfuerzo y dedicación que se le invierta.

El Instituto Politécnico Nacional desarrolla la capacidad de análisis, constante actualización, ímpetu y brinda prestigio en el ambiente profesional, es un privilegio pertenecer a esta institución.

La especialidad de computación me brindo las herramientas necesarias para desarrollarme profesionalmente en el área de Tecnología de la Información y especializarme en el área de Seguridad TI o seguridad informática o seguridad de la información que son sinónimos, y el tronco común de la Ingeniería en Comunicaciones y Electrónica me dio las bases para ser competitivo y desarrollar nuevas tecnologías, me dio capacidad de análisis para poder llevar a cabo el calificativo Ingeniería.

El área de Seguridad TI como prefiero llamarla porque engloba ambos rubros información y la tecnología que mueve la información es una de las áreas con mayor futuro porque ahora que la información es completamente digital, se deben desarrollar tecnologías y metodologías para resguardarla.

El modelo de Seguridad TI a según los expertos consta de tres elementos fundamentales que son:

- ✓ Confidencialidad
- ✓ Integridad
- ✓ Disponibilidad

Estos tres elementos se deben cumplir para garantizar que la información es segura, la confidencialidad es un elemento que siempre se ha buscado en cuanto a seguridad se refiere, es el elemento que por sí solo previene la divulgación no autorizada de información por quienes no tienen la necesidad o los derechos para verla.

La Integridad es el elemento que refiere los esfuerzos para prevenir la modificación inapropiada o no autorizada de sistemas e información.

La Disponibilidad se refiere al esfuerzo que se hacen para prevenir la interrupción de los servicios y la productividad.

Como menciona la Seguridad TI está en auge y debemos estar a la vanguardia del desarrollo y de implementar mejores prácticas.

La Seguridad TI viene acompañada de procesos, metodologías, líneas base, mejores prácticas como ITIL, Cobit, la norma ISO 27001, estándares PCI, etc.

Existen también certificaciones que avalan el nivel de conocimiento en el área de Seguridad TI como CISA, CISSP, Pen Testing, CCNA Security +, CISM, entre otras.

Que en conjunto son herramientas y caminos a seguir para minimizar lo más posible el riesgo de comprometer información, pero nunca se estará cien por ciento seguro, en otras palabras todo es vulnerable solo depende del tiempo y los recursos invertidos en vulnerarlo.

GLOSARIO

Spam: correo basura o mensaje basura, mensajes no solicitados no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. La palabra spam proviene de la segunda guerra mundial, cuando los familiares de los soldados en guerra les enviaban comida enlatada; entre estas comidas enlatadas estaba una carne enlatada llamada spam, que en los Estados Unidos era y sigue siendo muy común.

Spoofing: en términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

Se pueden clasificar los ataques de spoofing, en función de la tecnología utilizada. Entre ellos tenemos el IP spoofing (quizás el más conocido), ARP spoofing, DNS spoofing, Web spoofing o email spoofing, aunque en general se puede englobar dentro de spoofing cualquier tecnología de red susceptible de sufrir suplantaciones de identidad.

DNS (Domain Name System): es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

El servidor DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

Registro SPF (Convenio de Remitentes, del inglés Sender Policy Framework): es una protección contra la falsificación de direcciones en el envío de correo electrónico. Identifica, a través de los registros de nombres de dominio (DNS), a los servidores de correo SMTP autorizados para el transporte de los mensajes.

Este convenio puede significar el fin de abusos como el spam y otros males del correo electrónico. Pero aún no está estandarizado a nivel internacional.

SPF extiende el protocolo SMTP para permitir comprobar las máquinas autorizadas a enviar correo para un dominio determinado. La idea es identificar las máquinas autorizadas por su dirección IP, y que esta identificación la haga el responsable del dominio que recibirá el correo.

Una aproximación a la solución podría suponer que el remitente del correo, hace los envíos desde la misma máquina que los recibe. Como se puede resolver la dirección IP a donde se enviarían correos al remitente a través del registro MX del servicio DNS (RMX, del inglés Reverse MX), si esta dirección coincide con la que genera el envío, se puede entender que es el remitente real.

Registro MX (del inglés Mail eXchange record: es un tipo de registro, un recurso DNS que especifica cómo debe ser encaminado un correo electrónico en internet. Los registros MX apuntan a los servidores a los cuales envían un correo electrónico, y a cuál de ellos debería ser enviado en primer lugar, por prioridad.

Reverse MX: Existen varias soluciones de reverse MX, pero el objetivo es el mismo, el servidor receptor quiere confirmar que el correo recibido proviene de un servidor autorizado para enviarlos con el dominio origen.

