UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Gestión de usuarios privilegiados en infraestructura crítica

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniera en Computación

P R E S E N T A

Tania Gabriela Montero Trejo

ASESORA DE INFORME

Ing. Josefina Rosales Garcia

Ciudad Universitaria, Cd. Mx., 2018

Índice

1. Introducción y Objetivo

1.1 Introducción

En la actualidad, las organizaciones se enfrentan al aumento de las amenazas de ciberseguridad y también a los crecientes desafíos en cuanto a protección de información sensible y aplicaciones que residen en sus servidores. Al mismo tiempo tienen la necesidad de cumplir con requisitos regulatorios complejos. Estas demandas requieren controlar las acciones de los usuarios para gestionar el acceso a los sistemas y ser capaces de demostrar que los recursos son accesibles únicamente por personal autorizado y sólo cuando lo necesitan.

En las organizaciones, a menudo los administradores de sistemas tienen acceso libre a las cuentas que poseen los mayores privilegios, a su vez dichas cuentas son compartidas en la mayoría de los casos, esto se hace habitualmente mediante la distribución de la contraseña, lo cual es inherentemente riesgoso, ya que las contraseñas pueden ser fácilmente expuestas o compartidas con personas no autorizadas. Del mismo modo, la necesidad de compartir estas cuentas entre varios usuarios hace que sea difícil mantener identificadas a las personas responsables de la actividad privilegiada. La combinación de la falta de control sobre las contraseñas, derivando en cuentas compartidas y la falta de rendición de cuentas de los administradores provoca un riesgo significativo para las organizaciones.

Adicional a esto, muchos procesos y aplicaciones requieren del acceso a estas mismas cuentas privilegiadas. Este acceso se proporciona a menudo por la codificación de contraseñas en programas y secuencias de comandos *shell*, dejando estas contraseñas en texto claro y por lo general sin cambios durante largos periodos de tiempo o nunca, volviendo a este punto una enorme vulnerabilidad que si un atacante consigue violar, podría robar información muy sensible y causar un daño significativo no solo a la infraestructura de Tecnologías de la Información (TI) de una organización.

Por otra parte, muchas organizaciones necesitan cumplir con regulaciones como PCI, HIPAA, ISO 27001, entre otras, que les exigen el control de las contraseñas de los usuarios privilegiados. Cuando se someten a auditorias para cumplir estas regulaciones, los auditores están exigiendo demostrar activamente que tienen la capacidad de controlar a los usuarios privilegiados y de informar de sus actividades.

Por estas razones las organizaciones deben de estar muy conscientes de que la falta de control de identidades privilegiadas podría resultar en la pérdida/destrucción de información, daños provocados maliciosamente, multas, juicios y el desprestigio de la propia organización.

Actualmente, existen soluciones tecnológicas que apoyan a las organizaciones a aplicar controles a las cuentas privilegiadas, ayudando a cumplir con el complejo cumplimiento y los retos de seguridad de auditoría de estos usuarios, actuando como un guardia de seguridad en los servidores, permitiendo captar todas las acciones que los usuarios realizan, brindándole a las organizaciones con ello, la oportunidad de contar con solida evidencia forense de la actividad del usuario privilegiado, resultando en un mejor control de los usuarios, rendición de cuentas para la actividad de la cuenta privilegiada, un nivel más bajo de costos administrativos y la aplicación más sencilla de los procesos de auditoría.

1.2 Objetivo

El objetivo de este documento es describir los temas tecnológicos y administrativos a los que me enfrenté como profesional del área de sistemas, dedicada a la seguridad de la información, al desarrollar, habilitar y operar un proyecto de grandes dimensiones, donde el cliente presentó la necesidad de controlar las cuentas de usuarios privilegiados de su organización y documentar los retos y resultados logrados a partir de la aplicación de conocimientos y lecciones aprendidas después de participar en uno de los proyectos más grandes y trascendentes en el ámbito de seguridad informática.

El propósito buscado con esta reseña sobre la experiencia obtenida a partir de participar en este proyecto y los conocimientos aplicados, es solventar a través de este documento la obtención del grado académico de Ingeniero en Computación.

2. Descripción de la empresa y puesto de trabajo

2.1 Empresa

Scitum, es el resultado de la evolución y especialización de un grupo multidisciplinario de profesionales con amplia experiencia en TI, con la visión de ofrecer soluciones en seguridad de la información y servicios administrados. Surge cómo un modelo de negocio de servicios de seguridad informática novedoso e integral, con recursos tecnológicos y humanos de alta eficiencia y calidad, que se ha consolidado a través de la consultoría, la capacitación en nichos muy especializados, y la venta de productos y herramientas[1].

Su misión es crear un entorno digital seguro que contribuya a la evolución de la sociedad[1]. Valores como trabajo, crecimiento, austeridad, compromiso y responsabilidad social, apoyan la misión y sustentan tanto los principios empresariales como los principios de conducta.

La compañía nace el 19 de marzo de 1998, con el desarrollo de un modelo de consultoría pura en las ramas de informática y seguridad.

Para finales de 2006, el fondo estadunidense de inversión privada Advent International, invirtió en Scitum, adquiriendo el 51% de las acciones.

En 2009, Scitum incursiono en otros mercados, como Centro y Sudamérica, además de agregar a su oferta la transferencia de conocimiento como servicio a sus clientes.

En junio de 2010, Advent y otros accionistas privados, incluyendo miembros del equipo directivo, vendieron 82% de los títulos de Scitum a Teléfonos de México (Telmex), el proveedor líder de servicios de telecomunicaciones en México. Esta adquisición beneficio enormemente a la compañía al formar parte de una organización más grande y bien posicionada, aprovechando el continuo crecimiento del mercado de TI en México y la incursión en el mercado Latinoamericano.

[1] https://www.scitum.com.mx/Home/About

Formar parte de Telmex y Grupo Carso, proporciono a Scitum respaldo y capacidad financiera para abordar proyectos complejos y de gran envergadura, fortaleciendo la posición de liderazgo en México y Latinoamérica.

En 2012, como una iniciativa de Telmex IT en conjunto con Scitum, Telmex lanzó la plataforma de Seguridad TI, el primer servicio de esta plataforma denominado Seguridad Perimetral Administrada (SPA) contó con tecnología y procesos para monitorear y evitar ataques de robo de información a las empresas.

En septiembre de 2014 Telmex, incrementa la oferta de servicios que ya brindaba a través de Scitum, inaugurando el primer Centro de Ciberseguridad de México y Latinoamérica, el cual es el primero en su tipo en la región.

En el marco de la participación en la Tercera Semana Nacional de la Ciberseguridad, en noviembre del 2017, Telmex-Scitum y Policía Federal, firmaron un convenio de colaboración para fortalecer la cooperación entre instituciones públicas y privadas en torno a la seguridad informática.

Actualmente, Scitum como filial de Telmex, es la mayor empresa integradora de seguridad de información, con presencia en México y otros países de Latinoamérica[1], tiene más de 500 colaboradores y su facturación es mayor a 685 millones de pesos anuales.

2.2 Puesto de trabajo

El puesto que desempeño en Scitum es el de consultor en seguridad de la información senior, con más de nueve años de experiencia en el área de seguridad de la información. A través del tiempo que he colaborado en la empresa, he tenido la oportunidad de participar como *Computer Forensics Analyst, Team Leader, Service Manager* y *Product Manager* en el desarrollo de productos corporativos de *InfoSec*. Siempre en busca de seguir desarrollando los conocimientos adquiridos en mi formación en la carrera de ingeniería en computación y aumentar la experiencia como profesional en seguridad de la información.

Mi experiencia como *Service Manager* se ha forjado con diferentes proyectos del sector privado y gobierno, uno de ellos corresponde a la información plasmada en este documento.

El proyecto que describo a continuación, fue el más grande relacionado con seguridad de la información que se presentó en México en 2011. Durante los 3 años de participación en el proyecto, las funciones que desempeñe como *Service Manager* de uno de los servicios de este gran proyecto consistieron en:

- Definición, adquisición e implementación de la solución tecnológica de seguridad seleccionada para cubrir las necesidades del cliente.
- Implantación, gestión, mantenimiento y ajustes a las tecnologías de seguridad involucradas en el servicio.
- Gestión de la infraestructura que soportaba el servicio, administración de servidores SO y aplicativos, respaldos, etc.
- Diseñar y proponer políticas de seguridad estratégica para el control de acceso de los usuarios privilegiados.

[1] https://www.scitum.com.mx/Home/About

- Desarrollo de *scripts* para agilizar la operación y gestión de la tecnología utilizada para proveer el servicio.
- Gestión del equipo de operación (ingenieros de operación, QA y Analista) así como la interacción con los equipos de otros servicios.
- Impartir capacitación al equipo operativo.
- Negociación y trato con cliente de las actividades, necesidades y acuerdos del servicio.
- Diseño y creación de procesos para la gestión de las cuentas privilegiadas, así como apoyo en la instauración en las áreas internas de la organización del cliente.

3. Antecedentes

3.1 Conceptos fundamentales de la seguridad informática

Este informe, está enfocado en un proyecto de seguridad informática y como tal su marco teórico se encuentran en varios de los conceptos fundamentales de esta rama.

Hoy en día es muy importante en las organizaciones proteger la información y los sistemas de información del acceso no autorizado y evitar la modificación, alteración o destrucción de datos.

3.1.1 Seguridad de la información

Es el acto de proteger datos y sistemas de información contra accesos no autorizados, modificaciones ilícitas y alteración, revelación, corrupción y destrucción.

