

**FACULTAD DE INGENIERÍA, ARQUITECTURA Y
URBANISMO.**

**ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA
INDUSTRIAL.**

TESIS

**DISEÑO DE UN SISTEMA DE GESTIÓN PARA MEJORAR EL
SERVICIO DE ATENCIÓN EN LA PLATAFORMA DE
SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA
SISCOTEC DEL PERÚ S.A.C.**

**PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO
INDUSTRIAL**

Autor:

**Bach. Hurtado Saucedo, Christian Jerson
(ORCID: 0001-9937-7454)**

Asesor:

**Mg. Tuesta Monteza, Victor Alexci
(ORCID: 0002-5913-990X)**

Línea de Investigación:

Infraestructura, Tecnología y Medio Ambiente

**Pimentel – Perú
2021**

TESIS

DISEÑO DE UN SISTEMA DE GESTIÓN PARA MEJORAR EL SERVICIO DE ATENCIÓN EN LA PLATAFORMA DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA SISCOTEC DEL PERÚ S.A.C.

Aprobación del Jurado

Mg. Tuesta Monteza, Victor Alexci
Asesor

Dr. Ramos Moscol, Mario Fernando
Presidente del Jurado de Tesis

Ing. Simpalo Lopez, Walter Fernando
Secretario del Jurado de Tesis

Mg. Tuesta Monteza, Victor Alexci
Vocal del Jurado de Tesis

DEDICATORIA

Dedico mi investigación a mi querida madre, que con su dedicación y esmero me brindo el concepto del esfuerzo y la constancia, a un gran amigo que lo quiero y estimo como si fuera mi padre, sé que está feliz de compartir el cumplimiento de unos de mis objetivos, a mi bella hija y esposa por su amor y comprensión, por último, a toda mi familia, amigos, compañeros de trabajo que me dieron su apoyo para cumplir con esta meta.

AGRADECIMIENTO

Agradezco a los amigos que, de manera desinteresada, dedicaron su tiempo y conocimientos para que esta investigación se convirtiera en una realidad.

DISEÑO DE UN SISTEMA DE GESTIÓN PARA MEJORAR EL SERVICIO DE ATENCIÓN EN LA PLATAFORMA DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA SISCOTEC DEL PERÚ S.A.C.

DESIGN OF A MANAGEMENT SYSTEM TO IMPROVE THE ATTENTION SERVICE IN THE INFORMATION SECURITY PLATFORM OF THE COMPANY SISCOTEC DEL PERÚ S.A.C.

Hurtado Saucedo, Christian Jerson ¹

Resumen

La presente investigación tuvo por objetivo diseñar un sistema de gestión específicamente de un Centro de Operaciones de Seguridad (SOC), en la empresa Siscotec del Perú S.A.C., que permita una mejora del servicio de atención de las incidencias y/o eventos críticos en la plataforma de seguridad de la información que brindan a sus clientes.

La investigación es de tipo aplicada, que se trabajó con una muestra compuesta de 238 incidencias, comparando los resultados obtenidos cuando las incidencias eran atendidas con el sistema actual de ticket, versus los resultados obtenidos cuando las incidencias eran atendidas a través de un sistema de demo SOC. El resultado obtenido nos demuestra que existe una mayor eficiencia de seguridad en la información cuando las incidencias son atendidas a través de un SOC. Asimismo, se realizó una encuesta de satisfacción de los servicios brindados sin SOC y con el demo del SOC, los resultados obtenidos demostraron que existe una mayor eficiencia y satisfacción del cliente cuando las incidencias son atendidas con el sistema del SOC.

De la investigación se concluyó que para Siscotec la implementación de un SOC basado en etapas es factible y viable, cuyo costo de implementación se puede recuperar muy pronto.

Palabras Clave: Sistema de gestión, Centro de Operaciones de Seguridad (SOC), Seguridad de la información, Incidencias, Satisfacción.

¹ Adscrito a la Escuela Académica de Ingeniería Industrial, Pregrado, Universidad Señor de Sipán, Pimentel, Perú, email: hsaucedoc@crece.uss.edu.pe, Código ORCID: <https://orcid.org/0000-0001-9937-7454>.

Abstract

The objective of this investigation is to propose the implementation of a management system, specifically a Security Operation Center (SOC) at Siscotec del Perú S.A.C., that allows the improvement of the incident and/or critic events attention service of the information security platform that the company offers to their customers.

The type of this investigation is applied, which works with a composed sample of 238 cases, making the comparison of the attention of incidents between the current ticket system and the demo SOC system of Siscotec. The obtained result showed that exist a greater efficiency of information security when incidents are attended through a SOC. Likewise, we ran a satisfaction poll about the services offered by Siscotec without SOC and using the demo SOC system, and the obtained results showed that exist a greater efficiency when incidents are attended with a SOC system.

As a conclusion, the implementation of a SOC system satisfies the client requirements. For Siscotec, this implementation is based in viable and possible phases. Economically, in despite of the cost of a SOC implementation (which is expensive), this can be recovered with the attraction of new customers.

Keywords: *Management system, security operations center (SOC), information security, incidents, satisfaction.*

ÍNDICE

Dedicatoria	iii
Agradecimiento	iv
Resumen	v
Abstract	vi
I INTRODUCCIÓN.	14
1.1. Realidad problemática.	02
1.2. Trabajos previos.	37
1.3. Teorías relacionadas al tema.	42
1.4. Formulación del problema.	59
1.5. Justificación e importancia del estudio.	59
1.6. Hipótesis.	60
1.7. Objetivos.	61
1.7.1. Objetivo general.	61
1.7.2. Objetivos específicos.	61
II MATERIAL Y MÉTODO.	62
2.1. Tipo y diseño de investigación.	62
2.2. Población y muestra.	62
2.3. Variables, operacionalización.	64
2.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad.	65
2.5. Procedimiento de análisis de datos.	66
2.6. Aspectos éticos.	66
2.7. Criterios de rigor científico.	67
III RESULTADOS.	69
3.1. Resultados en tablas y figuras.	69
3.2. Discusión de los resultados.	75
3.3. Aporte practico.	78
CONCLUSIONES Y RECOMENDACIONES.	87
REFERENCIAS.	89
ANEXOS.	91

ÍNDICE DE TABLAS

Tabla 1. Preocupaciones de las grandes empresas en materia de seguridad por eventos críticos.	15
Tabla 2. Reporte 2018 de SLA de solución por grupo.	23
Tabla 3. Reporte de tickets por nivel de prioridad.	24
Tabla 4. Reporte de número de tickets por top causas.	25
Tabla 5. Reporte 2019 de SLA de solución por grupo.	26
Tabla 6. Casos de equipos sin agentes antivirus no reportados en tiempo real.	29
Tabla 7. Casos de equipos sin políticas de DLP no reportados en tiempo real.	30
Tabla 8. Casos de equipos sin políticas de firewall no reportados en tiempo real.	32
Tabla 9. Casos Virus Malware no reportados en tiempo real.	32
Tabla 10. Casos Spyware Grayware no reportados en tiempo real.	33
Tabla 11. Ranking de empresas competidores de Siscotec del Perú S.A.C.	35
Tabla 12. Empresas competidores de Siscotec del Perú S.A.C: con y sin Centro de operaciones de seguridad.	36
Tabla 13. Evaluación cualitativa de las alternativas presentadas.	41
Tabla 14. Evaluación cuantitativa de las alternativas presentadas.	42
Tabla N° 15: Promedio de incidencias no reportadas mes a mes 2018.	63
Tabla N° 16: Composición de la muestra.	64
Tabla N° 17: Operacionalización de las variables.	65
Tabla N° 18: Casos atendidos por SLA de solución por el sistema de tickets.	70
Tabla N° 19: Casos atendidos por tipo de incidencia por el sistema de Demo SOC.	71
Tabla N° 20: Casos atendidos por SLA de solución por el sistema de Demo SOC.	72
Tabla N° 21: Se solucionó su incidencia y/o requerimiento en la primera atención, por el sistema de tickets.	74
Tabla N° 22: Se solucionó su incidencia y/o requerimiento en la primera atención, por el sistema de SOC.	74