El nombre del dominio que el servidor receptor valida puede ser por:

- Header
- Reply-to
- From Command
- Nombre de dominio que regresa la consulta al DNS

Simple Mail Transfer Protocol (SMTP): es un protocolo de la capa de aplicación. Protocolo de red basado en texto, utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos.

Resumen del funcionamiento del protocolo SMTP.

- Cuando un cliente establece una conexión con el servidor SMTP, espera a que éste envíe un mensaje “220 Service ready” o “421 Service non available”
- Se envía un HELO desde el cliente. Con ello el servidor se identifica. Esto puede usarse para comprobar si se conectó con el servidor SMTP correcto.

- El cliente comienza la transacción del correo con la orden MAIL FROM. Como argumento de esta orden se puede pasar la dirección de correo al que el servidor notificará cualquier fallo en el envío del correo (Por ejemplo, MAIL FROM:<fuente@host0>). Luego si el servidor comprueba que el origen es válido, el servidor responde “250 OK”.

- Ya le hemos dicho al servidor que queremos mandar un correo, ahora hay que comunicarle a quien. La orden para esto es RCPT TO:<destino@host>. Se pueden mandar tantas órdenes RCPT como destinatarios del correo queramos. Por cada destinatario, el servidor contestará “250 OK” o bien “550 No such user here”, si no encuentra al destinatario.

- Una vez enviados todos los RCPT, el cliente envía una orden DATA para indicar que a continuación se envían los contenidos del mensaje. El servidor responde “354 Start mail input, end with <CRLF>.<CRLF>” Esto indica al cliente como ha de notificar el fin del mensaje.

- Ahora el cliente envía el cuerpo del mensaje, línea a línea. Una vez finalizado, se termina con un <CRLF>.<CRLF> (la última línea será un punto), a lo que el servidor contestará “250 OK”, o un mensaje de error apropiado.

- Tras el envío, el cliente, si no tiene que enviar más correos, con la orden QUIT corta la conexión. También puede usar la orden TURN, con lo que el cliente pasa a ser el servidor, y el servidor se convierte en cliente. Finalmente, si tiene más mensajes que enviar, repite el proceso hasta completarlos.

Puede que el servidor SMTP soporte las extensiones definidas en el RFC 1651, en este caso, la orden HELO puede ser sustituida por la orden EHLO, con lo que el servidor contestará con una lista de las extensiones admitidas. Si el servidor no soporta las extensiones, contestará con un mensaje "500 Syntax error, command unrecognized".

Las órdenes básicas de SMTP:

- HELO, para abrir una sesión con el servidor
- MAIL FROM, para indicar quien envía el mensaje
- RCPT TO, para indicar el destinatario del mensaje
- DATA, para indicar el comienzo del mensaje, éste finalizará cuando haya una línea únicamente con un punto.
- QUIT, para cerrar la sesión
- RSET Aborta la transacción en curso y borra todos los registros.
- SEND Inicia una transacción en la cual el mensaje se entrega a una terminal.
- SOML El mensaje se entrega a un terminal o a un buzón.
- SAML El mensaje se entrega a un terminal y a un buzón.
- VRFY Solicita al servidor la verificación del argumento.
- EXPN Solicita al servidor la confirmación del argumento.
- HELP Permite solicitar información sobre un comando.
- NOOP Se emplea para reiniciar los temporizadores.
- TURN Solicita al servidor que intercambien los papeles.

Una vez que el servidor recibe el mensaje finalizado con un punto puede almacenarlo si es para un destinatario que pertenece a su dominio, o bien retransmitirlo a otro servidor para que finalmente llegue a un servidor del dominio del receptor.

Un ejemplo de la transmisión de un correo por línea de comandos y se puede visualizar el protocolo SMTP es:

```
: 220 Servidor ESMTP

C: HELO miequipo.midominio.com
S: 250 Hello, please to meet you
C: MAIL FROM: <yo@midominio.com>
S: 250 Ok
C: RCPT TO: <destinatario@sudominio.com>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: Subject: Campo de asunto
C: From: yo@midominio.com
C: To: destinatario@sudominio.com
C:
C: Hola,
C: Esto es una prueba.
C: Hasta luego.
C:
C: .
S: 250 Ok: queued as 12345
C: quit
S: 221 Bye
```

Antispam (Mail Filter): El antispam es el método para prevenir el "correo basura". Tanto los usuarios finales como los administradores de sistemas de correo electrónico utilizan diversas técnicas contra ello. Algunas de estas técnicas han sido incorporadas en productos, servicios y software para aliviar la carga que cae sobre usuarios y administradores. No existe la fórmula perfecta para solucionar el problema del spam por lo que entre las múltiples existentes unas funcionan mejor que otras, rechazando así, en algunos casos, el correo deseado para eliminar completamente el spam, con los costos que conlleva de tiempo y esfuerzo.