Un modelo de seguridad simple pero ampliamente aplicable en esta rama es la tríada; Confidencialidad, Integridad y Disponibilidad CIA (por sus siglas en inglés *Confidentiality*, *Integrity* and *Availability*), tres principios fundamentales que deben garantizarse en cualquier tipo de sistema de seguridad. Estos principios son aplicables en cualquier tema de análisis de la seguridad y si cualquiera de los tres es violado puede tener graves consecuencias.

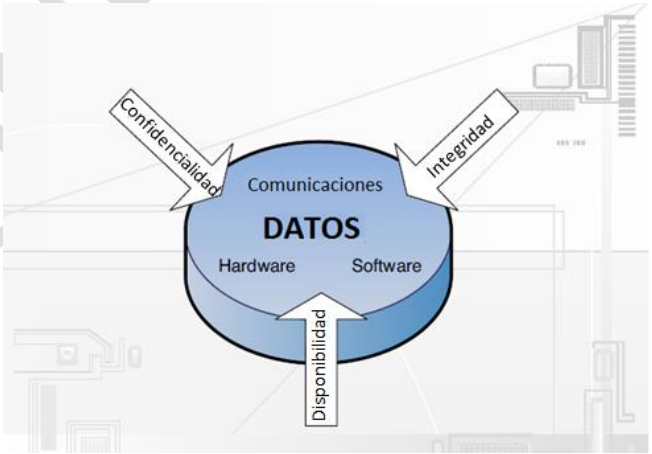

Fig. 1 - Triada CIA. Fuente: CompTIA Security+ Study Guide: SY0-401

- **Confidencialidad**

Impide la divulgación de información a personas no autorizadas. La confidencialidad es la garantía de que la información no sea revelada a personas no autorizadas, programas o

procesos. Para que la información sea confidencial, una organización debe trabajar duro para asegurarse de que sólo pueden acceder las personas autorizadas.

- **Integridad**

Esta se refiere a que los datos no han sido manipulados. La información debe ser precisa, completa y protegida de modificaciones no autorizadas. Cuando un mecanismo de seguridad proporciona integridad, protege los datos, o un recurso de ser alterado de manera no autorizada.

- **Disponibilidad**

Disponibilidad significa que los datos pueden ser obtenidos independientemente de cómo se almacena la información, accede o protege. La mayoría de la información debe ser accesible y estar disponible para los usuarios que lo soliciten y así puedan llevar a cabo tareas y cumplir con sus responsabilidades. También significa que los datos deben estar disponibles sin importar los ataques malintencionados que podría ser perpetrado en su contra.

Otros principios de seguridad relacionados con este proyecto y que sustentan el propósito del mismo dentro de la organización del cliente: Autenticación, Autorización y Responsabilidad:

- **Autenticación**

En la autenticación, la persona debe demostrar al sistema que él es quien dice ser: un usuario de la red autorizado, es decir, cuando la identidad de una persona se ha probado y confirmado por el sistema. Por lo general, esto requiere una identidad digital de un esquema de autenticación tipo nombre de usuario/contraseña, un PIN u otro.

- **Autorización**

Después de una autenticación exitosa, el sistema debe determinar si el usuario está autorizado a acceder al recurso en particular y qué acciones se le permite llevar a cabo en ese recurso, se puede determinar de varias maneras, incluyendo permisos, listas de control de acceso, la hora del día, y otras restricciones de acceso.

- **Responsabilidad (Accountability)**

La responsabilidad o rendición de cuentas se refiere a realizar un seguimiento de los datos, el uso de equipos y recursos de red, etc. A menudo significa registros de auditoría y control de los datos y recursos.

3.1.2 Auditoría

La rendición de cuentas se está convirtiendo en un factor muy importante en una red de seguridad hoy en día y para este proyecto era una necesidad imperiosa. La **auditoría** es la herramienta que permite asegurar que los usuarios son responsables de sus acciones, comprueba que las políticas de seguridad se aplican, y puede ser utilizada como herramienta de investigación.

Los registros de auditoría contienen información acerca de las actividades de operación del sistema, eventos de aplicación, y las acciones del usuario. Los registros de auditoría se pueden utilizar para verificar la salud de un sistema de control de la información de rendimiento o ciertos tipos de errores y condiciones. Los registros de auditoría también pueden ser utilizados para proporcionar alertas sobre cualquier actividad sospechosa que puede investigarse en un

momento posterior. Además, pueden ser de gran valor en la determinación de exactamente hasta donde un ataque ha llegado y el alcance de los daños que pudieron haber sido causados.

Los registros de auditoría generalmente se vuelven muy populares después de un fallo de seguridad, alguna acción en el sistema inexplicable o interrupciones del sistema.

Un administrador los puede utilizar para reconstruir las actividades que condujeron al evento. Los registros de auditoría también se pueden ver periódicamente para observar el comportamiento inusual de usuarios o sistemas, y para ayudar a entender la línea de base y la salud de un sistema.

Revisar la información de auditoría de forma manual puede ser abrumador, por esta razón ya existen en el mercado herramientas que permiten realizar esta tarea, permitiendo analizar eventos específicos como el rendimiento del sistema, la seguridad, la funcionalidad y la información de usuario que puede ser valiosa para un profesional de la seguridad o el administrador y los presentan en un formato útil.

Ya que los registros de auditoria contienen información tan importante, deben ser protegidos y sólo ciertos individuos (el administrador y/o personal de seguridad) deben ser capaces de ver, modificar y borrar. La integridad de los datos se puede asegurar con el uso de firmas digitales, herramientas de *hash*, y controles de acceso fuertes. Su confidencialidad puede ser protegida con controles de acceso y cifrado, si es necesario, y se deben almacenar en los medios independientes para evitar la pérdida o modificación de los datos. Todos los intentos de acceso no autorizados a los registros de auditoría deben ser capturados y reportados.

Los registros de auditoría se pueden utilizar para probar la culpabilidad de una persona, muestran cómo se llevó a cabo un ataque, o corroborar una historia. La integridad y la confidencialidad de estos registros estarán bajo escrutinio. Por lo tanto, deben ser adoptadas medidas apropiadas para garantizar que la confidencialidad e integridad de la información de auditoría no se vea comprometida de ninguna manera. Eliminar esta información puede destruir datos valiosos y evitar que el administrador detecte incidentes o alguna violación de la seguridad. Por lo tanto, los registros de auditoría deben ser protegidos por controles de acceso estrictos.

3.2 Precedente del proyecto

El proyecto que describo corresponde a un cliente estratégico de gran tamaño que presentaba la necesidad de dar continuidad a servicios tercerizados de seguridad y transformar sus capacidades de seguridad de la información[2] ubicadas en centros de datos Triara. Por estas necesidades generó el requerimiento de renovación de servicios administrados de seguridad de la información.

Mi cliente tenía la necesidad de contar con un proveedor que prestara, de manera integrada y unificada, los servicios de suministro, instalación, configuración, transición, implementación, protección, conectividad, detección, prevención, respuesta, optimización, auditoría, evaluación, aseguramiento, control, gestión, operación, soporte y mantenimiento de la infraestructura, componentes habilitadores y servicios de seguridad de la información, monitoreo y gestión de los

[2] Anexo Técnico - Términos de referencia Licitación Pública Nacional Mixta de Servicios No. LA-006E00001-N4-2011

anteriores, así como servicios asociados que agregaran valor tales como concientización, entrenamiento y soporte extendido[2].

En cuanto al servicio de gestión de usuarios privilegiados, mi cliente conocía que los usuarios privilegiados, como administradores de red, administradores de sistemas, y administradores de bases de datos, tenían acceso sin restricciones a todos los servidores, aplicaciones y bases de datos críticos de la organización.

Al tener la facultad de crear o eliminar perfiles de usuario y gestionar los privilegios, su función en el trabajo era fundamental para la continuidad del negocio, hacía necesario dicho acceso sin restricciones y con privilegios máximos. Sin embargo, esto representaba algunas amenazas, tanto internas como externas para mi cliente.

El desafío que enfrentaba mi cliente, como muchas organizaciones alrededor del mundo, era que, las actividades de los usuarios privilegiados pasaban desapercibidas. No podía visualizar las implicaciones de seguridad que tendrían las violaciones en las políticas por parte de ellos mismos, que se supone deberían cumplir las políticas.

Dada la gravedad del problema y las exigencias regulatorias bajo las cuales debe operar mi cliente, donde solicitan el monitoreo de los usuarios privilegiados para evitar incidentes, este se encontraba con el reto de proveer una estricta supervisión de usuarios privilegiados y capacidad de auditoría, sin afectar la productividad de su organización.

Mi cliente necesitaba garantizar en su organización el control de las cuentas con los máximos privilegios ya que hasta ese momento no tenía visibilidad de cuantas existían, quien tenía acceso a ellas, cuando eran utilizadas y en caso de incidentes no estaba en posibilidad de fincar responsabilidades, por tanto, mi cliente confiaba en cubrir las siguientes expectativas con el servicio de gestión de usuarios privilegiados durante la vigencia del contrato:

- Garantizar la continuidad y la mejora en el desempeño operativo de las aplicaciones y servicios de seguridad de información.
- Operar el servicio sobre una infraestructura de comunicaciones y seguridad de la información de alta velocidad, de alto desempeño y eficiencia, robusta, de alta disponibilidad las veinticuatro horas del día, los trescientos sesenta y cinco días del año.
- Proteger de vulnerabilidades de seguridad a los activos informáticos de su organización localizados en sus centros de datos.
- Contar con un esquema integrado de protección y aseguramiento de la información otorgando disponibilidad, confidencialidad e integridad.
- Centralización del procesamiento de la información bajo un esquema de seguridad escalable con acceso garantizado a los empleados de su organización.
- Incorporación de un modelo de administración de seguridad de la información con calidad de clase mundial.[2]

[2] Anexo Técnico - Términos de referencia Licitación Pública Nacional Mixta de Servicios No. LA-006E00001-N4-2011

4. Definición del problema o contexto de la participación profesional

No contar con un control adecuado de los usuarios privilegiados, impedía a mi cliente identificar las violaciones en las actividades que este tipo de usuarios podían conducir a hacer mal uso y causar un daño irreparable en la credibilidad de la organización y en su propia existencia.