Tabla N° 23: Comparativo de los coeficientes de confiabilidad de las encuestas.	77
Tabla N° 24: Casos presentados en clientes de Sistotec durante el periodo de estudio por el sistema de tickets.	140
Tabla N° 25: Casos atendidos por tipo de incidencia, por el sistema de tickets.	141
Tabla N° 26: Casos atendidos por nivel de prioridad o criticidad por el sistema de tickets.	142
Tabla N° 27: Casos atendidos por SLA de solución por el sistema de tickets.	143
Tabla N° 28: Casos presentados en clientes de Siscotec durante el periodo de estudio por el sistema de Demo SOC.	145
Tabla N° 29: Casos atendidos por tipo de incidencia por el sistema de Demo SOC.	146
Tabla N° 30: Casos atendidos por nivel de prioridad o criticidad por el sistema de Demo SOC.	147
Tabla N° 31: Casos atendidos por SLA de solución por el sistema de Demo SOC.	148
Tabla N° 32: Composición de la encuesta según la muestra.	150
Tabla N° 33: Tiempo utilizado para la solución del incidente y/o requerimiento por el sistema de tickets.	151
Tabla N° 34: Tiempo utilizado para la solución del incidente y/o requerimiento por el sistema de SOC.	151
Tabla N° 35: Calidad de la atención recibida del personal de Siscotec por el sistema de tickets.	152
Tabla N° 36: Calidad de la atención recibida del personal de Siscotec por el sistema de SOC.	153
Tabla N° 37: Se solucionó su incidencia y/o requerimiento en la primera atención, por el sistema de tickets.	154
Tabla N° 38: Se solucionó su incidencia y/o requerimiento en la primera atención, por el sistema de SOC.	154
Tabla N° 39: La incidencia fue reportada por usted, a través del sistema de ticket.	155

Tabla N° 40: La incidencia fue reportada por usted, a través del sistema de SOC.

156

ÍNDICE DE FIGURAS

Figura N° 1. Infecciones de malware por país.	16
Figura N° 2. Detecciones de Filecoder en países de LATAM durante 2017.	17
Figura N° 3. Porcentajes de empresas con incidencias de códigos maliciosos por tamaños de empresa.	17
Figura N° 4. Porcentaje de empresas que dijeron no tener incidentes de seguridad durante los últimos 12 meses por tamaño de empresa.	18
Figura N° 5. Incidencias de seguridad relacionados con ataques de ingeniería social.	18
Figura N° 6. Controles basados en gestión de seguridad.	19
Figura N° 7. Área encargada de la gestión de seguridad.	19
Figura N° 8. Evolución en la cantidad de empresas que cuentan con un área dedicada a la gestión de seguridad.	20
Figura N° 9. Porcentaje de empresas que consideran que el presupuesto destinado a seguridad no es suficiente.	20
Figura N° 10. Porcentaje de empresas que redujeron su presupuesto de seguridad.	21
Figura N° 11. Reporte de tickets solucionados por grupo durante el 2018.	23
Figura N° 12. Reporte de tickets solucionados por nivel de prioridad durante el año 2018.	25
Figura N° 13. Reporte de tickets top 10 causas más registrados durante el año 2018.	26
Figura N° 14. Reporte de tickets solucionados por grupo durante el 2019.	27
Figura N° 15. Equipos vulnerables por infección de virus y/o ataques cibernéticos dirigidos.	29
Figura N° 16. Equipos vulnerables posible fuga de información (N° de tarjetas de créditos).	30
Figura N° 17. Equipos vulnerables a ataques de ransomware wannacry.	32
Figura N° 18. Equipos infectados que pueden contagiar a los demás equipos conectados a través de la red.	33
Figura N° 19. Equipos infectados que pueden contagiar a los demás equipos conectados a través de la red.	33

Figura N° 20. Ranking de empresas competidores de Siscotec del Perú S.A.C.	36
Figura N° 21. Empresas competidores de Siscotec del Perú S.A.C con y sin SOC.	37
Figura N° 22. Etapas de atención de un SOC.	44
Figura N° 23. Diagrama de infraestructura de red.	47
Figura N° 24. Estación de Monitoreo.	48
Figura N° 25. Diseño Cuasi - experimental con post prueba y grupos intactos.	62
Figura N° 26. Porcentaje de casos atendidos por tipo de incidencia por el sistema de tickets.	69
Figura N° 27. Casos atendidos por SLA de solución por el sistema de tickets.	70
Figura N° 28. Casos atendidos por tipo de incidencia por el sistema de Demo SOC.	71
Figura N° 29. Casos atendidos por SLA de solución por el sistema de Demo SOC.	72
Figura N° 30. Tiempo utilizado para la solución del incidente y/o requerimiento por el sistema de tickets.	73
Figura N° 31. Tiempo utilizado para la solución del incidente y/o requerimiento por el sistema de SOC.	73
Figura N° 32. Solución de la incidencia y/o requerimiento por el sistema de tickets.	74
Figura N° 33. Solución de la incidencia y/o requerimiento por el sistema de SOC.	74
Figura N° 34. Casos atendidos por empresa (cliente) por el sistema de tickets.	140
Figura N° 35. Casos atendidos por tipo de incidencia por el sistema de tickets.	141
Figura N° 36. Porcentaje de casos atendidos por tipo de incidencia por el sistema de tickets.	142
Figura N° 37. Casos atendidos por nivel de prioridad o criticidad por el sistema de tickets.	143

Figura N° 38. Casos atendidos por SLA de solución por el sistema de tickets.	144
Figura N° 39. Casos atendidos por empresa (cliente) por el sistema de Demo SOC.	145
Figura N° 40. Casos atendidos por tipo de incidencia por el sistema de Demo SOC.	146
Figura N° 41. Casos atendidos por nivel de prioridad por el sistema de Demo SOC.	148
Figura N° 42. Casos atendidos por SLA de solución por el sistema de Demo SOC.	149
Figura N° 43. Tiempo utilizado para la solución del incidente y/o requerimiento por el sistema de tickets.	151
Figura N° 44. Tiempo utilizado para la solución del incidente y/o requerimiento por el sistema de SOC.	152
Figura N° 45. Calidad de la atención recibida del personal de Siscotec por el sistema de tickets.	153
Figura N° 46. Calidad de la atención recibida del personal de Siscotec por el sistema de SOC.	153
Figura N° 47. Solución de la incidencia y/o requerimiento por el sistema de tickets.	154
Figura N° 48. Solución de la incidencia y/o requerimiento por el sistema de SOC.	155
Figura N° 49. La incidencia fue reportada por usted, a través del sistema de ticket.	156
Figura N° 50. La incidencia fue reportada por usted, a través del sistema de SOC.	156

CAPITULO I

I Introducción

1.1. Realidad Problemática

La información de una empresa, hoy en día es el activo más preciado de la empresa, por ello es necesario implementar políticas de seguridad con el fin de salvaguardar dicha información antes ataques cibernéticos de cualquier tipo, que pongan en riesgo su conservación.

Asimismo, existe un mayor uso, de parte de las empresas como de las personas, de los servicios a través de aparatos móviles y de la nube, así como el uso de las redes internas y externas, de lo que se aprovechan los piratas informáticos para atacar y robar información o causar daños a los sistemas de la empresa.

En tal sentido los sistemas de información corren mayores riesgos de seguridad, esta inseguridad informática provenientes de diversas fuentes, ya sea a través de correos electrónicos, software malicioso, o por cualquier otro medio a través de Internet, etc., que pueden tener graves consecuencias tanto legales como económicas y pueden ocasionar espionaje, sabotaje, robo de información, fraudes basados en informática, así como daños a los equipos y a la data de la empresa. En tal sentido se debe tomar medidas que aseguren su integridad, disponibilidad y confidencialidad.

A fin de evitar o en todo caso disminuir dichos riesgos de seguridad, es conveniente contar con un sistema de seguridad que garantice una mejor gestión de la información, ellos van a permitir a las empresas contar con su información en una forma segura y libre de amenazas internas como externas, lo cual va permitirle aumentar su productividad y rendimiento, optimizando el uso de la tecnología, personal y procesos que emplea, de esta forma va a aumentar su eficiencia y valor.

