UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

"CREACIÓN DE UN CENTRO DE MONITOREO EN SEGURIDAD INFORMÁTICA"

INFORME DE ACTIVIDADES PROFESIONALES

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A :

ADRIAN QUINTANAR MONDRAGÓN

ASESOR:

M. C. ALEJANDRO VELÁZQUEZ MENA

2014

JURADO ASIGNADO

Presidente:	M.C. MARÍA JAQUELINA LÓPEZ BARRIENTOS
Vocal:	M.C. ALEJANDRO VELÁZQUEZ MENA
Secretario:	M.I. JORGE VALERIANO ASSEM
1er Suplente:	DR. VICTOR RANGEL LICEA
2do Suplente:	M.I. ÁNGEL CÉSAR GOVANTES SALDIVAR

Lugar donde se realizó el informe: MÉXICO, D.F.

ASESOR:

M.C. ALEJANDRO VELÁZQUEZ MENA

FIRMA

Dedicatoria

A Dios por darme la fortaleza y paciencia para realizar este sueño.

A mis padres Fernando y Yolanda, por apoyarme de principio a fin en mis estudios y proporcionarme los recursos necesarios para lograr esta meta.

A mi hermano Fer por la paciencia que me tuvo durante las noches de estudios.

A mi novia Verónica por estar en mi vida y presente en la realización de éste trabajo, quien me impulsa a ser mejor cada día.

A mi familia por sus consejos y por todo su cariño.

A todos mis grandes amigos por brindarme su amistad y apoyo incondicional.

"Comienza haciendo lo que es necesario,
después lo que es posible y de repente
estarás haciendo lo imposible"
San Francisco de Asís

Agradecimientos

A la Universidad Nacional Autónoma de México por brindarme una firme base académica, profesional y humana, desde mis estudios en el Colegio de Ciencias y Humanidades hasta concretar mis estudios en la honorable Facultad de Ingeniería.

A la empresa Sm4rt Security Services por darme la oportunidad y el apoyo necesario para desarrollar el presente informe.

A mis sinodales por guiarme en este proceso, la asesoría, sus consejos y aportaciones me permitieron concluir con esta importante etapa de mi formación académica.

Adrián Quintanar Mondragón

ÍNDICE

Índice de Figuras III
Índice de Tablas III
Resumen IV
CAPÍTULO I 1
INTRODUCCIÓN 1
1.1 Seguridad Informática 1
1.2 Antecedentes 2
1.3 Definición del problema 2
1.4 Objetivos 3
1.5 Contribuciones 3
1.6 Estructura del informe 3
CAPÍTULO II 5
ESTRUCTURA ORGANIZACIONAL 5
2.1 Organización 5
2.2 Actividades desempeñadas 6
CAPÍTULO III 9
DESCRIPCIÓN DE PROYECTOS 9
3.1 Objetivo General 9
3.2 Proyecto Evaluación de un Dispositivo de Detección de Intrusos (SIEM). 9
3.2.1 Objetivo 9
3.2.2 Descripción 9
3.3 Proyecto Aseguramiento de Activos Críticos 13
3.3.1 Objetivo 13
3.3.2 Descripción 13
CAPÍTULO IV 15
CREACIÓN DE UN CENTRO DE MONITOREO EN SEGURIDAD INFORMÁTICA 15
4.1 Objetivo 15
4.2 Descripción del Proceso Global 15
4.3 Análisis inicial 17
4.3.1 Declaración de servicios 18

4.3.2 Catálogo de Servicios 20
4.3.3 Responsabilidades del Área de Monitoreo-ISO 21
4.4 Registro de Turnos 25
4.4.1 Registro de Entrada 26
4.4.2 Registro de Salida 28
4.4.3 Registro de Administradores 30
4.5 Alertamiento y Monitoreo 30
4.5.1 Escalamiento Interno 32
4.5.2 Estado de los dispositivos 33
4.5.3 Monitoreo 45
4.5.4 Comunicación de Alertas 47
4.5.5 Generación de reportes mensuales 47
4.5.6 Proceso de Guardia 51
4.6 Cambios y Requerimientos 52
4.6.1 Generación de cambios 54
4.6.2 Requerimientos 54
4.6.3 Investigación 58
4.6.4 Planeación de visitas 59
4.6.5 Reportes ad hoc 60
4.7 Liberación de Servicio 60
CAPÍTULO V 62
RESULTADOS 62
4.1 Aportación Empresarial 62
4.2 Aportación Personal 62
CONCLUSIONES 65
GLOSARIO 69
REFERENCIAS 72

Índice de Figuras

2.1 Estructura General de Sm4rt Security Services……4

4.1 Proceso Global de Monitoreo...…….16

4.2 Metodología servicio de Monitoreo..……19

4.3 Registro de turno (Entrada)…….27

4.4 Registro de turno (Salida)…….29

4.5 Registro de turno (Administradores)……31

4.6 Matriz de Escalamiento…….34

4.7 Diagrama de Flujo de Monitoreo...……46

4.8 Comunicación de Alertas...……48

4.9 Proceso de Guardia...…….53

4.10 Flujo de Generación de Cambios....…….55

4.11 Flujo de Solicitud de Requerimientos Cliente/ISO/Monitoreo……...57

Índice de Tablas

4.1 Horario de atención…..……20

4.2 Horario de guardias……..……20

4.3 Eventos Windows……..……36

4.4 Eventos en UNIX……..……..36

4.5 Eventos en Base de Datos.……37

4.6 Eventos en Aplicaciones…...……37

4.7 Eventos en Dispositivos de Red…...……37

4.8 Clasificación de severidad de firmas……48

Resumen

El presente documento tiene la finalidad de dar a conocer las distintas actividades y proyectos que me permitieron realizar la planeación, creación y gestión de un área de servicios de monitoreo, trabajo realizado en la empresa Sm4rt Security Services.

Mi ingreso a Sm4rt en el mes de Agosto de 2011, representó un gran reto en mi crecimiento profesional, mi experiencia en el área de la seguridad era prácticamente nula, ya que a partir del término de mis créditos de la carrera a finales del año 2009, estuve laborando en proyectos de migración en la arrendadora Informática Aurum durante todo el año 2010 y posteriormente en el área de soporte técnico para la consultoría STAFF Informático donde laboré alrededor de 6 meses. Las actividades que en Sm4rt se realizan, entre las que destacan la administración de riesgos y la atención a incidentes de seguridad, me parecen muy interesantes y me encontraba motivado para afrontar el reto, lo cual me brindó la oportunidad de laborar con ellos.

Desde mi integración a Sm4rt, he tenido la oportunidad de participar en algunos proyectos y uno de ellos, el cual es el tema principal del presente reporte, es la creación de un área de servicios de monitoreo. Durante dicho proceso, me involucré en la participación de un proyecto a corto plazo, el cual consistía en la evaluación de un centralizador y correlacionador de eventos.

He laborado en la empresa Sm4rt durante dos años y 4 meses, pertenecí al área de monitoreo un año y medio, siendo analista de herramientas de seguridad, realizando tareas de monitoreo sobre sistemas de detección y prevención de intrusos, actividad en base de datos y administrando de igual forma, programas para el escaneo de vulnerabilidades de diversos sistemas operativos. Posteriormente me integré al área donde me encuentro hoy en día, Administración de Riesgos. He ido adquiriendo experiencia en el análisis, seguimiento y documentación a incidencias de seguridad, atención a requerimientos como escaneos éticos así como la elaboración de distintos reportes haciendo de su conocimiento al cliente, las recomendaciones de mejora para una mayor protección de la información.

CAPÍTULO I

INTRODUCCIÓN

1.1 Seguridad Informática

La Seguridad Informática [2] es la disciplina que se ocupa de diseñar normas, procedimientos y herramientas, orientados a proveer condiciones seguras y garantizar la disponibilidad, integridad y confidencialidad de los datos que residen en distintos sistemas de información.

Consiste en asegurar que los recursos del sistema informático de una organización sean utilizados correctamente y que el acceso a la información allí contenida, así como su modificación, sólo sea posible por las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Para lograr sus objetivos, la seguridad informática se fundamente en tres principios, que debe cumplir todo sistema informático:

Confidencialidad: Se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático. Se debe proteger los sistemas del acceso de personas o programas no autorizados.

Integridad: Se refiere a la validez y consistencia de los elementos de información almacenados y procesados en un sistema informático, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos.

Disponibilidad: Se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático. Es importante que los sistemas informáticos cuyo compromiso con el usuario, sea prestar servicio permanente.

1.2 Antecedentes

Sm4rt Security Services ya contaba con varios clientes importantes del sector privado, los cuales manejan grandes cantidades de información y están conformados por un alto número de personal. Dichos clientes, principalmente dedicados a ofrecer servicios de televisión de paga e Internet, tienen un alto flujo de información, tanto interna como externamente, por lo cual tenían la preocupación por proteger la información de sus activos críticos de sistemas o personas ajenas al negocio.

Uno de las posibles consecuencias de una intrusión a la red del cliente, es la pérdida de datos. Es un hecho frecuente y ocasiona muchos trastornos, sobre todo si no están al día de las copias de seguridad o no cuentan con un proceso periódico para la realización de dichas copias y validar la integridad de las mismas

Otro de los problemas más dañinos es el robo de información sensible y confidencial. La divulgación de la información que posee una empresa sobre sus clientes puede acarrear demandas millonarias contra esta.

Derivado de los puntos comentados anteriormente, surgió la importante necesidad de contar con un centro de monitoreo, donde Sm4rt apoyara al cliente con el cuidado de la información que reside en sus sistemas informáticos, críticos para la continuidad del negocio.

1.3 Definición del problema

La idea de crear un centro de monitoreo surge de la importancia de gestionar controles de seguridad informática en las organizaciones. Hoy en día existen diversas herramientas de seguridad que las empresas adquieren para el resguardo y monitoreo de su información.

Sm4rt al no contar con un área dedicada a ofrecer servicios de monitoreo, aunado a la creciente actividad de virus y ataques informáticos, se presentó la oportunidad de participar en el proyecto, el cuál fue un reto llevarlo a cabo, comenzando desde la propuesta de la creación del área hecha a los gerentes de la propia empresa, pasando por los requisitos técnicos hasta concretar la idea de llevar a cabo una operación idónea en el monitoreo y respuesta a incidentes en los distintos clientes con los que cuenta Sm4rt.

1.4 Objetivos

- El objetivo de la creación del área de monitoreo, es gestionar de forma reactiva y proactiva las amenazas, vulnerabilidades y en general incidentes de seguridad informática, con el objetivo de minimizar y controlar el impacto en la organización.
- Apoyar y asesorar al cliente para la administración, operación y rendimiento óptimo de herramientas de seguridad.
- Concientizar sobre los riesgos a los que las organizaciones y usuarios de computadoras se enfrentan en materia de seguridad de la información

1.5 Contribuciones

El principal aporte de la creación de un centro de monitoreo en la empresa Sm4rt, fue haber concretado un área la cual es un negocio base hoy en día de la empresa y que su principal cometido es asesorar al cliente en la protección de sus sistemas informáticos.

La consolidación del área ha permitido fortalecer la seguridad en distintos clientes, que se encuentran en el sector público y privado. Mis conocimientos aportados e investigaciones realizadas durante mi estancia en monitoreo, lograron concientizar al cliente de la importancia de una adecuada administración de sus sistemas y dispositivos de seguridad.

1.6 Estructura del informe

El presente informe se encuentra dividido en cuatro principales capítulos:

Dentro del segundo capítulo se da a conocer la estructura organizacional de Sm4rt y las actividades que he desempeñado desde mi estancia en monitoreo hasta el día de hoy como ISO (Information Security Officer).

En el tercer capítulo doy a conocer los proyectos en los cuáles he tenido participación y en los que me encuentro actualmente involucrado, dando una breve explicación de cada uno de ellos, describiendo los objetivos y actividades realizadas en dichos proyectos.

El cuarto capítulo se centra en el tema principal de este informe, dando a conocer las distintas etapas por las cuales atravesó el proyecto sobre la creación del área de monitoreo, desde mi participación como operador del área hasta mis aportaciones como analista, ofreciendo ideas y conocimientos para la mejora y liberación de los servicios.

Entre las actividades realizadas durante mi participación en el proyecto se encuentran la definición del alcance del área, declaración de servicios, el establecimiento de procesos dentro de la misma área así como con él cliente, asignación de tareas y responsabilidades, definición de los entregables y respuesta a incidentes, entre otras actividades más que detallaré en dicho capítulo.

En el quinto capítulo daré a conocer las distintas aportaciones que dejó la creación del centro de monitoreo, tanto para Sm4rt, a los mismos clientes, como para mi crecimiento y desarrollo profesional.

Por último se presenta un apartado que contiene el glosario con los términos manejados durante el presente informe, que conciernen a mi carrera así como las referencias de las distintas fuentes que fueron utilizadas como apoyo para concretar los distintos proyectos en los que he participado.

CAPÍTULO II

ESTRUCTURA ORGANIZACIONAL

2.1 Organización

Sm4rt, una empresa mexicana, altamente especializada en servicios de consultoría de seguridad informática desde el año 2004, tiene la metodología y habilidades para ayudar a reducir el riesgo de la información y asegurar el correcto cumplimiento de la normatividad interna, externa o de gobierno.

En Sm4rt, se brinda consultoría para desarrollar e implementar estrategias de seguridad informática, que cubran los requerimientos de negocio y de la industria. En la figura 2.1 se presenta la estructura general de la conformación de las distintas áreas de Sm4rt Security Services y la relación entre ellas.

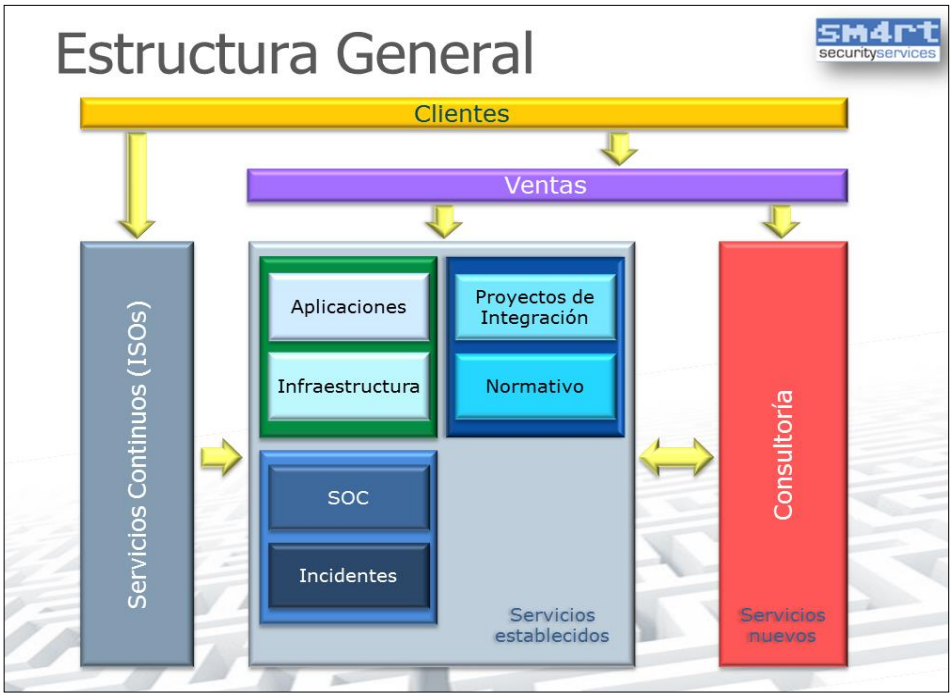


Figura 2.1 Estructura General de Sm4rt Security Services

El área de Consultoría tiene como objetivo el diseño, creación e innovación de soluciones de seguridad y riesgos de información a la medida del cliente. Entre sus servicios está el análisis y definición de estrategias de gestión de riesgos basados en una clasificación avanzada de la información. Esto permite a la organización gestionar y enfocar los esfuerzos de protección de manera eficiente y eficaz.

El área de Evaluación se encarga de llevar a cabo pruebas de penetración, análisis de vulnerabilidades, evaluación y el cumplimiento de seguridad de los activos críticos del cliente.

En el área de Normatividad, los servicios que desempeña son el diseño de políticas y procesos, indicadores de seguridad, diseño de estándares de configuración segura y el seguimiento/cumplimiento del marco normativo.

Monitoreo y respuesta a incidentes, es la parte nueva que se integra a esta estructura y donde se encuentra mi participación principal del proyecto a desarrollar en el presente documento. El objetivo de ésta área es la administración de los dispositivos de seguridad que monitorean cualquier incidencia en los activos más importantes de los clientes y responder de manera adecuada y oportuna a los incidentes.

Y por lo último la parte de servicios continuos, donde hoy en día me encuentro situado como Consultor Jr, la principal tarea de esta área es la administración de riesgos, análisis de riesgos de información y el cumplimiento normativo como lo son SOx (Sarbanes-Oxley) [3], PCI (Payment Card Industry) y LFPDPPP (Ley Federal de Protección de Datos Personales en Posesión de los Particulares) [4].

2.2 Actividades desempeñadas

A continuación daré mención de las actividades que realicé durante mi estadía en el área de servicios de monitoreo, posteriormente describiré las responsabilidades y tareas que tengo asignadas como Oficial de Seguridad de la Información.

Las actividades que desempeñé durante mi estancia en el área de servicios de monitoreo durante un año y medio fueron:

- Monitoreo de recepción de eventos de seguridad (IPS, IDS, DAM, SIEM).
- Monitoreo diario de firmas en los dispositivos IPS & IDS, DAM, SIEM, investigación y clasificación de falsos positivos, actualización de políticas.
- Creación y ejecución de reportes básicos bajo demanda del cliente.
- Creación y ejecución de alertas básicas bajo demanda del cliente.
- Manejo de procedimientos de investigación, notificación y escalamiento para eventos sospechosos u incidentes.
- Creación y documentación para reporte mensual a cliente.
- Capacitación y explicación de actividades para grupo de monitoreo (Actividad Interna).
- Monitoreo de nivel de actualizaciones en los equipos (Firmwares, actualizaciones S.O., parches de seguridad, reléase).
- Escaneo a los activos críticos de los clientes en busca de vulnerabilidades.