Lo descrito en el apartado anterior, era el escenario que prevalecía en el proyecto "Servicios Administrados de Seguridad de la Información (SASI)", del que fui parte durante tres años. La organización de mi cliente requería, para el logro de sus objetivos institucionales, dar continuidad a la estrategia de seguridad de la información para salvaguardar su información y garantizar su integridad, confidencialidad y disponibilidad[2], por lo que mediante la publicación de una licitación mi cliente solicito los requerimientos para cumplir dicha tarea.

Mi objetivo fue implantar un servicio denominado "Control de Acceso para Claves Privilegiadas" con la finalidad de monitorear y controlar las cuentas con mayores privilegios dentro de las plataformas críticas de operación de la organización de mi cliente (Sistemas Operativos y Bases de Datos).

Como *Service Manager* de este servicio mi tarea consistió en integrar una solución para la automatización del servicio, así mismo, fui responsable por las actividades de instalación, configuración, monitoreo y gestión, de dicha solución.

Para el arranque del servicio, habilité mil doscientos componentes tecnológicos cómo mínimo indispensable requerido por mi cliente y la proyección para toda la duración del proyecto fue de dos mil cómo máximo. Los componentes fueron:

- Servidores Windows.
- Servidores con tecnología UNIX (Linux SUSE y HP-UX).

Los sistemas de base de datos los cuales consideré en la integración del servicio fueron:

- Alrededor de doscientos Manejadores Informix
- Doscientos Manejadores ORACLE y
- Ciento cincuenta MS SQL Server

Para poner en marcha la implementación del servicio, generé un inventario de usuarios privilegiados, cuentas y grupos con privilegios existentes en el ambiente de operación de mi cliente. En el desarrollo de este inventario, ejecuté una estrategia dirigida hacia las áreas de mi cliente, dueñas de la administración de la infraestructura crítica. Dicha estrategia comprendió mesas de trabajo donde se firmaron acuerdos para la entrega de la información correspondiente.

La información obtenida en el inventario evidenció la necesidad inmediata de la implantación del servicio de gestión de usuarios privilegiados en la infraestructura crítica de mi cliente, ya que en el universo de dispositivos dentro del alcance del servicio encontré solo dos cuentas con los mayores privilegios para ambientes Windows y una para ambientes UNIX, que estaban

[2] Anexo Técnico - Términos de referencia Licitación Pública Nacional Mixta de Servicios No. LA-006E00001-N4-2011

compartidas por un promedio de doce usuarios en la primer plataforma y veintiséis en la segunda, identificando además que los mismos usuarios de la plataforma UNIX tenían acceso privilegiado a las bases de datos aun cuando no todos debieran tener dichos accesos.

Dentro de las tareas de implementación, debí definir en conjunto con mi cliente, las políticas y estándares base a aplicar a los usuarios privilegiados, esto comprendió la definición de la lista de comandos permitidos por plataforma y las reglas de monitoreo para dichas cuentas.

También realicé la redefinición en conjunto con las áreas involucradas de mi cliente, del proceso y procedimiento de alta, baja y modificaciones de cuentas de usuarios privilegiados en las plataformas de sistemas operativos y bases de datos, para incluir aquellas actividades que por la naturaleza del servicio fue necesario modificar en los procesos o procedimientos vigentes en ese momento.

Asimismo, realicé un seminario de entrenamiento al personal de mi cliente encargado de llevar a cabo las tareas de administración de cuentas privilegiadas.

La estrategia de despliegue del servicio hacia los servidores que fueron elegidos como parte del alcance por mi cliente, la definí en conjunto con él para evitar afectar la operación de dicha infraestructura. En la estrategia consideré los siguientes puntos:

- **Piloto de pruebas**. Llevé a cabo un piloto con doce servidores (la definición de los servidores para la prueba piloto la designó mi cliente), para probar que la solución propuesta no afectaba negativamente al ambiente de producción de mi cliente. Antes de la ejecución del piloto entregué a mi cliente un documento con los detalles de la prueba:
    - Diagrama de solución.
    - Alcance de servidores.
    - Funcionalidades a probar (la configuración base definida).
    - Esquema de soporte y apoyo durante la prueba piloto.
    - Condiciones de éxito del piloto. *Check list* de cumplimiento de las actividades y pruebas realizadas.
- **Despliegue Masivo.** El despliegue masivo del servicio, lo inicié 10 días después del término de la prueba piloto. Para ello, entregué a mi cliente 5 días antes del inicio del despliegue masivo, el plan detallado de despliegue, con los ajustes identificados como resultado de la prueba piloto.

Con la estrategia de despliegue definida, ejecuté las actividades para la implementación, operación, gestión y verificación del servicio descritas a continuación:

a) Habilitación

- Entregué la infraestructura necesaria para la implementación del servicio de gestión de usuarios privilegiados para un mínimo de mil doscientos y un máximo de dos mil dispositivos.
- Proveí todo lo necesario para realizar la actualización del software de esta solución tanto en los equipos en donde lo implementé como en las consolas de administración. La solución tecnológica utilizada fue seleccionada de acuerdo a las necesidades expuestas por mi cliente en el documento de licitación, eligiendo la solución que cubría los requerimientos y de la cual dentro de Scitum ya se tenía un dominio y se encontraba homologada con las características de funcionamiento y seguridad que exige el mercado.

- Realicé una revisión de configuración y políticas trimestralmente a una muestra del 10% de los clientes instalados por área.
- Instalé y configuré las consolas de solución en el centro de datos de mi cliente en Apodaca, N.L y Querétaro. Para la instalación y configuración de la solución consideré el apego a los procesos y procedimientos de control de cambios de mi cliente para la integración de la infraestructura al centro de datos.
- Antes de la realización del piloto de pruebas, trabajé en conjunto con otras áreas para tener disponible la mesa de ayuda para dar soporte a las áreas que formaron parte del piloto.
- Asimismo, trabajé con las áreas dueñas de la infraestructura participante en el piloto para que llevaran a cabo las labores de respaldo de información de los dispositivos involucrados.
- Diez días después de la conclusión de la prueba piloto y después de haber realizado los ajustes correspondientes al plan de trabajo, inicié con el despliegue masivo de la solución y su configuración base, con base en dicho plan.
- Documenté toda la implementación del servicio, considerando las políticas y/o perfiles que existían.
- Con la habilitación del servicio puse a punto todos los puestos de servicio definidos en el alcance, tomando como base las configuraciones definidas con mi cliente.
- Aun cuando el servicio fue administrado por mí y mi equipo de trabajo, mi cliente requirió cuentas de acceso de sólo lectura hacia la interfaz de administración basada en Web de la tecnología de gestión de usuarios privilegiados, para fines de visibilidad y/o consultas personalizadas.

b) Entrega y Soporte

- **Monitoreo e identificación de patrón de uso de usuarios privilegiados**

Para lograr la configuración más adecuada a las necesidades de mi cliente, consideré una etapa de monitoreo, donde identifiqué y documenté el patrón de uso de las cuentas privilegiadas. Dicho patrón de uso me sirvió como parámetro para el ajuste de las políticas base.

- **Análisis y ajuste de políticas y catálogos**

Una vez que terminé la etapa de monitoreo y documentación del patrón de uso de los usuarios privilegiados, realicé el análisis de los resultados y propuse a las áreas designadas por el cliente, el ajuste a las políticas y estándares de control de los usuarios privilegiados, con base en el resultado de dicho monitoreo. Así mismo, las áreas de mi cliente me entregaron sus criterios sobre dicho ajuste. Realicé el ajuste del catálogo de servicios base para integrar aquellos que fueron detectados como necesarios, durante la etapa de monitoreo.

- **Monitoreo y Gestión del Servicio**

Como parte de las labores de monitoreo y gestión del servicio tenía consideradas las siguientes actividades:

- Resolví las solicitudes de soporte técnico especializado, a fin de evitar pérdidas de información en los equipos en los que se encontraba instalada la solución tecnológica de este servicio.
- Correlacioné alertas de incidentes/eventos generados por el servicio.

- Administré los elementos tecnológicos a través de procesos de gestión de cambios, configuraciones y versiones de acuerdo con los requerimientos del cliente.
- Ejecuté actividades de mantenimiento de los elementos tecnológicos a través de la actualización de parches, firmas de detección y versiones, corrección de problemas y acciones para la prevención de fallas.
- Afiné la solución con base en el resultado del monitoreo continuo de los patrones de uso de comandos.
- Gestioné y afiné reglas de usuarios privilegiados para apegarlas a las necesidades de mi cliente.
- Asistí al área de seguridad del cliente para solución de incidentes.
- Generé reportes periódicos de monitoreo y reportes bajo demanda.

c) Medición y verificación

- Cada 6 meses revisé la implementación de la normatividad definida previamente para este servicio y en caso de así identificarlo llevé a cabo propuestas con las actualizaciones pertinentes.
- Así mismo, realicé la integración al tablero de control del cliente con los indicativos de niveles de servicio.
- Los niveles de servicio (SLA's) que debí cumplir para este servicio fueron:
  - Monitoreo de Actividad Sospechosa.
  - Gestión de Incidentes de Seguridad.
  - Control de Cambios.
  - Disponibilidad de la Infraestructura de Seguridad Administrada.
  - Soporte a Fallas.