Debemos tener presente que el empleo de tecnología avanzada permite reducir incidentes de bajo nivel de complejidad, permitiendo al analista concentrarse en resolver los eventos críticos de mayor complejidad que afecten a áreas cruciales de la empresa, por ello es importante contar con un Centro de Operaciones de Seguridad que proporcione el servicio de detección y reacción a incidentes y/o eventos críticos, lo cual va a facilitar la toma de decisiones adecuadas para continuar con la operatividad de la empresa.

A continuación, presentamos algunos de los aspectos más importantes del estudio realizado por ESET Security Report Latinoamérica (2018), relativo a la seguridad de la información en las empresas de Latinoamérica, cabe señalar que en dicho estudio no se consideró las empresas de Brasil ni de Bolivia:

Según la siguiente tabla, las principales preocupaciones de las grandes empresas en materia de seguridad son:

Tabla 1. Preocupaciones de las grandes empresas en materia de seguridad por eventos críticos

:EVENTO CRITICO	2017	2018
Vulnerabilidad	59%	55%
Ransomware	54%	57%
Malware	52%	53%
Robo de información	52%	51%

Fuente: ESET Security Report 2018.

Elaboración propia.

Se nota un crecimiento de las amenazas del ransomware, que ha venido creciendo año a año, por este motivo es imperativo tomar algunas acciones a efectos de proteger la información de este tipo de ataques.

En lo referente a las vulnerabilidades, si bien es cierto que se detecto un decrecimiento de 4 puntos porcentuales, no se debe de descuidar la protección a este tipo de ataque, por lo que se recomienda que las empresas deban preocuparse

por detectar las principales fallas de sus sistemas a efectos de prevenir ataques futuros.

En cuanto a los malware, se nota un crecimiento de 1 punto porcentual, y este tipo de ataque se está empleando desde un gran espectro de plataformas digitales lo que los hace más peligrosos para la seguridad de la empresa.

El robo de información obtuvo un decrecimiento de 1 punto porcentual, este tipo de amenazas puede originarse por ataques externos como por fraudes y es considerado como una de las principales preocupaciones de las empresas.

Otro aspecto importante del estudio realizado por ESET es que no existe una gran diferencia entre las empresas encuestadas en cada país de Latinoamérica, tal como se puede ver en la siguiente figura:

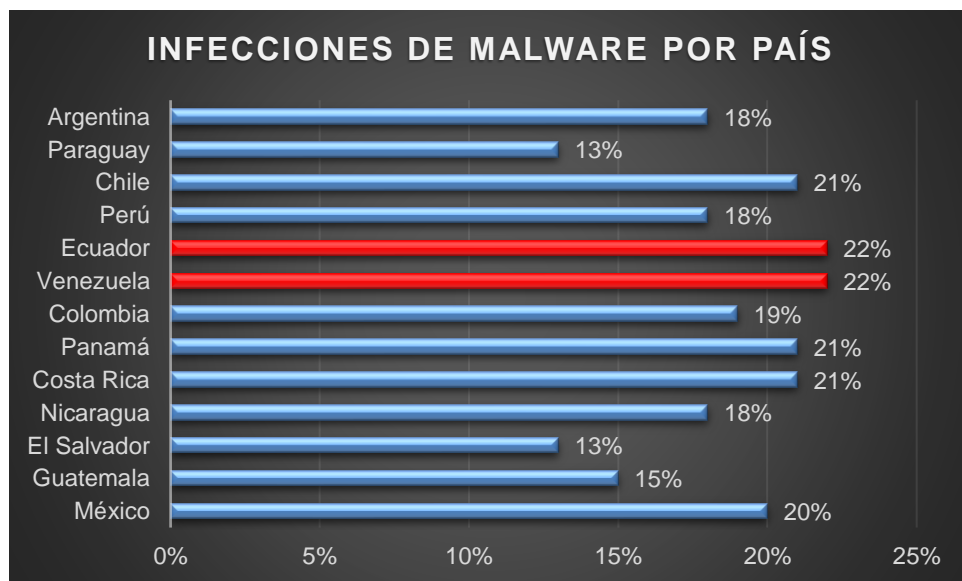


Figura N° 1. Infecciones de malware por país
Fuente: ESET Security Report 2018.

Como podemos observar en el Perú se presentó un índice de infecciones de malware del orden del 18% al igual que Argentina y Nicaragua ocupando el quinto lugar en todo Latinoamérica.

Analizando la figura N° 2 podemos decir que en el año 2017 el Perú fue el país con mayores casos de detección de códigos maliciosos, seguido de México.

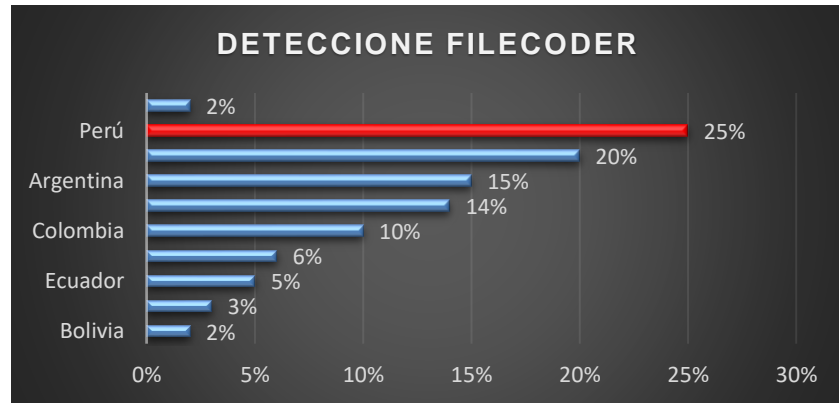


Figura N° 2. Detecciones de Filecoder en países de LATAM durante 2017
Fuente: ESET Security Report 2018.

En la figura N° 3 podemos observar que no existe mayor diferencia entre el porcentaje de empresas atacadas con códigos maliciosos según sea su tamaño.

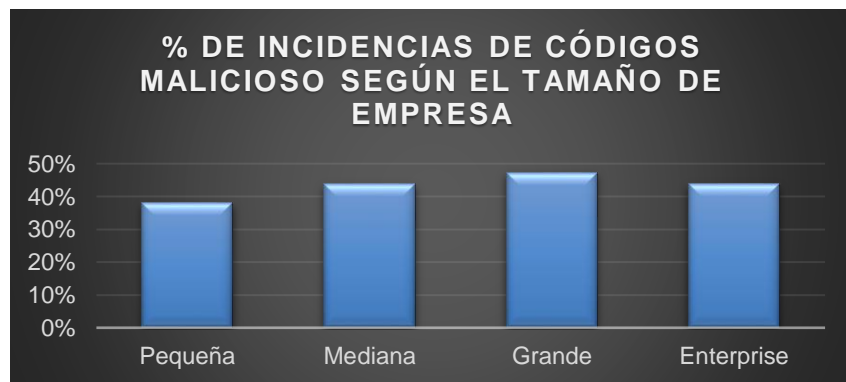


Figura N° 3. Porcentajes de empresas con incidencias de códigos maliciosos por tamaños de empresa
Fuente: ESET Security Report 2018.

En lo referente a no tener incidentes de seguridad durante los últimos 12 meses por tamaño de empresa, el informe de ESET, tal como podemos observar en la figura N° 4, nos indica que tal vez las grandes empresas cuentan con los servicios de un Centro de Operaciones de Seguridad que les permite detectar a tiempo este tipo de ataques y tomar las decisiones correctas a fin de evitarlos y/o corregirlos.

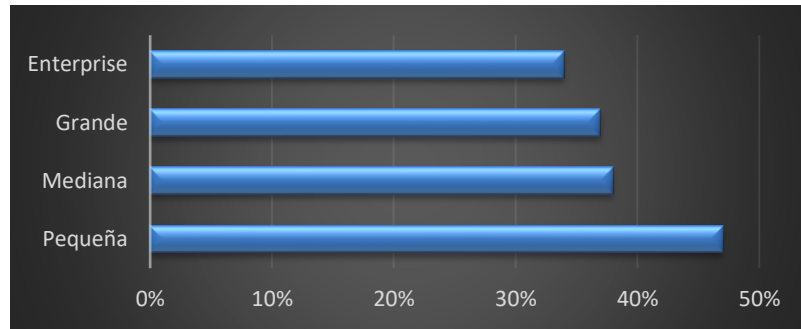


Figura N° 4. Porcentaje de empresas que dijeron no tener incidentes de seguridad durante los últimos 12 meses por tamaño de empresa
Fuente: ESET Security Report 2018.