Hasta el momento, mi participación en dos de las áreas de Sm4rt, Monitoreo y Administración de Riesgos, me ha permitido desenvolverme profesionalmente y estar adquiriendo nuevas habilidades y conocimientos, incrementando mi interés por el área de la seguridad informática.

Mi trabajo en el área de monitoreo me permitió adquirir las bases necesarias para tomar nuevas responsabilidades en el área de Administración de Riesgos como Oficial de Seguridad de la Información, donde mis actividades se desarrollan directamente en sitio con el cliente.

La principal tarea a cargo como ISO es coordinar las actividades para el cumplimiento de veinte controles de seguridad respecto a la Ley SOx para las aplicaciones críticas del cliente. La Ley Sarbanes-Oxley (SOx) promueve que todas las empresas que cotizan en la bolsa de los Estados Unidos de América, aseguren la existencia y funcionamiento adecuado de controles internos en las diferentes regiones geográficas donde operan, todo esto con el objetivo de garantizar la transparencia de sus operaciones.

Entre las actividades que desempeño actualmente y de las cuales llevo una gestión son:

- Cumplimiento regulatorio y gestión de riesgos de seguridad informática.
- Generación de políticas y estándares
- Administración de vulnerabilidades
- Revisión de controles de seguridad en aplicaciones
- Seguimiento a los riesgos identificados a través del Hackeo ético y escaneos externos
- Revisión de reportes sobre la centralización y correlación de bitácoras de activos críticos.
- Análisis de vulnerabilidades de aplicaciones y su infraestructura

Y los objetivos de cada una de estas actividades las menciono a continuación:

- ✓ Cumplimiento de un marco de control de seguridad informática en la organización, así como la gestión de los riesgos.
- ✓ Difusión de políticas de seguridad informática del corporativo, así como hacer una revisión de la implementación de los estándares.
- ✓ Identificación y seguimiento a las vulnerabilidades internas de seguridad que puedan existir en los activos de las aplicaciones críticas de SOx.
- ✓ Evaluación del nivel de seguridad en las aplicaciones del cliente.
- ✓ Revisión manual de bitácoras de seguridad de las aplicaciones críticas para cumplimiento SOx y de la infraestructura que las soporta (Bases de Datos y Servidores).
- ✓ Revisar el nivel de cumplimiento de controles de seguridad en las aplicaciones, así como en la infraestructura que soporta a las mismas.

CAPÍTULO III

DESCRIPCIÓN DE PROYECTOS

3.1 Objetivo General

El objetivo de esta sección es dar una breve explicación de los proyectos en los que participé durante mi estancia en el área de monitoreo de Sm4rt y en los que me encuentro participando hoy en día como Oficial de Seguridad de la Información.

3.2 Proyecto Evaluación de un Dispositivo de Detección de Intrusos (SIEM).

3.2.1 Objetivo

El objetivo de la evaluación de una herramienta SIEM (Security Information and Event Managment), solicitada por uno de nuestros clientes, es saber si dicho dispositivo cuenta con los requisitos para el cumplimiento de centralización y correlación de eventos como lo establece el estándar de administración y retención de bitácoras.

3.2.2 Descripción

Derivado de la Ley de SOx que nace en Estados Unidos con el fin de monitorear a las empresas que cotizan en la bolsa de valores de Nueva York y sus filiales, uno de nuestros clientes, que ofrece servicios de entretenimiento a través de televisión por suscripción, solicitó el apoyo para evaluar una herramienta SIEM, con el objetivo de cumplir con uno de los controles que se establecen en la Ley SOx. Dicho control tiene como objetivo la implementación de un mecanismo de monitoreo en los sistemas para identificar violaciones de seguridad.

La centralización de bitácoras consta de almacenar y normalizar cada uno de los eventos de seguridad que son enviados o extraídos de los diferentes dispositivos por protocolos o métodos definidos por el centralizador.

Con el objetivo de Sm4rt en apoyar a sus clientes con el cumplimiento de la ley ya mencionada, el área de normatividad ha desarrollado estándares, uno de ellos es el de administración y retención de bitácoras, el cual tiene la finalidad de acotar los lineamientos necesarios para la generación de bitácoras (logs). El uso de estos archivos debe permitir el monitoreo y correlación de eventos, y la reconstrucción de información en caso de algún incidente de Seguridad.

La implementación y evaluación de la herramienta SIEM para el cliente se dividió en dos fases:

a) Fase 1: Integración e implementación del SIEM
    a. Centralizar bitácoras por plataformas
        i. Servidores Windows
            1. Accesos
            2. Administración de cuentas y grupos
            3. Bloqueo de cuentas
            4. Reinicio de contraseñas
            5. Borrado de Log de Seguridad
            6. Cambios en las políticas
            7. Encendido, Apagado, Reinicio
        ii. Servidores UNIX
            1. Accesos
            2. Administración de usuarios ABC
            3. Comando SU, SUDO, FTP
            4. Encendido, Apagado, Reinicio
        iii. Bases de Datos
            1. Accesos
            2. Creación de usuarios
            3. Eliminación de usuarios

4. Creación de tablas
5. Alteración de tablas
6. Eliminación de tablas
7. Asignación / Revocación de permisos
8. Encendido, Apagado

iv. Dispositivos de Red

1. Accesos
2. Cambios de configuración
3. Eventos AAA
4. Violaciones ACL

b) Fase 2: Puntos a evaluar del SIEM

a. Extracción y Recuperación

i. Lista de plataformas soportadas sin la necesidad de un desarrollo de un traductor

ii. Validación de recepción de eventos en el SIEM utilizando diferentes clientes

iii. Integración de activos con acceso al motor de correlación en tiempo real

b. Almacenamiento y normalización

i. Arquitectura de la tecnología

ii. Qué tamaño de almacenamiento manejan

iii. Tiempo que se guardan las bitácoras

iv. Periodos de actualización

v. Capacidad de interpretar cada uno de los códigos o tipos de eventos de las diferentes plataformas para dispositivos que no generan detalle

c. Procesamiento y presentación

i. Capacidad de realizar una correlación de datos en tiempo real y/o histórico

ii. Tipo de alertas

iii. Tipo de reportes

iv. Personalizar plantillas para la generación de reportes por plataforma.

d. Soporte

i. Capacidad de realizar una correlación de datos en tiempo real y/o histórico

ii. Tipo de alertas

iii. Se pueden configurar más reglas

iv. Tipo de reportes

v. Personalizar plantillas para la generación de reportes por plataforma.

Una vez llevadas a cabo las dos fases anteriores en el periodo de Octubre de 2011 a Enero de 2012, se identificaron los siguientes problemas:

- Generación de estadísticas y análisis de modo general; No se tiene la capacidad para analizar datos respecto a activos (distinción por tipo)
- El crecimiento de registros de modo exponencial implica poco espacio. Se estima el consumo total del disco en menos de dos meses con los activos actualmente centralizados
- Soporte. El personal especializado en la herramienta se encuentra en EU
- Se identifican las siguientes limitantes en la herramienta:
  - Storage. No es expandible por medios externos o del fabricante; para aumentar el espacio y capacidad de almacenamiento se requiere de la implementación de modelos con mayor capacidad
  - Depuración. No es posible efectuar depuración de registros para liberar espacio. Afecta a enviados y almacenados. El único modo de liberación es la eliminación de eventos de manera remota y mediante el proveedor.
  - Centralización. Falta de traductores o agentes que ayuden a la recolección y envío de logs de acuerdo a la infraestructura del cliente.

Para concluir la evaluación del dispositivo, se dieron a conocer los resultados finales al cliente, donde la herramienta SIEM, no cumplió con los requisitos establecidos en el estándar de retención de bitácoras, llevando a cabo el análisis y evaluación de una

herramienta SIEM con un distinto proveedor, con el que hoy en día opera satisfactoriamente el centro de monitoreo.

3.3 Proyecto Aseguramiento de Activos Críticos

3.3.1 Objetivo

Mediante la revisión de aplicaciones y escaneos internos, es posible identificar vulnerabilidades que pueden poner en riesgo la confidencialidad, integridad y disponibilidad en la información del cliente.

3.3.2 Descripción

Cada año, se elabora una estrategia para identificar las vulnerabilidades en los activos críticos del cliente y de esta forma, trazar un plan de trabajo que nos permita atacar estos riesgos de forma proactiva antes de que sea explotada la vulnerabilidad. Esta actividad la he realizado a partir de Noviembre de 2012, fecha en que tomé el cargo de ISO en el cliente que se dedica al negocio de los centros de entretenimiento y sorteo de números.

El aseguramiento de los activos y aplicaciones críticas del cliente consta de lo siguiente:

1.- Administración de vulnerabilidades de activos críticos

Actividades

- Identificación de vulnerabilidades a través de escaneos periódicos:
  - Definición junto con el cliente las direcciones IP a escanear.
  - Definir un calendario anual de las direcciones IP a escanear mes con mes.
- Reporte y escalamiento de vulnerabilidades a los responsables por parte del cliente:
  - Ejecución de los escaneos a través de una herramienta especializada.
  - Identificación de las vulnerabilidades de seguridad y sus posibles soluciones de mitigación.
  - Elaboración y entrega del reporte de hallazgos al cliente
- Seguimiento a las actividades de mitigación:
  - Definición del plan de mitigación con el cliente.

- Obtención de evidencia de la mitigación.

2.- Administración de vulnerabilidades de aplicaciones

Actividades

- Evaluar periódicamente las aplicaciones críticas del negocio, que incluye la revisión de los siguientes módulos:
  - Autenticación
  - Validación de entrada de datos
  - Administración de la configuración
  - Cifrado de la información
  - Bitácoras
  - Manejo de sesiones
  - Gestión de errores
- Definición de los controles de seguridad que se deben incluir en el desarrollo y/o adquisición de aplicaciones.
- Emisión de acciones de mitigación de vulnerabilidades.
- Seguimiento a la implementación de controles de seguridad en las aplicaciones.

Cabe mencionar que la mitigación de vulnerabilidades se lleva a cabo durante todo el año, trazando un plan que se adapte a la situación del negocio sin afectar las operaciones y evitando implicaciones en sus activos críticos por lo cual es importante validar los tiempos disponibles para ejecutar las tareas de mitigación.

CAPÍTULO IV

CREACIÓN DE UN CENTRO DE MONITOREO EN SEGURIDAD INFORMÁTICA

4.1 Objetivo

El proyecto de la creación de un centro de monitoreo tiene como objetivo gestionar de forma reactiva y proactiva las amenazas, vulnerabilidades y en general los incidentes de seguridad informática.

Proporcionar soluciones rápidas y eficaces frente a incidentes de seguridad, mejorando la operación y tratamiento de la información a través de la gestión y monitoreo continuo, en análisis de logs y la respuesta inmediata a potenciales amenazas de seguridad.

Garantizar una protección efectiva de los activos de información, proporcionando evidencias, análisis y recomendaciones para incrementar los niveles de seguridad protegiendo las inversiones tecnológicas y la continuidad de las operaciones.

4.2 Descripción del Proceso Global

El papel principal de la creación y operación del centro de monitoreo de Sm4rt consiste en proporcionar los servicios de monitoreo constante que ayudarán al cliente a detectar alertas, generar análisis para prevenir, detectar y tratar los ataques cibernéticos y otros incidentes de seguridad de TI con base en los procedimientos en la gestión de seguridad informática y la administración parcial o completa de las herramientas de monitoreo.

La implementación y definición de los servicios del área de monitoreo consistió en el análisis de cuatro principales módulos los cuales se pueden apreciar en la Figura 4.1, y que se mencionan a continuación y se dará el detalle de cada uno de ellos a lo largo del capítulo presente:

- Análisis inicial: Conocer la situación actual del cliente permitió definir un catálogo de servicios que se ofrecerían y una descripción de responsabilidades que se estarían asignando en cada uno de los servicios.
- Registro de turnos: Es importante que entre cada cambio de turno se dieran a conocer las alertas o requerimientos solicitados para dar continuidad y brindar un servicio de monitoreo óptimo.
- Alertamiento y monitoreo: Definición del flujo de actividades e implementación de la operación del centro de monitoreo.
- Tickets y solicitudes: Atención a los requerimientos específicos y mejora continua a los servicios ofrecidos al cliente.

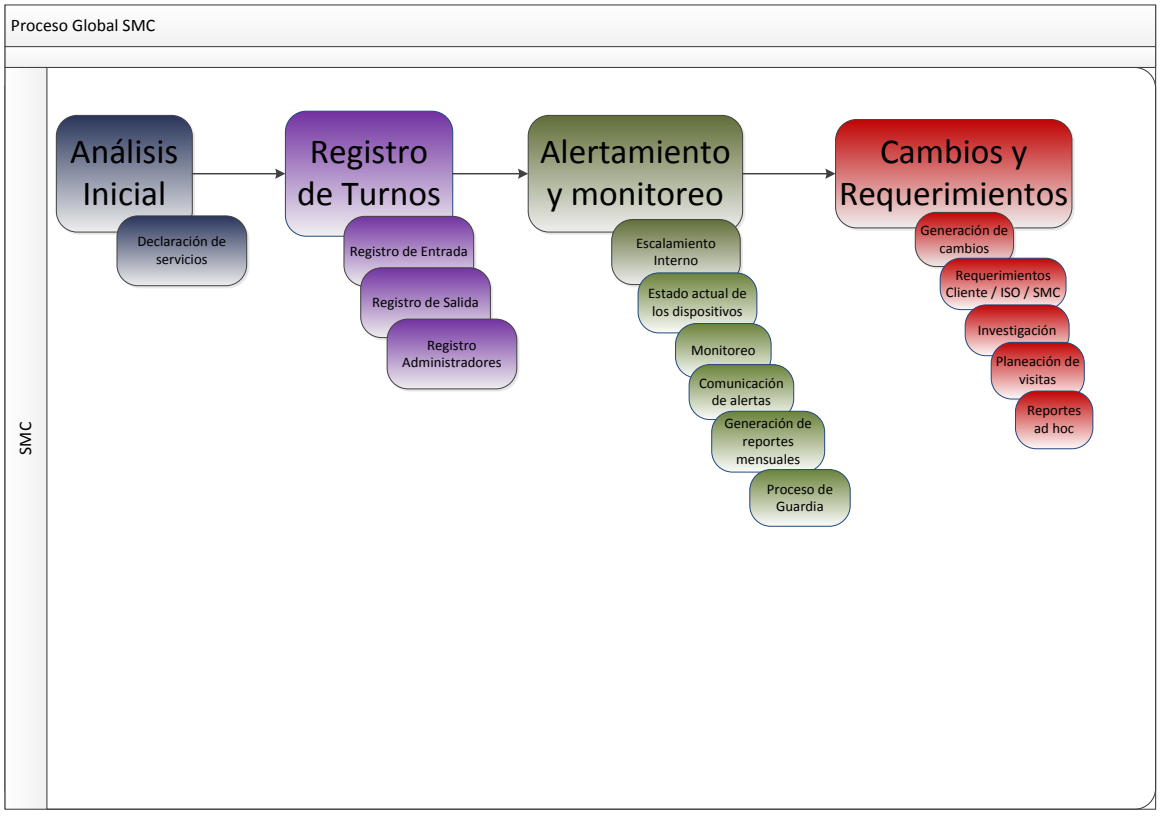


Figura 4.1 Proceso Global de Monitoreo

4.3 Análisis inicial

Una vez definido el objetivo de la creación de un centro de monitoreo, fue necesario plantear la situación actual de Sm4rt ante este proyecto y de igual forma conocer el panorama de los clientes con los que ya contaban con herramientas de seguridad.

El personal involucrado en dicho proyecto definió los perfiles necesarios para operar el centro de monitoreo, desde el personal de aprendiz de monitoreo hasta consultores Sr. Se determinaron los requisitos técnicos para llevar a cabo un monitoreo de las distintas tecnologías de los clientes, se realizó la solicitud de un servidor con las especificaciones técnicas mínimas necesarias para levantar el servicio, pantallas de monitoreo, el software para trabajar con máquinas virtuales y la tarjeta controladora para multipantalla. De igual forma fue requerida la solicitud de una conexión VPN (Virtual Private Network) a la red de Sm4rt para seguir controlando las herramientas de seguridad desde cualquier sitio con Internet.

Sm4rt al ofrecer un servicio de monitoreo, se vio en la necesidad de conocer el panorama de los distintos clientes, ya que algunos contaban con al menos una herramienta de seguridad y en algunos otros casos se estaba dando el asesoramiento para que el cliente adquiriera la tecnología que cumpliera con los requisitos para la protección de la información y se adaptara a las necesidades del negocio.

Por lo tanto se definió un proceso ante esta situación que comentaba anteriormente, el cual se divide en dos principales etapas, si el cliente contaba o no con la tecnología.

Si el cliente contaba con la tecnología, se hacía un análisis del tipo y propósito de la herramienta, recababa toda la información posible desde la ubicación física del equipo como el tipo de información que resguardaba, era indispensable conocer las reglas definidas ya en la herramienta para adaptarlas a las políticas de la empresa, así como saber, si contaba con la vigencia de soporte técnico por parte del proveedor de la tecnología y el tipo de licencia que se tenía. Todos estos factores fueron de gran apoyo para definir procesos de monitoreo y atención a incidentes, los cuales se hablará en capítulos posteriores; de igual forma se dieron a conocer al cliente las recomendaciones y requerimientos para operar sus herramientas de manera óptima y eficiente.

El segundo caso, donde el cliente no contaba con la tecnología pero requería del servicio de monitoreo, se hacía un análisis dependiendo de las necesidades del cliente y el tipo de información a proteger. El equipo de monitoreo realizaba una selección de las mejores tecnologías y proveedores que se adaptaban a las necesidades del cliente, una vez definido este punto se elaboraba un plan de trabajo entre Sm4rt-Proveedor-Cliente, esto con el objetivo de instalar, configurar y poner en funcionamiento la herramienta de seguridad. Todo este proceso de implementación de la herramienta es crucial para la operación del monitoreo de la tecnología, en el cual se dan de alta los activos a proteger y se realizan una serie de pruebas para validar la aplicación de políticas, envío de alertas, verificar la alta disponibilidad y atender cualquier implicación posterior a la instalación y puesta en marcha de la herramienta de seguridad.

