

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación



“IMPLEMENTACIÓN DE UN SISTEMA DE MESA DE
AYUDA INFORMÁTICO HELP DESK PARA LA GESTION
DE REQUERIMIENTOS QUE SE PRESENTAN EN UN
SOC”

EXAMEN DE GRADO (COMPLEXIVO)

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:
**MAGISTER EN SISTEMAS DE INFORMACIÓN
GERENCIAL**

AUTOR:

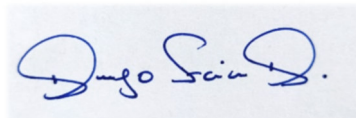
DIEGO ANTONIO FARIA DOMINGUEZ

GUAYAQUIL – ECUADOR

AÑO: 2021

AGRADECIMIENTO

Agradezco a Dios por su infinita misericordia y haberme dado sabiduría y entendimiento para alcanzar cada una de mis metas propuestas, a mi gran familia, a mi Madre Doris Domínguez que ha sabido guiarme y tener siempre esas palabras precisas para continuar, a mi esposa Stefany Suarez quien es mi complemento, y a mis amigos Sara Zambrano, Elena Armijos, Jesús Jácome, Lucy Caregua y Juan Carlos Sellan quienes han estado presente en todo este proceso de estudio.



Lic. Diego Faria Domínguez


DEDICATORIA

Este trabajo va dedicado a mi Papá Eusebio Domínguez quien desde pequeño me enseñó el camino de Dios y sembró en mi los valores para ser un hombre de bien y sé que desde el Cielo está orgulloso de mí y a mi madre Doris Domínguez quien ha sido padre y madre aquí en la tierra, que hizo hasta lo imposible para que pueda tener una buena educación. Gracias infinitas a los dos por todo su amor.

TRIBUNAL DE EVALUACIÓN



MSIG. Lenin Freire Cobo
COORDINADOR MSIG



MSIG. Juan Carlos García
PROFESOR MSIG

RESUMEN

La empresa dedicada a la seguridad informática brinda sus servicios a 6 organizaciones entre ellas identidades bancarias, públicas y privadas a nivel nacional. A inicios de su operatividad no contaban con un sistema que le permita al departamento del SOC cuyas siglas significan Centro de Operaciones de Seguridad, llevar el control y registro centralizado de los incidentes y requerimientos enviados a sus clientes.

Estos incidentes y requerimientos eran registrados en un archivo Excel almacenado en el file server el cual era compartido dentro de la red interna, sin embargo, su funcionalidad era limitada en comparación al servicio que se ofrece puesto que demandaba mucho tiempo y recursos por parte de los analistas.

En base a esta problemática y previo análisis, la empresa privada optó por contratar el sistema de mesa de ayuda Freshservice que es una herramienta ITSM (Gestión de servicios de tecnologías de la información) que permite registrar, evaluar y realizar un seguimiento de todos los incidentes y requerimientos ingresados por los agentes de manera que se tenga un flujo de atención efectiva.

El documento describe la implementación del sistema de mesa de ayuda Freshservice, su funcionalidad, desempeño y las ventajas que permite obtener. Además, se detalla el proceso de atención de los incidentes, canales de atención, escalamientos, horarios y más información relevante que ha sido reestructurada para poder ofrecer un mejor servicio.

ÍNDICE GENERAL

DEDICATORIA	iii
TRIBUNAL DE EVALUACIÓN	iv
RESUMEN	v
ABREVIATURAS Y SIMBOLOGÍA	viii
INTRODUCCIÓN	xii
CAPÍTULO 1	1
1. GENERALIDADES	1
1.1 Antecedentes	1
1.2 Descripción del problema	2
1.3 Solución Propuesta	3
1.4 Objetivo General	4
1.5 Objetivo Específicos	4
1.6 Metodología	4
CAPÍTULO 2	7
2. METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN.	7
2.1 Infraestructura de red de la organización	7
2.2 Recursos	8
2.2.1 Tecnológicos (Hardware / Software)	8

2.2.2	Humanos (Roles y Responsabilidades).....	10
2.2.3	Freshservice	13
2.3	Proceso de atención de incidentes y requerimientos	20
2.3.1	Canales de atención	24
2.3.2	Escalamientos	24
2.3.3	Horarios	26
2.4	Indicadores y SLA de solución implementada	26
2.5	Costos de la solución	27
CAPÍTULO 3.....		29
3.	ANÁLISIS DE RESULTADOS DE LA SOLUCIÓN.....	29
3.1	Registro de las Incidencias.....	29
3.2	Automatización en tareas	30
3.3	Auditoria de problemas.....	33
3.3.1	Generación de Informes	33
3.4	Toma de decisiones	34
3.4.1	Análisis de informes de monitoreo.....	34
CONCLUSIONES Y RECOMENDACIONES		35
BIBLIOGRAFÍA.....		38
ANEXOS		39

ABREVIATURAS Y SIMBOLOGÍA

CSIRT	Equipo de respuesta a incidentes Informáticos.
Freshservice	Sistema de gestión de Incidentes y solicitudes.
ITIL	Biblioteca de Infraestructura de Tecnología de la Información.
ITSM	Gestión de servicios de tecnología de la información.
KPI	Indicador clave de rendimiento.
SAAS	Software como Servicio.
SLA	Acuerdo de Nivel de Servicio.
SOC	Centro de Operaciones de Seguridad.
TI	Tecnología de la Información.

ÍNDICE DE TABLAS

Tabla 1 Características Firewall: Fortigate 60D	8
Tabla 2 Proveedores de Internet.....	9
Tabla 3 Servidores Virtuales - Características	10
Tabla 4 Roles y Responsabilidades del área del SOC	11 - 13
Tabla 5 Clasificación y nivel de criticidad de evento/incidentes	22
Tabla 6 Tipos de eventos/incidentes.....	23
Tabla 7 Nivel de criticidad del evento/incidente	24
Tabla 8 Niveles de escalamiento del cliente	25
Tabla 9 Niveles de escalamiento del SOC.....	25
Tabla 10 Tiempos de SLA referente a la Prioridad de incidentes	26
Tabla 11 Plan general con costos y tiempos aproximados de la implementación.....	27

ÍNDICE DE FIGURAS

Figura 1.1 Ciclo de vida de ITIL V3.....	6
Figura 2.1 Infraestructura de red antes de la implementación del sistema.....	8
Figura 2.2 Organigrama del SOC	11
Figura 2.3 DashBoard Paneles	15
Figura 2.4 Gráfica de sección de Informes	16
Figura 2.5 Prototipo de incidente ingresado en la mesa de ayuda	18 - 19
Figura 2.6 Infraestructura de Red con Freshservice	20
Figura 2.7 Ciclo de vida de la gestión y respuesta a un incidente de seguridad	21
Figura 3.1 Ejemplar de correo enviado por la mesa de ayuda a personal encargado.....	31
Figura 3.2 Ejemplar de correo enviado por la mesa de ayuda al analista asignado	32
Figura 3.3 Ejemplar de correo de notificación a analista cuando se cierra un ticket	32
Figura 3.4 Flujo de atención efectiva de mesa de ayuda.....	34

INTRODUCCIÓN

La organización privada orientada a la seguridad informática brinda varios servicios entre ellos el monitoreo de red 24/7 y emisión de reportes a diferentes clientes a nivel nacional. Sus clientes principales son seis los cuales tienen sus propias sucursales.

EL SOC es el departamento encargado de atender las incidencias de seguridad de sus clientes y a la vez responsable del seguimiento y solución que se le da a las mismas. Inicialmente no se tenía implementado un sistema de gestión de incidencias y requerimientos, por tal motivo los analistas ocupaban mucho tiempo y recursos en actualizar la base de datos de incidencias que se encontraba guardada en un archivo Excel, por tal motivo la organización decidió implementar un sistema de Mesa de ayuda que permita la automatización de tareas y optimice los tiempos de atención de cada uno de los requerimientos e incidencias.

Esta propuesta detalla los pasos para la implementación de Freshservice en la organización, sus ventajas y beneficios a la organización. Adicionalmente se describen los canales de atención, como son categorizadas las incidencias y cuales son los KPI que la organización debe mantener alineados con el sistema, entre otros.

Esta mejora en cuanto a la gestión y seguimiento de las incidencias ha permitido brindar un mejor servicio por parte de la organización aumentando así el nivel de satisfacción por parte de sus clientes.

CAPÍTULO 1

GENERALIDADES.

1.1 Antecedentes

Empresa privada con varios años de experiencia en el mercado está dedicada a la seguridad Informática y brinda soluciones integrales de negocio sustentados en las tecnologías de la información y comunicación, garantizando así la confidencialidad, integridad y disponibilidad de la información, cumpliendo con requisitos aplicables en base a seguridad de la información. Dentro de sus departamentos se encuentra el Centro de Operaciones de Seguridad (SOC) que es el equipo responsable de asegurar la información utilizando metodologías y procesos estratégicos. Actualmente este servicio se está ofreciendo a seis organizaciones, tanto públicas como privadas donde se provee el servicio

monitoreo 24/7. El mencionado servicio consiste en monitorear, analizar y emitir reportes de eventos presentados en base al SLA acordado para que el cliente tome acciones correctivas. Si el cliente ha tenido un evento de gran magnitud y se necesita un análisis más profundo se da el servicio CSIRT (Computer Incident Response Team) que consiste en emitir un informe más detallado con todos los indicadores de compromiso con acciones y recomendaciones que deben tomar para evitar el ataque tratado al futuro o como poder solventar el evento presentado en ese momento.