Con respecto a las incidencias de seguridad relacionados con ataques de ingeniería social, el informe de ESET nos indica que este se ha mantenido casi estable desde 2016 y 2017 con un 15 a 16 %, tal como se puede observar en la siguiente figura:

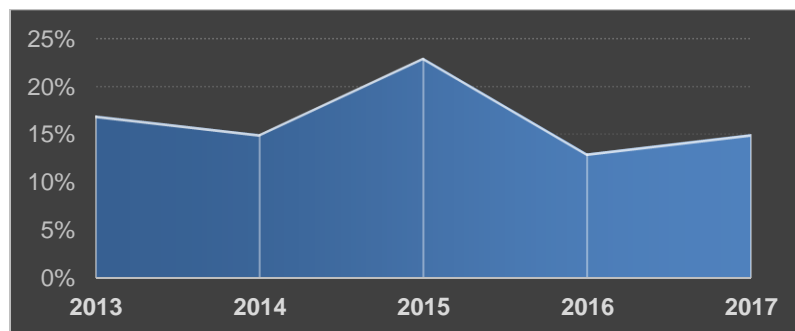


Figura N° 5. Incidencias de seguridad relacionados con ataques de ingeniería social
Fuente: ESET Security Report 2018.

Generalmente son las grandes empresas las que cuentan con diferentes controles de seguridad de in formación, tal vez sea como consecuencia de la disponibilidad de recursos y dinero con que cuentan.

En la siguiente figura se muestra los diferentes controles de seguridad basados en gestión que adoptan las empresas:

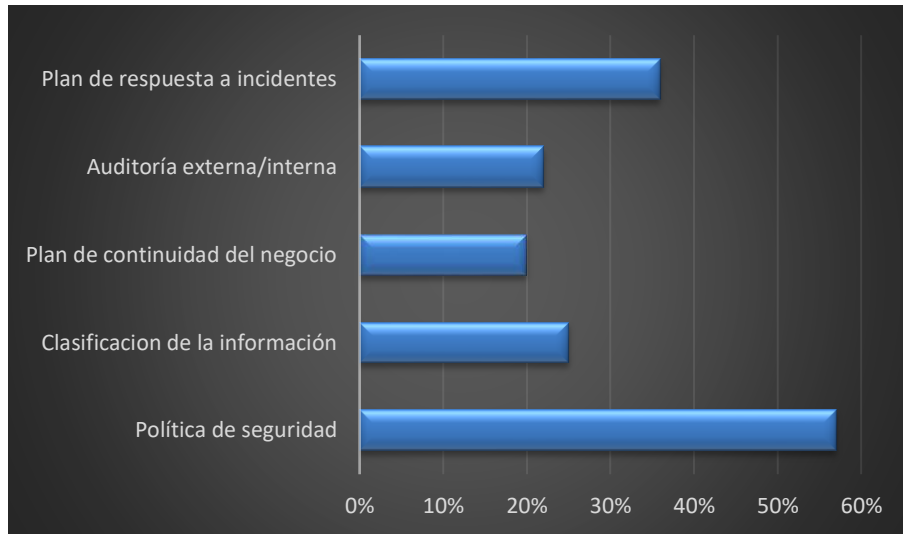


Figura N° 6. Controles basados en gestión de seguridad
Fuente: ESET Security Report 2018.

Por otro lado, es preocupante que el 11% de las empresas encuestadas no cuenten con un área de seguridad de información, tal como se observa en la figura siguiente

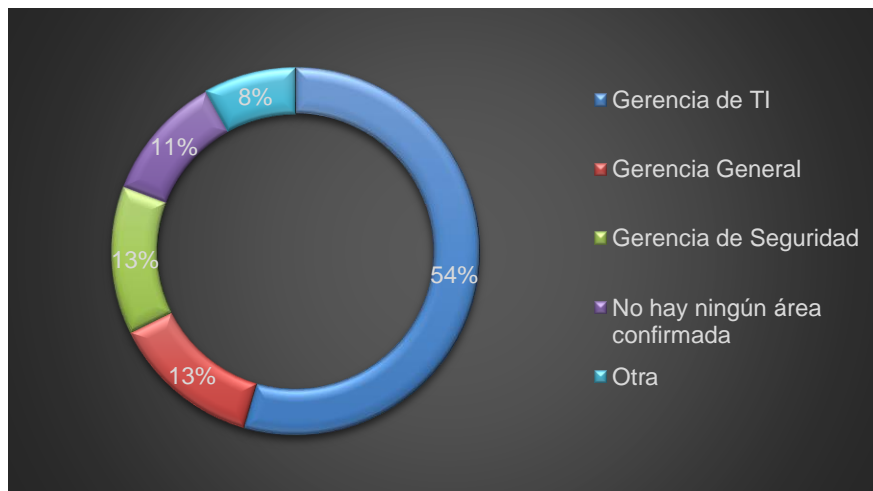


Figura N° 7. Área encargada de la gestión de seguridad
Fuente: ESET Security Report 2018.

En la siguiente figura podemos visualizar el incremento de organizaciones que tienen un área encargada de la seguridad de información:

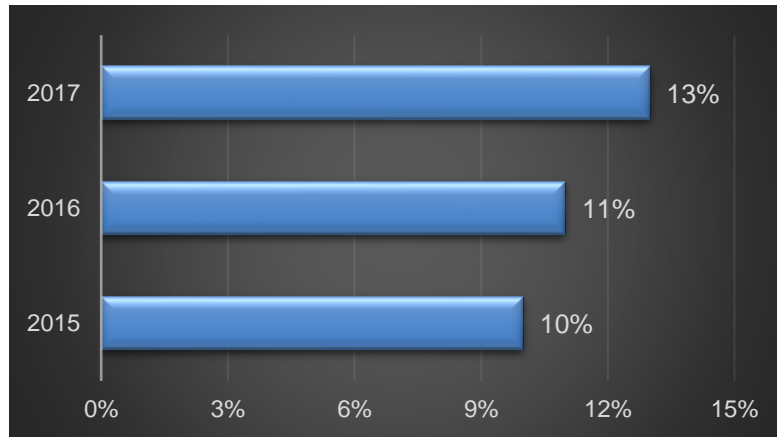


Figura N° 8. Evolución en la cantidad de empresas que cuentan con un área dedicada a la gestión de seguridad
Fuente: ESET Security Report 2018.

Este hecho es preocupante, en razón del bajo crecimiento de empresas que tienen un área de seguridad de información y si a esto le agregamos que el número de empresas que considera que su presupuesto de seguridad no es suficiente (ver figura siguiente), pero que no invierten más recursos para tal fin, el tema de inseguridad de información se agrava.

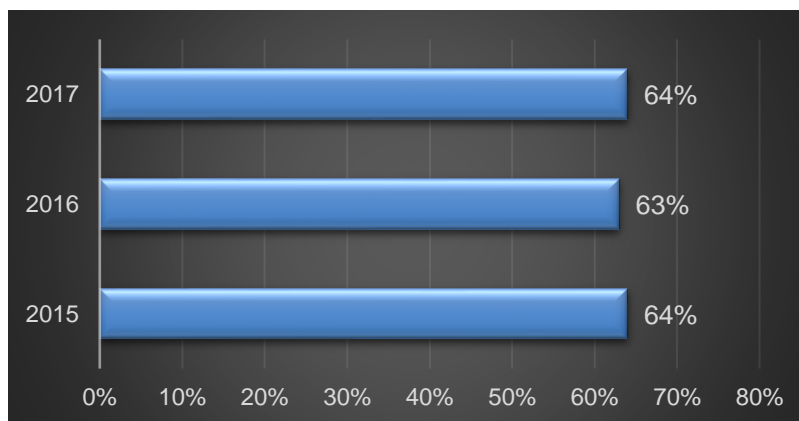


Figura N° 9. Porcentaje de empresas que consideran que el presupuesto destinado a seguridad no es suficiente
Fuente: ESET Security Report 2018.