En la figura 4.2 se resume en un diagrama la metodología de servicio que definió el área para conocer la situación actual de cada uno de sus clientes.

4.3.1 Declaración de servicios

Conforme se fue conociendo el panorama de cada uno de los clientes, todos ellos del sector privado y que en su mayoría ofrecen servicios de entretenimiento por televisión de paga, telefonía e Internet, se establecieron los alcances y servicios que se ofrecerían de manera general. Dichos clientes manejan increíbles cantidades de información sensible y crítica para el negocio, por lo cual era importante definir a detalle la declaración de los servicios a otorgar.

El objetivo de la declaración de servicios permitió conocer las actividades y responsabilidades asignadas a cada personal involucrado en el monitoreo desde el aprendiz de monitoreo hasta los Oficiales de Seguridad que se encontraban en sitio con el cliente, para establecer la mejor comunicación posible e identificar y reportar oportunamente incidentes de seguridad de la información y/o actividades sospechosas.

El alcance que se nos permitió establecer en un inicio, debido al poco personal con el que se inició el proyecto, es el que se describe a continuación, el cual aplicaba para cada uno de los clientes.

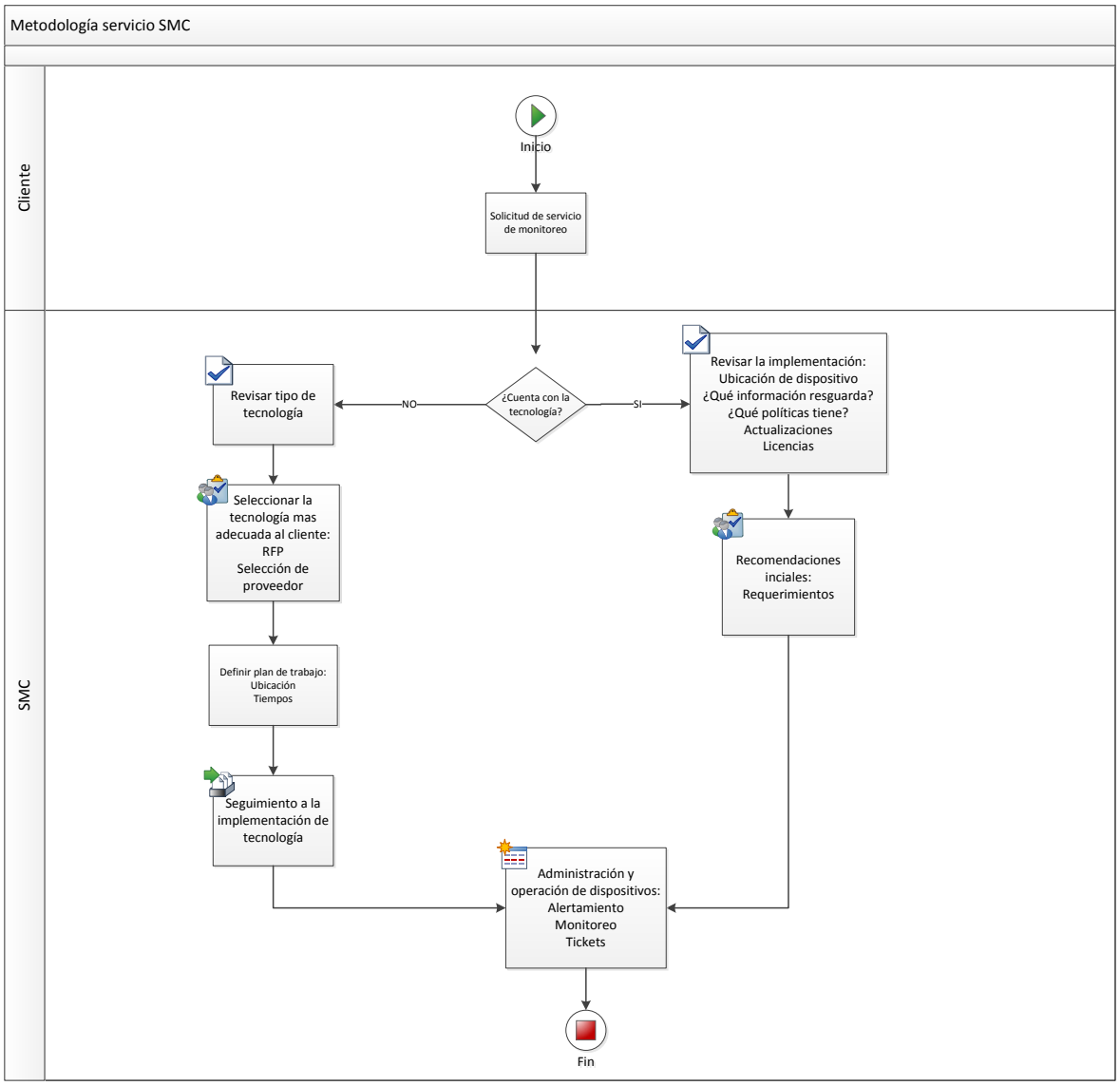


Figura 4.2 Metodología servicio Monitoreo

Administración y Monitoreo de X consola de administración con hasta X número de activos:

- Monitoreo en tiempo real en un horario de 8 am a 10 pm de lunes a viernes. Para el resto del día, fines de semanas y días festivos, se hará la atención de las alertas críticas configuradas en los equipos.

- El horario de atención en oficinas está establecido en la Tabla 4.1:

Tabla 4.1 Horario de atención

Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo
De 8:00 a 22:00 horas	De 8:00 a 22:00 horas	De 8:00 a 22:00 horas	De 8:00 a 22:00 horas	De 8:00 a 22:00 horas	No laborable	No laborable

- El horario de guardias para la notificación de algún incidente y/o alertas está establecido en la Tabla 4.2:

Tabla 4.2 Horario de guardias

Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo
Guardia de 22:00 a 8:00 horas	Guardia de 22:00 a 8:00 horas	Guardia de 22:00 a 8:00 horas	Guardia de 22:00 a 8:00 horas	Guardia de 22:00 a 8:00 horas	Guardia 24 horas	Guardia 24 horas

4.3.2 Catálogo de Servicios

A continuación se describen los servicios ofrecidos por parte del centro de monitoreo:

- Seguridad en Base de Datos: Administrar y operar dispositivos de monitoreo de bases de datos para identificar y reportar oportunamente incidentes de seguridad de la información.
- Prevención y detección de intrusos: Supervisar constantemente las actividades sospechosas en los activos de la organización para identificar y reportar oportunamente incidentes de seguridad de la información por medio de Sistemas de Prevención de Intrusos.
- Centralización y correlación de bitácoras: Supervisar constantemente las bitácoras de activos en la organización para identificar y reportar oportunamente incidentes de seguridad de la información por medio de la centralización y correlación de bitácoras.

4.3.3 Responsabilidades del Área de Monitoreo-ISO

El objetivo de este apartado tiene como objetivo dar a conocer las responsabilidades que se determinaron para el personal de monitoreo y personal de Administración de Riesgos (ISO's) de Sm4rt, para brindar el servicio de administración y monitoreo de dispositivos de seguridad hacia los clientes.

4.3.3.1 Responsabilidades Generales

A continuación se describen las responsabilidades generales que tiene el personal de monitoreo, para brindar los servicios correspondientes:

- Monitorear eventos registrados en la consola o dispositivo de seguridad (IPS, SIEM, DAM)
- Configurar los dispositivos de seguridad para enviar alertas de acuerdo a un cierto nivel de criticidad
- Definir en conjunto con los ISO's una matriz de clasificación de alertas de acuerdo a su nivel de criticidad por cliente
- Definir los acuerdos de nivel de servicio (SLA):
    - Alcance
    - Objetivo
    - Descripción de actividades
- Entregar a los ISO's reportes mensuales de cada uno de los dispositivos de seguridad, que contemple lo siguiente:
    - Resumen Ejecutivo
    - Detalle Técnico
- Elaborar reportes específicos a solicitud del cliente
- Definir en conjunto con los ISO's una matriz con tipos de requerimientos y sus tiempos de respuesta por cliente
    - Gestionar/Solicitar/Coordinar con el cliente la entrega de diagramas de infraestructura de su red:
        - Diagrama de red
        - Diagrama de conexiones
        - Diagrama lógico

- Dar recomendaciones de seguridad para solucionar incidentes detectados por los dispositivos de seguridad.
- Comunicar los incidentes detectados por los dispositivos de seguridad de manera adecuada y oportuna:
    - En caso de que sea un incidente crítico comunicar directamente al cliente y al ISO vía correo electrónico/llamada telefónica.
    - En caso de que sea un incidente con menor criticidad comunicar vía correo/llamada telefónica al ISO.
- Configurar los dispositivos de seguridad para bloquear ataques o firmas de ataques.
- Revisar el estado actual de los dispositivos de seguridad en los siguientes puntos:
    - Licencias, actualizaciones, firmas, almacenamiento, etc.
- Presentar los resultados mensuales de cada dispositivo de seguridad con el cliente
- Dar soporte del dispositivo de seguridad en sitio en caso de cualquier falla:
    - Soporte Primer nivel
        - Analizar la posible falla en el dispositivo de seguridad
        - Re-establecer la configuración inicial o un estado anterior para su funcionamiento
    - Soporte Segundo nivel
        - En caso de que no se pueda resolver dicha falla, se contacta al proveedor para dar solución
        - La apertura de los casos ante soporte de las diferentes herramientas debe ser gestionada por proveedores y/o por el cliente.
- Registrar todos los eventos (Ticket) en bitácora ya sea de :
    - Control de cambios
    - Incidentes
    - Solicitud de requerimiento por parte del cliente
    - Solicitud de requerimiento por parte del ISO
- Dar seguimiento a:
    - Las recomendaciones propuestas para el cierre de un incidente

- Estatus y cierre de cada uno de los eventos generado en bitácora (ticket)

- Dar apoyo en los mantenimiento de red hechos por el cliente si solo si el cliente lo solicita.
- Generar una matriz de control de cambios para cada uno de los dispositivos de seguridad en el cliente que considere:
  - Fecha de cambio
  - Horario propuesto
  - Tiempos considerados
  - Acciones a realizar
  - Tipo de afectación
- Apoyar y dar seguimiento en la implementación de los dispositivos de seguridad con las siguientes actividades:
  - Realizar pruebas de verificación en las configuraciones de los dispositivo
  - Verificar que se cumplan los tiempos establecidos con el proveedor
  - Comunicar desviaciones al ISO por parte del proveedor en la implementación de los dispositivos de seguridad:
    - Tiempos y alcance
- Generar un procedimiento de planeación de visitar con el cliente para control de cambios u cualquier soporte en sitio con el cliente.
- Dar capacitación del servicio, de las funciones y actividades que realiza el centro de monitoreo al área de Administración de Riesgos.

4.3.3.2 Responsabilidades por tipo de tecnología

IPS (Intrusion Prevention System)

Revisión de status de firmas de seguridad en los dispositivos IPS:

- Actualización de firmas
- Análisis de impacto de firmas a aplicar
- Revisión de nuevas firmas a implementar en el dispositivo

DAM (Database Activity Monitoring)

- Dar seguimiento en la definición de roles y perfiles en las bases de datos a monitorear
- Dar seguimiento en la definición de direcciones IP que deben tener acceso a las bases de datos a monitorear
- Rotación de bitácoras en el dispositivo

SIEM (Security Information and Event Management)

- Dar recomendaciones del tipo de bitácoras que se deben de registrar en el centralizador por tipo de plataforma (Windows, Linux, Dispositivos de red, BD, etc)
- Apoyo técnico para la definición del tipo de bitácoras por plataforma a centralizar
- Apoyo técnico para las implicaciones de encender las auditorías definidas por cada plataforma

4.3.3.3 Responsabilidades del Oficial de Seguridad (ISO)

A continuación se describen las responsabilidades generales que tiene el personal de Administración de Riesgos, para brindar el servicio de administración y monitoreo de dispositivos de seguridad:

- Gestionar cualquier solicitud de requerimiento de parte del cliente hacia el área de monitoreo, de acuerdo a la matriz de requerimientos que se defina
- Entregar/Generar/Pedir la lista de activos actualizados de acuerdo a la criticidad para el cumplimiento SOx (Alta, media o baja) de :
    - Aplicaciones
    - Servidores Windows/Linux/etc
    - Bases de datos
    - Dispositivos de red
- Apoyar al área de monitoreo a contactar al cliente en sitio en caso de alertas o requerimientos no contestados o pendientes.
- Definir la matriz de contactos por cliente para que en caso de algún incidente o evento se les comunique.

- Definir la matriz de escalamiento por cada uno de los clientes para casos de algún incidente, cambio u evento.
- Definir en conjunto con el área de monitoreo, el procedimiento de control de cambios por cada uno de los clientes
- Coordinar la junta de presentación de resultados mensuales en caso de requerirlo el cliente
- Gestionar y validar los accesos del personal de monitoreo, a las instalaciones del cliente en caso de requerirlo de manera oportuna
- Gestionar y validar los accesos del personal de monitoreo al site de cada cliente, en caso de requerirlo de manera oportuna
- Dar seguimiento a las recomendaciones proporcionadas por monitoreo para la solución de incidentes, eventos u cambios
- Notificar cualquier desviación, queja, o sugerencia al área
- Definir el procedimiento de atención y respuesta a incidentes del lado del cliente
- Atención de desviaciones en la implementación de los dispositivos de seguridad con el proveedor y/o con el cliente
- Acudir a las capacitaciones que el centro de monitoreo realice del servicio, de las funciones y actividades que proporciona
- Gestionar el espacio físico y nodos de red necesarios para que personal de monitoreo realice sus actividades correspondientes.

4.4 Registro de Turnos

Como se comentaba en el alcance de la declaración de servicios, debido al poco personal con el que se contaba dentro del proyecto de monitoreo, se establecieron horarios de operación y guardias para la atención de alertas y verificación del funcionamiento correcto de los distintos dispositivos de seguridad.

4.4.1 Registro de Entrada

La atención de alertas y revisión del buen funcionamiento del dispositivo de seguridad eran esenciales para dar un servicio adecuado de monitoreo, por lo cual se diseñó el proceso de registro de turnos para operadores y administradores.

En este apartado se describirá el proceso de registro de entrada de los operadores (Figura 4.3), ya que el área se dividía en personal de operación y administración.

De acuerdo al horario establecido de atención por parte de Sm4rt, el primer operador en llegar a la oficina debía realizar una serie de actividades las cuales menciono a continuación:

- Revisar cada una de los dispositivos de seguridad, esto con el objetivo de validar que estuvieran recibiendo eventos en tiempo real y validar las conexiones VPN con cada uno de los clientes. En ocasiones el dispositivo solía desconectarse y dejar de registrar eventos, lo cual era perjudicial para algún análisis forense, ya que no se tendría registro de los eventos.
- En caso de que algún servicio esté detenido o alguna consola desconectada, el operador tiene el deber de volver a levantar el servicio correspondiente, en caso de que las fallas sean externas a la operación de monitoreo, deberá apoyarse de alguno de los administradores para notificar la falla con el Oficial de Seguridad y reestablecer el servicio lo antes posible.
- En cada uno de los dispositivos se tiene la configuración de envío de alertas críticas al correo de cada uno de los integrantes del equipo de monitoreo, las cuales deben de revisarse inmediatamente, para dar seguimiento a cada una de ellas, hacer su respectiva notificación a los administradores y, en caso necesario, al cliente.
- De igual forma se revisan alertas de nivel medio y bajo, ya que los dispositivos tienen una configuración por default de las alertas, una alerta de nivel bajo detectada por la herramienta podría llegar a ser alta, esto derivado de una post investigación y análisis en conjunto con ISO y cliente.

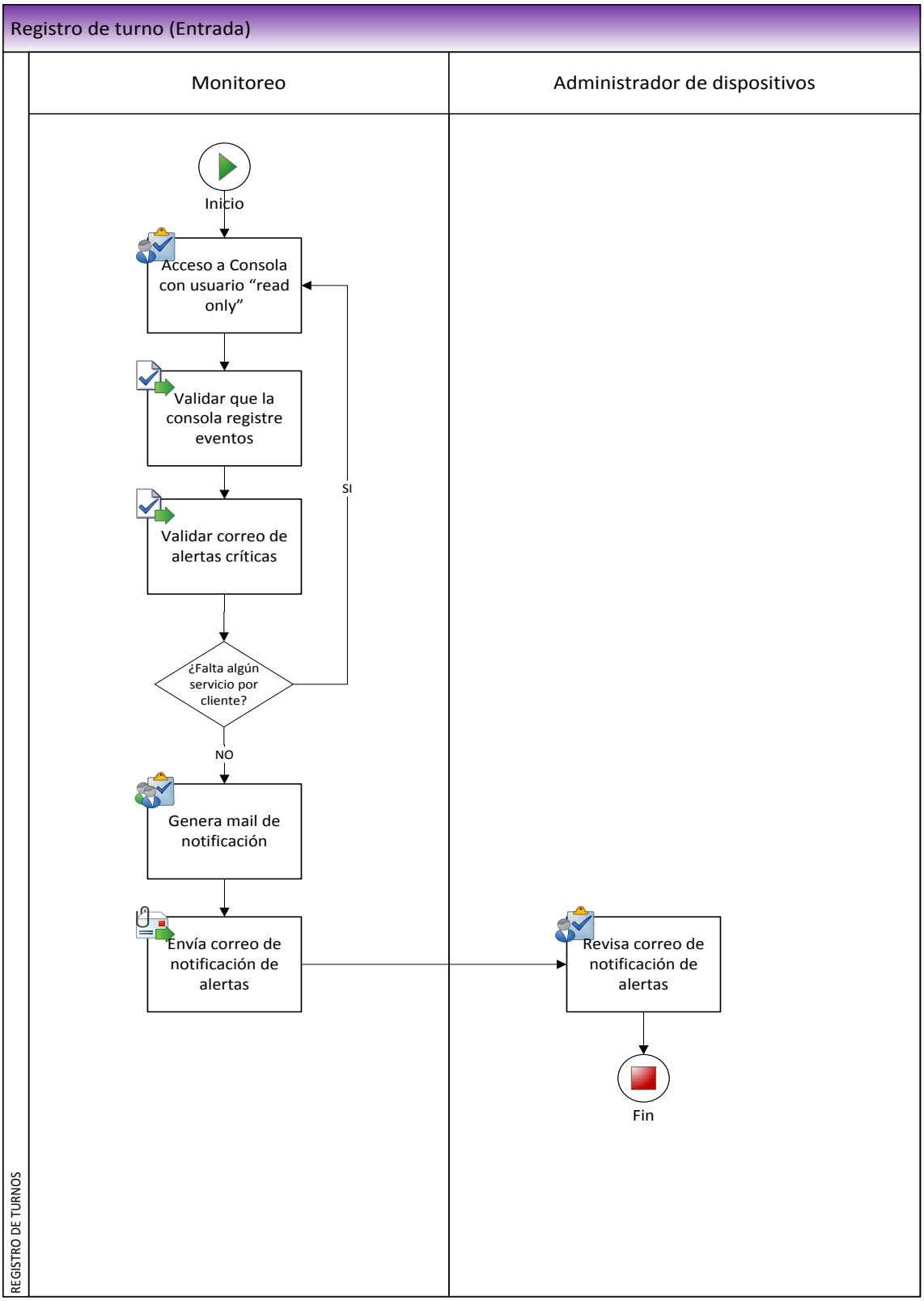


Figura 4.3 Registro de turno (Entrada)

4.4.2 Registro de Salida

Al finalizar el horario establecido de operación en las oficinas de Sm4rt, se tenía la actividad de validar que las diferentes herramientas de seguridad quedaran funcionando correctamente, esto con el objetivo de seguir monitoreando desde cualquier sitio que contara con internet.