1.2 Descripción del problema

Desde el inicio de operaciones, la organización registraba los requerimientos en un archivo Excel compartido en un servidor centralizado dentro de la red interna. En este archivo se llevaba el control de las incidencias presentadas y solicitudes realizadas por las organizaciones. Sin embargo, preparar los reportes solicitados por los clientes demandaba mucho tiempo y recursos por parte de los analistas, dado que la labor se debía realizar de forma manual. En ocasiones el cliente solicitaba en reiteradas ocasiones el mismo reporte debido a la excesiva cantidad de tiempo que se tomaba en realizarlo.

Otra problemática se suscitaba, al ser un archivo compartido frecuentemente se debía esperar que un analista finalizara la creación del requerimiento llenando cada uno de sus campos (ticket, nombre del incidente, IP origen, IP destino, etc.) para que el otro analista pueda comenzar a realizar el suyo aumentando así el tiempo de entrega estimado del reporte.

1.3 Solución Propuesta

Debido al proceso que actualmente maneja la empresa privada para el registro y control de incidencias, se propone la siguiente solución para optimizar el tiempo de respuesta y mejorar la gestión de la organización. Se recomendó contratar Freshservice, una herramienta de gestión de servicios de tecnologías de la información (ITSM), la cual utiliza servicios de alojamiento y datos en la nube como el SaaS (Software como servicio) y permite a los usuarios conectarse con clientes y brindar diversos servicios para la organización.

Freshservice ofrece muchas funcionalidades que fueron implementadas en la empresa, la cual les permite obtener las ventajas descritas a continuación:

- ✓ Registro detallado de toda la información relevante de los incidentes de servicio.
- ✓ Medir el rendimiento del trabajo en tiempo real.
- ✓ Automatización y mejoras en tareas que consumen tiempo en la mesa de servicio.
- ✓ Auditoria de problemas en la mesa de servicio.
- ✓ Activar acciones concretas para eventos importantes, como el envío de una notificación por correo electrónico.
- ✓ Tomar decisiones informadas por el monitoreo en cuanto al desempeño del Servicedesk.
- ✓ Generar informes y mejorar su prestación de servicios con funcionalidades predefinidas y personalizadas.

Para hacer un seguimiento del estado de las incidencias, el sistema de gestión de Freshservice, ofrece un DashBoard de monitoreo que analiza y muestra de forma visual los indicadores clave de desempeño (KPI), con las métricas de los datos fundamentales ingresados en la mesa de servicio.

1.4 Objetivo General

Implementar un sistema que permita la optimización en la gestión de solicitudes, Incidentes y generación de estadísticas para la toma de decisiones y mejora continua del servicio.

1.5 Objetivo Específicos

- a) Identificar las necesidades y los requerimientos del Centro de Operaciones de Seguridad (SOC).
- b) Implementar Servicedesk como nuevo sistema de gestión.
- c) Establecer el catálogo de servicios para el sistema de mesa de ayuda.
- d) Reducir los tiempos de emisión de reportes de eventos presentados y requerimientos solicitados por el cliente.

1.6 Metodología

Con el fin de brindar un mejor servicio y mejorar las capacidades de la organización, este proyecto se basó en la fundamentación práctica e integrada que proporciona la metodología ITILv3 cuyas siglas significan Biblioteca de Infraestructura de Tecnología de la Información que no es más que un conjunto

de publicaciones que proporciona mejores prácticas y recomendaciones en la Gestión de Servicios de TI. [1] Es una estrategia de trabajo con la que es posible alcanzar una gestión de servicios de TI muy eficiente como se puede ver reflejado en los resultados que han obtenido las empresas con mayor éxito [2]

Estas guías que garantizan la calidad de servicio de TI, proporcionan valor al cliente y al negocio utilizando múltiples herramientas, procedimientos y una estructura específica para la implementación que ayuda en el control, operación y administración de los recursos [1]. Entre sus ventajas se podría destacar la mayor agregación de la organización de TI con el Negocio al proveer precisión, velocidad y disponibilidad en base a los niveles de servicio acordados. Su estructura es mucho más sencilla a diferencia de otros marcos de referencia. Permite a las organizaciones entregar servicios apropiados y asegurarse constantemente que están alcanzando las metas del negocio. [3]

Los procesos específicos del proyecto expuesto se profundizan en cada una de las etapas del ciclo de vida de ITIL.

Estrategia del Servicio: En esta etapa fue donde se autorizó el uso de Servicedesk como mesa de ayuda para la gestión de incidentes definiendo los servicios que se prestarán tanto a los clientes como a los usuarios internos de la organización y el costo estimado a utilizar para su implementación.

Diseño del Servicio: En esta etapa se desarrollaron nuevos servicios y se mejoraron los existentes en base al perfil del usuario garantizando el cumplimiento de los requerimientos y solicitudes de los clientes.

Dentro de las categorías del catálogo de servicios de Servicedesk, se diseñó el template de la sección “solicitud de servicios” donde previo análisis se añadieron

campos relevantes como Descripción, IP Origen, IP destino, Raw Data, Equipo afectado, etc. que permitan ofrecer información precisa ofreciendo así un servicio más eficiente.

Transición del Servicio: En esta etapa se implementó los servicios anteriormente diseñados dentro de los parámetros establecidos; calidad, tiempo y costo.

Operación del Servicio: Fase donde se ejecutaron las tareas operativas y de mantenimiento del servicio de mesa de ayuda para luego evaluarse los resultados dados en base al acuerdo de nivel de servicio (SLA),

Mejora Continua del Servicio: Basados en las mediciones y resultados en esta etapa se alinearán y realinearán los servicios con las necesidades cambiantes de negocio distinguiendo los que son rentables y aquellos que podrán ser mejorados



Figura1.1 Ciclo de vida de ITIL V3

Fuente: <http://inventarios.org/2016/03/04/los-7-pasos-de-la-mejora-de-procesos-definidos-en-iti/>

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN.

2.1 Infraestructura de red de la organización.

Uno de los pilares fundamentales del Centro de Operaciones de Seguridad es su infraestructura tecnológica. Dentro de su estructura de red interna se utilizaba el file server para almacenar el archivo Excel llamado Bitacora.xls, donde se llevaba el control de las incidencias y requerimientos solicitados por los clientes. Debido a los inconvenientes detallados anteriormente se procedió a la implementación de Freshservice para optimizar el tiempo de respuesta y mejorar la gestión de la organización. En la siguiente gráfica se detalla la infraestructura de la empresa antes de la implementación de Freshservice.

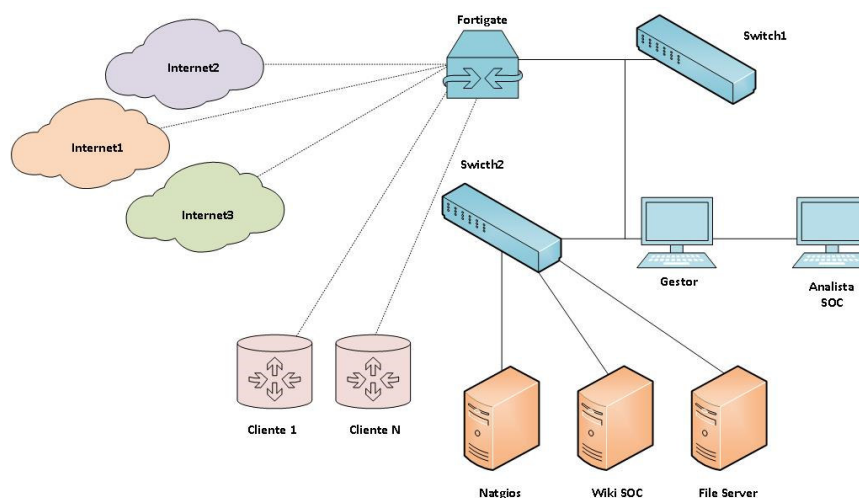


Figura 2.1 Infraestructura de red antes de la implementación del sistema.

Fuente: Elaboración propia.

2.2 Recursos

En la siguiente sección se detalla los recursos tecnológicos y humanos contemplados en la implementación del sistema para la gestión de incidentes, así como las ventajas proporcionadas por Freshservice.

2.2.1 Tecnológicos (Hardware / Software)

La empresa privada posee un equipo Fortigate60D como firewall de seguridad cuyas características se encuentran detalladas en la tabla 1.

Equipo	Firewall: Fortigate 60D
Descripción	Enterprise-Class 1. Console Port 2. USB Management Port for FortiExplorer 3. USB Port 4. 2x GE RJ45 WAN Ports 5. 1x GE RJ45 DMZ Ports 6. 7x GE RJ45 Internal Ports / 5x GE RJ45 Internal and 2x GE PoE Ports on POE models

Beneficios y características clave	
Seguridad unificada	La protección de múltiples amenazas desde un solo dispositivo amplía la seguridad y disminuye los costos.
Licencias simplificadas	Licencias de usuario ilimitadas y funciones integrales.
Interfaces multipuerto	Las múltiples interfaces de red permiten la segmentación de datos para su cumplimiento.