Sin embargo, es alentador que el número de empresas que han disminuido su presupuesto de seguridad se haya reducido, como podemos ver en la figura siguiente:

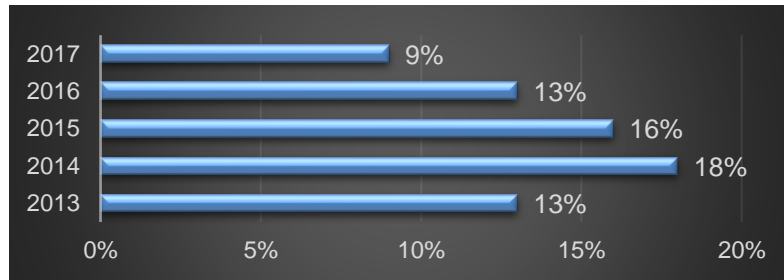


Figura N° 10. Porcentaje de empresas que redujeron su presupuesto de seguridad
Fuente: ESET Security Report 2018.

Finalmente, según lo analizado en dicho informe podemos decir que la seguridad de información es un problema vital que afrontan las empresas.

La empresa Siscotec del Perú S.A.C., se dedica a brindar servicio de implementación y soporte a soluciones de seguridad de información y redes de a través de un sistema web de emisión de Tickets publicado en modalidad 24x7x365. Adicionalmente para entregar mayor valor se pueden monitorear las consolas de las soluciones implementadas en nuestros clientes a través de conexiones remotas. Por ejemplo, en la consola de administración:

- a. De una solución de antivirus se integran otros módulos como: seguridad para protección Smartphone y tablets, control de aplicaciones a instalar, encriptación de discos duros, Data Loss Prevention (DLP) y Firewall e IPS de host.
- b. Antispam. Actualmente Siscotec del Perú S.A.C., tiene implementado un sistema de tickes (ver Anexo N° 1) que en ciertas ocasiones presentan dificultades o deficiencias en la administración de resolución de casos en tiempo real a los problemas presentados en los equipos de sus clientes, mostrando molestias en los usuarios de sus clientes. Estas incidencias se reportan a diario vía correo corporativo (ver Anexo N° 2) y a través de las consolas de agentes antivirus que se encuentra instaladas en cada cliente (ver Anexo N° 3), información que va directamente al área de ingeniería y soporte de Siscotec, la cual se encarga de registrar las incidencias presentadas y gestionarlas para ser resueltas en tiempo real.

El sistema de tickets permite a los usuarios reportar incidencias y/o requerimientos, de igual forma Siscotec usa el sistema para reportar casos que

requieran ser atendidos de forma inmediata por los clientes quienes a través de sus áreas de TI deberán ejecutar acciones de remediación.

Usualmente los usuarios no reportan algunas incidencias presentadas en sus equipos; este tipo de incidencias son evidenciadas al momento de la generación del reporte mensual de los registros de logs de la consola antivirus de cada cliente (ver Anexo N° 3), siendo identificadas como casos no reportados en tiempo real.

Dentro de los casos no reportados en tiempo real que son evidenciados en los reportes mensuales podemos identificar alertas por fuga de información, vulnerabilidades detectadas, conexiones sospechosas, infecciones recurrentes entre otros, que debido a las limitancias del software administrado (no ayuda a identificar la causa, convirtiéndose en una deficiencia en el servicio de la seguridad informática.

Con la implementación de un Centro de Operaciones de Seguridad (SOC) donde se tenga herramientas especializadas en la prevención, detección a través del monitoreo de los eventos y registros realizados en la consola antivirus y de otras soluciones con las que cuenta cada cliente, permitiría a Siscotec identificar y prevenir de forma proactiva las incidencias y/o eventos críticos ejecutando planes de acción y remediación de forma efectiva y eficiente, mitigando el nivel de riesgo en la infraestructura tecnológica de sus clientes y reduciendo la cantidad de los casos de incidencia no reportados.

El Centro de Operaciones de Seguridad (SOC) ayudará a Siscotec no solo brindar al cliente el servicio de administración y monitoreo de la consola antivirus, si no también sumar el servicio de monitoreo adicional de otras soluciones de seguridad implementadas por el cliente, permitiendo a Siscotec una mayor rentabilidad, incrementando de sus utilidades, generación de nuevos puestos de trabajo y para el cliente sería beneficioso contar con sistema integrado que le permita monitorear y alertar en tiempo real sus softwares de seguridad ante eventos de infección en sus equipos informáticos, correos maliciosos, fuga de información y ataques cibernéticos.

A continuación, en las siguientes tablas y su representación gráfica (figuras) se detalla los casos registrados a través del sistema de tickets por aéreas de atención, cabe señalar que una incidencia reportada por el sistema de ticket se genera al inicio con un ticket de color verde, conforme va pasando el tiempo y antes de que venza el tiempo de servicio este cambia a color amarillo y cuando el tiempo de servicio de atención venció cambia a color rojo:

Tabla 2. Reporte 2018 de SLA de solución por grupo:

Grupos	Tickets con SLA Verde	Tickets con SLA Amarillo	Tickets con SLA Rojo	Total Tickets
Peru.Base Datos y Servicios	1655	198	178	2031
Peru.Comunicaciones	4245	235	166	4646
Peru.Licenciamiento Microsoft	149	18	18	185
Peru.Plataforma POS	386	121	11	518
Peru.Plataforma Windows	6302	1169	1074	8545
Peru.Seguridad Informatica	1350	394	127	1871
Peru.Servicios EndPoint	607	61	72	740
Total general	14694	2196	1646	18536

Fuente: Siscotec del Perú SAC.
Elaboración propia.



Figura N° 11. Reporte de tickets solucionados por grupo durante el 2018
Elaboración propia.

Como podemos observar en la tabla y figura anterior, en el año 2018 se presentaron 1646 casos de un nivel de criticidad crítica y alto que se atendieron fuera del tiempo de servicio estimado (SLA). Estos casos están referidos a

incidentes o defectos muy serios, problemas menores no identificados y/o disturbio en el sistema, que está causando que el sistema causando sea vulnerable a una probable causa de incidente, que ocasione interrupciones recurrentes, una degradación en el rendimiento, o una pérdida de capacidad importante que resulte en una baja de rendimiento del Sistema tal que ocasione reclamos de usuarios o peor aún se convierta vulnerable a ataques cibernéticos.

Asimismo, se presentaron 2196 casos de un nivel de criticidad normal que fueron atendidos antes que venza el tiempo de servicio (SLA) por lo que el registro de cierre de ticket pasa a un color amarillo. Estos casos están referidos a incidentes o defectos, problemas, o disturbios menores en el sistema que no afecta el rendimiento, el servicio o la operación y mantenimiento. Igualmente se presentaron 14694 casos de un nivel de criticidad bajo que generan un ticket de color verde. Este tipo de severidad está conformado por determinadas acciones de control básico, tales como consultas, planeación de algún cambio, etc. En la siguiente tabla y figura presentamos datos estadísticos de los grupos por niveles de prioridad en la atención:

Tabla 3. Reporte de tickets por nivel de prioridad:

Grupo	Ticket Rojo		Ticket Amarillo	Ticket Verde		Total general
	0 - Alerta Roja	1 - Critical	2 - High	3 - Medium	4 - Low	
Peru.Base Datos y Servicios		178	198	1516	139	1431
Peru.Comunicaciones	2	164	235	1816	2429	4899
Peru.Licenciamiento Microsoft		18	18	79	70	189
Peru.Plataforma POS	1	10	121	328	58	518
Peru.Plataforma Windows	100	974	1169	4814	1488	8353
Peru.Seguridad Informatica	6	121	394	1170	180	1171
Peru.Servicios EndPoint	43	19	61	366	241	975
Total, general	152	1494	2196	1089	4605	18536
	1646		2196	14694		18536

Fuente: Siscotec del Perú SAC.
Elaboración propia.