Mi cliente esperaba solventar la problemática que presentaba con las cuentas de usuarios privilegiados con la habilitación del servicio requiriendo que cubriera las siguientes características:

d) Auditoría

- Brindarle agentes para los sistemas a administrar, incluyendo UNIX, Linux y Windows, que le permitieran registrar (grabar) la actividad del usuario permitiendo reproducir la misma posteriormente (registro de actividades de los usuarios privilegiados).
- También podía operar sin necesidad de la instalación de agentes para ciertos dispositivos, donde el uso de un dispositivo intermedio es utilizado como punto de acceso a los mismos.
- El servicio registraba toda la actividad del usuario durante sesiones privilegiadas en dispositivos UNIX, Linux y Windows.
- El servicio proporcionaría herramientas de reproducción de sesiones (similares a las de un DVR) para visualizar sesiones de usuario grabadas para dispositivos UNIX, Linux y Windows. Esto incluía la captura de toda la información de entrada y salida del dispositivo.

e) Administración

- El servicio incluyó una interfaz de usuario gráfica para administración y creación de políticas.

- Gestionaba de manera centralizada políticas para todos los dispositivos administrados.
- Distribuía automáticamente políticas a todos los puntos de decisión y aseguraba la consistencia en la aplicación de las mismas.
- El servicio contaba con herramientas para probar reglas y políticas antes de que se enviaran y aplicaran en producción.
- La implementación o despliegue se gestionaba centralizadamente, y no resultaba invasivo en su proceso para los dispositivos finales.
- Podía realizar actualizaciones al servicio y las políticas sin afectación al tiempo operativo de servicio (*uptime)*.
- La aplicación de nuevas reglas y políticas de acceso las realizaba en tiempo real, sin requerir que el usuario reiniciara su sesión.

f) Arquitectura

- El servicio ofrecía mecanismos de redundancia que evitaba modelos de implementación con puntos de falla únicos.
- También ofrecía redundancia para bases de datos de auditoría.
- Contaba nativamente con mecanismos de tolerancia a fallos y balanceo de carga.
- La arquitectura de este servicio la diseñé para soportar al menos mil doscientos y un máximo dos mil dispositivos para todas las plataformas (UNIX, Linux y Windows).

g) Integración

- El servicio se integró con una solución para correlación de eventos de seguridad.

h) Administración de Usuarios Privilegiados

- El servicio me permitió gestionar permisos y comandos administrativos en dispositivos UNIX y Linux.
- También me permitió gestionar accesos administrativos a servidores Microsoft Windows.
- La administración del servicio me permitió definir reglas de acceso granulares (por comandos) en dispositivos UNIX, Linux.
- El servicio me permitió aplicar políticas a grupos en servidores.
- La conectividad entre la estación de trabajo del usuario final y los servidores Windows protegidos por la solución los realizaba a través de un túnel seguro.
- El servicio permitió que administradores observaran, tanto en tiempo real como el histórico, la actividad realizada por un usuario en servidores UNIX, Linux y Windows locales o remotos.
- Contaba con una bóveda de credenciales para almacenar las contraseñas administrativas de acceso a Windows y con ello se evitaba exponer contraseñas administrativas a los usuarios cuando accedan a sesiones privilegiadas en servidores Windows.

i) Bitácoras y reportes

- El servicio consumía y procesaba archivos de bitácoras (*logs*) de los dispositivos administrados sin requerir intervención manual para ello.
- Integró y envió datos de bitácoras a un sistema de correlación de eventos externo sin necesidad de intervención manual ni de personalización extensiva.

- Contaba con reportes pre-definidos como parte de la solución y estos no requerían hardware o bases de datos adicionales a la de la misma solución.

j) Seguridad

- El servicio ofreció monitoreo y grabación del 100% de pulsaciones de teclado (*keystroke*) durante una sesión privilegiada.
- Tuvo la funcionalidad de correlacionar actividad del usuario con políticas en tiempo real (detección de anomalías en tiempo real).
- También podía asignar calificadores de riesgo para toda la actividad del usuario basadas en una combinación del usuario privilegiado, el servidor accedido y el comando tecleado.
- Permitía acceso a servidores Windows basado en políticas para usuarios o grupos específicos.

k) Alta Disponibilidad

- El servicio contaba con redundancia para bases de datos de auditoría.
- Ofreció nativamente mecanismos de alta disponibilidad (tolerancia a fallas) y balanceo de carga de forma automática.

5. Metodología utilizada

Dentro de la organización en la que laboro, todos los proyectos se ejecutan bajo una metodología propietaria y apegada a las mejores prácticas de la industria enfocadas al control y supervisión de tecnología de la información mediante procesos y funciones, dirigidos a cumplir estándares de seguridad en todos los aspectos que involucran la entrega y prestación de servicios.

La metodología SCISO (Scitum Information Security Operations) de mejores prácticas, patentada por Scitum y basada en estándares internacionales como ITIL, COBIT, ISO 9000, ISO 27000 y algunas referencias de SANS Institute, para asegurar el más elevado nivel de calidad de servicios prestados a los clientes.

Esta metodología, además de ser utilizada para realizar la operación dentro de Scitum, es un producto que se comercializa a los clientes, permitiendo la implantación y transferencia metodológica de procesos y procedimientos de gestión de la información, que facilitarán sustancialmente la generación de los resultados y mejora continua.

La metodología se aplica en el Centro de Operaciones de Seguridad (SOC por sus siglas en inglés) de Scitum, y comprende procesos, procedimientos y guías para medir la eficacia de la operación en términos de cumplimiento.

Con esta metodología pude realizar la gestión y monitoreo del proyecto que describo en este documento, estas actividades se proporcionó mi equipo de trabajo, mayormente de manera remota desde las instalaciones del SOC en Scitum, considerando la conectividad de red necesaria hacia los centros de datos de mi cliente, tomando en cuenta los aspectos de redundancia y seguridad para mantener la operación aún en caso de contingencia, además de contar con todos y cada uno de los recursos humanos necesarios para la prestación del servicio.

La metodología plantea el monitoreo permanente de los elementos del servicio solicitados durante la vigencia del contrato, con el fin de verificar el estado de cada uno de los elementos que lo soportan y tomar las acciones necesarias en caso de presentarse un evento que ponga en riesgo la operación del servicio.

5.1 Funciones del SOC

El objetivo del SOC bajo los lineamientos de la metodología es el de la administración, supervisión, gestión y monitoreo de los servicios y configuraciones de seguridad, para el análisis proactivo y reactivo con el fin de proteger las aplicaciones e información interna del cliente.

La función principal del SOC es monitorear el estado de operación de los componentes de la infraestructura tecnológica de seguridad, así como recolectar las alertas que generen, normalizar y correlacionar la información que de ellas se deriven y emitir los reportes que serán enviados a los responsables de seguridad del cliente, de tal manera que puedan manejar y responder a potenciales incidentes de seguridad o incidentes en curso a fin de tomar las medidas necesarias para contenerlos.

La administración de la seguridad (el monitoreo, gestión y solución de incidentes de seguridad), se opera en un régimen de siete días de la semana por veinticuatro horas cada día, durante toda la vigencia del contrato del cliente, y cuenta con la cantidad de ingenieros necesarios para cumplir los acuerdos de nivel de servicio y horarios solicitados.

La metodología cuenta con procedimientos detallados para la administración de incidentes, manejo de alarmas y análisis de información y correlación de eventos.

Además, cubre las siguientes funciones:

- Administración de la infraestructura de seguridad informática para ayudar a mantener configuraciones óptimas para asegurar la confidencialidad, integridad y disponibilidad de la información.
- Envío de alertas y recomendaciones que se deberán atender y aplicar.
- El SOC se encarga de brindar el soporte para cualquier incidencia registrada por las soluciones que administra y/o que le sea reportada.
- Actualización de memorias técnicas y documentos de control relacionados.
- Generación de reportes.
- Coordinación con otras entidades relacionadas con respuesta a incidentes para atender casos de incidentes de seguridad.

5.2 Gestión del Servicio

5.2.1 Monitoreo de la Infraestructura

El monitoreo de infraestructura se realiza con soluciones basadas en software y hardware, permitiendo identificar y ejecutar acciones hacia los elementos de la red administrados. Tiene la capacidad de monitorear dichos componentes, hacer análisis de forma automática, y en particular análisis de causa raíz y correlación de eventos provenientes de los distintos dominios de infraestructura que soportan los servicios. La detección y notificación de fallas se realiza en tiempo real.

a) Monitoreo de la disponibilidad y utilización de la infraestructura

Se realiza la visualización e interacción en línea desde un punto remoto (SOC de Scitum), de todos los dispositivos de seguridad que formen parte de los servicios y que así lo requiera, observando sus funciones principales, desempeños, bitácoras, alarmas, eventos y reportes para conservar su mejor funcionamiento y desempeño todo el tiempo posible.

El SOC notifica durante la operación, de cualquier situación de indisponibilidad que se llegue a presentar en la infraestructura de seguridad. Así mismo al sobrepasar algún umbral de desempeño de la infraestructura administrada, además de realizar un diagnóstico en cumplimiento con los niveles de servicio definidos para restablecer los indicadores de desempeño adecuados a la operación del cliente.

b) Monitoreo Activo (Eventos de Seguridad)

Identifica y notifica de nuevas vulnerabilidades, ataques, virus, y malware en general que pueda impactar a los sistemas o aplicaciones del cliente. De esta manera el SOC genera alertas de seguridad junto con recomendaciones a seguir.