Tabla 1 Características Firewall: Fortigate 60D

Fuente: <https://www.avfirewalls.com/datasheets/FortiGate/FortiGate-60D>

Además, cuenta con 3 interfaces de túneles de internet, especificado en la tabla 2, para garantizar la disponibilidad y balanceo de carga. Adicional tiene 6 clientes a nivel nacional, entre ellos entidades bancarias, servicios públicos, compañías privadas, etc.

Proveedor	Ancho de banda	Descripción
Centurylink	10 MB	Enlace principal para VPN de clientes.
Claro	3 MB	Enlace de contingencia de VPN clientes
TV Cable	6 MB	Enlace de navegación.

Tabla 2 Proveedores de Internet

Fuente: Documento de Plan de continuidad de la empresa privada.

Dentro de su estructura interna se encuentra un Switch que permite la conexión de las máquinas de los usuarios finales, como las del Gestor, Arquitecto de Seguridad, Oficial de Seguridad, Analistas, entre otros. Además, se tiene tres servidores virtuales almacenados en el Equipo virtualización HPProliant G8 los cuales se encuentran detallados en la tabla 3.

Servidor	Descripción	Tipo
Nagios	Es el sistema de monitoreo de redes que permite controlar el estado de salud de los equipos de los clientes como servicios de red	virtualizado

	(SNMP, SMTP, HTTP.) y sus recursos del hardware como consumo de memoria, procesador, disco duro, etc. basados en un umbral acordado con ellos mismos.	
Wiki Soc	Es la base de conocimientos de la organización donde se encuentra información relevante de los clientes y la forma de proceder de manera centralizada para que pueda ser utilizada por los analistas.	virtualizado
File Server	Es el lugar de almacenamiento centralizado de la empresa privada donde se encontraban alojados todos los archivos entre ellos la Bitacora.xls.	virtualizado

Tabla 3 Servidores Virtuales – Características

Fuente: Documento Diagrama de Red de la empresa privada.

2.2.2 Humanos (Roles y Responsabilidades)

La organización cuenta con un total de 16 colaboradores, de manera jerárquica. La empresa se encuentra estructurada por el Gerente de Servicios, quien maneja la empresa privada de seguridad, seguidamente está el área administrativa y contable del SOC con servicios generales y también el Coordinador de Servicios quien lidera la mesa de servicios con ayuda del Oficial de seguridad de la información, Analista CSIRT, Arquitecto de Seguridad & TI y Gestor del SOC quien a su vez es responsable de los analistas de seguridad.

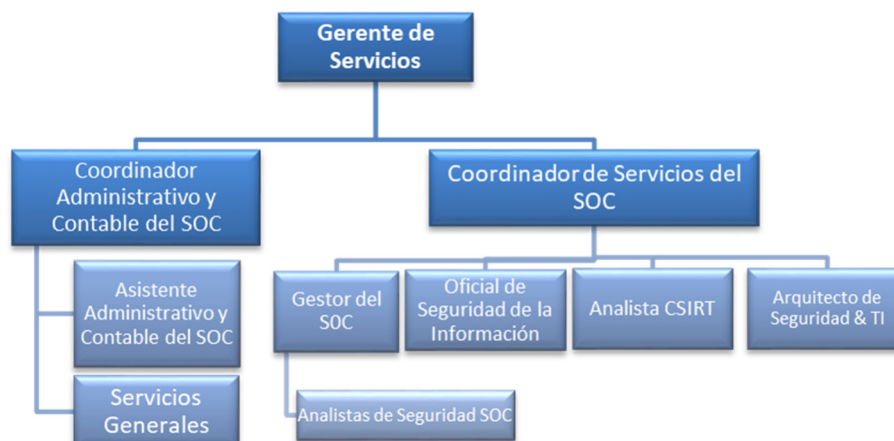


Figura 2.2 Organigrama del SOC.

Fuente: Documento Estructura Organizacional y organigrama de la empresa.

A continuación, se describe en la siguiente tabla los roles y responsabilidades de los actores que intervienen en el proceso de atención de los incidentes con la ayuda del sistema Freshservice, los cuales pertenecen al área de servicio del SOC.

Rol	Responsabilidades
Coordinador de servicios del SOC	<ul style="list-style-type: none"> - Evaluar, dar a conocer y gestionar la aprobación de las principales iniciativas para aumentar la Seguridad de la Información, conforme con las competencias y responsabilidades asignadas. - Gestionar el suministro continuo de recursos humanos, económicos y tecnológicos para la Gestión de Seguridad de la Información. - Evaluar, analizar y gestionar los incidentes de seguridad de la información en coordinación con el Gestor del SOC, Analista CSIRT, Oficial de Seguridad de la Información y Arquitecto de Seguridad & TI. Para los casos que aplique sanciones al personal se debe involucrar al área Administrativa.

Gestor del SOC	<ul style="list-style-type: none"> - Implementar controles de seguridad definidos en la Política de Seguridad de la Información y fomentar en el personal operativo (analistas de seguridad SOC) la responsabilidad del manejo de la seguridad de la información desde la perspectiva de la confidencialidad, integridad y disponibilidad de la información. - Participar en la planificación e implementación de la gestión de la continuidad del servicio del Centro de Operaciones de Seguridad. - Gestionar los incidentes de seguridad de la información de acuerdo con el procedimiento establecido para tal efecto.
Oficial de seguridad de la información	<ul style="list-style-type: none"> - Gestionar la seguridad de la información conforme a las normativas y estándares que apliquen. - Verificar y dar seguimiento al cumplimiento de controles de seguridad del SGSI para que sean implementados y operados de acuerdo con las políticas y procedimientos de SOC. - Garantizar el correcto uso de la información de acuerdo con los parámetros de seguridad establecidos. - Garantizar el buen uso de su cuenta de usuario, estando obligado a mantener la confidencialidad y reserva de ésta siendo así el único responsable por su correcto uso.
Analista CSIRT	<ul style="list-style-type: none"> - Ejecutar evaluaciones de vulnerabilidades técnicas en los sistemas de procesamiento de información. - Garantizar la protección de los equipos o activos asignados ante daño, pérdida o robo. - Garantizar la confidencialidad e integridad de la información relacionada a eventos e incidentes de seguridad de nuestros clientes, así como la información que pertenece a la empresa.
Arquitecto de la seguridad & TI	<ul style="list-style-type: none"> - Garantizar la seguridad de la información en las redes y protección de la infraestructura de soporte.

	<ul style="list-style-type: none"> - Garantizar la aplicación de controles de seguridad para la gestión de control de accesos. - Garantizar la disponibilidad de la información mediante la aplicación de controles de seguridad como lo son respaldos de información. - Monitorear y comunicar las fallas en los sistemas de procesamiento de información o de comunicación, permitiendo así tomar medidas correctivas.
Analistas de seguridad	<ul style="list-style-type: none"> - Asistir a los cursos o talleres de capacitación en seguridad de la información, registrar su asistencia y de ser el caso rendir la evaluación correspondiente. - Garantizar el correcto uso de la información de acuerdo con los parámetros de seguridad establecidos. - Firmar el acuerdo de confidencialidad de la información en el cual se compromete a mantener la integridad, calidad y confidencialidad de la información del Centro de Operaciones de Seguridad. - Notificar de modo imperativo de carácter obligatorio y sin excepción al jefe inmediato y al Oficial de Seguridad de la Información, cuando se detecten hechos o eventos que descubran circunstancias que puedan afectar a la operatividad del SOC en temas de seguridad de la información.

Tabla 4 Roles y Responsabilidades del área del SOC

Fuente: Documento Manual de responsabilidades de la empresa privada.

2.2.3 Freshservice

Debido al proceso que maneja la empresa privada para el registro y control de incidencias, se optó como solución para la optimización y eficiencia de la organización el uso del sistema Freshservice, que es una herramienta inteligente de gestión de servicios de tecnologías de la

información (ITSM), con la capacidad de gestionar requerimientos, optimizar flujos de trabajo y tareas aumentando el rendimiento y los estándares de productividad de la organización.

Este sistema de mesa de ayuda utiliza servicios de alojamiento y datos en la nube como el SaaS (Software como servicio) y permite a los usuarios conectarse con clientes y brindar diversos servicios para la organización.

[4]

Freshservice brinda muchas funcionalidades, las cuales permite obtener las ventajas descritas a continuación [5]:

- Registro de todos los detalles relevantes de los requerimientos o solicitudes de servicio.
- Mejorar la cultura de trabajo en la organización.
- Cuantificar el rendimiento del trabajo en tiempo real.
- Habilidad de fusionar las tareas de la mesa de servicio, con los objetivos de los proyectos.
- Automatización y mejoras en tareas que consumen tiempo en la mesa de servicio.
- Gestión de base de conocimiento de la empresa
- Auditoria de problemas en la mesa de servicio.
- Activar acciones concretas para eventos importantes, como el envío de una notificación por correo electrónico.
- Tomar decisiones informadas por el monitoreo en cuanto al desempeño del Servicedesk.

- Generar informes y mejorar su prestación de servicios con funcionalidades predefinidas y personalizadas.

Para realizar el seguimiento del estado de las incidencias, el sistema de gestión de Freshservice, proporciona un dashboard de monitoreo, donde se muestra de forma visual los indicadores clave de desempeño (KPI), con las métricas de los datos fundamentales ingresados en la mesa de servicio. [5]

En el Dashboard Paneles se pueden visualizar de manera gráfica y en tiempo real la gestión de tickets en base a categorías personalizadas como por ejemplo tickets cerrados por clientes, tickets abiertos y cerrados de un determinado cliente, tickets falsos positivos, entre otros.