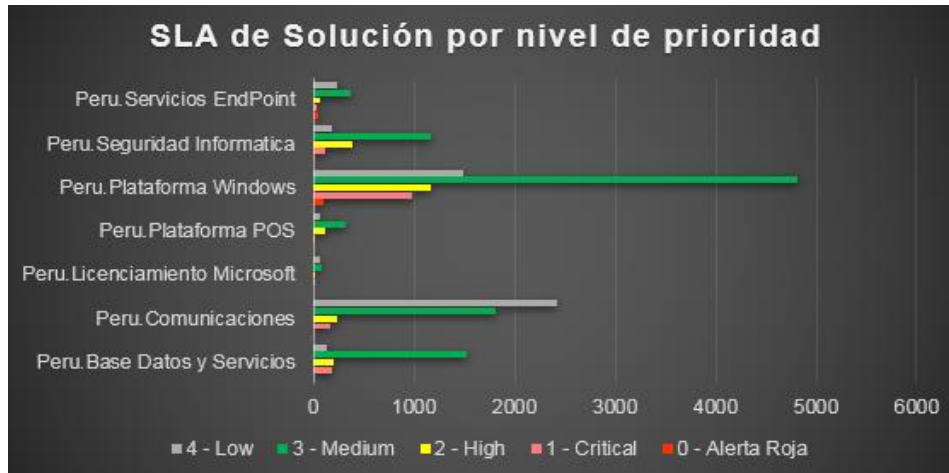


Figura N° 12. Reporte de tickets solucionados por nivel de prioridad durante el año 2018
Elaboración propia.

En cuanto a las causas de las incidencias, tenemos que la gran mayoría se refiere diversos requerimientos efectuados por los usuarios, según podemos ver en la tabla y figura siguiente:

Tabla 4. Reporte de número de tickets por top causas:

Causas	Cantidad
01.Desconocimiento del Usuario	42
02.Error de Conectividad	227
03.Error de Configuración	123
04.Error de Datos	5
05.Error de Hardware	11
06.Error de Software	22
07.No determinado	3744
08.Problema de Seguridad	45
09.Requerimiento	13971
10.Otros	346
Total:	18536

Fuente: Siscotec del Perú SAC.
Elaboración propia.

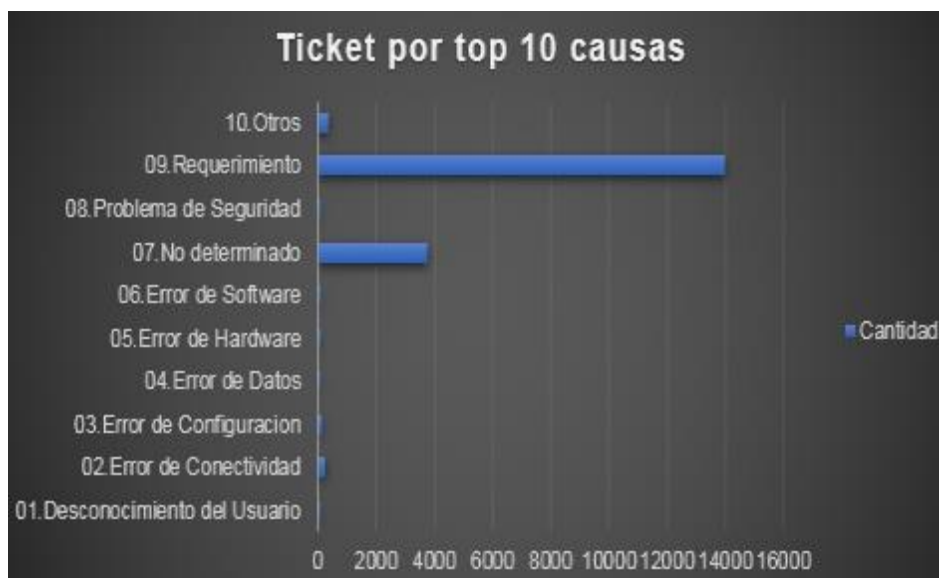


Figura N° 13. Reporte de tickets top 10 causas más registrados durante el año 2018
Elaboración propia.

En cuanto a los casos reportados en lo que va el año 2019, presentamos la siguiente data estadística en forma de tabla y figura:

Tabla 5. Reporte 2019 de SLA de solución por grupo:

Grupos	Tickets con SLA Verde	Tickets con SLA Amarillo	Tickets con SLA Rojo	Total Tickets
Peru.Plataforma Windows	2921	68	14	3003
Peru.Comunicaciones	1227	21	9	1257
Peru.Base Datos y Servicios	718	103	14	835
Peru.Seguridad Informatica	657	198	19	874
Peru.Servicios EndPoint	208	13	4	225
Peru.Plataforma POS	154	14		168
Peru.Licenciamiento Microsoft	18		1	19
Peru.Plataforma Kioscos	5			5
Total general	5908	417	61	6386

Fuente: Siscotec del Perú SAC.
Elaboración propia.



Figura N° 14. Reporte de tickets solucionados por grupo durante el 2019
Elaboración propia.

De acuerdo a la entrevista realizada al jefe del departamento de ingeniería y soporte Juan Manuel Araoz Baca, se detalla el proceso que se realiza a diario con respecto a las incidencias gestionadas (Ver Anexo 4): “El proceso más importante, actualmente es el control de incidencias de los sistemas corporativos que se encuentran en producción y cuya atención y solución son la prioridad diaria del personal.” Según esta información se aprecia la importancia de la información que manejan para satisfacer todas y cada una de las necesidades de los usuarios.

Para tener una idea más concreta sobre el proceso de gestión de incidencias se detalla de la siguiente manera, a su vez por medio de un diagrama de flujo (Ver anexo 5):

ACTIVIDAD	DESCRIPCIÓN	RESPONSA BLE	REGISTR O
1. Reportar Incidente	<p>Comunica al área de Seguridad de Información mediante correo o herramienta Ticket donde debe de brindar lo siguiente en base a:</p> <p>Si el incidente tiene relación con la llegada de un correo electrónico no solicitado e infectado:</p> <ul style="list-style-type: none"> • Brindar el correo no solicitado como adjunto (no reenviado). <p>Si el incidente tiene relación con código malicioso:</p> <ul style="list-style-type: none"> • indicar de forma detallada los problemas presentados, incluyendo observaciones que podrían ayudar a identificar la causa del incidente. <p>Si el incidente es un ataque dirigido:</p>	1. Usuario / Colaborador	1. TK 2. CE

	<ul style="list-style-type: none"> indicar de forma detallada los problemas presentados, incluyendo observaciones que podrían ayudar a identificar la causa del incidente. <p>Si el incidente es por difusión no autorizada de información:</p> <ul style="list-style-type: none"> Indicar: Fecha y hora del evento, o Ubicación del documento (Número de piso 4, 8, 9, 10 o 12), o Detalles del documento (si estuvo dentro de un folder, etc.) 		
2. Derivar Incidente	<p>Si el incidente tiene relación con la llegada de un correo electrónico no solicitado e infectado:</p> <ul style="list-style-type: none"> Asigna el ticket de atención a ingeniería y soporte (SISCOTEC) para su revisión y análisis. <p>Si el incidente tiene relación con código malicioso:</p> <ul style="list-style-type: none"> Asigna el ticket de atención a ingeniería y soporte (SISCOTEC) para que asignen a un ingeniero de soporte y pueda intervenir el equipo afectado. <p>Si el incidente tiene relación con información digital:</p> <ul style="list-style-type: none"> Se derivará la atención a ingeniería y soporte (SISCOTEC) para que revise en los logs si hubo alguna actividad sospechosa. 	2. Coordinador	2. CE
3. Atender Incidente	Emite una respuesta preliminar sobre las acciones a realizar y el tiempo de solución para conocimiento. Toma conocimiento del incidente, involucra a las áreas asociadas al evento y toman acciones inmediatas.	3. Ingeniero e Soporte -Siscotec	-
4. Notificar Solución	Una vez tomada acción al incidente deberá brindar un informe donde se incluya lo siguiente: <ul style="list-style-type: none"> Descripción general del incidente. Activo de información afectado. Riesgo materializado. Causa Raíz. Impacto. Acciones inmediatas. Plan de mitigación 	3. Ingeniero e Soporte -Siscotec	1. TK 2. CE