También era de suma importancia verificar el funcionamiento del software que se encargaba de enviar vía correo electrónico, un estatus de los diferentes monitores donde se visualizaban las distintas consolas de operación. Con esto podíamos consultar desde los celulares asignados a la operación, el funcionamiento de las diferentes herramientas.

A continuación se enlista el proceso realizado al finalizar el turno del día y que se aprecia su flujo en la figura 4.4:

- Revisión de conexión en cada una de las consolas de los diferentes dispositivos de seguridad. Era de suma importancia corroborar el funcionamiento de los clientes que permitían hacer la conexión VPN a cada una de las localidades donde se encontraban físicamente los equipos. Dicho protocolo era el sustento de operación y administración de la mayor parte de las consolas.
- Validación de registro de eventos en tiempo y forma de cada uno de las consolas.
- Verificar el funcionamiento del sistema de alertamiento de cada consola, al igual que el programa encargado de enviar un estatus de las herramientas de seguridad, al correo de cada uno de los integrantes del área de monitoreo.
- Enviar un correo de notificación sobre las alertas que deben ser analizadas al día siguiente en el primer turno.
- Por último, enviar un reporte a cada uno de los Oficiales de Seguridad respecto al funcionamiento y estado de sus herramientas de seguridad, y notificarles en caso de encontrar alguna anomalía dentro de la operación de las mismas.

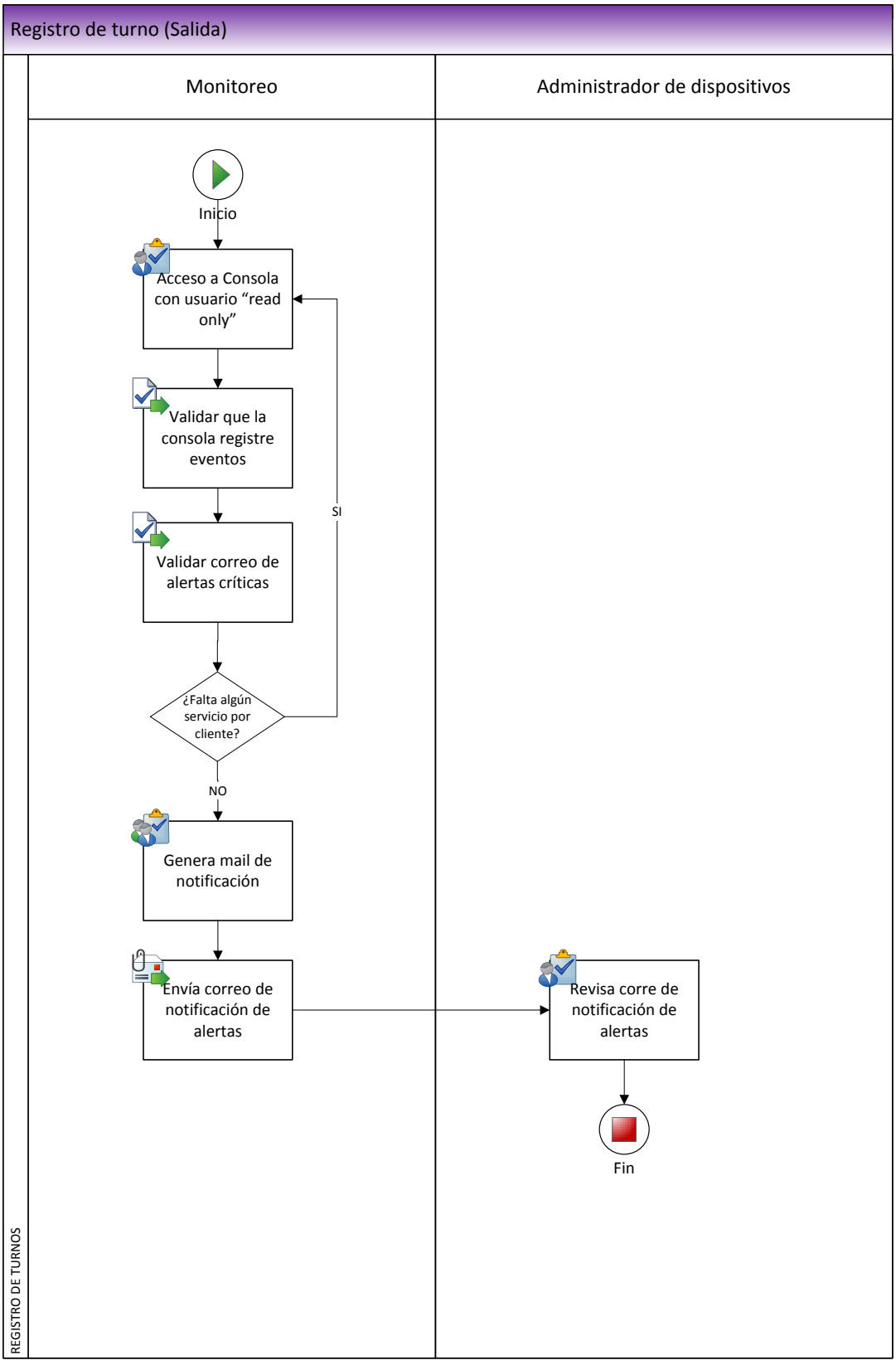


Figura 4.4 Registro de turno (Salida)

4.4.3 Registro de Administradores

Los administradores realizan su registro haciendo una revisión periódica de los eventos que detectaban las herramientas. Al contar con mayor conocimiento y experiencia, tienen la capacidad de analizar eventos más específicos que no eran tan sencillos de detectar para un operador.

El administrador realiza el análisis correspondiente de la eventualidad, si requería de alguna investigación más a fondo, solicitaba el apoyo de alguno de los operadores mediante un correo electrónico, donde ya había una previa descripción del evento y de los puntos a investigar.

El operador, una vez hecha la labor correspondiente, hacía una retroalimentación con el administrador, y con base a la información obtenida, se generaba el análisis final, emitiendo las observaciones pertinentes y notificando al equipo de trabajo, ver figura 4.5.

Ya realizadas las observaciones, en caso de ser necesario, se hacía una notificación al cliente para continuar con la investigación de la eventualidad y, en caso contrario, se generaba una bitácora de investigación para tenerla como base de conocimientos para futuros eventos similares e ir compartiendo las experiencias al grupo.

Cabe resaltar que una de las fortalezas que presentaban los administradores era el apoyo a todo el equipo sin importar el nivel de conocimiento, ya que se buscaba tener en el área el mayor conocimiento posible para atender cualquier ataque, evento o incidente que se pudiera presentar en alguno de los clientes.

4.5 Alertamiento y Monitoreo

Hemos llegado al punto clave del desarrollo del presente trabajo, ya que en este apartado se dará a conocer los procesos principales y los retos que se presentaron para brindar el mejor servicio posible hacia los clientes, contando con el mínimo número de recursos humanos.

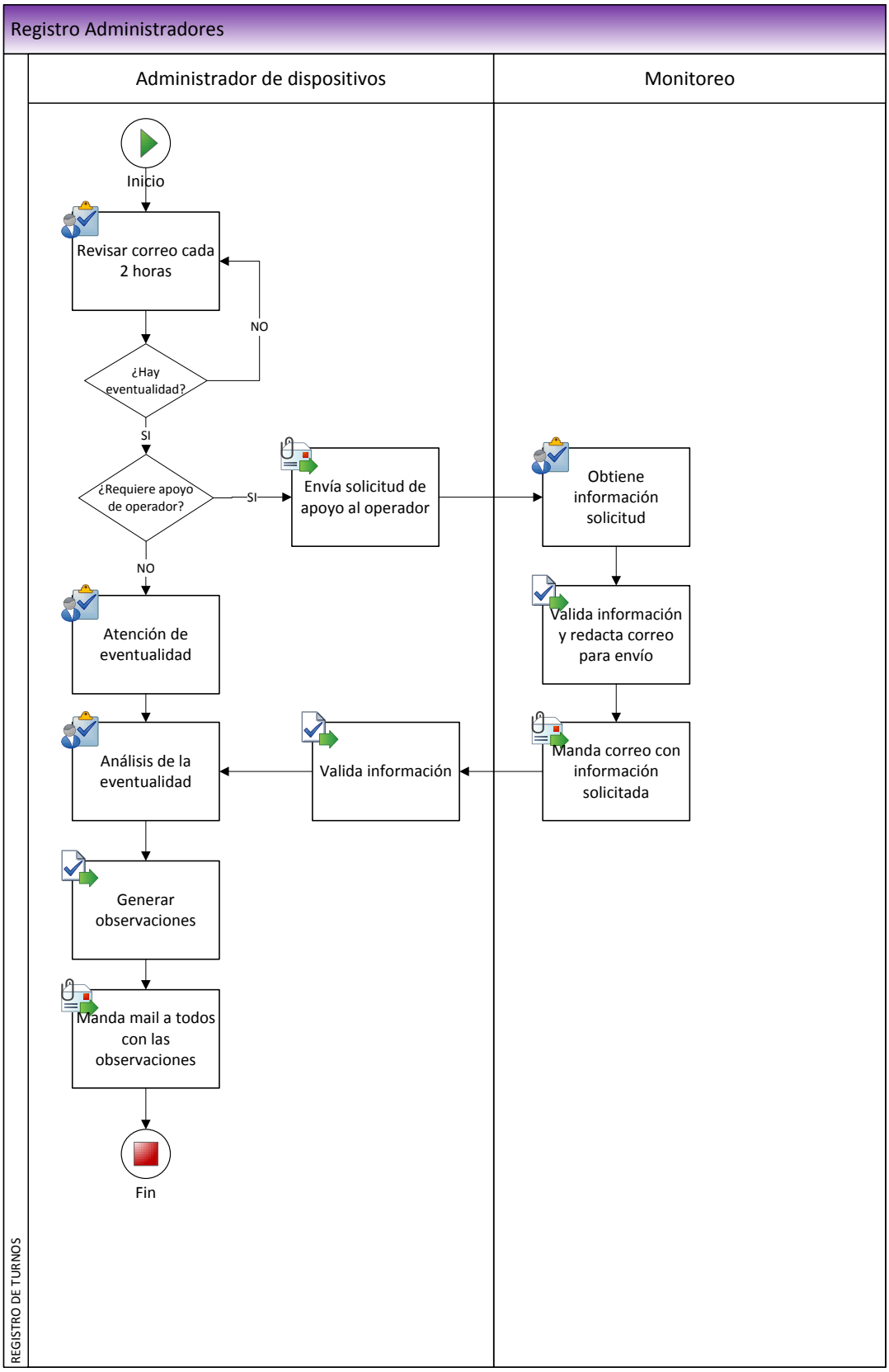


Figura 4.5 Registro de turno (Administradores)

En capítulos anteriores se ha mencionado sobre los inicios de la creación del centro de monitoreo, comenzando con un estatus de cómo se encontraba el área recién creada, partiendo de la declaración de servicios a proporcionar, conllevando a la asignación de responsabilidades, junto con la parte correspondiente de Sm4rt (ISO´s) en cada uno de los clientes.

El proceso de registro de turnos nos permitió dar un servicio óptimo durante el horario de operación del cliente, el sistema de alertamiento, revisión constante de los estados de operación de las herramientas y con la aportación del análisis y conocimiento de los administradores permitieron atender alertas que iban desde un nivel bajo hasta un nivel crítico en tiempo y forma.

4.5.1 Escalamiento Interno

Dentro del área de monitoreo, un factor importante ante la respuesta a incidentes o algún evento registrado por las herramientas de seguridad, es la comunicación. Por tal motivo era necesario elaborar una matriz de escalamiento (Figura 4.6) para la atención de las alertas o sucesos que se pudieran presentar.

Son tres niveles los que tenían definidos en el área:

Nivel uno Aprendiz de monitoreo

- Nivel encargado de visualizar los eventos en cada una de las herramientas en cada cliente. El personal de este nivel tiene la responsabilidad de notificar al nivel dos de eventos, tanto conocidos como desconocidos, previo a contar ya con una base de conocimientos para dicha clasificación.

Nivel dos Consultor Jr Operador

- El personal en este nivel tiene la tarea de registrar las actividades realizadas hasta el momento y dar seguimiento al monitoreo de la actividad presentada. Es responsable de realizar un análisis del evento para su clasificación correspondiente y ser ingresado a la base de conocimientos. Otorgar una solución temporal o definitiva del problema.

Nivel 3 Consultor Sr Administrador

- El nivel más alto dentro del área de monitoreo, encargado de determinar la naturaleza del evento desconocido, implementar una solución completa y satisfactoria al cliente. Notificar a niveles inferiores del evento desconocido para una retroalimentación a toda el área. Seguimiento a los eventos y alertas ya reportados al cliente. Principal nivel en tener contacto con el Oficial de Seguridad para reportar el evento suscitado.

De esta forma se realiza la comunicación de las alertas registradas, el principal cometido de esta dinámica, es impulsar el trabajo en equipo, y ante cualquier nuevo evento o amenaza que se pudiera presentar, el área contaba con la retroalimentación basada en la investigación y tareas que realizaba cada personal en sus diferentes niveles, con el fin de tener una mayor operación proactiva que reactiva.

Una vez que la alerta había sido reportada al cliente, el Oficial de Seguridad se encargaba de notificar al personal correspondiente, ya que en cada uno de los clientes, también se tenía una matriz interna de escalamiento. Cerrado el caso, el ISO hacía la notificación al área de monitoreo, teniendo una conclusión y análisis final del evento.

4.5.2 Estado de los dispositivos

Un paso antes de iniciar el proceso de monitoreo en forma, era de suma importancia tener el concepto y estado actual de cada una de los dispositivos de seguridad, con el objetivo de plantear una estrategia general para llevar a cabo el cumplimiento de un operación completa y en forma de las distintas consolas de administración.

Como bien comentaba en un principio, son tres las principales tecnologías con que contaban la mayoría de los clientes: SIEM, DAM e IPS.

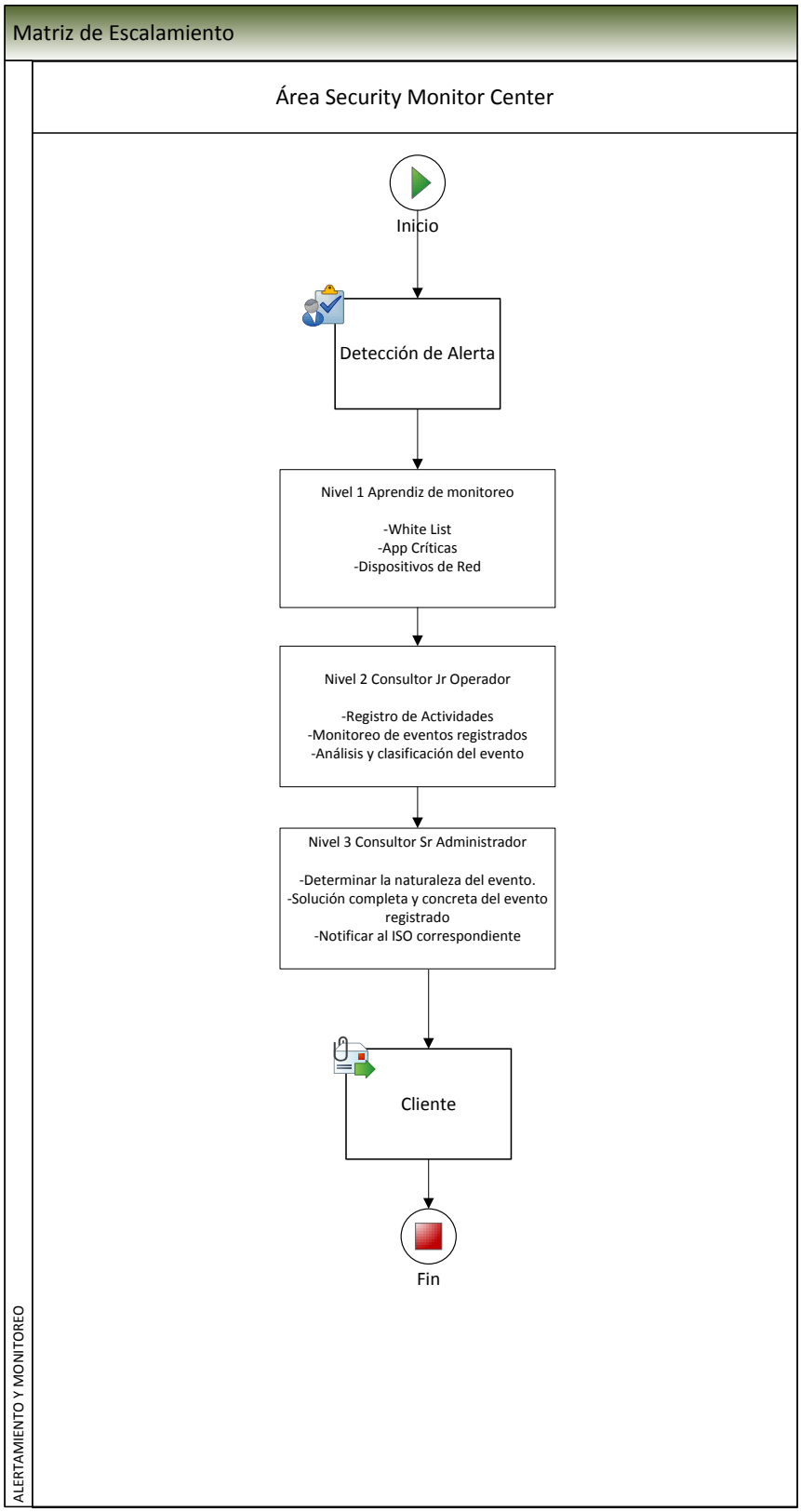


Figura 4.6 Matriz de Escalamiento

4.5.2.1 SIEM

La centralización de bitácoras consta de almacenar y normalizar cada uno de los eventos de seguridad que son enviados o extraídos de los diferentes dispositivos por protocolos o métodos definidos por el centralizador.