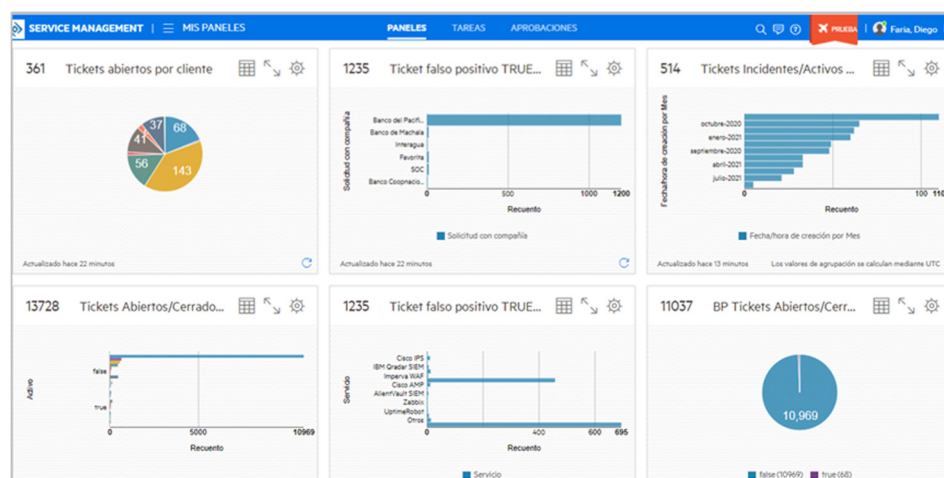


Figura 2.3 DashBoard Paneles.

Fuente: Sistema de Gestión de incidencias Freshservice.

En la sección de informe permite exportar información de manera gráfica y actualizada en base a los indicadores seleccionados. En la imagen 2.4 se visualiza el informe operativo indicando los requerimientos que se

encuentran abiertos por parte de cada uno de los analistas y empleados de la organización.

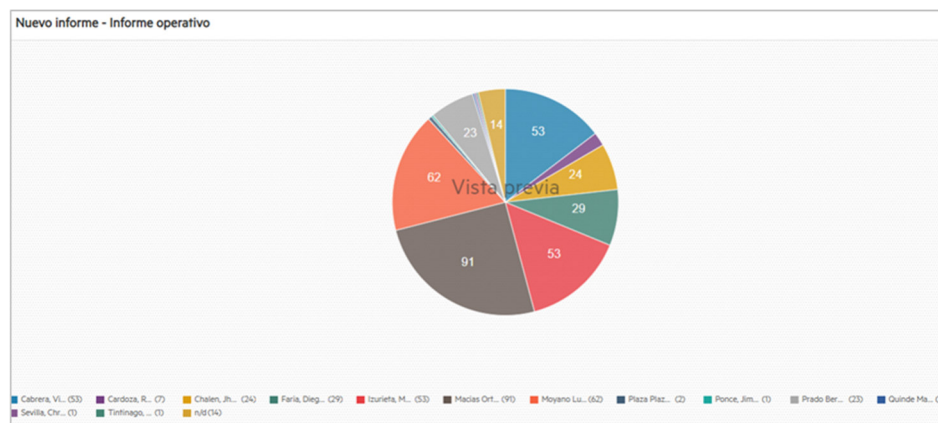


Figura 2.4 Gráfica de sección de Informes.

Fuente: Sistema de Gestión de incidencias Freshservice.

Como parte de la ficha de gestión, el sistema permitirá el registro de las incidencias o requerimientos con información relevante dividida en cinco secciones las cuales se detallan a continuación:

Detalles de la solicitud

- Tipo de evento por plataforma. - Corresponde al nombre del evento que se presentó.
- Descripción- Información detallada del incidente o requerimiento.
- Registrar número de sucesos: Cantidad de eventos presentados.
- Registro Inicio Alerta. - Indica la fecha y hora en la que se efectuó la actividad a registrar.
- Solicitud con compañía. - Nombre de la empresa a quien se reporta el incidente.

- Nombre del cliente: Grupo o nombre de la persona encargada de gestionar el requerimiento (Es a quien va dirigido el correo emitido por la mesa).
- IP Origen: Corresponde a la dirección IP de donde proviene el evento.
- IP Destino: Corresponde a la dirección IP hacia donde fue dirigido el evento.
- Servicio: Herramienta donde se presentó el evento.
- IP Activo Afectado: IP del equipo interno del cliente que está siendo afectado por el evento.
- Registro de origen: Nombre del equipo afectado.
- Raw Data: Parte de la información del mensaje transmitido.
- Creador de la solicitud. - Nombre del agente o personal técnico que reporta el incidente.

Clasificación

- Impacto. - Efecto causado en la organización.
- Urgencia. - Nivel de prioridad que debe ser atendido el ticket.
- Categoría: Clasificación del evento o incidente según su naturaleza.
- Registro Fin Alerta. - Fecha y hora que se terminó de crear la incidencia en la mesa.

Asignación

- Hora de notificación: Fecha y hora de la asignación.

- Asignación: Agente quien dará seguimiento interno al requerimiento creado.
- Grupo del centro de: Área al que pertenece el agente.

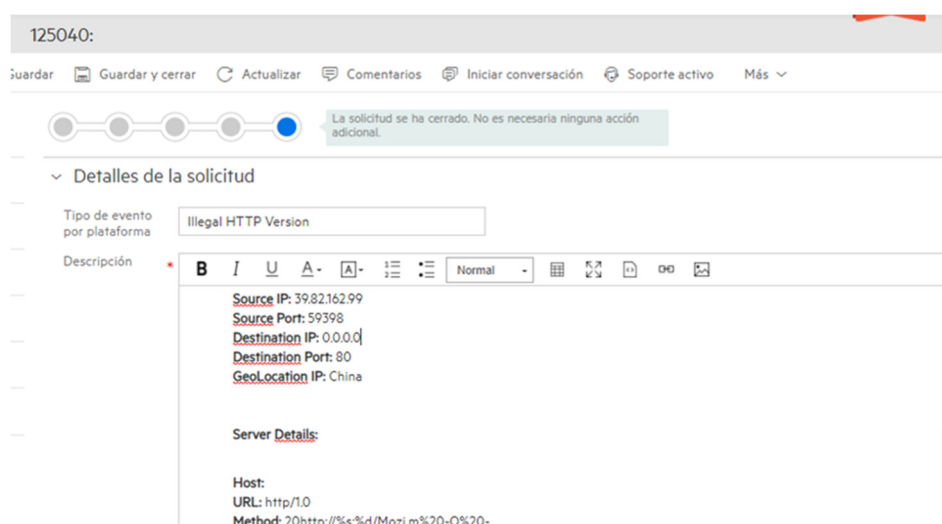
Resolución

- Solución. - Se registra la gestión realizada por el cliente.
- Falso positivo. - Marca que indica que no se debe gestionar el ticket.
- Gestión de conocimiento. - Marca que identifique si la tarea aplica para la base de conocimiento.

Datos Adjuntos

- Para adjuntar archivos relevantes relacionados con el ticket.

A continuación, la figura 2.5 expone un ejemplar de un incidente ingresado en la mesa de servicios con los datos que deben ser considerados.



125040:

Guardar Guardar y cerrar Actualizar Comentarios Iniciar conversación Soporte activo Más ▾

La solicitud se ha cerrado. No es necesaria ninguna acción adicional.

✓ Detalles de la solicitud

Tipo de evento por plataforma:

Descripción

B I U A- A- 1= 2= Normal -

Source IP: 39.82.162.99
Source Port: 59398
Destination IP: 0.0.0.0
Destination Port: 80
GeoLocation IP: China

Server Details:

Host:
URL: http/1.0
Method: 20http://%s:%d/Mozi.m%20-O%20-

IP Origen	39.82.162.99	IP Destino	0.0.0.0
Raw Data	<pre><46>LEEF:1.0 ImpervaSecureSphere 3.5.0 Protocol:None Alert ID=828165 devTimeFormat={see note} devTime=Thu Aug 26 04:21:32 ECT 2021 Alert type=Protocol src=39.82.162.99 dst=0.0.0.0 urlName=n/s Application name=Default Web Application Service name=Documentos Pacificard Alert Description=Illegal HTTP Version Severity=Medium Simulation Mode=false Immediate Action=None</pre>		
Servicio	Imperva WAF	IP Activo Afectado	0.0.0.0
Registro de Origen	Imperva WAF	Ticket Externo	58464
Estado	Preparado	Fecha/hora de creación	jueves, 26 de agosto de 2021 04:40:36
Creador de la solicitud	Faria, Diego		

Clasificación			
Urgencia	Medio	Prioridad	Baja
Tipo de solicitud	Solicitud de servicio TI	Impacto	Bajo
Categoría	Delivery and Attack \ Código Malicioso \ Alertas de Vulnerabilidades Web		
Solicitud con compañía	SOC	Registro de alerta	26/08/2021 04:25
Registro fin alerta	26/08/2021 04:40		

Gestion incidente			
Asignación			
Asignación actual	Centro de servicios	Hora de notificación	26/08/2021 04:43
Grupo del centro de...	Analistas	Propietario	Faria, Diego

Resolución			
Solución	<pre>Ing. Luis F : Gracias por la alerta. 58390 - Se procede a bloquear la IP y el IOC relacionado. Favor cerrar ticket</pre>		
Código de finalización	Resuelto por el cliente	<input type="checkbox"/>	¿Falso Positivo?
Fecha/hora de cierre	jueves, 26 de agosto de 2021 04:55:29		
Soluciones sugeridas		Encontrar más soluciones	

Datos adjuntos (1) + Añadir dato adjunto

58464_125040_ReporteEvent... (93799 KB) hace 17 minutos

Figura 2.5 Prototipo de incidente ingresado en la mesa de ayuda.