Según la entrevista realizada al Jefe del Departamento de Ingeniería y Soporte Juan Manuel Araoz Baca, se puede deducir que:

- 1º La información relacionada a las incidencias se registra en un sistema de tickets y en reportes mensuales.
- 2º No se tiene un historial oficial de cómo se desarrollaron los casos y resoluciones.
- 3º El proceso de asignar a un ingeniero de soporte lo realiza nuestro sistema web de tickets y lo administra y da seguimiento el Jefe del Departamento de Soporte que mantiene reuniones semanales con los ingenieros de soporte para no desmejorar el tiempo de resolución de los casos que se atienden.
- 4º El tiempo de respuesta para la atención de las incidencias actualmente es de 30 minutos para las incidencias de nivel crítico, 1 hora para las incidencias de nivel alta 4 horas para las incidencias de nivel normal y 8 horas para las incidencias de nivel baja. Sin embargo existen casos o incidencias de un nivel de criticidad crítico y alta que son atendidas fueran del tiempo de servicio estimado (SLA).

A continuación, presentamos una tabla con información cuantitativa sobre casos de incidencias y/o eventos críticos presentados en las diversas empresas a las cuales Siscotec les brinda el servicio y que son registrados a través de la consola antivirus, así como su respectiva representación gráfica (figura):

Tabla 6. Casos de equipos sin agentes antivirus no reportados en tiempo real:

ítem	Formulación	Banco Falabella	Viajes Falabella	Corredora de Seguros Falabella	Cía Operadora de Gas del Amazonas	Qroma	Sunat
1	Setiembre - Diciembre 2107	37	24	20	289	310	
2	Enero - Diciembre 2018	124	27	142	222	245	310
3	Enero - Julio 2019	21	17	45	228	223	32

Fuente: Siscotec del Perú SAC.
Elaboración propia.

La cantidad de equipos Sin Agentes antivirus es obtenida al realizar un comparativo de los equipos registrados en la consola antivirus versus el inventario de equipos del cliente. Este comparativo se hace cada mes y ello es informado al cliente en los reportes mensuales que se remite a los mismos con la finalidad de que este tome la acción de desplegar la instalación de agente antivirus en equipos que no se reportan en la consola antivirus.



Figura N° 15. Equipos vulnerables por infección de virus y/o ataques cibernéticos dirigidos. Elaboración propia.

En lo referente a equipos que no tienen una configuración de política DLP, es decir sin políticas de data loss prevention se genera del reporte mensual de

estado de agentes antivirus y el servicio de DLP con identificadores de números de tarjeta de crédito, ambos administrados desde una consola y que restringe la copia no autorizada de los usuarios mediante los diferentes canales como Exchange client mail, web mail, http, print, file write, por lo cual están propensos a fuga de información, presentamos la tabla y figura siguiente:

Tabla 7. Casos de equipos sin políticas de DLP no reportados en tiempo real:

ítem	Periodo	Banco Falabella	Viajes Falabella	Corredora de Seguros Falabella
1	Setiembre - Diciembre 2107	694	37	66
2	Enero - Diciembre 2018	2809	337	309
3	Enero - Julio 2019	1354	94	112

Fuente: Siscotec del Perú SAC.
Elaboración propia.



Figura N° 16. Equipos vulnerables posible fuga de información (N° de tarjetas de créditos)
Elaboración propia.

En relación a los equipos vulnerables a ataques de ransomware wannacry, es decir sin políticas de Firewall de antivirus estos de generan del reporte mensual de estado de agentes antivirus registrados en la consola antivirus de cada cliente; donde se identifica los equipos que no tienen aplicados la política de firewall de antivirus. Un equipo sin políticas de firewall de antivirus es vulnerable a:

- Escaneos internos de aplicativos no autorizados;
- Movimientos laterales de amenazas que pueden infectar la Red
- Brechas de seguridad no detectadas

Con respecto a los equipos con virus Malware y spyware grayware, podemos decir que la cantidad de equipos que se encuentran infectados es obtenida mediante la consulta de los registros de los resultados de escaneo:

1. Real time: Que es el escaneo automático en tiempo real, ante un evento sospechoso ejecutado por el usuario; como por ejemplo la conexión de un dispositivo pendrive, descarga de archivos de internet y/o correo, o mediante la instalación de un software sospechoso.
2. Shedule Scan: Responde a un escaneo programado de los equipos, este escaneo programado se tiene configurado en los clientes todos los días de la semana a horas 1:00pm con un tiempo límite de 1 hora.
3. Manual Scan: Es el escaneo ejecutado directamente por el usuario del equipo.
4. Scan Now: Es el escaneo de equipo ejecutado directamente desde la consola antivirus por el administrador de antivirus.

Todos los escaneos tienen como finalidad de detectar y eliminar amenazas sin problemas y los resultados de los mismos son asentados en la base de datos de la consola antivirus.

Ante estos resultados podemos decir que hay acciones requeridas por el agente antivirus como:

- 1) Reiniciar el equipo para completar la eliminación del archivo malicioso,
- 2) Eliminar de forma manual los archivos y directorios infectados

Dentro de los resultados también podemos encontrar detecciones de vulnerabilidad por falta de parches de seguridad de sistema operativo que puede conllevar a un ataque ransomware que es un programa malicioso, este término se fragmenta en las palabras inglesas “ransom” y “ware” que significan rescate y mercancía, sin embargo, en este caso significa secuestro de datos, este tipo de software malicioso cifra la data de los usuarios o del equipo comprometido, y cobra un rescate por obtener el código de descifrado.

Los casos de vulnerabilidad por falta de parches de seguridad de sistema operativo deben ser reportados con la seriedad al cliente para que tome la acción de

instalar los parches de seguridad del sistema operativo windows de los equipos de los usuarios y/o servidores. A continuación, presentamos las tablas y figuras siguientes:

Tabla 8. Casos de equipos sin políticas de firewall no reportados en tiempo real:

ítem	Periodo	Banco Falabella	Viajes Falabella	Corredora de Seguros Falabella
1	Octubre - Diciembre 2018	170	104	119
2	Enero - Julio 2019	614	237	243

Fuente: Siscotec del Perú SAC.
Elaboración propia.



Figura N° 17. Equipos vulnerables a ataques de ransomware wannacry.
Elaboración propia.

Tabla 9. Casos Virus Malware no reportados en tiempo real:

ítem	Periodo	Banco Falabella	Viajes Falabella	Corredora de Seguros Falabella	Cía Operadora de Gas del Amazonas	Qroma	Sunat
1	Octubre - Diciembre 2107	254	10	129	152	89	
2	Enero - Diciembre 2018	507	39	233	115	114	452
3	Enero - Julio 2019	54	0	5	82	87	76

Fuente: Siscotec del Perú SAC.
Elaboración propia.

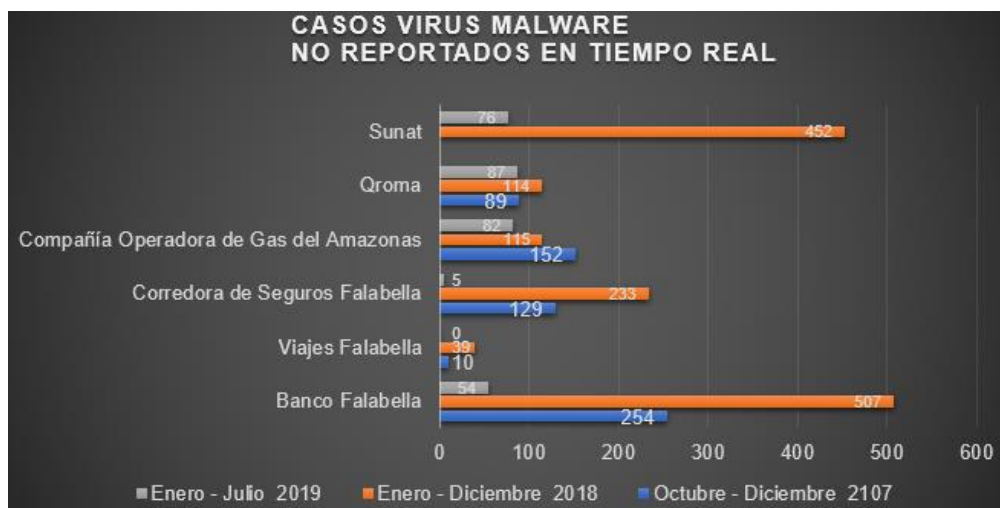


Figura N° 18. Equipos infectados que pueden contagiar a los demás equipos conectados a través de la red.
Elaboración propia.