El SOC cuenta con las capacidades de correlación de eventos para determinar posibles ataques, anomalías y comportamiento sospechoso de los sistemas monitoreados. Este sistema es una solución líder en el mercado que proporciona al SOC alertas de seguridad de eventos en tiempo real, monitoreo y desglose de la funcionalidad forense, lo que contempla la recolección del log de cada uno de los dispositivos de seguridad.

c) Administración de la Infraestructura

La administración de infraestructura comprende el control y administración de cambios, donde se considera la atención a los requerimientos del cliente en cuanto a solicitud de cambios, reporte y atención de incidentes de seguridad, así como consultas con relación al estado de la seguridad.

Así también el manejo de Incidentes de Seguridad, los cuales se reportan de manera expedita y documentada, los incidentes/eventos atendidos incluyen accesos no autorizados, negación del servicio (DoS), pérdida de confidencialidad, infecciones por virus en uno o varios sistemas y accesos VPN IPSEC.

d) Actualización de Software

Parte de las actividades que el SOC realiza por proceso es la actualización e incorporación de nuevas versiones, *fixes* o parches que vaya liberando los distintos fabricantes de todos los servicios.

e) Respaldo de Configuraciones

Mantener respaldada la configuración de toda la infraestructura que administra el SOC para garantizar la continuidad de la operación y procesos operativos que se requieran.

Fig. 2 – Gestión de servicios.

5.2.2 Mesa de Servicio

La mesa de servicio, es el único punto de contacto con los proveedores tecnológicos, las áreas de negocio y el usuario final, y es la responsable de registrar y dar seguimiento a los diferentes eventos relacionados con los procesos y servicios de TI, como por ejemplo incidentes, requerimientos, atención de problemas y solicitudes de cambios, entre otros.

La mesa de servicio opera siete por veinticuatro durante toda la vigencia del contrato del cliente para brindar la atención adecuada.

Las tareas que realiza la mesa de servicio son: recibir, atender, registrar, realizar análisis causa-raíz, canalizar y resolver los tickets de incidentes o fallas a las áreas de atención correspondientes, dar seguimiento, escalamiento de incidentes, análisis de tendencia, notificación y dar solución a las solicitudes informando al cliente oportunamente; así mismo, genera un registro histórico con consulta, reporte y seguimiento en línea, sobre el tipo de fallas presentadas y la forma como se solucionaron.

El sistema de la mesa de servicio cuenta con un método de consulta en línea sobre los tickets, para su seguimiento y la forma como se les dio la atención. Así también cuenta con métodos de notificación de los tickets vía correo electrónico o teléfono.

El ciclo de vida de cada evento, así como el detalle del nivel de servicio están definidos dentro del proceso de incidentes, problemas, cambios y atención de requerimientos operativos.

Fig. 3 – Flujo de Operación Mesa de Servicio. Fuente: Licitación Pública Nacional Mixta de Servicios No. LA-006E00001-N4-2011, Anexo Técnico

La mesa de servicio gestiona los siguientes procesos y procedimientos de administración de servicios:

- Procedimiento de solución de fallas: El objetivo es asegurar la aplicación de la metodología SCISO para el uso y la operación de la mesa de servicio. Este procedimiento maneja categorizaciones identificadas para las posibles fallas de los servicios, el flujo operativo que contempla a todos los involucrados de inicio a fin, la matriz de escalación y contactos para seguimientos.
- Administración de Incidentes: El objetivo del proceso es el restablecimiento del servicio ante un incidente o falla que interrumpa su operación, en el menor tiempo posible, minimizando el impacto sobre su operación y cumpliendo con los niveles de servicio acordados.
- Administración de Configuración: Este proceso existe para llevar el control y dimensionamiento actualizado de la infraestructura de seguridad, que soporte el servicio del cliente, de tal manera que se cuente con información fiable y actualizada de los equipos instalados y conectados y de su configuración física y lógica.
- Administración de Cambios: Tiene como objetivo supervisar y regular la implementación de modificaciones a la infraestructura de hardware y software con la que se soportan los servicios del cliente.

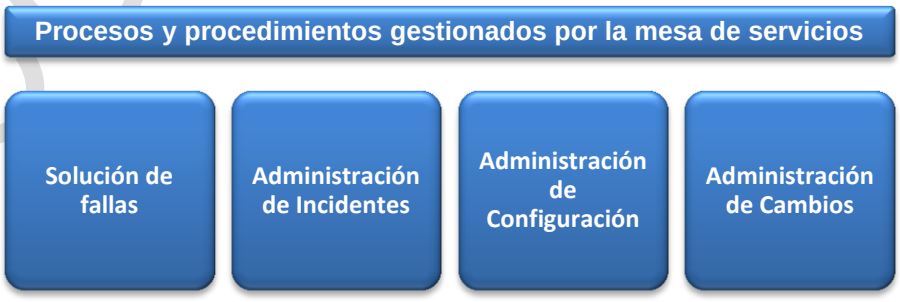

Fig. 4 – Procesos y procedimientos mesa de servicios

Para la correcta ejecución de los procesos y procedimientos, así como una comunicación eficaz con el cliente la mesa de servicio, además de contar con su matriz de escalación, la cual

contendrá al menos la información de los contactos para su localización en todo momento, así como los tiempos establecidos para pasar al siguiente nivel, también cuenta con una matriz de escalación de contactos y responsables del personal asignado por el cliente a fin de coordinar la restauración de los servicios oportunamente.

5.2.3 Soporte a la Operación

a) Atención a Fallas

La metodología cuenta con procesos establecidos para la apertura de reportes o requerimientos por parte del cliente en la mesa de servicio y para llevar a cabo el proceso de gestión de fallas, dentro del que se consideran las siguientes funciones:

- Diagnóstico en línea del primer nivel de la falla reportada.
- Asignación de severidad al reporte de falla.
- Información en línea sobre hallazgos relativos a la falla.
- Identificar y notificar la causa de la raíz de problemas presentados en el servicio.
- Asegurar que los recursos apropiados se asignan conforme sea necesario para identificar y remediar la falla, y dar seguimiento al informe sobre cualquier consecuencia de la falla.
- Proporcionar al cliente un reporte escrito detallado que informe la causa y el procedimiento para corregirla, o construir a partir de estos reportes una base de conocimiento que sea almacenada en un determinado repositorio.
- Verificar que todas las acciones razonables se han tomado para prevenir la repetición de tal falla.
- Sustitución de equipamiento en caso de ser requerido.

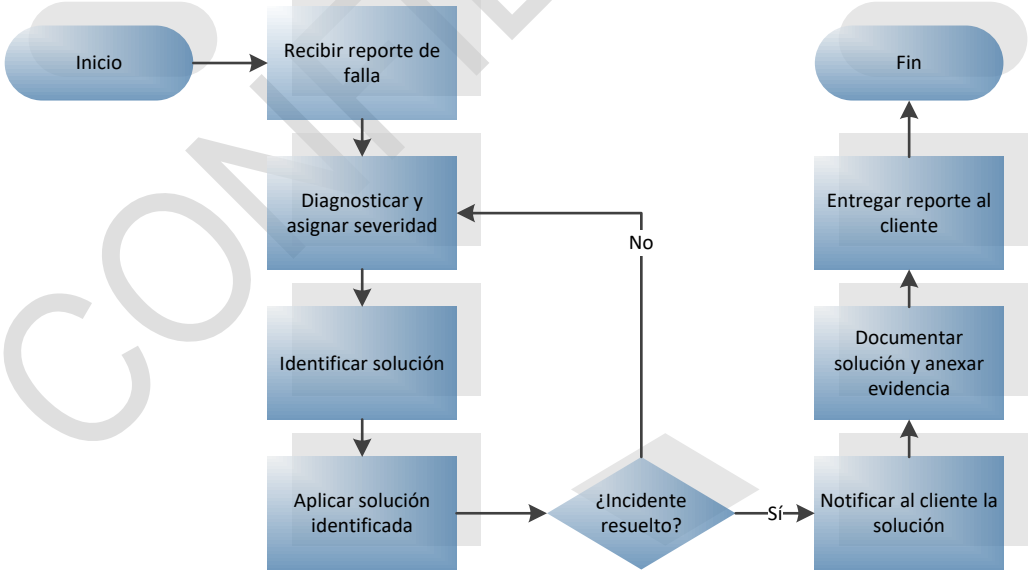

Fig. 5 – Flujo de Atención a Fallas.

Se lleva el control, la administración, seguimiento y actualización de la información generada para cualquier tipo de incidente y problema que se presente durante la prestación del servicio, manteniendo al tanto de la información generada al cliente

durante el proceso de atención, para determinar tiempo de falla así como la hora y fecha de restauración de acuerdo a los niveles de servicio requeridos.

Para la resolución existen 3 niveles de soporte los cuales fluirán de acuerdo a la severidad de la falla.

- **Primer Nivel de Soporte** - Primera línea de atención al cliente, se atienden todos los problemas comunes del mismo e identifican problemas potenciales para escalarlos al segundo nivel.
- **Segundo Nivel de Soporte** - El segundo nivel de soporte lo conformar ingenieros con la mayor experiencia en las tecnologías manejadas, en su mayoría personal con más de 5 años de experiencia en el campo. Están destinados a resolver problemas complejos y que requieran atención especializada.
- **Tercer Nivel de Soporte** – Está conformado por el centro de atención avanzado y personalizado del fabricante de la tecnología.