Fuente: Sistema de Gestión de incidencias Freshservice.

El siguiente gráfico muestra la infraestructura actual con la que cuenta la organización teniendo al sistema de gestión de incidencias ya

implementado de tal forma que cumpla con los estándares y normas relacionadas con el área de tecnología, seguridad y servicio. En el mismo, se puede observar a Freshservice como un servicio SaaS en la nube, con el cual se puede acceder desde cualquier ordenador con las respectivas credenciales de autenticación.

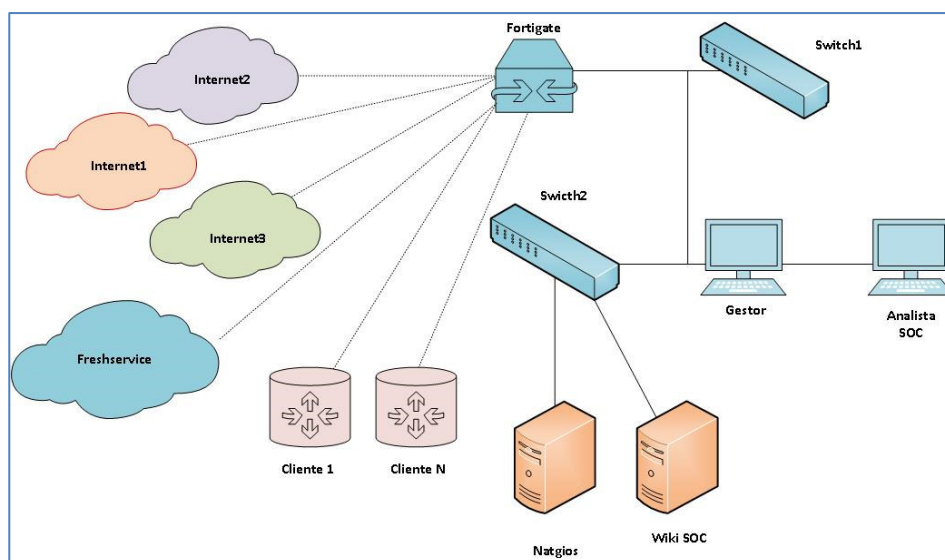


Figura 2.6 Infraestructura de Red con Freshservice.

Fuente: Elaboración propia.

2.3 Proceso de atención de incidentes y requerimientos

La gestión de eventos e incidentes de seguridad se desarrolla a través de una serie de etapas, que tiene como objetivo detectar, evaluar y generar información útil para la toma de decisiones basada en hechos que ocurren y hechos históricos. El proceso puede resumirse de la siguiente manera:



Figura 2.7 Ciclo de vida de la gestión y respuesta a un incidente de seguridad.

Fuente: Documento Procedimiento para la gestión de eventos e incidentes.

A continuación, se procede a detallar el Protocolo Análisis y comunicación de Alertas de Seguridad que la empresa privada realiza con los clientes.

1. Inicia con el monitoreo de las diferentes herramientas de Seguridad
2. Al momento de encontrar un Evento y/o Incidente de Seguridad se procede al análisis respectivo tomando en cuenta las 5-Tuple Correlation / Common Artifact Element.
3. Se realiza el análisis tanto la Origen/IP Destino con aplicativos centrados en tecnología OSINT, Whois, Status Domain, Malware Analysis (Ip-Tracker / Mxtoolbox / VirusTotal). Además, se revisan los Logs enviados al Siem.
4. Se notifica al cliente por medio de un reporte vía correo del análisis realizado adicionando Raw Data para una revisión más profunda por el departamento de seguridad del cliente, dependiendo la criticidad del evento se procede a comunicar vía llamada telefónica, tomando en

5. consideración que este proceso debe estar dentro de los 15 minutos permitidos o el tiempo establecido con el cliente.
6. En caso de no tener respuesta se procede escalar el evento o incidente al punto de contacto que esté definido de acuerdo con el servicio contratado por el cliente
7. Una vez que el equipo de respuesta de incidentes indique su gestión realizada ante el evento se procede con el cierre del requerimiento, en caso de que no haya respuesta se vuelve a notificar al cliente via correo electrónico por parte del Gestor.

Para la categorización de los eventos/incidentes en la mesa de ayuda se detalla a continuación en la tabla 5 la clasificación de los sucesos que se presentan en las herramientas de seguridad de los clientes.

CLASIFICACIÓN	TIPO DE EVENTO/INCIDENTE	NIVEL DE CRITICIDAD
Reconnaissance and Probing	Reconocimiento/Recurrencia de eventos de seguridad	BAJO
Delivery and Attack	Código malicioso	Alto
	Fraude	Alto
	Accesos No autorizados	Medio
	Listas negras	Alto
Exploitation & Installation	Denegación de Servicio	Medio
	Intrusiones	Alto
System Compromise	Falla de equipos y sistemas	Medio
	Estado de salud de recursos tecnológicos	BAJO

Tabla 5 Clasificación y nivel de criticidad de evento/incidentes

Fuente: Documento Procedimiento para la gestión de eventos e incidentes

La tabla 6 describe los Tipos de eventos o incidentes que podrían presentarse dentro de la red de los clientes.

TIPO DE EVENTO/INCIDENTE	EVENTOS/INCIDENTES
<u>Reconocimiento/Recurrencia de eventos de seguridad</u>	<ul style="list-style-type: none"> * Escaneo de puertos * Intento de conexiones a través de puertos * Ingeniería social * Examinar sitios web corporativos * Verificar nombres de dominio * Recurrencia de eventos
<u>Código Malicioso</u>	<ul style="list-style-type: none"> * Ataques de malware * Virus informático * Ransomware * Phishing * Instalación exitosa de código malicioso * SPAM * Injection * Cross Site Scripting * URL infectadas
<u>Denegación de Servicio</u>	<ul style="list-style-type: none"> * Interrupción de servicios tecnológicos * Tiempo de respuestas con umbrales fuera de lo normal * Ataques específicos a sistemas operativos para disminuir su rendimiento
<u>Fraude</u>	<ul style="list-style-type: none"> * Eventos de Fraude
<u>Accesos no autorizados</u>	<ul style="list-style-type: none"> * Intentos reiterativos de acceso a sistemas de información o consultas de información no autorizadas * Intentos de acceso fallido * Deshabilitación de usuarios por accesos fallidos * Ataques de fuerza bruta * Hackeo
<u>Intrusiones</u>	<ul style="list-style-type: none"> * Alertas de Intrusiones
<u>Listas negras</u>	<ul style="list-style-type: none"> * Alertas de IP en Blacklist
<u>Falla de equipos y sistemas</u>	<ul style="list-style-type: none"> * Falla en las redes de comunicaciones * Fallas en los sistemas de información * Sistemas inaccesibles
<u>Estado de salud de recursos tecnológicos</u>	<ul style="list-style-type: none"> * Cambio de estado de equipos o VPN * Alerta de VPN no autorizadas * Equipos sin logs * Estado de Interfaces * Conexiones elevadas desde IP no autorizadas * Patrones de tráfico anómalo * Alto consumo de memoria y CPU * Alteración de tráfico en la red * Cambio en el uso de la red ejecución de comandos para recopilar información de red.

Tabla 6 Tipos de eventos/incidentes

Fuente: Documento Procedimiento para la gestión de eventos e incidentes

A continuación, en la Tabla 7 se describe el nivel de criticidad de incidentes que se utiliza con el fin de gestionar los mismos según su necesidad.

PRIORIDAD	DESCRIPCION
ALTO	El incidente causa daños a activos de información, interrumpiendo procesos críticos, funcionamiento de aplicativos o plataformas de seguridad, incluye aquellos incidentes que afecten a la imagen o reputación de la empresa, teniendo un alto impacto sobre el negocio
MEDIO	El incidente afecta a activos de información e interrumpe la operación o funcionamiento de aplicativos o plataformas de seguridad afectando directamente a objetivos de procesos determinados.
BAJO	No se interrumpe el normal funcionamiento de la operación o funcionamiento de aplicativos o herramientas pudiéndolo controlar fácilmente con recursos existentes. Estos incidentes se deben ser monitoreados para evitar un cambio en el impacto.

Tabla 7 Nivel de criticidad del evento / Incidente

Fuente: Documento Procedimiento para la gestión de eventos e incidentes

2.3.1 Canales de atención



Dentro de los canales de comunicación establecidos con el cliente para una mejor gestión de eventos e incidentes presentados en sus herramientas de seguridad se tienen SMS,

WhatsApp, correo electrónico y llamada telefónica.

2.3.2 Escalamientos

Se procede a escalar mediante llamada telefónica el evento o incidente en base al servicio contratado por el cliente. Cada nivel de escalamiento tiene definido el punto de contacto.