La gran mayoría de los sistemas y aplicaciones disponibles en una red corporativa genera eventos que son almacenados en logs. Esencialmente, es una lista grande de eventos ordenada cronológicamente. Existen protocolos específicos para transportar estos eventos. Un SIEM completo debe ofrecer formas flexibles de recolectar los eventos.

- Acceso centralizado y consistente a todos los logs y eventos
- Archivo de histórico para análisis forense
- Herramientas sofisticadas para la generación de informes
- Disparo inmediato de alertas y notificaciones de acuerdo a las reglas preestablecidas
- Relación de eventos que ocurren en múltiples sistemas y que, en el contexto individual, tienen relevancia.

Un sistema SIEM [5] debe contar con tres principales funciones: la extracción, almacenamiento/normalización y correlación de eventos. Dicho sistema tiene sus respectivos dispositivos para realizar las funciones antes mencionadas y podamos contar con los beneficios de una completa tecnología SIEM.

La estrategia general planteada con cada uno de los clientes, fue el saber, que activos críticos se tenían que monitorear por cumplimiento. Saber las plataformas de los activos a centralizar era necesario, ya que según el sistema operativo, correspondían ciertos pasos de configuración.

Se solicitaba la criticidad de la operación de los activos, ya fueran de Producción, Desarrollo, SOx, pruebas, entre otros, con el fin de hacer la respectiva clasificación dentro de la herramienta.

Cada uno de los clientes contaba con el estándar para la administración y retención de bitácoras, dicho documento tenía la finalidad de acotar los lineamientos necesarios para la

generación de logs. El uso de estos archivos debe permitir el monitoreo y correlación de eventos, y la reconstrucción de información en caso de algún incidente de seguridad.

El contenido de las bitácoras debe ser el suficiente para establecer qué eventos ocurrieron, los recursos que ocupó y los resultados de éstos, para que en caso de que exista algún incidente, sea posible conocer los cambios que se han realizado y definir responsables.

Estos son los datos requeridos en cada bitácora:

- Fecha y Hora del evento (TimeStamp)
- Cuenta de usuario
- Activos involucrados (origen y destino)
- Nombre de los activos e IP´s
- Tipo de Evento
- Resultado del evento (exitoso o fallido)

Loe eventos requeridos por cumplimiento de normativas de seguridad son las siguientes:

- Tabla 4.3 Eventos Windows

Evento	Resultado
Audit account logon events	Exitoso/Fallido
Audit account logon management	Exitoso/Fallido
Logon and logoff	Exitoso/Fallido
Restart and Shutdown	Exitoso/Fallido
File/Object Access	Exitoso/Fallido
Process Traking	Exitoso/Fallido
Security Policy Changes	Exitoso/Fallido
User/Group Management	Exitoso/Fallido
Directory Service Access	Exitoso/Fallido

- Tabla 4.4 Eventos en UNIX

Evento	Resultado
Login	Exitoso/Fallido
User/Group Management	Exitoso/Fallido
Restart and Shutdown	Exitoso/Fallido
Command SU/SUDO	Exitoso/Fallido

- Tabla 4.5 Eventos en Base de Datos

Evento	Oracle	SQL
Failed login	Auditoría interna	errorlog
Successfull login	Auditoría interna	errorlog
Create	Auditoría interna	audit
Alter	Auditoría interna	audit
Drop	Auditoría interna	audit
Grant-Revoke	Auditoría interna	audit
Shutdown	Alert log	errorlog
Startup	Alert log	errorlog

- Tabla 4.6 Eventos en Aplicaciones

Evento	Resultado
Login	Exitoso/Fallido
User/Group Management	Exitoso/Fallido
Critical Transactions	Exitoso/Fallido

- Tabla 4.7 Eventos en Dispositivos de Red

Evento	Resultado
Login	Exitoso/Fallido
Configuration changes	Exitoso/Fallido
Access console	Exitoso/Fallido
Violantions ACL	Exitoso/Fallido
Events AAA	Exitoso/Fallido

Una vez activas todas las bitácoras mencionadas anteriormente se definían las alertas a configurar en el sistema SIEM, al igual que los reportes que se requerían para la fase de centralización y correlación de eventos.

4.5.2.1.1 Configuración actual

Como se mencionó al principio del informe, algunos clientes que contrataban los servicios de Sm4rt, ya contaban con la tecnología y con la centralización de algunos activos, por lo tanto se solicitaba en conjunto con el Oficial de Seguridad, un estatus de los dispositivos actualmente centralizados de acuerdo a la lista definida para cumplimiento.

Validar si los eventos ya centralizados estaban alineados de acuerdo al estándar de administración y centralización de bitácoras. Si la tecnología contaba con las licencias vigentes y si cubrían las necesidades del cliente.

Se trazaba un plan de trabajo Monitoreo/ISO/Cliente/Proveedor para la centralización de los activos faltantes por monitorear.

De igual forma se solicitaba la información respecto a la ubicación física y lógica del dispositivo, diagramas que nos proporcionaban los clientes era parte importante para conocer con que dispositivos de red se conectaba el dispositivo, y entender mejor alguna situación que se pudiera presentar, en caso de alguna incidencia de comunicación con el dispositivo.

Se definieron los reportes que el cliente solicitaba para dar a conocer los acontecimientos y eventos suscitados en el periodo de tiempo definido por el cliente, más adelante abordaré el tema de los entregables.

Tener bien establecidas las matrices de escalamiento tanto internas como con el cliente, permitían establecer la comunicación adecuada con el personal correspondiente para la atención o notificación de cualquier evento presentado durante esta etapa.

Un punto importante para la operación adecuada de la herramienta de seguridad, era solicitar al proveedor, un usuario de operación y otro para la administración, esto podía variar dependiendo del contrato que se tuviera con el cliente, ya que en algunos casos, personal interno, es decir con el cliente, podían llevar ciertas tareas administrativas.

Al cliente se le hacía directamente la solicitud de una conexión VPN para realizar la operación y administración vía remota y segura del dispositivo de seguridad.

El tema de almacenamiento y respaldo de la información manejada por el dispositivo de seguridad, era parte del cumplimiento del estándar de retención de bitácoras.

Las bitácoras pueden almacenarse en dos diferentes esquemas, cada uno con sus ventajas y sus desventajas. El tipo de esquema que se seleccione depende de la capacidad de la infraestructura.

- Almacenamiento in-situ: Los archivos de las bitácoras son respaldados dentro del mismo servidor en el que se generan; no obstante, no se desliga al responsable de la aplicación de las transacciones registradas en esta herramienta.
- Almacenamiento centralizado: Se dispone de un servidor en el que se guardan y centralizan todas las bitácoras de los sistemas que las generen. Este esquema ayuda a la coordinación y tratamiento de la información. Es uno de los más sencillos ya que permite la minería y recuperación de datos de un mismo servidor.

Los archivos de registros de bitácoras no deben ser expuestos, por lo que cualquier transferencia de dichos archivos debe ser realizada mediante protocolos seguros como SSH (Secure Shell) y SSL (Secure Sockets Layer) por mencionar algunos.

Para el respaldo de logs de los activos monitoreados, se debe contar con una copia de seguridad de las bitácoras, si los medios de almacenamiento son extraíbles, estos deben ser etiquetados indicando el tipo de información almacenada, fecha de registro y hora.

4.5.2.2 IPS

Los sistemas de prevención de intrusiones, también conocidos como sistemas de prevención y detección de intrusos, son dispositivos de seguridad de red que supervisan el tráfico de red y/o actividades maliciosas del sistema. Las principales funciones de los sistemas de prevención de intrusos son identificar las actividades maliciosas, registrar la información sobre esta actividad, bloquear y/o notificarlo.

Un Sistema de Prevención de Intrusos (IPS) [6], al igual que un Sistema de Detección de Intrusos (IDS), funciona por medio de módulos, pero la diferencia es que este último alerta al administrador ante la detección de un posible intruso, mientras que un Sistema de Prevención de Intrusos establece políticas de seguridad para proteger el equipo o la red de un ataque; se podría decir que un IPS protege al equipo proactivamente y un IDS lo protege reactivamente.

Los IPS se categorizan en la forma que detectan el tráfico malicioso:

- Detección Basada en Firmas
- Detección Basada en Políticas

- Detección Basada en Anomalías
- Detección Honey Pot.

Al igual que se realizó con el sistema SIEM se trazó una estrategia general, esto con el fin de saber que se pretendía proteger con esta tecnología en cada uno de los clientes, su función principal es la protección perimetral, una mala ubicación física del equipo, no permitiría hacer un uso óptimo de la herramienta y de las políticas de seguridad.

En general, los clientes contaban con dos tipos de IPS, basados en firmas y otros en políticas, en ambos casos se solicitaban información específica para apoyarlo en la operación y administración del dispositivo, según sea el caso.

Los IPS funcionan a través de sensores, los cuáles se ubicaban estratégicamente en segmentos de la red del cliente, por lo tanto, era necesario que el cliente nos proporcionara los diagramas de red, para saber, si el equipo se encontraba en una ubicación óptima y conveniente para la protección perimetral del cliente. Una lista de usuarios, dispositivos y segmentos a proteger por el IPS eran de apoyo para la operación y administración de dichos equipos.

Se solicitaba de igual forma al cliente, si contaba con alguna clasificación de alertas, puesto que, los dispositivos basados en políticas vienen con una configuración de fábrica, las alertas críticas que la herramienta registraba, podría tratarse de un nivel medio o bajo para el negocio, según la investigación correspondiente, partiendo de esta clasificación, el área de monitoreo trabajaba en conjunto con el Oficial de Seguridad en una nueva clasificación, notificando aquellas alertas críticas o sospechosas para el negocio.

4.5.2.2.1 Configuración actual

En el caso de los IPS, todos los clientes ya contaban con al menos un dispositivo referente a esta tecnología, por lo tanto, al tomar la operación de estas herramientas, se hizo un reconocimiento general de las consolas, es decir, identificar el tipo de configuraciones que se tenía en ese momento y las políticas que estaban en modo de bloqueo.

La idea de este reconocimiento, era saber si las políticas configuradas eran las adecuadas para la operación y seguridad del cliente. Por lo tanto, se hizo una extracción de la herramienta y un informe sobre cada una de ellas, lo que llevó a realizar un trabajo de limpieza y mejora en conjunto con los Oficiales de Seguridad, para tener las mejores prácticas de seguridad dentro de las herramientas.

Era importante saber la carga de tráfico que podían soportar los canales de comunicación en dichos dispositivos, ya que un desbordamiento en el canal de comunicación podía provocar que no todas las firmas se estuvieran registrando.

Saber el tiempo en que el dispositivo guardaba en línea los diferentes tipos de ataques fue otro punto importante a obtener, ya que esto permitía hacer un análisis forense sobre alguna anomalía o incidente y saber con cuantos días pasados podíamos contar con la información.

Otra tarea realizada recién comenzada con la operación, fue saber la configuración de reportes y de alertas que se podían generar de la herramienta, el servicio de alertamiento vía correo era un gran apoyo para alertar aquellas firmas que se consideraban críticas para la operación del cliente. La generación de reportes nos permitía obtener un informe en el instante en que estaba sucediendo el evento, para así ofrecerle la mayor información posible al cliente del ataque que se estaba suscitando; que en muchos caso podían resultar falsos positivos, conclusión que se obtenía después de haber hecho un análisis a detalle.

La entrega de reportes para informar al cliente las firmas detectadas con mayor concurrencia, eventos anómalos, requerimientos solicitados, etc., serán tratados en un tema más adelante.

Un caso especial con un cliente, Sm4rt no tenía el control absoluto de la herramienta, es decir, no éramos administradores de la herramienta IPS, por lo tanto, dábamos un apoyo para monitorear los eventos que se fueran presentando, así que se estableció una matriz de comunicación, para que se nos hiciera saber de aquellos cambios e implementaciones en las políticas y la configuración en los distintos sensores del IPS.

De igual forma fue solicitada una conexión VPN para monitorear las herramientas así como un usuario de operación y de administración, a excepción de los IPS´s donde no teníamos el rol de administrador de la consola principal.

La función de respaldos en los IPS´s consiste en resguardar periódicamente la configuración de cada uno de los dispositivos ante cualquier incidente o anomalía que presentara la herramienta, y regresar a un estado anterior, los dispositivos para continuar con la operación normal de monitoreo. Dichos respaldos se hacen en un servidor reservado para las actividades relacionadas con la operación del área.

4.5.2.3 DAM

Las bases de datos almacenan información extremadamente valiosa y confidencial. Una cantidad creciente de regulaciones de conformidad obligan a las organizaciones a hacer auditorías del acceso a dicha información restringida y a protegerla de los ataques y del mal uso.

La herramienta DAM (Database Activity Monitoring) [7] ofrece monitoreo de forma continua y en tiempo real todas las operaciones de las bases de datos, proporcionando a las organizaciones cadenas detalladas de auditoría que indican el quién, qué, cuándo, dónde y cómo de todas las transacciones.

Este tipo de tecnologías, hace auditorías de los usuarios con privilegios que tienen acceso directo a los servidores de bases de datos, así como a los usuarios sin privilegios que tienen acceso a través de diversas aplicaciones.

A la vez que hace auditorías selectivas de la información restringida, los dispositivos DAM monitorean en tiempo real toda la actividad de las bases de datos, a fin de detectar fugas desconocidas de información, transacciones SQL (Structured Query Language) [8] no autorizadas, y ataques a los protocolos y a los sistemas. Tanto si se originan en aplicaciones como en usuarios con privilegios, dentro de la red o en los mismos servidores de bases de datos, se puede alertar, y como opción, bloquear los ataques malintencionados.

Entre otras funciones que realizan los dispositivos DAM se encuentran las siguientes:

- Audita todos los accesos a la información confidencial, tanto de los usuarios de las aplicaciones como de los usuarios con privilegios.
- Alerta o bloquea los ataques a las bases de datos y las solicitudes anormales de acceso, en tiempo real
- Detecta y crea parches virtuales de las vulnerabilidades de los programas de bases de datos, con base en las investigaciones, reduciendo la ventana de exposición. Los parches virtuales minimizan la ventana de riesgo y reducen drásticamente el riesgo de infracciones de la información, mientras se prueban e implementan los parches de las bases de datos.
- Identifica los derechos de acceso excesivos a la información confidencial y a los usuarios latentes
- Agiliza la respuesta ante incidentes

Bien, como se puede comprender, el dispositivo DAM, es una de las herramientas esenciales para la protección de la información de las bases de datos de los clientes. En este caso, ninguno de nuestro clientes contaba con la implementación de esta herramienta, por lo cual con todo ellos se inició el proyecto desde el levantamiento de requerimientos, se trabajó en conjunto con el proveedor de los servicios de la herramienta DAM, el cliente, el oficial de seguridad y el personal correspondiente del área de monitoreo.

El plan comenzó planteándole al cliente que bases de datos se requerían proteger, una vez definidos, se trabajaba en conjunto con el proveedor de la herramienta de seguridad, la integración de cada una de las bases de datos, se fueron activando una a una las auditorías necesarias, tanto para registrar actividad DML (Data Manipulation Language) como DDL Data Definition Language).

Una vez integradas todas las bases de datos, se comenzó con la práctica de analizar eventos permitidos y no permitidos para la generación de políticas de bloqueo, privilegios de usuarios, con el fin de registrar y alertar la actividad no autorizada.

4.5.2.3.1 Configuración actual

Derivado de la implementación desde ceros del dispositivo DAM, se tenía ya el conocimiento y configuración a diferencia de las otras herramientas, las cuales ya estaban implementadas.

Se tenía el registro de cada política implementada, las bases de datos que se registraban por cada cliente, que tipo de auditorías se tenían, así como el control de las licencias y el número de bases de datos que se podía ingresar por consola. De igual forma, se tenían los diagramas y la ubicación física bien conocida de los dispositivos, en varios casos era necesario ir hasta el sitio donde se encontraban las cajas de los equipos para hacer ciertas configuraciones, derivado a que la administración de dichos equipos se hacía mediante una línea de comandos a las cuales accedíamos mediante el protocolo SFTP (Secure File Transfer Protocol) para la extracción de paquetes de datos, con el fin de analizar cualquier evento anómalo o de incidencia a la operación del negocio.

Los reportes solicitados por el cliente fueron personalizados según las necesidades del cliente, los cuales se abordarán en un tema posterior.