Los *tickets* son típicamente atendidos por los ingenieros fluyendo del primer nivel al tercer nivel dando tiempo a cada nivel de resolver el problema, de acuerdo a los niveles de servicio requeridos y en el orden que se muestra a continuación.

Fig. 6 – Niveles de Soporte. Fuente: Licitación Pública Nacional Mixta de Servicios No. LA-006E00001-N4-2011, Anexo Técnico.

Asignación de Severidades

Para asignar la severidad a una falla, el ingeniero del centro de operaciones y el cliente determinarán el grado de afectación y asignarán el grado de severidad a la falla. Todos los casos abiertos por correo electrónico deberán ser abiertos con severidad 3 (S3), si el cliente desea una más alta, deberá comunicarse vía telefónica al centro de operaciones.

Descripción de severidades:

- **Severidad 1:** Representa un incidente de alto impacto dado el riesgo que representa.
- **Severidad 2:** Representa un incidente serio en el que hay una degradación más no una afectación de negocio a los servicios e infraestructura que es protegida mediante los dispositivos de seguridad.
- **Severidad 3:** Representa un incidente menor que no trae consecuencias de impacto de negocio a los servicios e infraestructura protegida por los dispositivos de comunicaciones y/o seguridad.
- **Severidad 4:** Son casos considerados como “Preventivos” para fines de mejora u optimización de cualquier servicio.

b) Mantenimiento de los Servicios

Realizar las tareas de mantenimiento preventivo y correctivo para la totalidad de componentes habilitadores y de infraestructura dentro del alcance de los servicios

prestados, de acuerdo a la estrategia de entrega y soporte, apegándose a las mejores prácticas de ITIL (IT Infrastructure Library).

El SOC tiene la responsabilidad del mantenimiento de la infraestructura, del hardware y software de los equipos que se encuentren bajo su gestión y/o que formen parte de la solución tecnológica que es parte del servicio.

Las ventanas de tiempo de mantenimiento son programadas e informadas con anticipación al cliente, con objeto de minimizar el impacto en la operación.

En el caso de mantenimientos correctivos, se proporcionan los procedimientos para reportar el incidente, estos incluyen, matriz con los niveles de escalación incluyendo información de los contactos (nombre, puesto, teléfono oficina y móvil, número de localizador) y tiempos establecidos entre cada nivel.

El mantenimiento correctivo se realiza cuantas veces sea necesario durante la vigencia del contrato del cliente, de acuerdo a las especificaciones técnicas del fabricante y consistirá en la reparación y/o reemplazo de las partes dañadas del equipo o cuando ocurra una falla. Si el equipo en cuestión no puede ser reparado, será sustituido por otro equipo de características técnicas iguales o superiores.

c) Actualización de las Plataformas

La renovación de la infraestructura de hardware y/o software sobre una base continua, para asegurar que los componentes del sistema permanezcan vigentes con la oferta del mercado y pueda cumplir satisfactoriamente los niveles de servicio.

Esto incluye:

- Análisis proactivos sobre los reportes de alerta de software que pongan en riesgo la infraestructura de la red administrada.
- Certificación del nuevo sistema operativo en ambiente controlado previo a su instalación en la red de producción, sea disparado por el soporte de nuevas funcionalidades o por la administración de ciclo de vida del elemento.
- Establecimiento, implantación y administración de políticas apropiadas para actualizar y complementar las versiones de software, sistemas operativos o firmware de los equipos activos que forman parte de los servicios del cliente.
- Implantar y administrar políticas apropiadas para actualizar y complementar las versiones de software, sistemas operativos y los parches o correcciones necesarias a las soluciones de seguridad, optimización, monitoreo y gestión que forman parte de los servicios del cliente.

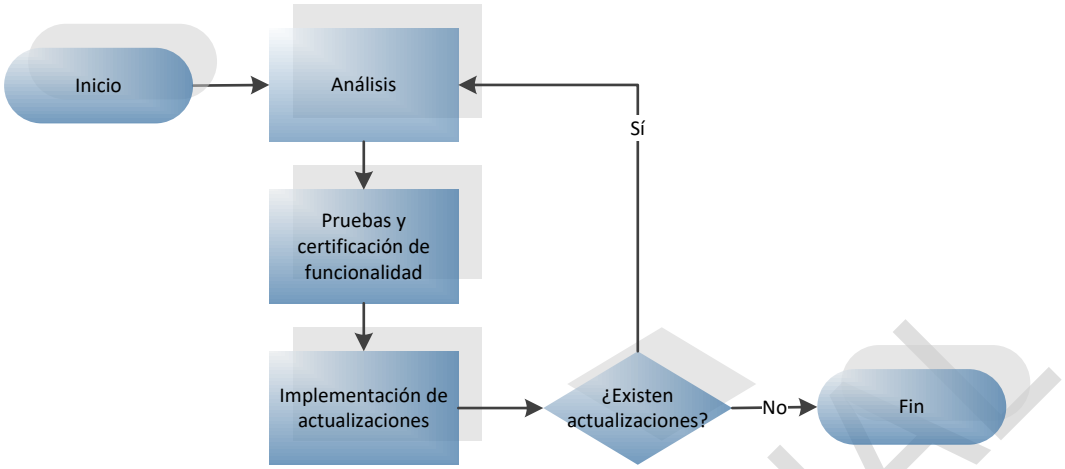

Fig. 7 – Flujo de Actualización de Plataformas.

5.3 Documentación del Servicio

a) Memoria Técnica

Toda la información técnica generada durante el transcurso de los trabajos, así como la implementación y despliegue de los servicios, se documentan en una memoria técnica. Este material se concentra en una base de conocimiento, la cual servirá para los futuros mantenimientos correctivos y preventivos, o modificaciones futuras del cliente.

La memoria técnica también contiene toda la información administrativa (solicitud de requerimientos, documentos de asignación, justificaciones, catálogos de componentes habilitadores, procesos establecidos en la operación, entre otros), la cual conformará la base de conocimiento del proyecto.

b) Repositorio de Información

Como parte de los procesos que se ejecutan para la operación de los servicios en el SOC, se registra, almacena y mantiene actualizada toda la información y documentación generada por los servicios ofrecidos.

5.4 Mejores Prácticas

Con objeto de contar con una adecuada administración de la seguridad, el SOC cumple con las mejores prácticas a continuación descritas:

- Cuenta con personal con experiencia comprobable en seguridad de información con certificaciones en seguridad reconocidas como CISSP, CISA o CISM, así como certificaciones de nivel profesional y el nivel más alto de la tecnología del fabricante de la infraestructura utilizada en los diferentes servicios que administra.
- SCISO se apega a metodologías reconocidas internacionalmente, basadas en las siguientes mejores prácticas en la prestación de los distintos servicios de seguridad de información:
    - ISO/IEC 27001:2005 e ITIL
    - ISSAF y CoBIT

- La metodología SCISO cuenta con un proceso de administración de riesgos que le permita identificar y cuantificar riesgos así como seleccionar los controles de seguridad correspondientes para garantizar los niveles de servicio acordados con el cliente.
- Así mismo se cuenta con un proceso de administración de incidentes de seguridad de información, así como la conformación del equipo de respuesta y administración de incidentes. Este proceso cuenta con la Certificación ISO/IEC 27001:2005 para el proceso de administración de incidentes relacionados con la operación del SOC.
- Se cuenta con un programa de auditorías, a intervalos planeados, tanto internas como de terceras partes, para validar el cumplimiento que se tiene dentro de la empresa de políticas, procesos y procedimientos documentados como práctica regular, asociadas con los servicios brindados, incluyendo el cumplimiento con regulaciones, normas y/o estándares internacionales.
- También cuenta con las medidas de protección física necesarias para garantizar que sólo personal autorizado tendrá acceso a los recursos de cómputo, comunicaciones e información de la empresa.
- Así mismo, se cuenta con un proceso documentado, utilizado para llevar a cabo la administración de vulnerabilidades, el perfil del personal involucrado, la(s) tecnología(s) utilizada(s), el alcance del servicio (recomendaciones para el cierre de vulnerabilidades).
- Todo se encuentra apegado a una política de seguridad de información documentada y aprobada por la Dirección General de la empresa.
- Existe un área interna de seguridad de información con responsabilidades bien definidas y reconocidas, personal competente, capacitado, respaldada por la Dirección General.
- Cuenta con controles de seguridad que minimizan el riesgo que representan eventos de software malicioso, como virus, gusanos, troyanos, etc., así como el desarrollo de servicios y productos generados bajo un esquema de seguridad en su ciclo de vida.
- Todos los cambios de infraestructura, hardware, software y sistemas de información, pasan por un riguroso proceso de control de cambios, debidamente documentado, que incluye el que estos cambios sean sometidos a pruebas de compatibilidad y estabilidad en un ambiente de pruebas independiente al de producción.
- El personal adscrito a los diferentes proyectos tiene firmados acuerdos de confidencialidad que cubren tanto los intereses de la empresa como los de sus clientes.

6. Resultados

La estrategia del proyecto la diseñé de tal manera que su implementación resultó gradual, controlada y flexible, acorde con las necesidades de la organización de mi cliente, y lo efectué en los plazos establecidos, de manera que el cliente podía disponer de otro tipo de servicios en niveles superiores, dependientes de la infraestructura relacionada con el proyecto, tales como la instalación de aplicaciones necesarias para soportar servicios internos de TI y servicios al público.