Basados en el SLA, el Analista de Seguridad SOC comunica el evento o incidente al primer nivel de escalamiento, esto se lo realiza durante el lapso de los 10 primeros minutos del evento, pasado este tiempo y si no hubiese respuesta se procederá a escalar al siguiente nivel y de ser necesario se llega hasta el cuarto nivel que es el Gerencial. En caso de no recibir contestación a lo reportado en los tiempos máximos establecidos por el SLA o que la atención que, de inconclusa, se debe comunicar al Gestor del SOC quien definirá las acciones a tomar para obtener una respuesta.

A continuación, la tabla 8 muestra una guía de niveles de escalamiento que se aplica con los clientes.

Relevancia	Escalamiento
Nivel 1	Standby, Técnico, o Analista
Nivel 2	Jefe, encargado o supervisor, especialista, coordinador
Nivel 3	Subgerentes, oficial de seguridad de la información
Nivel 4	Gerente

Tabla 8 Niveles de escalamiento del cliente

Fuente: Documento Procedimiento de notificación y escalamiento

Para el control interna del SOC, se establecen los niveles de escalamiento, de acuerdo a la siguiente tabla:

Relevancia	Escalamiento
Nivel 1	Analista de Seguridad Informática
Nivel 2	Gestor del SOC
Nivel 3	Coordinador del SOC
Nivel 4	Gerente de Servicios

Tabla 9 Niveles de escalamiento del SOC

Fuente: Documento Procedimiento de notificación y escalamiento

2.3.3 Horarios

El servicio de Seguridad Gestionada es brindado desde la ciudad de Guayaquil y se ofrece de manera interrumpida en horario extendido 7x24 los 365 días del año, incluyendo fines de semana y feriados mediante turnos rotativos por parte de los Analistas de Seguridad SOC capacitados en las plataformas y productos de seguridad de la información. En cuanto a los horarios de atención de los clientes, dependerá del acuerdo con cada uno de ellos.

2.4 Indicadores y SLA de solución implementada

Con el fin de acreditar el cumplimiento de lo dispuesto en las cláusulas establecidas con los clientes, se han definido SLAs (Acuerdo de nivel de servicios), que documentan los objetivos de nivel de servicio y especifica las responsabilidades del proveedor de servicios de TI y del cliente. Estos SLA son establecidos junto con el Nivel de criticidad de eventos/incidentes donde el cliente puede solicitar pruebas tecnológicas para verificar que se estén cumpliendo. A continuación, en la tabla 9 detalla un referencial SLA.

Prioridad	SLA
Bajo	En este nivel no se interrumpe el normal funcionamiento de la operación por lo que los eventos o solicitudes son analizados y enviados vía correo electrónico dentro de los 20 primeros minutos desde que se presentó.
Medio	En este nivel el incidente afecta a activos de información e interrumpe la operación por lo que se procede a llamar al punto de contacto y se emite el correo con la información respectiva dentro de los 15 primeros minutos desde que se presentó.

Alto	En este nivel el incidente causa daños a activos de información por lo que dentro de los 5 primeros minutos se llama al punto de contacto, se escribe al grupo de WhatsApp donde se encuentra todo el grupo de los agentes incluyendo la máxima gerencia y finalmente en 10 minutos adicionales se emite el correo con la información del evento previo análisis.
------	---

Tabla 10 Tiempos de SLA referente a la Prioridad de incidentes

Fuente: Documento Procedimiento de notificación y escalamiento

2.5 Costos de la solución

Bajo el siguiente cronograma se realizó la implementación de los cambios en la organización donde se describen algunas actividades y recursos requeridos para llevar a cabo la integración de la mesa de servicios Freshservice en la organización privada [6].

FASES	TIEMPO/MES	COSTO	OBJETIVO
FASE I - Identificación del cambio analista de proceso	1	\$1,200.00	Identificar los grupos y personas que requieren involucrarse en el cambio, evaluar alternativa de solución
FASE II - Planificación del cambio analista de proceso Consultor de ITIL	2	\$2,400.00 \$3,000.00	Planificar los cambios por grupo y como interactúan. Definir las estrategias a ejecutar para la implementación efectiva donde el personal este involucrado activamente.
FASE III - Implementación de Cambio analista de proceso Capacitación Contratar nuevo personal Licencia de Freshservice	4	\$4,800.00 \$4,000.00 \$5,400 \$2,136	Capacitación ITIL, contratar servicio freshservice, contratar personal para segundo agente, difusión de resultados esperados, nuevos roles, cambios en los flujos de trabajo
FASE IV - Gestión del cambio analista de proceso	2	\$2,400.00	Monitoreo, validación de resultado esperados, ajustes en indicadores, comunicar resultados
TOTAL	9	\$25,336.00	

Tabla 11 Plan general con costos y tiempos aproximados de la implementación.

Fuente: Elaboración Propia

La implementación de cambios en la organización tuvo cuatro fases donde existió la necesidad de recursos adicionales en cada una de ellas los cuales se detallan los siguientes:

Se requirió de un analista de proceso con una remuneración mensual de \$1.200 donde su participación debió estar en todas las fases del proyecto, por un tiempo de 9 meses en los cuales trabajó en colaboración con los gerentes y personal para validar la operación actual de negocio y diseñar modelos de procesos futuros, el costo total para el proyecto es de \$10.800.

El consultor de ITIL tuvo una remuneración mensual de \$1.500, participando durante 2 meses en la fase de la planificación del cambio, realizando el plan de implantación de los procesos ITIL, coordinando y proporcionando las mejores prácticas en la continuidad de negocio en TI. con un costo total para la organización de \$3.000.

En la fase de implementación se tuvo que contratar un nuevo personal teniendo el rol de Agente de mesa de servicio, el cual canalizará las solicitudes de los usuarios por medio de la plataforma freshservice. Al momento de reportar alguna incidencia, realiza la generación de reportes y alertas sobre los tickets de servicios generados. El costo mensual de este recurso es de \$450 y anual de \$5.400.

Con respecto a la licencia de la plataforma Freshservice la cual está diseñado especialmente para implementar la Mesa de Servicio se realizó la contratación del plan Pro que cumple con las gestiones contempladas para la empresa privada con un costo de \$89 mensuales y un costo anual de \$2.136. Las capacitaciones especializadas ITIL y sobre la plataforma, fueron realizadas como parte de la implementación y tuvieron un costo de \$4.000.

CAPÍTULO 3

ANÁLISIS DE RESULTADOS DE LA SOLUCIÓN.

Conforme a la solución aplicada en la sección anterior, a continuación, se detallan los resultados obtenidos sobre la implementación y algunas de las ventajas que se consiguieron post implementación del sistema de gestión de incidentes Freshservice.

3.1 Registro de Incidencias

La gestión de incidencias, o tratamiento de los errores de la empresa, es importante puesto brindan soluciones a los diferentes sucesos que produzca interrupción o que afecte el buen servicio que se ofrece a los clientes.

Estas incidencias son detectadas a través de diversas técnicas de investigación, reportadas por las herramientas de monitorización o pueden ser canalizadas por parte del cliente para luego ser registradas dentro de la mesa de servicios que es un punto principal de contacto entre la organización, los clientes y proveedor de servicios y que además centraliza la información para una mejor gestión.

Estos incidentes son registrados por los recursos del departamento del SOC donde el mayor porcentaje los realizan los analistas de seguridad para que seguidamente puedan ser gestionados por el departamento de TI o responsables de cada organización. Con la mesa de ayuda Freshservice los incidentes son ingresados de forma paralela sin tener la necesidad de que un agente finalice para que el otro continúe con el ingreso, de manera que se optimiza el tiempo de reporte y sea enviado dentro del SLA establecido.

Algunos de los campos de la mesa de ayuda contienen un * indicando que son obligatorio llenarlos puesto que la información consignada en estos campos es de mucha importancia debido a que son usados como indicadores para la realización de las gráficas en el dashboard de paneles y para la elaboración de informes. Algunos de estos campos también son solicitados por parte del cliente para la misma función.

3.2 Automatización en tareas

La automatización de tareas repetitivas y complejas ha ayudado en la agilidad al momento de resolver los incidentes y ha permitido reducir intensamente la mano

de obra y utilizarlo en tareas de mayor valor mejorando así la satisfacción de los clientes. Una de ellas es el envío de correo automático de Notificaciones a la persona encargada, es decir que, al momento de generar un ticket, en la ficha de registro de incidencias existe un campo llamado “Nombre del cliente” donde se ubica el Grupo o nombre de la persona encargada de gestionar el requerimiento y es a ellos que se envía automáticamente el correo emitido por la mesa una vez creado el ticket como lo muestra la imagen 3.1.

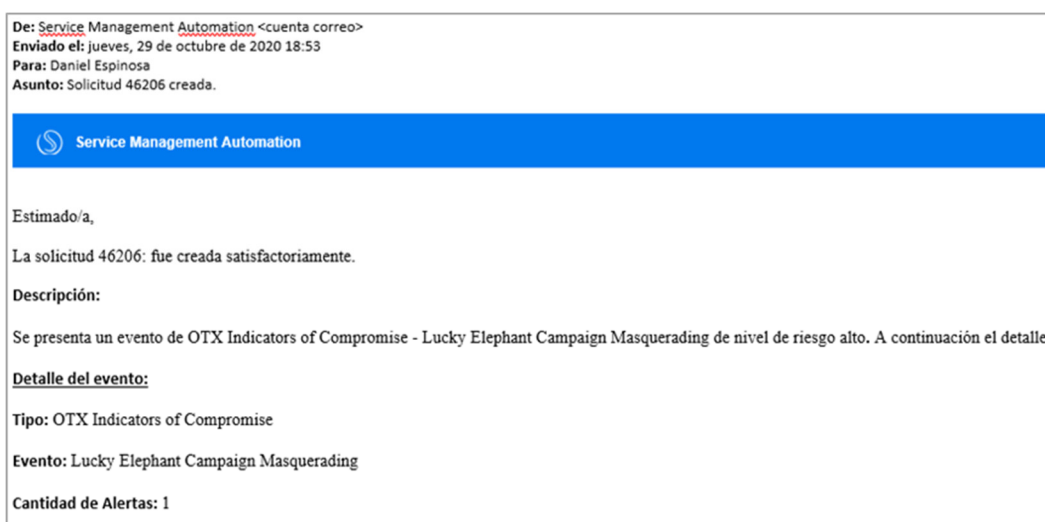


Figura 3.1 Ejemplar de correo enviado por la mesa de ayuda a personal encargado.