Las técnicas antispam se pueden diferenciar en dos técnicas de filtrado, locales y no locales, una técnica local es colocar diccionarios de palabras para contener correos con palabras contenidas en los diccionarios, una técnica no local es la configuración del registro SPF.

IP Pública: Es la que tiene asignada cualquier equipo o dispositivo conectado de forma directa a Internet. Algunos ejemplos son: los servidores que alojan sitios web como Google, los router o módems que dan a acceso a Internet a otros elementos de hardware que forman parte de su infraestructura. Las IP públicas son siempre únicas. No se pueden repetir.

IP Privada: Se utiliza para identificar equipos o dispositivos dentro de una red doméstica o privada. En general, en redes que no sean la propia Internet y utilicen su mismo protocolo.

Las IP privadas están en cierto modo aisladas de las públicas. Se reservan para ellas determinados rangos de direcciones. Son estos:

- Para IPv4

  De 10.0.0.0 a 10.255.255.255

  172.16.0.0 a 172.31.255.255

  192.168.0.0 a 192.168.255.255

  169.254.0.0 a 169.254.255.255

DMZ (Zona Desmilitarizada): En terminología militar, una zona desmilitarizada o zona neutral es un área, por lo general la frontera o límite entre dos o más potencias militares (o alianzas), donde la actividad militar no está permitida, por lo general por medio de un tratado de paz, un armisticio u otros acuerdos bilaterales o multilaterales. A menudo una zona desmilitarizada se encuentra en una línea de control y constituye una frontera internacional de facto, lo mismo para las redes.

Role Base Access Control (RBAC).

Es una metodología adoptada por el NIST National Institute of Standards and Technology que ha sido utilizada desde finales de 1960 y principios de 1970, sin embargo surge en la década de los 90 como una tecnología prometedora para gestión y aplicación de la seguridad en toda empresa a gran escala, en gran parte a la inexistente mejora en el tradicional Mandatory Access Control (MAC) and Discretional Access Control (DAC) usada en muchos sistemas y redes, por lo tanto RBAC es una metodología alternativa a las metodologías MAC y DAC además de ser viable de implementar en empresas a gran escala.

ANEXO1. REFERENCIA DE TABLAS Y GRAFICAS

TABLAS.

FIGURAS

es.wikipedia.org/wiki/Spoofing
http://osvdb.org/
http://nvd.nist.gov/home.cfm

Fig12. Log Error. Propietaria

Fig13. Logs SMTP.
http://technet.microsoft.com/en-us/library/cc482977.aspx

Fig14.Diagrama Antispam. Propietaria

Fig15.Grafica de flujo de validación SPF
http://support.google.com/a/bin/answer.py?hl=es-419&hlrm=es&answer=33786
https://postmaster.live.com/snds/?lc=1033
http://www.ietf.org/rfc/rfc4408.txt

Fig16. Muestra de comportamiento de correo hacia Hotmail
https://postmaster.live.com/snds/?lc=1033

BIBLIOGRAFÍA

Libro 1
Título: The UNIX Programing Environment
Autor: Brian Kernighan
Editorial: Rob Pike
Año de edición: 1993

Libro 2
Título: DNS and BIND
Autor: Criket Liu & Paul Albitz
Editorial: O´REILLY
Año de edición: 1998

Libro 3
Título: OFICIAL (ISC)2 GUIDE TO THE CISSP CBK
Autor: Harold F. Tipton
Editorial: CRC Taylor&Francis Group
Año de edicion: 2012

Libro 4
Título: ALL IN ONE CISSP
Autor: Shon Harris
Editorial: McGrawn Hill
Año de edición: 2010

Libro 5
Título; Security in Computing, 4th Edition
Autorr: Charles P. Pfleeger and Shari Lawrence
Editorial: Pfleeger
Año de edición: 2003

REFERENCIAS DE INTERNET

http://csrc.nist.gov/groups/SNS/rbac/case_studies.html

http://www.microsoft.com/mscorp/safety/content/technologies/senderid/wizard/default.aspx

http://answers.microsoft.com/en-us/windowslive/forum/email/why-are-the-emails-sent-to-hotmail-rejected-for/b64e3e4a-0d93-40c8-8e28-4be849012f9c

http://nvd.nist.gov/home.cfm

http://www.sans.org/newsletters/

http://sectools.org/tag/vuln-scanners/

http://technet.microsoft.com/en-us/library/cc482977.aspx

http://www.cgisecurity.com/

www.symantec.com