La implantación del proyecto me llevó a conseguir el control de los accesos y consolidación de las cuentas privilegiadas de la organización, trabajé en conjunto con el cliente para Identificar y eliminar todas las cuentas privilegiadas que estaban en desuso, reduciendo al mínimo posible el número de cuentas de usuarios privilegiados, lo que me permitió limitar considerablemente la superficie vulnerable de cara a una posible brecha de seguridad. Esto lo realicé generando un

inventario completo de las cuentas de usuarios privilegiados, registradas y categorizadas debidamente como:

- Administración local por defecto.
- Administrador individual.
- Cuentas de servicio.
- Administrador de dominio.
- Emergencia.
- Administrador de aplicaciones.
- Administrador de máquina virtual.

Con el inventario documentado, establecí en conjunto con mi cliente, un procedimiento estandarizado para la aprobación y revocación de privilegios de acceso para los usuarios que tendrían privilegios en sus diferentes grados, involucrando tanto a las áreas operativas como de seguridad en la aprobación y me permitió crear un control de quién y cuándo solicitaba una cuenta con privilegios, ésto me dio la oportunidad de brindarle a mi cliente una visión integral de la modificación de la relación de un empleado con respecto a la organización (por un cambio de puesto, abandono de la empresa, etc.), cuándo había acumulación de privilegios y la justificación debida para obtener un incremento de los mismos. Así mismo, en este proceso contemplé la cancelación o eliminación de las cuentas para usuarios privilegiados, cuando terminaban su relación laboral con mi cliente o cambiaban de puesto, cabe mencionar que esta actividad no existía antes de que se implementara el servicio.

Con la implantación de este proceso para el servicio de gestión de usuarios privilegiados, logré dar identidad a cada usuario, evitando el préstamo de cuentas con privilegios, cada usuario contaba con su cuenta y contraseña personalizadas. La solución tecnológica implementada me permitió tener la trazabilidad y auditoria de cada uno de ellos, no solo en logs ya que contaba con el video de cada una de las sesiones creadas por cada uno de los usuarios, permitiéndome rastrear actividades y fincar responsabilidades cuando fue necesario.

Así también, habilité un plan de contingencia para acceder y administrar la infraestructura crítica donde implementé el servicio de gestión de usuarios privilegiados, en este plan contemplé cuentas con privilegios resguardadas por personal designado por mi cliente que solo se liberaron en situaciones críticas y con la justificación documentada.

Otro punto sumamente importante que logré implementar fue el procedimiento de renovación de contraseñas de las cuentas privilegiadas, utilicé las características de la solución tecnológica para forzar a los usuarios a realizar los cambios en periodos de noventa días. Para los casos de contingencia, las contraseñas se renovaron inmediatamente después de culminar el incidente, bajo un esquema donde la mitad de la contraseña era colocada por el área de operación y la otra mitad por el área de seguridad.

Durante la vigencia del contrato de mi cliente, consideré la mejora continua del servicio de gestión de usuarios privilegiados a través de la actualización tecnológica y mediante el soporte de nuevas funcionalidades, optimicé el servicio. Esto lo logré garantizando que la infraestructura y los componentes habilitadores que proporcione para la provisión del servicio, se mantuvieran actualizados, tanto en la última versión estable de software que liberó el fabricante de los mismos, como mediante la actualización del sistema operativo y parches de seguridad cuando fue necesario.

Dentro de esta mejora continua también realicé la revisión y actualización de políticas sobre los perfiles solicitados por mi cliente, dentro de la plataforma de gestión de usuarios privilegiados. El respaldo de estas políticas, en conjunto con las configuraciones tanto del aplicativo como de la infraestructura los realicé cada semana para garantizar la continuidad del servicio en caso de una contingencia.

Para facilitar el monitoreo del servicio y como parte de los requerimientos de mi cliente, llevé a cabo la integración con una solución de correlación de eventos para que entregara información hacia un tablero de control de seguridad (indicadores de seguridad y desempeño). Apoyándome de esta integración y gracias a toda la información generada por la solución tecnológica para gestionar los usuarios privilegiados, realicé el monitoreo y seguimiento a cualquier indicio de actividad sospechosa.

Utilizando la metodología SCISO, ejecuté las actividades de administración y monitoreo, apoyándome del equipo de trabajo a mí cargo, esto me permitió mantener la operación del servicio disponible en un esquema siete por veinticuatro durante toda la vigencia del contrato.

Bajo la premisa de agilizar la gestión y monitoreo del servicio, realicé la automatización de tareas como generación y envió de notificaciones tanto de la infraestructura como de la solución tecnológica, esto lo pude llevar a cabo con la creación de scripts que ejecutaba desde el sistema operativo donde se implementó la solución tecnológica que soportaba el servicio. Así también, me apoyé de las funcionalidades del correlacionador para generar reportes automáticos y de forma programada sobre actividad sospechosa y en casos de investigación procesar con mayor velocidad los registros de actividad de usuarios específicos.

En relación a las investigaciones, en diferentes oportunidades, mi cliente tuvo la necesidad de solicitarme información sobre la actividad de usuarios derivada de incidentes en la infraestructura crítica donde tenía integrado el servicio. Estas investigaciones dieron bastante visibilidad del servicio de gestión de usuarios privilegiados al interior de la organización de mi cliente, ya que al poder mostrar evidencia de la actividad de los usuarios, comando a comando y presentar los videos de las sesiones, las diferentes áreas de la organización de mi cliente tuvieron oportunidad de fincar responsabilidades y conseguir rendición de cuentas de los usuarios involucrados en los incidentes.

El resultado global sin lugar a dudas, fue haber logrado implementar, operar y madurar el servicio a mi cliente que no contaba con controles sobre sus cuentas de usuarios privilegiados, darle la visibilidad de cuantos, quienes y donde se encontraban, permitirme brindarle la posibilidad de mantener el control y auditar la responsabilidad individual de los usuarios privilegiados quienes son una pieza clave y sensible de cualquier organización.

7. Conclusiones

Los proyectos de seguridad de la información siempre representan un gran reto, si bien cada día las organizaciones son más conscientes del riesgo que corre su infraestructura de TI y más aún la información contenida en ella, aún falta mucho camino por recorrer en cuestión de educación y comprensión de las consecuencias que representa un ciberataque a una organización.

Las empresas no se enfocan en proteger la capa más interna de su infraestructura, donde están los administradores de los sistemas, los usuarios con mayor privilegio en una organización. Las amenazas más importantes y de mayor impacto están en los usuarios internos, sin embargo, la prioridad se ha enfocado más a protegerse de los externos porque estos representan un mayor volumen y sus ataques tienen mucha más visibilidad.

Afortunadamente, en muchas organizaciones ahora existe mayor conciencia sobre el tema de seguridad y también hay más conocimiento sobre el riesgo que representan los usuarios privilegiados; en la mayoría se evidencia una gran preocupación por prevenir fugas de información, además de que ya existen diversas regulaciones que deben cumplir o estándares que se deciden seguir y que solicitan de manera explícita una adecuada gestión de usuarios privilegiados (por ejemplo la Ley Federal de Protección de Datos Personales en Posesión de Particulares, regulaciones de la CNBV, PCI, SOX, ISO27001, etcétera) .

Ese fue el caso del proyecto que describí en este documento, una gran organización que necesitaba gestionar las cuentas de los usuarios privilegiados de su infraestructura crítica de producción para conseguir control y rendición de cuentas, lo cual logré a través de la implantación de un servicio integral, adoptando procesos y procedimientos, apoyándome de una solución tecnológica. El inicio del proyecto fue difícil al tratar de cambiar la forma de operar y malos hábitos de los administradores, las áreas operativas trataron de detener el servicio en varias ocasiones, sin embargo, una postura firme del área de seguridad y el respaldo de la dirección general de la organización de mi cliente, favoreció la permanencia y crecimiento del servicio.

Evolucionar hacia una gestión eficaz de usuarios privilegiados en la organización de mi cliente incluyó un proceso de adaptación, todo proceso de implantación de un sistema de gestión de usuarios privilegiados implica la consolidación de identidades y el control de los accesos. Para conseguir lograr el objetivo de este servicio, en primer lugar, implanté un modelo para asegurar los accesos privilegiados. El logro de que cada proceso adoptado por la empresa para la ejecución del servicio llegara a convertirse en un “procedimiento rutinario”, me permitió conseguir que las cuentas privilegiadas estuvieran protegidas. El plan estratégico identificó a todos los actores principales, y logré definir claramente el área de responsabilidad de cada grupo. Y, lo más importante, el plan identificó las funciones y las responsabilidades de los usuarios dentro de la organización que necesitaban acceso a las cuentas privilegiadas. Después de decidir las funciones y responsabilidades para aquellos que necesitaban privilegios, especificamos los requisitos individualmente, para lo cual han de registrar la identidad y el uso, lo que posibilita el rastreo y el periodo de vigencia de una cuenta de usuario, desde la provisión hasta el fin de la misma.

Una vez que tuve documentado el plan, la implementación de accesos con privilegios restringidos, de forma que los usuarios solo pudieran tener acceso a lo que necesitan y, por último, con el apoyo de la solución tecnológica realicé el registro y monitoreo de todas las actividades relacionadas con los usuarios privilegiados, con ello evité que se diluyera la responsabilidad individual, lo que me permitió el rastreo de las actividades de cada uno de los administradores. Mi objetivo no fue otro que unificar la identidad de los usuarios que contaran con privilegios en todas las plataformas para reducir la complejidad de la gestión de las mismas.

A la fecha este cliente continúa con el servicio, en otra fase del proyecto ya con mayor alcance, manejando la gestión de usuarios privilegiados como parte habitual de su operación.