Fuente: Correo corporativo de la Empresa privada

También existe un campo llamado “Asignación” que hace referencia al nombre del analista de seguridad quien dará seguimiento interno al requerimiento creado y de igual forma como en el ejemplo anterior una vez que se crea el ticket se envía automáticamente una notificación vía mail indicando el requerimiento asignado.

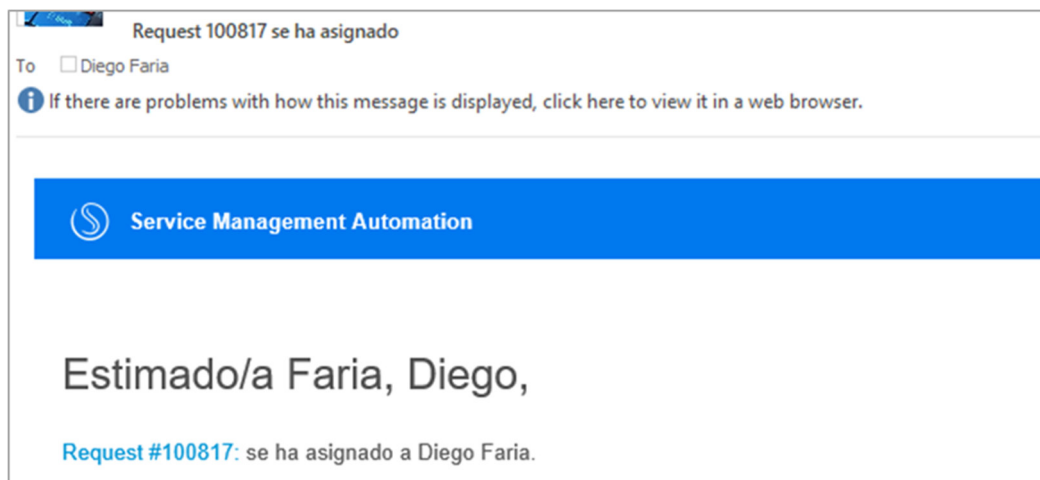


Figura 3.2 Ejemplar de correo enviado por la mesa de ayuda al analista asignado.
Fuente: Correo corporativo de la Empresa privada

Además, se recibe un correo de notificación una vez que el agente asignado para el seguimiento del requerimiento ingrese la solución por parte del cliente en la mesa y cierre el ticket como se visualiza en la imagen 3.3

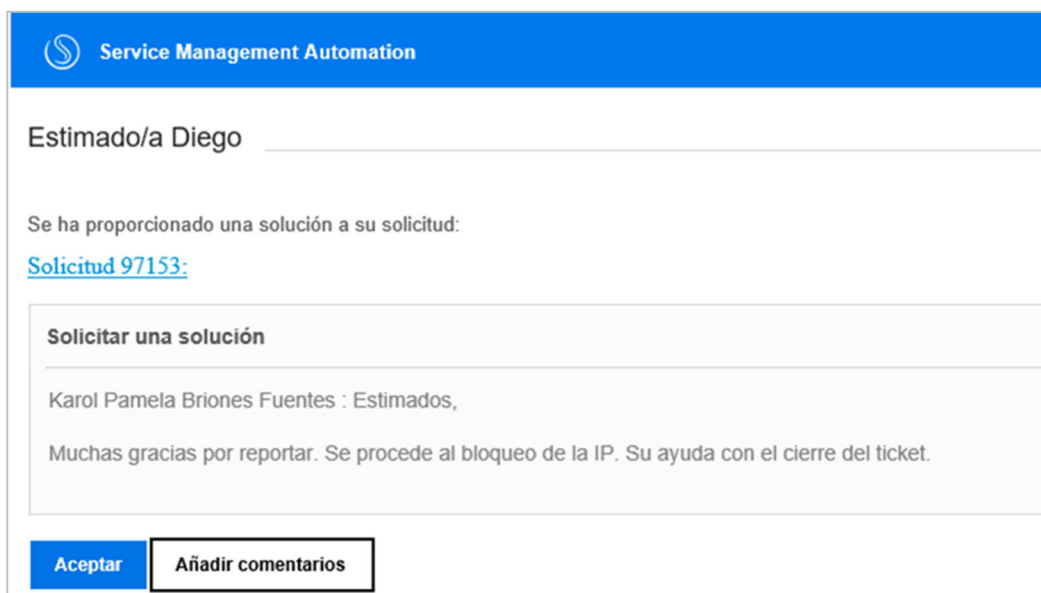


Figura 3.3 Ejemplar de correo de notificación a analista cuando se cierra un ticket.
Fuente: Correo corporativo de la Empresa privada

3.3 Auditoria en Problemas

La valoración de desempeño de la mesa de servicio ayuda a identificar posibles debilidades que puedan afectar a la resolución de un problema o incidente, esto es posible mediante el uso del dashboard de paneles que permite visualizar estadísticamente información de manera gráfica como por ejemplo el porcentaje de los tickets abiertos y cerrados de los agentes de seguridad.

Además, mediante este dashboard también es posible visualizar estadísticas de los incidentes reportados a los clientes como por ejemplo los eventos que se han reportado de las herramientas de seguridad de los clientes por categoría, la cantidad de eventos que son falsos positivos, entre otros permitiendo así que se tomen medidas correctivas.

3.3.1 Generación de informes

Uno de los servicios ofrecidos de la organización es la entrega de informes semanales, mensuales y trimestrales, también en ocasiones son pedidos de manera esporádica para la toma de decisiones.

La mesa de ayuda permite generar diferentes reportes técnicos con información actualizada y detallada de los eventos presentados dentro de un rango de tiempo que son enviados a los clientes.

Por lo tanto, la ejecución de estos documentos aumenta la visibilidad de los datos, mejora el tiempo de entrega de estos y a su vez el servicio de atención al cliente.

3.4 Toma de decisiones

Una de las características de la mesa de servicio es la de generar varios indicadores y/o PKI que junto a la generación de los informes y documentación ayudan a tomar decisiones previo identificación y análisis de los problemas encontrados en la información precisa recolectada. La documentación que se genera y que es emitida a los clientes facilita la toma de decisiones como por ejemplo el alto índice de falsos positivos por accesos no autorizados a la base de datos del cliente, esta información les ayuda a que el cliente evalúe y reestructure sus reglas y que solo se puedan visualizar las correctas alarmas. De esta forma aumenta el nivel de satisfacción de los clientes debido al servicio recibido.

3.4.1 Análisis de informes de monitoreo

Con la ayuda del dashboard el Gestor del SOC puede planificar, organizar, evaluar y realizar un seguimiento de los requerimientos abiertos y cerrados por los analistas de seguridad y la gestión que se realice a estos mismos de manera que se tenga un flujo de atención efectiva de mesa de ayuda como lo muestra la imagen 3.4



Figura 3.4 Flujo de atención efectiva de mesa de ayuda
Fuente: Elaboración propia

CONCLUSIONES Y RECOMENDACIONES

Se detallan las conclusiones y recomendación para la organización privada, las cuales están basadas en la información descrita a lo largo de este proyecto.

CONCLUSIONES

1. El sistema de mesa de ayuda informático Freshservice para la gestión de incidentes optimiza el tiempo de gestión de incidencias y permite realizar la generación de informes aumentando así el nivel de satisfacción de los clientes debido al servicio recibido.
2. El Centro de Operaciones de Seguridad (SOC) conoce el uso del sistema de mesa de ayuda de tal manera que pueden aprovechar de manera positiva las ventajas que el mismo brinda.
3. Los perfiles de los usuarios se encuentran validados y funcionando de forma óptima en bases a las funciones que realiza cada cargo operativo dentro del sistema.
4. El gestor del SOC puede obtener información del sistema Freshservice en tiempo real de manera que pueda tomar decisiones alineando los procesos de gestión con el fin de mejorar el SLA.

RECOMENDACIONES

1. Se recomienda que la organización privada aproveche en un futuro las funcionalidades de Freshservice al máximo como la base de conocimiento.
2. Se recomienda que la organización mantenga constante capacitación para los analistas del SOC sobre el sistema Freshservice y actualizaciones del mismo.