Se tenía la matriz de comunicación por ambas partes, cliente-Sm4rt, con el fin de reportar, notificar y atender cualquier eventualidad anómala, incidencia o evento desconocido. Derivado de que Sm4rt era el dueño del control de la operación de los DAM, se podían crear los usuarios necesarios, no había limitación y se tenía el módulo de asignación de privilegios, ya que habían usuarios que se le otorgaba al cliente, pero estos solo contaban con el acceso a consulta de ciertos monitores y auditorías del DAM, esto para evitar algún cambio por accidente en la configuración de la herramienta. Se accedía vía VPN a las consolas de administración del DAM.

Estos dispositivos que se tenían en ese momento, se encontraban en modo espejo, es decir, todo el tráfico que pasaba por la consola del DAM era enviada a un repositorio, información que se podía consultar en cualquier momento para el análisis forense o el estudio a detalle de alguna eventualidad desconocida.

4.5.3 Monitoreo

El área de monitoreo de Sm4rt participaba en distintas actividades, siendo el objetivo principal el monitorear las distintas herramientas de seguridad de los clientes, a continuación listaré los pasos del proceso (Figura 4.7) que se tenía definido y la participación de los diferentes niveles de personal, incluso llegando, en casos específicos, a la gerencia del área.

- Los operadores, encargados de revisar cada una de las pantallas donde se encontraban las consolas de los dispositivos de seguridad, tenían la labor principal de detectar alguna actividad anómala o reportar cualquier alerta crítica que registraran las herramientas.
- Una vez detectada dicha actividad se hacía un registro en una bitácora que se tenía en el área para un control de los incidentes detectados con cada uno de los clientes, con el fin de ir generando una base de conocimientos. En dicha base podíamos consultar si la actividad detectada, anteriormente ya se había registrado algún caso similar. Esta era la base para dar comunicado de la alerta al cliente proporcionando la mejor solución.
- El operador daba seguimiento al caso hasta ser cerrado, en caso de que la solución no fuera satisfactoria, se notificaba al administrador en turno, el cual iniciaba un proceso de investigación, para definir el tipo de actividad. Una vez encontrada dicha solución derivado de un proceso de investigación y aporte de conocimientos de toda el área, se volvía proporcionar al cliente, en espera de saber si se solucionaba el problema presentado. Si el tema era solucionado, se registraba y se hacía una retroalimentación a toda el área, para hacerles saber a detalle la solución que había resuelto el problema.
- Caso contrario a que el administrador no proporcionara la solución al problema, se hacía una escala a nivel de gerencia, cabe mencionar que el gerente del área cuenta con amplios y profundos conocimientos de seguridad, lo cual permitía tener un mejor panorama ante cualquier eventualidad que se pudiera presentar. Una vez reportado el incidente a la gerencia se hacia la apertura de un nuevo caso, lo cual se

le notificaba al cliente, el nivel al cual había llegado el problema y se le proporcionaba una solución definitiva.

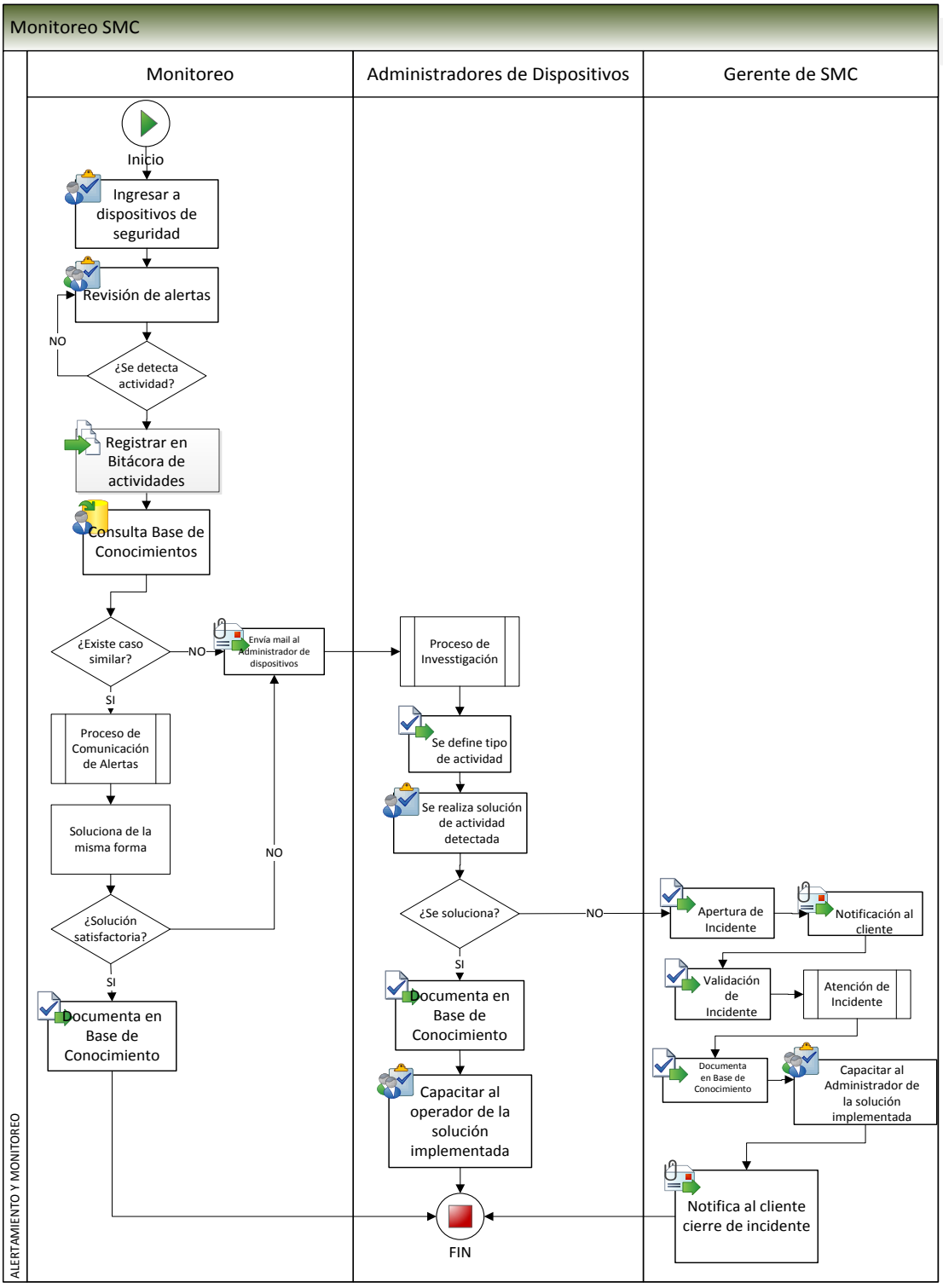


Figura 4.7 Diagrama de Flujo de Monitoreo

- Una vez resuelto el problema se hacía una retroalimentación desde el nivel más alto dentro del área de monitoreo hasta el primer nivel que era la parte operativa, haciendo el cierre definitivo del caso y añadiendo la solución a la base de conocimientos.

4.5.4 Comunicación de Alertas

Como se observa en la Figura 4.8, existe un módulo con la matriz de escalamiento, la cual era necesario definirla desde un principio; dicha matriz está involucrada en varios de los procesos definidos en el área de monitoreo.

Una vez identificado el personal a notificar, se le hacía de su conocimiento el incidente reportado a través de los medios necesarios, los cuáles podían ser con un correo electrónico o llamada telefónica (como bien mencioné en un punto del presente documento), el área contaba con celulares para apoyar a la operación del área y hacer una notificación en tiempo y en forma, sin importar el sitio donde se encontrara el operador.

4.5.5 Generación de reportes mensuales

Derivado de los dispositivos de seguridad que se tenían, se hacían tres principales reportes, uno por cada dispositivo, a continuación se describe el objetivo de cada uno de ellos y la información que se incluía en cada uno de ellos.

4.5.5.1 IPS

El presente reporte para la herramienta de seguridad se dividía en los siguientes rubros su contenido:

- Top 10 de alertas detectadas.
- Top 10 de equipos atacados.
- Top 10 de equipos atacantes.
- Incidentes detectados
- Registro de cambios y actualización de políticas

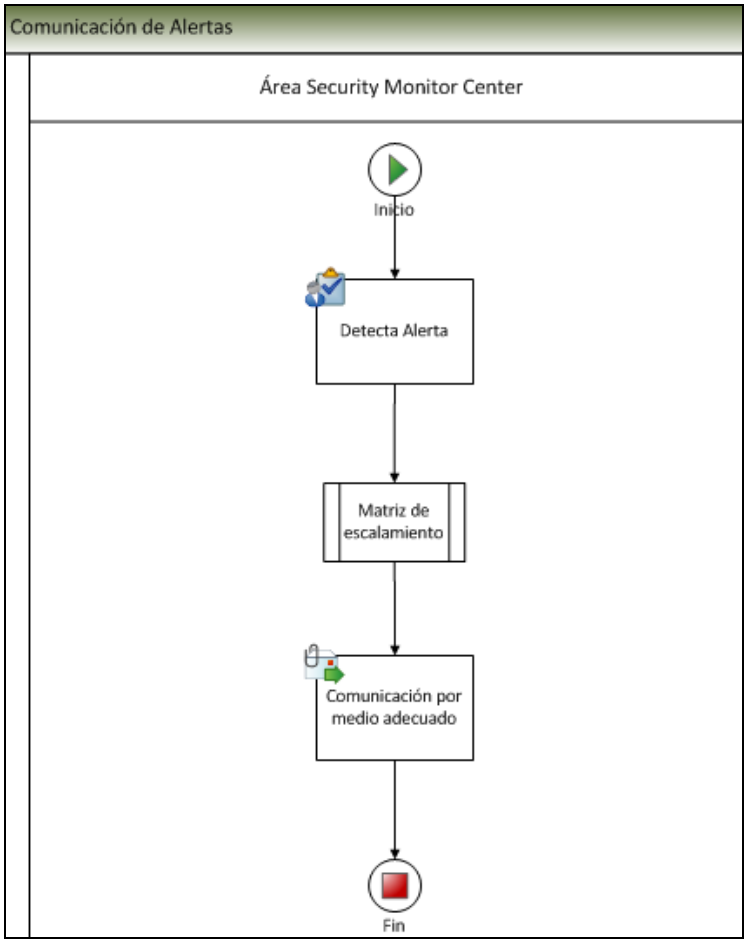


Figura 4.8 Comunicación de Alertas

El objetivo de incluir los puntos antes descritos, era para realizar un análisis y ofrecer las recomendaciones que pudieran aplicarse en la consola de administración del IPS y con ello robustecer la seguridad del cliente.

En el presente reporte se mencionaba la clasificación de severidad en que se podían clasificarse una firma:

Tabla 4.8 Clasificación de severidad de firmas

Severidad	Descripción
Alto	Alerta que requiere un análisis exhaustivo, representa una vulnerabilidad grave y que de concretarse afectaría totalmente el servicio o compromete la integridad de los sistemas.
Medio	Alerta que requiere análisis profundo, representa una vulnerabilidad considerable, que puede

	afectar parcial o totalmente el servicio.
Bajo	Alerta que requiere análisis, representa una vulnerabilidad mínima, pero que si se concreta un ataque puede provocar interrupciones en el servicio.
Información	Alerta clasificada como solo de notificación, no representa una vulnerabilidad grave.

De igual forma se hacía mención del histórico de firmas detectadas, con el cometido de hacer un análisis detallado al cliente de las actividades registradas durante el mes, de igual forma permitía observar el progreso en la mitigación de vulnerabilidades o el descartar falsos positivos, los cuales eran común que se presentaran.

4.5.5.2 SIEM

El objetivo de dichos reportes era el dar un status del cumplimiento e implementación de la centralización de bitácoras en los activos críticos de acuerdo al estándar para la administración y retención de bitácoras y a la lista de dispositivos entregada por el Oficial de Seguridad.

El reporte estaba dividido en las siguientes secciones:

- Integración de dispositivos:
  - En esta sección se presentan las actividades y/o solicitudes pendientes con respecto a la integración, implementación y revisión de equipos a centralizar en el sistema SIEM.
- Cumplimiento de registro de bitácoras:
  - Sección donde se muestra el cumplimiento de registro de bitácoras de acuerdo al estándar para la administración y retención de bitácoras en las diferentes plataformas. De igual forma se daba a conocer el cumplimiento de recepción y revisión de eventos en el sistema.
- Rendimiento:
  - Se daba un reporte del almacenamiento de bitácoras, con el fin de llevar un control de los respaldos.
  - Se muestra el porcentaje de procesamiento que tiene el dispositivo para el almacenamiento y normalización de eventos.

- Siguientes pasos:
    - Se programaban las actividades de acuerdo al estándar para la activación y retención de bitácoras con el fin de cumplir con el 100% de las normativas, en este caso, la ley SOx.
- Incidentes detectados:
    - En esta sección se muestra una relación de los incidentes que se presentaron durante el transcurso del mes y aquellos que siguen en un estatus de seguimiento a la solución.
- Registro de cambios y actualización de políticas
    - Tanto para un control interno como con el cliente, se llevaba un control de los cambios que se realizaban dentro del sistema.

4.5.5.3 DAM

El objetivo del reporte es dar un status de las actividades realizadas durante el mes en curso, reportando las problemáticas e incidentes presentados. De igual forma se da a conocer un detalle de los cambios y configuraciones realizadas a la consola, políticas y auditorías actualmente activas en el DAM, finalizando con un informe del estado general de la consola.

El reporte estaba dividido en las siguientes secciones:

- Actividades realizadas
    - En esta sección se dan a conocer las modificaciones y activación de auditorías, ejecución de purgas, entrega de reportes bajo demanda del cliente, así como pruebas realizadas.
- Problemáticas
    - En esta sección se dan a conocer los problemas que se presentaron en la herramienta DAM así como en el servicio de operación y monitoreo.
- Pendientes
    - Aquí se listan los requerimientos basados en las problemáticas presentadas, así como haciendo mención de los responsables directos en atender el

requisito como el estatus en que se encontraba, con el objetivo de no dejar de atender ningún caso.

- Monitoreo
    - En esta sección se muestra la actividad relevante presentada con la operación de las bases de datos y una relación de los incidentes que se presentaron durante el transcurso del mes.
- Incidentes
    - Se daba un reporte de la fecha y la descripción del incidente reportado durante el mes, así como mención del estatus, si estaba resuelto, en proceso o no se había atendido aún.
- Cambios y configuraciones
    - Se muestra un listado de las modificaciones hechas a las políticas y auditorías configuradas en la herramienta DAM, así como cambios a las bases de datos o a la infraestructura del cliente.

4.5.6 Proceso de Guardia

Para continuar con la revisión de las herramientas de seguridad en los fines de semana, se tenía establecido un proceso de guardia, a pesar de no dar un servicio operativo como tal al cliente, Sábados y Domingos, se hacía notificación de cualquier evento anómalo para que fuera revisado a primera hora del día Lunes.

En caso de ser un incidente mayor, se le notificaba al ISO para que hiciera las llamadas pertinentes y en caso de ser necesario se hacía una visita en sitio donde se presentara el incidente.

Como ya se ha dado mención, en cada uno de los dispositivos se hacía una configuración de las alertas críticas o de aquellos eventos que el cliente ya había reportado en su momento como no permitido. Estas alertas llegaban vía correo a cada uno de los integrantes del equipo y de igual forma estaban configurada para llegar vía telefónica al dispositivo móvil que teníamos asignados.

De esta forma podíamos ser notificados al instante de cualquier alerta detectada en los dispositivos. Según el personal asignado a la guardia, le correspondía revisar cada dos horas, vía remota, las consolas de los dispositivos de seguridad y mandar un correo del estatus de ellas, ya que en algunos casos, los equipos se podían desconectar o dejar de recibir eventos.

El recibir una alerta, el operador notificaba al administrador vía telefónica, mientras se registraba en la bitácora de actividades el evento reportado y se enviaba un correo de registro de dicha alerta. El operador quedaba en espera de las indicaciones del administrador mientras éste realizaba un análisis de la alerta detectada, determinando si se trataba de un falso positivo o no, en caso de ser una actividad perjudicial para el cliente, se notificaba, a través de la matriz de escalamiento ya definida tanto internamente como con el cliente, al personal correspondiente.

Quedando así reportado el incidente en el momento sucedido, al cual se le dará seguimiento una vez que sea revisado por parte del personal del cliente, donde generalmente, el área de sistemas e infraestructura trabaja en un horario de 24x7.

En la figura 4.9 se muestra el proceso definido para las guardias en el horario no operativo del cliente.

4.6 Cambios y Requerimientos

En el presente capitulo se dará a conocer el procedimiento cuando el Oficial de Seguridad y/o Cliente requerían de algún cambio de configuración en las diferentes herramientas de seguridad o algún requerimiento en particular.

Era de suma importancia registrar y notificar, cualquier cambio en los diferentes dispositivos de seguridad, ya sea cambio de política, configuración, performance, generación de reportes, alertamiento, etc., con el objetivo de tener conocimiento, de quién lo hizo, por qué, cuándo, quién lo solicitó y el proceso que realizó para ejecutar la tarea solicitada.