8. Bibliografía y referencias

8.1 Referencias

- **Libros**

Emmett Dulaney, Chuck Easttom. (2014). *CompTIA Security+ Study Guide: SY0-401, 6ta (sexta) edición*. Indianápolis, Indiana: John Wiley & Sons Inc.

Servicio de Administración Tributaria. (2011). *Licitación Pública Nacional Mixta de Servicios No. LA-006E00001-N4-2011, Anexo Técnico*. México: SAT.

Shon Harris. (2007). *CISSP All-in-One Exam Guide, 4ta (cuarta) edición*. New York: McGraw Hill Companies.

Richard Kissel. (2013). *NISTIR 7298*, *Revision 2 Glossary of Key Information Security Terms*. Editor Computer Security Division Information Technology Laboratory.

- **Artículo de revista electrónica**

Acevedo Juárez, Héctor. (2010). *ITIL: ¿qué es y para qué sirve?*. 1(1), 14-19. Sitio oficial revista Magazcitum – El magazine para los profesionales de la seguridad de TI. Recuperado de http://www.magazcitum.com.mx/?p=50#.WtTSsYjwbIV http://www.magazcitum.com.mx/?p=323#.WtTWA4gbPIV

- **Página web**

Sitio oficial Scitum (2018). *Conócenos*. Recuperado de https://www.scitum.com.mx/Home/About

NIST (2018). *COMPUTER SECURITY RESOURCE CENTER, Glossary*. Recuperado de https://csrc.nist.gov/Glossary/?term=5289#AlphaIndexDiv

8.2 Bibliografía

Emmett Dulaney, Chuck Easttom. (2014). *CompTIA Security+ Study Guide: SY0-401, 6ta (sexta) edición*. Indianápolis, Indiana: John Wiley & Sons Inc.

Servicio de Administración Tributaria. (2011). *Licitación Pública Nacional Mixta de Servicios No. LA-006E00001-N4-2011, Anexo Técnico*. México: SAT.

Shon Harris. (2007). *CISSP All-in-One Exam Guide, 4ta (cuarta) edición*. New York: McGraw Hill Companies.

Sitio oficial Scitum (2018). *Conócenos*. Recuperado de https://www.scitum.com.mx/Home/About

9. Anexos

9.1 Glosario

- **Acceso**: Es el flujo de información entre un sujeto y un objeto[3].
- **Amenaza:** Es cualquier peligro potencial a información o sistema[3].
- **Control de Acceso**: Son características de seguridad que controlan como los usuarios y sistemas se comunican e interactúan con otros sistemas y recursos.
- **Datos:** Subconjunto de información en un formato electrónico que permite su recuperación o transmisión.
- **Información:** Una instancia de un tipo de información.
- **Incidente:** Violación o amenaza inminente de violación de las políticas de seguridad informática, políticas de uso aceptable o prácticas estándar de seguridad.
- **Log:** Registro de los eventos que ocurren dentro de los sistemas y redes de una organización[4].
- **Log de auditoría:** Registro cronológico de las actividades del sistema. Incluye registros de los accesos al sistema y las operaciones realizadas en un período determinado.
- **Objeto:** Es una entidad pasiva que contiene información, un objeto puede ser una computadora, una base de datos, un archivo, un programa, directorio o un registro dentro de una base de datos[4].
- **Password:** Es una cadena de caracteres protegida que es usada para autenticar un individuo.
- **Riesgo:** El nivel de impacto en las operaciones de la organización (incluida la misión, funciones, imagen o reputación), los activos de la organización, individuos o las personas encargadas de la operación de un sistema de información dado el impacto potencial de una amenaza y la probabilidad de que esa amenaza ocurra.
- **Riesgo de seguridad de la información:** Riesgo para las operaciones de la organización (incluida la misión, funciones, imagen, reputación), activos de la organización, individuos, otras organizaciones y naciones debido a la posibilidad de acceso no autorizado, uso, divulgación, interrupción, modificación o destrucción de información y/o sistemas de información. Ver Riesgo.
- **Sujeto:** Es una entidad activa que requiere acceso a un objeto o a los datos contenidos dentro de un objeto. Un objeto puede ser un usuario, programa o proceso que accede a un objeto para cumplir una tarea[4].
- **Seguridad de la información:** Protección de información y de los sistemas de información contra el acceso no autorizado, el uso, la divulgación, la interrupción, la modificación o la destrucción con el fin de proporcionar confidencialidad, integridad y disponibilidad.
- **Seguridad de los sistemas de información - (INFOSEC):** Protección de los sistemas de información contra el acceso no autorizado o la modificación de la información, ya sea en almacenamiento, procesamiento o tránsito, y contra la denegación de servicio a los

[3] CISSP All-in-One Exam Guide, 4ta (cuarta) edición.

[4] COMPUTER SECURITY RESOURCE CENTER https://csrc.nist.gov/Glossary/?term=5289#AlphaIndexDiv

usuarios autorizados, incluidas las medidas necesarias para detectar, documentar y contrarrestar tales amenazas.

- **Tecnología de la información:** Cualquier equipo o sistema o subsistema interconectado de equipos que se utiliza en la adquisición, el almacenamiento, la manipulación, la gestión, el movimiento, el control, la visualización, la conmutación, el intercambio, la transmisión o la recepción automáticos de datos o información por parte de una organización. El equipo es utilizado por una organización directamente o por un tercero en virtud de un contrato con la organización que: 1) requiere el uso de dicho equipo; o 2) requiere el uso, en gran medida, de dicho equipo en la prestación de un servicio o el suministro de un producto. El término tecnología de la información incluye computadoras, equipos auxiliares, software, firmware y procedimientos similares, servicios (incluidos los servicios de soporte) y recursos relacionados[5].
- **Vulnerabilidad:** Es una falla o debilidad en un hardware, software o procedimiento que puede proporcionar a un atacante una puerta para entrar a una computadora o red y tener un acceso autorizado a recursos dentro de un ambiente. Una vulnerabilidad se caracteriza por la ausencia o débil protección que puede ser explotada.

9.2 ITIL

ITIL *(IT Infrastructure Library, biblioteca de infraestructura de TI)* = Marco de referencia que describe un conjunto de mejores prácticas y recomendaciones para la administración de servicios de TI, con un enfoque de administración de procesos.

En 1987 la CCTA, un organismo del gobierno británico (ahora llamado la OGC) inició un proyecto llamado GITIMM (Government IT Infrastructure Management Method), en el cual involucraron a varias firmas de consultoría para investigar y documentar las mejores prácticas para planear y operar la infraestructura de TI. Poco después, conforme el proyecto evolucionaba de administración de infraestructura a administración de servicios de TI, se le cambió el nombre a ITIL.

Como marco de referencia, ITIL se creó como un modelo para la administración de servicios de TI e incluye información sobre las metas, las actividades generales, las entradas y las salidas de los procesos que se pueden incorporar a las áreas de TI.

Desde sus inicios ITIL fue puesta a disposición del público en forma de un conjunto de libros, de ahí su nombre, para que las organizaciones de todo el mundo pudieran adoptarlo. La primera versión consistía de 10 libros principales que cubrían dos grandes temas: “Soporte al servicio” y “Entrega del servicio”, amén de una serie de libros complementarios que cubrían temas tan disímbolos como la administración de la continuidad o cuestiones relacionadas con cableado. Posteriormente, en 2001 se hizo una reestructura importante que reunió los 19 libros principales en sólo 2, mientras que otros temas siguieron en libros separados, dando así un total de 7 libros para la segunda versión de ITIL:

- Soporte al servicio (1).
- Entrega del servicio (2).

[5] NISTIR 7298, Revision 2 Glossary of Key Information Security Terms

- Administración de la seguridad (3).
- Administración de la infraestructura ICT (4).
- Administración de las aplicaciones (5).
- La perspectiva del negocio (6).
- Planeación para implantar la administración de servicios (7).

Precisamente con la versión 2, a mediados de los años 90, ITIL fue reconocido como un "estándar de facto" para la administración de servicios de TI, el cual, como siempre, tuvo que seguir evolucionando para considerar las nuevas escuelas de pensamiento y alinearse mejor a otros estándares, metodologías y mejores prácticas, lo que llevó en 2007 a la liberación de la versión 3 de ITIL.

ITIL V3 sólo consta de cinco libros, que están estructurados en torno al ciclo de vida del servicio:

- Estrategia de servicios.
- Diseño de servicios
- Transición de servicios.
- Operación de servicios.
- Mejora continua de servicios.

Esta nueva estructura organiza los procesos de ITIL V2 con contenido y procesos adicionales encaminados a una mejor administración del periodo de vida de los servicios de TI. Partiendo de esta observación, podemos afirmar que la V3 refuerza el foco en los servicios de TI, sin dejar de lado los procesos, pero haciendo patente que aunque los procesos son importantes son secundarios y sólo existen para planificar, entregar y dar soporte a los servicios.[6]

ITIL es un conjunto de mejores prácticas y recomendaciones para la administración de servicios de TI, con un enfoque de administración de procesos. Los libros de ITIL listan una serie de procesos y funciones que se recomienda implantar para una mejor entrega de los servicios que las áreas de TI proporcionan a sus usuarios. La idea es que toda organización de TI opere con un enfoque de procesos para la administración de servicios de TI, empleando ITIL como una guía sobre qué procesos implantar y cuáles son las características principales de dichos procesos.[7]

[6] ITIL: ¿qué es y para qué sirve? (parte 1) http://www.magazcitum.com.mx/?p=50#.Ws_HO4jwbIU
[7] ITIL: ¿Qué es y para qué sirve? (parte 2) http://www.magazcitum.com.mx/?p=323#.Ws_LdojwbIU