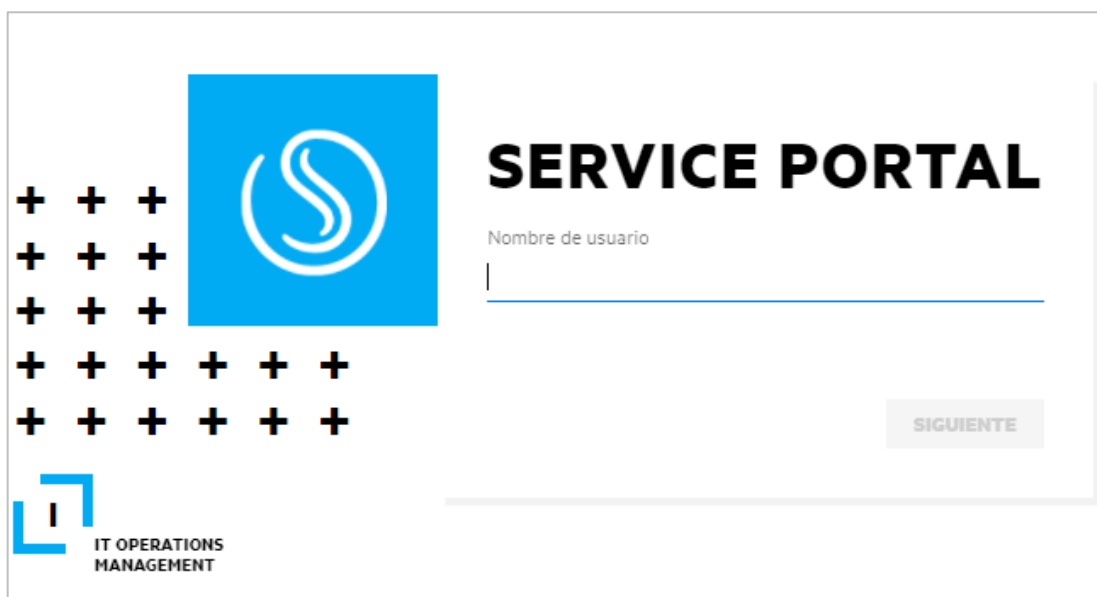
BIBLIOGRAFÍA

- [1] Supersalud. (2019, Dic 28). GSDE01 [Online]. Disponible en: <https://docs.supersalud.gov.co/PortalWeb/planeacion/AdministracionSIG/GSDE01.pdf>
- [2] ItilMatias. (2019, Dic 28). Ventajas y Desventajas ITIL [Online]. Disponible en: <http://itilmatiasc.blogspot.com/2017/05/ventajas-y-desventajas-de-til.html>
- [3] MiBlogTecnico. (2019, Dic 28). Procesos ItilV3 [Online]. Disponible en: <https://miblogtecnico.wordpress.com/2017/10/03/procesos-til-v3-2011/>
- [4] SCRIBD (2021, Sept 10). Gestión de Activos TI [Online]. Disponible en: <https://es.scribd.com/document/497558879/Freshservice-Software-Para-Gestion-de-Activos-de-TI>
- [5] Helpdeskpymes (2020, Dic 18). Herramientas de ticketing [Online]. Disponible en: <https://helpdeskpymes.com/herramientas-de-ticketing/>
- [6] Freshworks Inc. (2016, Jun 28). How Freshservice Is Helping to Transform IT Service Management [Online]. Disponible en: <https://freshservice.com/pdf/How-Freshservice-is-Transforming-IT-Service-Management.pdf>

ANEXOS

ANEXO A

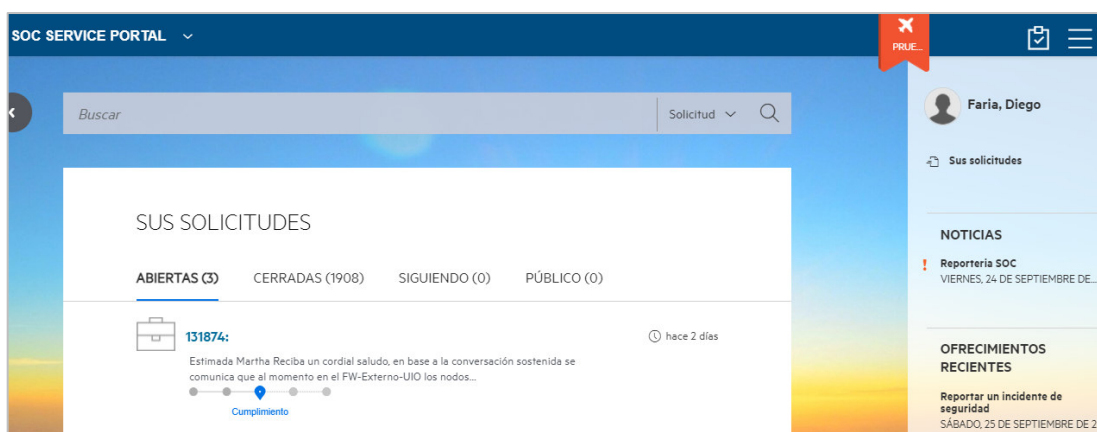
Interfaz de acceso al sistema para usuario



The screenshot shows the login page for the Service Portal. On the left, there is a logo consisting of a grid of plus signs and a blue square with a white 'S' inside. Below the logo is the text 'IT OPERATIONS MANAGEMENT'. To the right, the text 'SERVICE PORTAL' is displayed in large, bold, black letters. Below this, there is a label 'Nombre de usuario' followed by a text input field. A 'SIGUIENTE' button is located at the bottom right of the form area.

ANEXO B

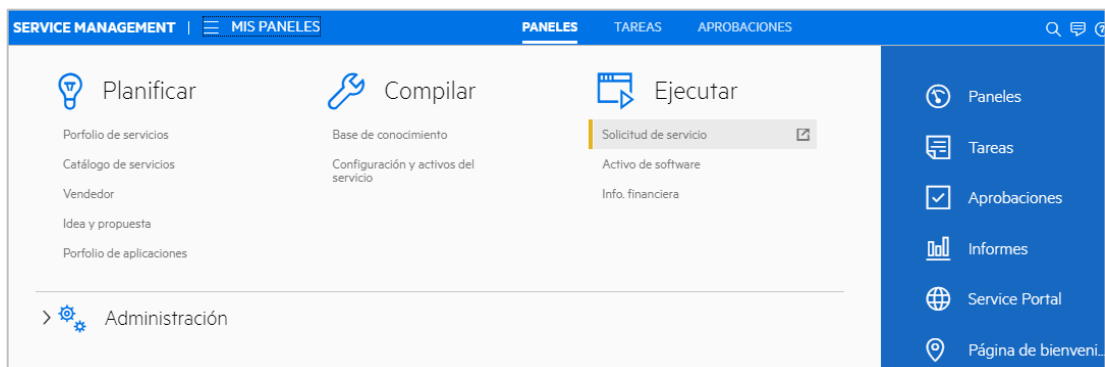
Interfaz principal del usuario en el sistema



The screenshot displays the main dashboard of the Service Portal. At the top, there is a dark blue header with the text 'SOC SERVICE PORTAL' and a search bar. The main content area is titled 'SUS SOLICITUDES' and features four tabs: 'ABIERTAS (3)', 'CERRADAS (1908)', 'SIGUIENDO (0)', and 'PÚBLICO (0)'. The 'ABIERTAS' tab is selected, showing a list of tickets. The first ticket is numbered '131874' and has a status of 'Cumplimiento'. The right sidebar contains a user profile for 'Faria, Diego', a 'Sus solicitudes' section, a 'NOTICIAS' section with a 'Reporteria SOC' announcement, and an 'OFRECIMIENTOS RECIENTES' section with a 'Reportar un incidente de seguridad' announcement.

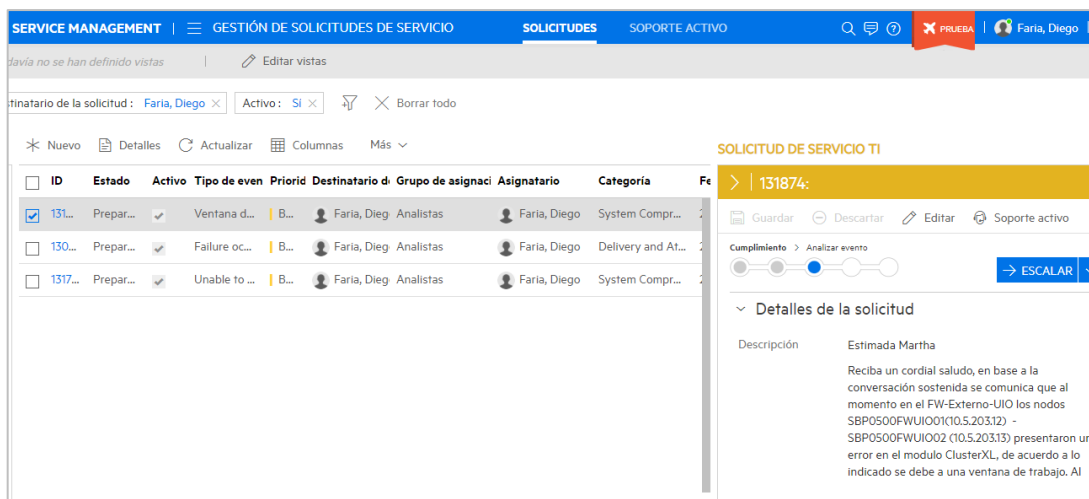
ANEXO C

Catálogo de Servicios de Freshservice



ANEXO D

Interfaz del appliance Solicitud de servicio



ANEXO E

Diagrama de flujo de actividades