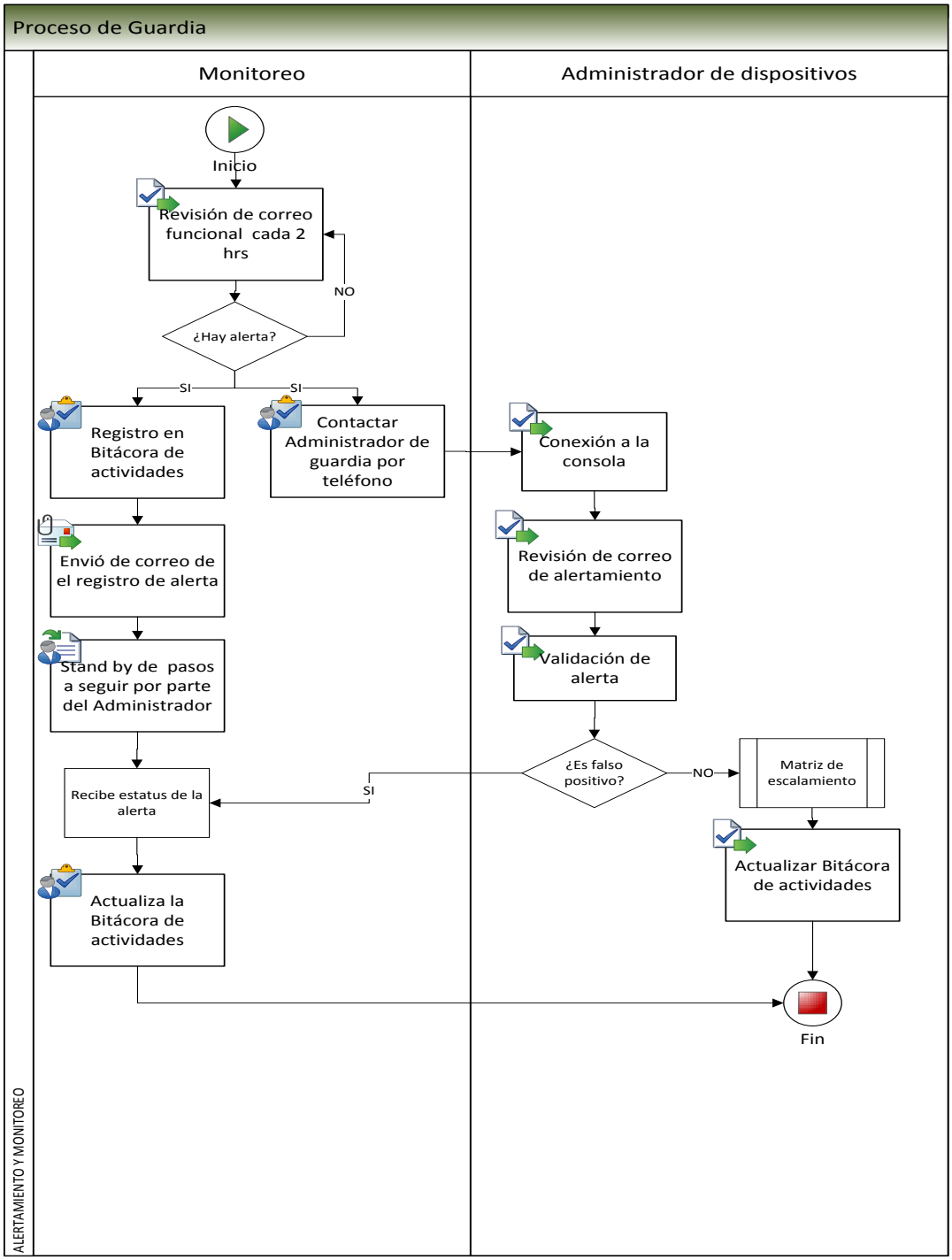


Figura 4.9 Proceso de Guardia

El tener este control nos permitía, en caso de existir alguna implicación después de haber ejecutado el requerimiento, resolver de manera óptima y en tiempo el problema presentado, ya que se conocían paso a paso, los cambios realizados en los dispositivos de seguridad y

quién estuviera en ese momento a cargo de la operación en el centro de monitoreo, pudiera realizar, sin contratiempos, el proceso correspondiente para dar solución al inconveniente.

4.6.1 Generación de cambios

Ya sea por necesidad del negocio u optimización del servicio de operación entre el ISO y área de monitoreo, constantemente el Oficial de Seguridad realizaba peticiones al área para aplicar cambios, ya sean en las auditorías o políticas de la herramienta o como podría darse el caso de realizar alguna configuración en la arquitectura de la herramienta.

El procedimiento de generación y aplicación de cambios (Fig. 4.10) se describe a continuación:

- El Oficial de seguridad realizaba la solicitud del cambio vía correo electrónico, (era importante tener evidencia de todo lo realizado por cualquier incidente que pudiera presentarse).
- El administrador del dispositivo por parte de equipo de monitoreo, se encargaba de revisar y analizar el requerimiento solicitado por el Oficial de Seguridad. Una vez que se tenían todos los elementos necesarios para ejecutar la tarea, se aplicaba el cambio dentro del horario establecido por el ISO. Finalmente, se enviaba un correo de notificación al equipo de monitoreo del cambio realizado para documentar el proceso realizado.
- En caso de faltar algún requisito para el cambio, se solicitaba al ISO la información faltante, de igual forma, al final de la ejecución del cambio, se le notificaba la aplicación del cambio solicitado por este.

4.6.2 Requerimientos

A diferencia del flujo que se vio en el tema anterior, en el diagrama que se puede ver en la Figura 4.11, se encuentra involucrado directamente el cliente, ya que había solicitudes que venían directamente de las direcciones de consultoría de sistemas del negocio, no solamente era aplicar cambios en la configuración de las herramientas, en muchos casos eran temas de investigación para apoyar al cliente en dudas o dar recomendaciones para la mejora del servicio y aseguramiento de la información.

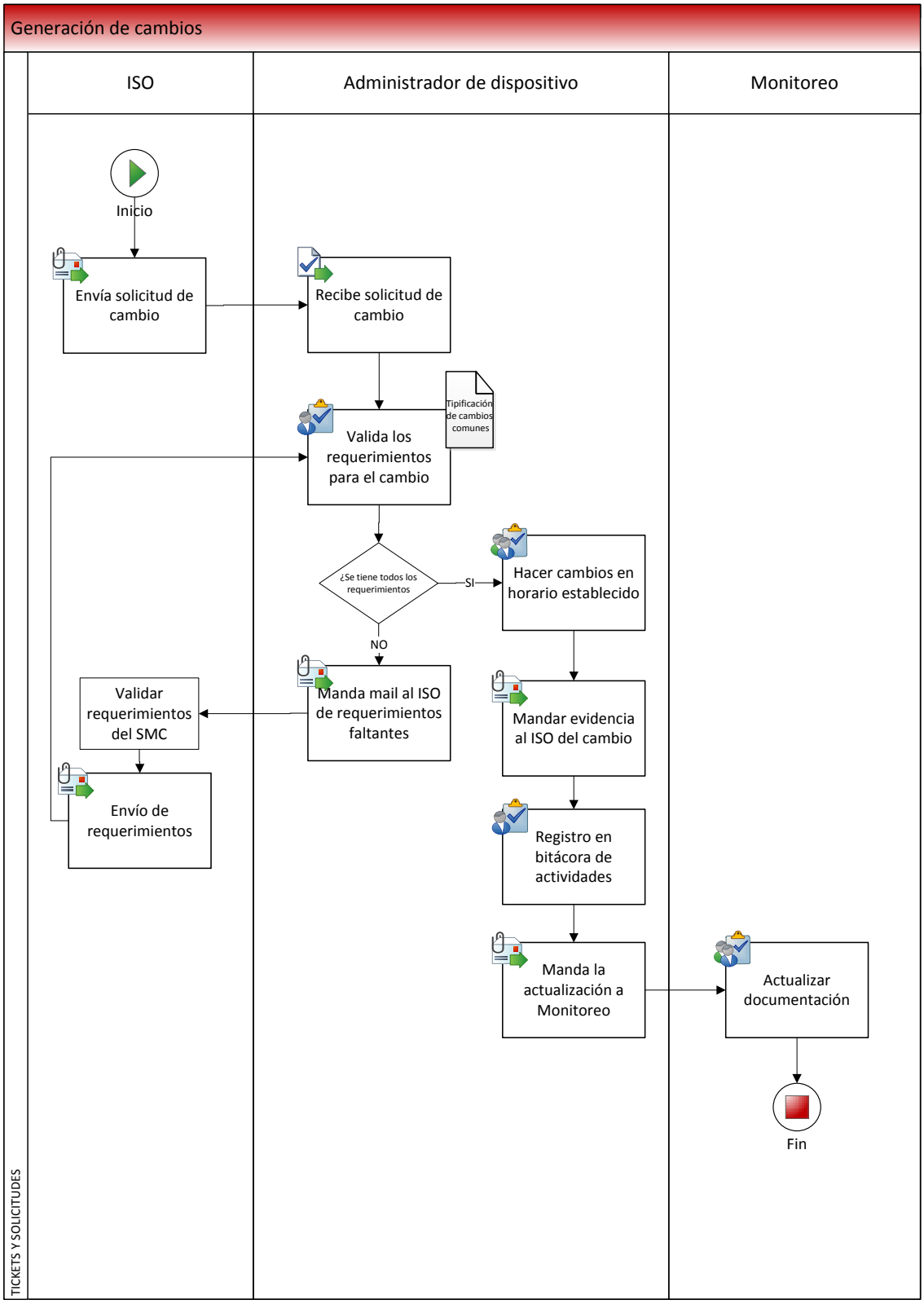
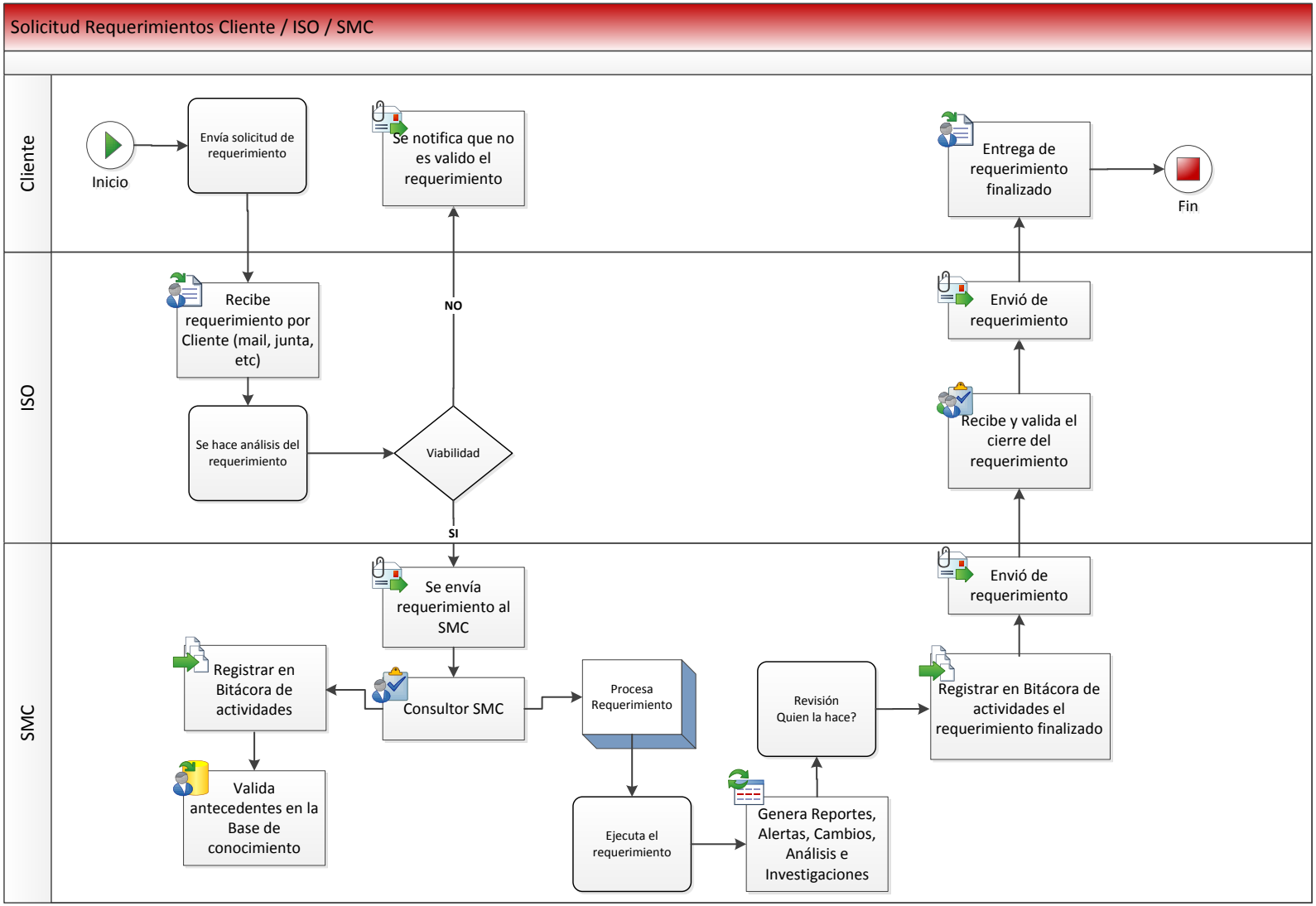


Figura 4.10 Flujo de Generación de Cambios

A continuación daré una descripción del proceso que se tenía definido entre el Cliente/ISO/Monitoreo para llevar a cabo la atención de requerimientos:

- Del lado del cliente, las reuniones para tratar temas de seguridad son muy constantes, de las cuales generalmente siempre surgen requerimientos que debe aplicar el equipo de monitoreo. Así sea una solicitud que se comentó en alguna junta o llamada telefónica, el ISO tiene la obligación de hacer llegar el requerimiento por escrito al área de monitoreo; puede ir acompañada la notificación de una llamada telefónica, pero para fines de operación del centro de monitoreo, este debe tener evidencia por escrito del requerimiento, en dicho correo debe ir copiado el personal involucrado por parte del cliente.
- Una vez analizado el requerimiento por parte del Oficial de Seguridad y definir si era factible o no dicha solicitud, ésta llegaba al equipo de monitoreo, donde tanto personal de monitoreo y administradores, como el gerente de área en algunos casos, analizaban los puntos del requerimiento, registrando y documentando cada paso a ejecutar.
- Se generaban los reportes, correos, cambios a aplicar, proceso de investigación, alertas, derivados del requerimiento solicitado, enviando todo este proceso documentado al Oficial de Seguridad, haciendo la notificación final y cerrar por parte del equipo de monitoreo, el requerimiento que nos fue solicitado ejecutar.
- El oficial de seguridad se encargaba posteriormente de validar los cambio y hacer la notificación pertinente al cliente, dándole a conocer el proceso que se realizó, el antes y después del cambio y presentando los resultados finales y de esta forma se cerraba al 100% el requerimiento.
- Por parte del equipo de monitoreo, se registraba el proceso realizado, para tenerlo en la base de conocimientos del área y tomarlo como consulta para posteriores requerimientos, - iguales o similares - y hacer una mejora constante en los servicios ofrecido por parte del área.



- Figura 4.11 Flujo de Solicitud de Requerimientos Cliente/ISO/Monitoreo

4.6.3 Investigación

El área de la seguridad de la información es un mundo de conocimientos, uno aprende a ser autodidacta, ya que muchos temas derivados de incidentes de seguridad, el surgimiento de nuevos ataques y técnicas para vulnerar la seguridad del cliente, nuevos virus, eventos desconocidos, etc., nos vemos en la necesidad de consultar todas las fuentes posibles de información con el objetivo de ofrecer al cliente una respuesta y solución clara, precisa y eficiente.

La mayor parte de las investigaciones eran derivadas de los requerimientos del cliente, como lo mencioné al principio de este documento, uno de los proyectos en que participé, trataba del análisis de una herramienta de seguridad SIEM, cuyo objetivo consistía en tomar la decisión sobre si era o no eficaz para el cliente en cuestión. Esto conllevó a la investigación del funcionamiento del equipo, revisar manuales, estudiar conceptos que nos permitiría tomar la mejor conclusión para el cliente.

Durante mi estancia en el equipo de monitoreo, me apoyaba de herramientas y fuentes de información para realizar el análisis de alertamientos de seguridad, eventos desconocidos o incidentes de seguridad. Haré mención de algunas fuentes que me permitieron ofrecer una solución al cliente ante cualquier evento que perjudicara la seguridad de la información.

Muchas de las tecnologías operadas contaban con sus propios manuales de administración, sin embargo, en muchas ocasiones resultaba muy limitada la información que ofrecían. Era muy común apoyarnos de herramientas de análisis de tráfico como WireShark [9], que en lo personal, fue de gran apoyo para realizar distintas investigaciones, como el análisis de paquetes, y analizar, por ejemplo, que la herramienta DAM estuviera procesando de forma correcta las sentencias que recibía el dispositivo, ya que hubo un caso donde los paquetes llegaban truncados, que impedían que la actividad fuese registrada en el DAM, de manera que resultaba imperativo informarle al cliente y al proveedor del servicio para que tomase las medidas necesarias y resolver el problema presentado.

Fuentes como OWASP (Open Web Application Security Project) [10], el catálogo ofrecido por MITRE (CVE List, Common Vulnerabilities and Exposures) [11], artículos emitidos por la misma subdirección de Seguridad de la Información de la UNAM [12], blogs como

SecuritybyDefault [13] con publicaciones relevantes a ataques de seguridad como el XSS (Cross Site Scripting), por hacer mención a unas cuántas fuentes, permitían hacer una investigación, lo más detallada posible; quiero resaltar el buen trabajo en equipo que se fomenta dentro de la consultoría Sm4rt, ya que la adquisición de conocimientos de los diferentes integrantes del área, eran compartidos y se hacía siempre la respectiva retroalimentación dando una respuesta al por qué de las cosas.

4.6.4 Planeación de visitas

Para implementar mejoras al servicio, el equipo de monitoreo proponía al Oficial de Seguridad de los respectivos clientes, realizar visitas a los distintos administradores de bases de datos, de servidores, de usuarios, de seguridad física y de las diferentes aplicaciones con las que contaba el cliente.

Estas visitas tenían como objetivo revisar con cada uno de los administradores, lo que se tenía configurada en cada una de las herramientas para ser más proactivos que reactivos. Un ejemplo de esto es el DAM, herramienta en la cual se tenían definidas políticas y auditorías, con sus correspondientes alertas y reportes pre configurados. La idea era recibir una retroalimentación de los DBA´s (Database Administrator) para afinar las políticas ya establecidas o en su caso la creación de más reglas para notificar al cliente de manera oportuna y en tiempo, logrando prevenirlos de algún ataque o evento desconocido.

Este trabajo representa un mejor control y entendimiento de la información que recibían las diferentes herramientas de seguridad, pues con la investigación realizada previamente (y que mencioné en capítulos anteriores) se podía identificar de forma más clara, si una alerta crítica para un IPS era real o podría tratarse de una actividad normal.

Mientras más conocimiento tuviéramos de la operación del cliente, de sus servidores, bases de datos, infraestructura, el cometido de sus aplicaciones, mejor sería para nosotros tener un panorama amplio de la información procesada y analizada a través de las herramientas de seguridad.

4.6.5 Reportes ad hoc

Como se hace mención en el título de este apartado, no siempre se hacían únicamente los reportes definidos que se entregaban al cliente mensualmente, a veces el cliente o el mismo Oficial de Seguridad solicitaba reportes bajo demanda, para conocer el estatus de algún servidor, aplicación o para el monitoreo de ciertos usuarios, algo en específico.

Un ejemplo de un reporte ad hoc, de los cuales hice gran cantidad durante mi estancia en monitoreo, fue la generación de reportes de actividades de usuarios desde la herramienta DAM, estos eran personalizados de acuerdo a lo solicitado por el ISO, ya sea para conocer, por ejemplo, que accesos tuvo tal usuario, en tal día y hora, con gráficas y tablas según sea el caso. En el reporte mensual se daba un estatus de estos reportes solicitados a lo largo del mes por los diferentes clientes.

4.7 Liberación de Servicio

Una vez contratado los servicios con Sm4rt Security Services, al cliente se le otorgaba un documento final conocido como SOW (Statement of Work) que era una definición de servicios entre el cliente y Sm4rt.

El contenido del documento tenía como objetivo principal, le declaración de servicios que había solicitado el cliente, referente a seguridad de las bases de datos, prevención y detección de intrusos y centralización y correlación de bitácoras, entre otros servicios que se pudieran brindar dentro del área.

Se especificaba el alcance, es decir, el número de dispositivos a monitorear, los horarios en que se le daría atención al cliente en oficinas y de igual forma el horario de guardias.

Se definían las actividades a realizar de las diferentes áreas involucradas como el cliente, el Oficial de Seguridad y la propia área de monitoreo.

Descripción de los entregables mensuales a reportar al cliente así como su contenido, niveles de servicio, es decir, tiempo de respuesta ante cualquier evento de seguridad. Se

hacía mención, de igual forma, los requerimientos solicitados por parte del área de monitoreo para una operación óptima de la herramienta de seguridad.

Se establecía dentro del mismo documento el personal dedicado al servicio de administración y monitoreo de dispositivos. La penalización en caso de incurrir con algunos de los puntos establecidos dentro del contrato y, por último, el apartado de firmas de conformidad entre cliente y Sm4rt.

Todos los puntos mencionados anteriormente fueron desarrollados y descritos a lo largo del presente documento, ya que el cometido del área de monitoreo era ofrecer dichos servicios de operación y administración, los cuales se plasmaban en escrito a través del documento SOW ya mencionado.

CAPÍTULO V

RESULTADOS

En este capítulo presentaré las aportaciones que le brindé a la empresa Sm4rt Security Services y las aportaciones que obtuve al desarrollar mi trabajo profesional con ellos.

4.1 Aportación Empresarial

Los socios que conforman la empresa Sm4rt, venían trabajando en diferentes proyectos donde el objetivo era innovar y formalizar un servicio en particular de la seguridad. Apoyé a darle vida a dicho servicio el cual consistía en un área de monitoreo y respuesta a incidentes.

El centro de monitoreo, hoy en día, cuenta con una oficina explícitamente para el desarrollo de las actividades de monitoreo, la cual está conformada por diez personas en turnos de 24x7x365, que está cerrando nuevos contratos y atrayendo nuevos clientes de renombre.

Este proyecto se fundamentó tan bien, se estructuró de manera correcta, la operación se mantuvo en tiempo y forma, que gracias a ellos, el área de monitoreo es un negocio base de la empresa.

Se ha tenido el reconocimiento por parte de clientes del servicio ofrecido, mi trabajo aportado al igual que mis ideas y conocimientos, y sobre todo las investigaciones que me llevaron a realizar los distintos retos que se me presentaron en el crecimiento y formación del área, en conjunto con el gran esfuerzo de mis compañeros y gerente del área, el centro de monitoreo de Sm4rt se ha consolidado y es gratificante que gracias a ello, la empresa siga reclutando gente que aporte un crecimiento al área y sea una fuente de trabajo.

4.2 Aportación Personal

Cabe mencionar que Sm4rt, fue mi primera fuente de trabajo relacionado con temas de seguridad de la información, fue un reto que decidí afrontar derivado a mi nula experiencia

en el campo. Cada día se me presentaba un reto, veía un tema nuevo a diario, lo cual me llevaba a realizar una serie de investigaciones, ser autodidacta, a trabajar en equipo, a la capacidad de generar soluciones y dar la mejor recomendación para mitigar los riesgos que se pudieran presentar. Dicha empresa me abrió las puertas y recibí el apoyo de mis compañeros para superarme en cada tarea y actividad que se me habían asignado.

Los conocimientos y experiencias que he adquirido han sido también fruto de mi esfuerzo. Mi desempeño desde la participación dentro del área de monitoreo hasta mis actividades que desarrollo hoy en día como Oficial de Seguridad, me han permitido tener un panorama amplio de todo lo que rodea el mundo de la seguridad de la información y su importancia en las empresas.

En este tiempo que he laborado en Sm4rt, puedo notar un considerable cambio en mi desarrollo y crecimiento profesional, hoy tengo la capacidad de trabajar en sitio con el cliente y poder establecer soluciones, debatir temas de seguridad con personal de diferentes cargos, administradores, operadores, gerentes, directores, etc., proponer recomendaciones para la mitigación de riesgos, me ha forjado una gran confianza y seguridad en mi persona, con la motivación de seguir afrontando nuevos retos y el de apoyar a mis colegas en su formación profesional.

A continuación menciono los principales puntos en los que me he desarrollado dentro de Sm4rt y las aportaciones que me ha brindado:

- Operación y administración de dispositivos de seguridad como son IPS, IDS, DAM, SIEM y Firewall aplicativo.
- Adquisición de experiencia en el análisis, seguimiento y documentación de incidencias. Atención a requerimientos como escaneos éticos y la elaboración de distintos reportes haciendo de su conocimiento al cliente, de aquellas actividades que representan un riesgo, de igual forma, a dar las recomendaciones de mejora para una mayor protección de la información.
- Llevar a cabo la gestión de riesgos de seguridad de la información así como la revisión de controles de seguridad y de acceso en las aplicaciones. Generación de políticas y

estándares para los clientes, programación de actividades para el hackeo ético llevando a cabo el análisis de vulnerabilidades de aplicaciones y su infraestructura.

- Generación de las bases para realizar auditorías de seguridad en siete diferentes capas: Seguridad Física, Aplicaciones, Gobernabilidad, Administración de Usuarios, Base de Datos, Servidores y de Red, esta revisión la llevo a cabo en diferentes clientes con el objetivo de darles un panorama de cómo se encuentran a nivel de seguridad, indicando sus fortalezas y debilidades junto con las recomendaciones para mitigar los riesgos identificados en dicha revisión.

CONCLUSIONES

Sm4rt ha sido el lugar donde se han generado un cúmulo de vivencias, gente, experiencias y conocimientos, que han influido en mi forma de visualizar el mundo ahora, poniendo en práctica el aprendizaje obtenido durante la carrera y las prácticas realizadas en los laboratorios de la Facultad de Ingeniería.

Aún terminando el plan de estudios de la carrera, uno sigue adquiriendo conocimientos fuera de las aulas, principalmente, el proyecto descrito en el presente trabajo me permitió ver mis fortalezas y debilidades, el haber iniciado mis labores en Sm4rt con la asignación de este proyecto, me abrió las puertas hacia el área de la seguridad de la información. En los proyectos que participé en monitoreo fueron las bases para desempeñar hoy en día mis actuales actividades. Todo lo visto en las aulas durante mi formación universitaria, era tan solo una pizca de todo lo que uno puede experimentar fuera de ellas, todo lo aprendido de los profesores eran apenas las bases para seguir con mi formación profesional fuera de la facultad.

Durante la creación del centro de monitoreo, uno se da cuenta que no sólo es cuestión de tener la mejor tecnología para proteger la información, también depende mucho de la operación y administración correcta de la herramienta para sacar el mejor provecho de la tecnología, no sólo basta con instalar y conectar.

El papel desempeñado por los operadores y administradores del centro de monitoreo es crucial, de nosotros dependía la detección de amenazas y protección de las activos más importantes de las organizaciones que cuentan con nuestros servicios. La seguridad no solo regía en los dispositivos de seguridad, el análisis y capacidad de razonamiento de los eventos detectados, la daba el personal del área de monitoreo

Es importante que las empresas no sólo se queden con la inversión de tecnologías costosas, temas como el manejo de una correcta configuración, monitoreo, seguimiento, implementación de políticas, auditorías, alertas y análisis de los controles de seguridad y tecnologías implementadas a través de dichas inversiones, no se realiza correctamente o

simplemente no se hace. La creación de un SOC en Sm4rt vino a poner orden en sus clientes y robustecer la seguridad con la que ya contaban.

La creación del SOC, no sólo es un servicio o proceso de monitoreo y validar que los equipos estén encendidos y funcionando correctamente, derivado de este trabajo, podemos tener una visión más allá de lo que está a simple vista en un centro de monitoreo. La esencia de un SOC es el de gestionar el riesgo que pueda afectar la seguridad de la información en sus tres principales pilares, confidencialidad, integridad y disponibilidad. Es necesario definir que lineamientos regirán el centro de monitoreo, como se estructurará, que jerarquías se deben de manejar, los alcances de las actividades asignadas a cada personal, todos estos puntos se llevaron a cabo en la creación del centro de monitoreo.

No fue una tarea sencilla, ya que se contaba con poco personal iniciado el proyecto, pero se cumplieron cada uno de los objetivos planteados.

La implementación de políticas de seguridad son indispensables en cualquier organización, ya que a partir de éstas, nosotros logramos apoyar a los clientes en la protección de su información, con base a los lineamientos establecidos en las políticas, nosotros damos las recomendaciones necesarias para ese cumplimiento y ofrecer los servicios necesarios para la protección de su información.

Es muy importante también recalcar que los tiempos de respuesta son cruciales para la contención de cualquier ataque que se pueda presentar, fueron lineamientos que se establecieron con cada uno de los clientes, lo que permitió tener una comunicación adecuada con cada uno de los administradores responsables en los negocios. Como bien se describe en este trabajo, establecer matrices de escalamiento, vías de comunicación y los diferentes flujos dependiendo del caso, permitieron siempre ofrecer de manera oportuna, respuestas en tiempo y forma de los ataques, alertamientos o incidentes de seguridad presentados.

La generación de informes, reportes y la documentación de cada evento o proceso realizado con el cliente es fundamental para crear una base de conocimientos en el equipo y realizar la retroalimentación necesaria para mantener un nivel adecuado de operación en el área de monitoreo, es importante el compartir experiencias y conocimientos en el grupo, esto

permite que el área se fortalezca y estemos listos para reaccionar ante cualquier evento que se pueda presentar o en su caso, y el mejor de los escenarios, el de prevenirlos.

Cada año se presentan nuevos ataques informáticos, virus, malware, robos de identidades, casos de ingeniería social, por lo tanto, no solo es necesario contar con las tecnologías de resguardo de la información, sino también es esencial hacer conciencia de todos los riesgos que puede implicar el no llevar a cabo buenas prácticas se seguridad, tanto con los usuarios como con los mismos administradores de los distintos dispositivos de red, bases de datos y de sistemas operativos. Esto se puede lograr haciendo comunicados de seguridad a toda la empresa, como hoy en día se aplican en varias empresas. Ya que muchos usuarios desconocen el riesgo, de incluso responder un simple correo electrónico, y ser víctimas de un problema llamado phishing.

Algo que puedo resaltar de haber estado en un centro de monitoreo, así como desempeñar mi papel de Oficial de Seguridad en la actualidad, es que el factor humano es sumamente importante en el cuidado de la información del negocio, es verdad que las herramientas de seguridad robustecen la seguridad del cliente, teniendo a usuarios que hagan un uso correcto del software y equipo de cómputo, acatando los controles de acceso a la red corporativa, a los sistemas de información así como el buen uso el cumplimiento de una política robusta de contraseñas, disminuirá la actividad de alertamientos en dispositivos como el IPS, ya que en monitoreo, muchas de las alertas detectadas, era por el uso de software no permitido, lo que puede poner en riesgo la seguridad de la información.

Si algo me ha dejado muy en claro mi participación en Sm4rt es que la seguridad es un proceso continuo que exige estar actualizado y sobre todo aprender sobre, de las propias experiencias.

Para terminar, quiero resaltar los buenos valores que se difunden dentro de la empresa Sm4rt, y sobre todo el buen trabajo en equipo que se hace, he tenido la oportunidad de estar tanto en el área de monitoreo y ahora como Oficial de Seguridad, realizando auditorias de seguridad, lo que me ha fomentado ser una persona sumamente ética y llevando a la práctica los buenos principios que me han forjado en casa, como la honestidad y la humildad, cumpliendo con mis responsabilidades, inculcándome el valor de la información

y haciendo conciencia de los riesgos que en la actualidad existen por no contar con los debidos controles de seguridad para el resguardo de la información en las empresas.

GLOSARIO

ACL: Listas de control de acceso, permiten un control del tráfico de red, a través de una serie de instrucciones. Cada instrucción permite o rechaza tráfico, usando uno o más de los siguientes criterios: el origen del tráfico; el destino del tráfico; el protocolo usado.

Bitácora: Una bitácora es un registro oficial de eventos durante un periodo de tiempo en particular. Para los profesionales en seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación.

DAM: Database Activity Monitoring, herramienta que permite auditar y monitorear las bases de datos en tiempo real. De igual forma tiene la función de detectar y bloquear ataques, accesos no autorizados, fugas de información y el permitir identificar actividades fraudulentas.

DDL: lenguaje artificial para definir y describir los objetos de la base de datos, su estructura, relaciones y restricciones

DML: Lenguaje artificial de cierta complejidad que permite el manejo y procesamiento del contenido de la base de datos.

Detección Basada en Firmas: Una firma tiene la capacidad de reconocer una determinada cadena de bytes en cierto contexto, y entonces lanza una alerta.

Detección Basada en Políticas: En este tipo de detección, el IPS requiere que se declaren muy específicamente las políticas de seguridad. Por ejemplo, determinar que hosts pueden tener comunicación con determinadas redes.

Detección Honey Pot: Aquí se utiliza un ‘distractor’. Se asigna como Honey Pot un dispositivo que pueda lucir como atractivo para los atacantes. Los atacantes utilizan sus recursos para tratar de ganar acceso en el sistema y dejan intactos los verdaderos sistemas. Mediante esto, se puede monitorizar los métodos utilizados por el atacante e incluso

identificarlo, y de esa forma implementar políticas de seguridad acordes en nuestros sistemas de uso real.

Eventos AAA: corresponde a un tipo de protocolos que realizan tres funciones: Autenticación, Autorización y Contabilización (Authentication, Authorization and Accounting en inglés). La expresión protocolo AAA no se refiere pues a un protocolo en particular, sino a una familia de protocolos que ofrecen los tres servicios citados.

FTP: es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor.

Hotfix: es un paquete que puede incluir varios archivos y que sirve para resolver un bug específico dentro de una aplicación informática.

LFPDPPP: la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

MITRE (CVE List): es una lista o diccionario a disposición del público y de uso gratuito de identificadores normalizados de vulnerabilidades y exposiciones comunes de equipo.

OWASP: Open Web Application Security Project, es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro.

PCI: Payment Card Industry, es un estándar que ayude a las organizaciones que procesan, almacenan y/o transmiten datos de tarjetahabientes (o titulares de tarjeta), a asegurar dichos datos, con el fin de prevenir los fraudes que involucran tarjetas de pago débito y crédito.

Phishing: es una técnica de captación ilícita de datos personales (principalmente relacionados con claves para el acceso a servicios bancarios y financieros) a través de correos electrónicos o páginas web que imitan/copian la imagen o apariencia de una entidad bancaria/financiera.

SFTP: Secure File Transfer Protocol, es un protocolo del nivel de aplicación que proporciona la funcionalidad necesaria para la transferencia y manipulación de archivos sobre un flujo de datos fiable.

SLA: Service Level Agreement, traducido como Acuerdo de Nivel de Servicio, es un documento habitualmente anexo al Contrato de Prestación de Servicios. En el SLA se estipulan las condiciones y parámetros que comprometen al prestador del servicio (habitualmente el proveedor) a cumplir con unos niveles de calidad de servicio frente al contratante de los mismos (habitualmente el cliente).

Sniffer: un analizador de paquetes es un programa de captura de las tramas de una red de computadoras.

SQL: Structured Query Language, es un lenguaje de base de datos normalizado, utilizado por los diferentes motores de bases de datos para realizar determinadas operaciones sobre los datos o sobre la estructura de los mismos.

SSH: Secure SHell, nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, de igual forma permite copiar datos de forma segura.

SSL: Secure Socket Layer, proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar.

SUDO: (switch user do), es una utilidad de los sistemas operativos tipo Unix, como Linux, BSD, o Mac OS X, que permite a los usuarios ejecutar programas con los privilegios de seguridad de otro usuario (normalmente el usuario root) de manera segura.

XSS: El Cross-site Scripting o XSS es un problema de seguridad en las páginas web, generalmente por vulnerabilidades en el sistema de validación de datos entrantes. Un ataque XSS consiste en enviar un script malicioso a la página, ocultándolo entre solicitudes legítimas.

REFERENCIAS

Páginas Web y organizaciones

1.- http://www.outpost24.com/?lang=es

2.- http://www.sans.org/information_security.php

3.- http://www.soxlaw.com/

4.- http://inicio.ifai.org.mx/_catalogs/masterpage/Consultar-la-LFPDPPP.aspx

5.- https://latinamerica.rsa.com/node.aspx?id=3170

6.- http://www.mcafee.com/mx/products/network-security-platform.aspx

7.- http://www.imperva.com/products/dsc_database-activity-monitoring.html

8.- http://technet.microsoft.com/es-es/library/ms174377.aspx

9.- http://www.wireshark.org/

10.- https://www.owasp.org/index.php/OWASP_Top_Ten_Project

11.- http://cve.mitre.org/

12.- http://www.seguridad.unam.mx/index.html

13.- http://www.securitybydefault.com/2010/01/eu2010es-el-fail-es-para.html