Tabla 10. Casos Spyware Grayware no reportados en tiempo real:

ítem	Periodo	Banco Falabella	Viajes Falabella	Corredora de Seguros Falabella	Cía Operadora de Gas del Amazonas	Qroma	Sunat
1	Octubre - Diciembre 2017	49	14	7	15	35	
2	Enero - Diciembre 2018	206	114	114	111	178	382
3	Enero - Julio 2019	48	0	18	21	29	23

Fuente: Siscotec del Perú SAC.
Elaboración propia.

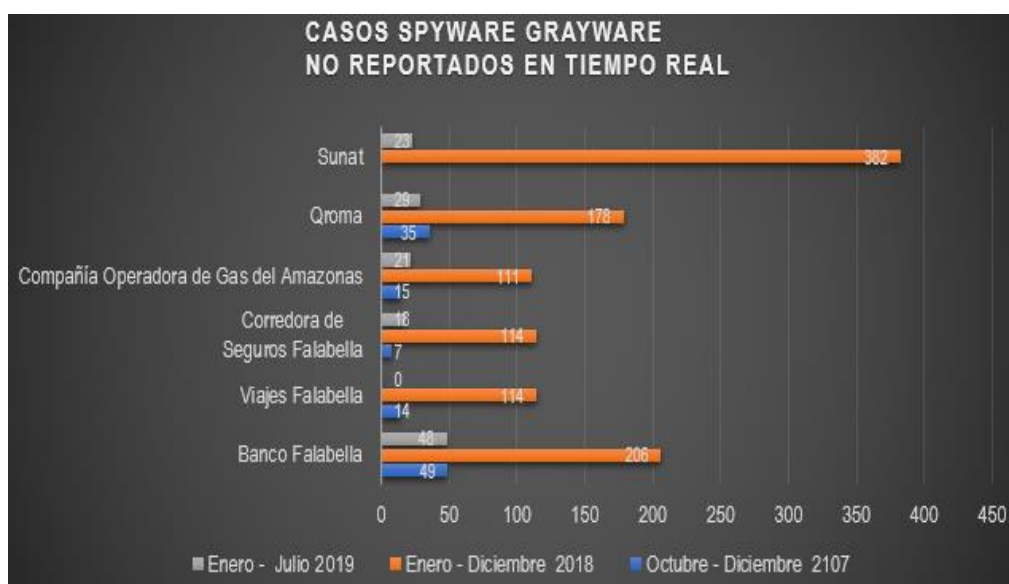


Figura N° 19. Equipos infectados que pueden contagiar a los demás equipos conectados a través de la red.
Elaboración propia

Los clientes de Siscotec tienen una cantidad considerable de casos no reportados en tiempo real los cuales están representados por cada una de las figuras descritas anteriormente; estos casos hacen referencia a:

- 1º Incidencias no son reportados por los usuarios del cliente a través del sistema de tickets
- 2º Incidencias por una instalación no correcta y validada del agente antivirus en equipos próximos a entregar a los usuarios.
- 3º Incidencias y/o eventos críticos propias a la naturaleza de manipulación de los usuarios del hardware y software no autorizado en los equipos.

Estas incidencias son evidenciadas al momento de la generación del reporte mensual que Siscotec elabora para sus clientes.

Si Siscotec contara con un SOC estos casos no reportados en tiempo real se reducirían considerablemente lo cual mejoraría el servicio; ya que la atención de las incidencias y eventos críticos y o ejecuciones de acciones de remediación en la mayoría de los casos se realizaría de forma proactiva (efectiva, eficiente y medible); mitigando los riesgos que puedan afectar a sus clientes.

El servicio que brinda Siscotec del Perú S.A.C., al ser a medida, provee la mejor seguridad que puede entregar con múltiples fabricantes, de los cuales tienen ingenieros certificados garantizando el soporte post-venta. Debido a que sus clientes cuentan con otras de soluciones de software, surge la necesidad de centralizar la gestión de estos mismos en un sistema integral que monitoree y brinde alertas en tiempo real ante posibles vulnerabilidades y/o ataques cibernéticos, y permita una correcta toma de decisiones a nivel seguridad.

Unificar las diferentes soluciones que se puedan dar, es un tema muy complejo y podría no ser conveniente para los clientes debido a que no todos los fabricantes destacan en todas las verticales de seguridad de la información o redes. Por lo que al proponer una arquitectura de seguridad y redes aplicada al usuario; es necesario involucrar a soluciones de distintos fabricantes y tener todas las habilidades de consultoría y técnicas necesarias para dicho fin.

Los directivos de la empresa Siscotec del Perú S.A.C., son conscientes de que el servicio de seguridad que ofrecen a sus clientes tiene algunas limitaciones y no es suficiente, por lo que deben migrar a un SOC, para ello se necesita efectuar un análisis situacional del área que brinda el servicio de seguridad de información que brindan a sus clientes, y en base a los resultados de este análisis se elabore un plan para desarrollar un SOC y de esta forma brindar un mejor servicio de seguridad minimizando los costos de sus clientes y les ofrezca una mayor confianza en el tratamiento de su información.

Es importante analizar las empresas competidoras de Siscotec del Perú S.A.C, que brindan los mismos servicios en el mercado nacional, así tenemos que sus principales competidores son las empresas Neosecure SAC y Secure Soft SAC, según podemos observar en la siguiente tabla:

Tabla 11. Ranking de empresas competidores de Siscotec del Perú S.A.C:

Sector	Secure Soft S.A.C	Neosecure S.A.C	Think Networks Perú S.A.C.	Grupo Radical S.A.C.	ETEK	Imperia Soluciones Tecnológicas S.A.C	Grupo Electrodata S.A.C.	Tech Solutions Integrated SAC	Orion Perú S.A.C.	Information Technology Bussiness SAC	Cimacom Data S.A.C	Hant Solutions SAC
Financiero	26	20	10	8	6	3	6	4	5	4	2	3
Minería	3	5	4	5	7	3	1	2	2	3	3	2
Energía	5	2	5	6	5	2	3	1	1	2	2	4
Industria	11	8	3	5	8	4	2	1			2	
Comercio	8	4	7	5			1					1
Telecomunicaciones	6	5	2	3			1	3	0	0	5	2
Comunicaciones	1	3	2	8	3		1		1	5	2	1
Educación	2	5	8	10	18	7	7	3	2	2	1	
Salud	1	12	9	5	5	1	2		3		2	1
Gobierno	9	12	10	7	6	2	4	1	2			1
Total clientes	72	76	60	62	58	22	28	15	16	16	19	15

Fuente: Siscotec del Perú SAC.
Elaboración propia.

La representación gráfica de la competencia es el siguiente:



Figura N° 20. Ranking de empresas competidores de Siscotec del Perú S.A.C
Elaboración propia.

Para fines de la presente investigación es interesante saber si los principales competidores de Siscotec cuentan con un Centro de operaciones de seguridad toda vez que Siscotec tiene 56 clientes y ocupa la posición sexta del Ranking de empresas que brindan este servicio, para ello presentamos la siguiente tabla:

Tabla 12. Empresas competidores de Siscotec del Perú S.A.C: con y sin Centro de operaciones de seguridad:

Ítem	Empresas del Rubro	SOC
1	Secure Soft S.A.C	Si
2	Neosecure S.A.C	Si
3	Think Networks Perú S.A.C.	Si
4	Grupo Radical S.A.C.	Si
5	ETEK	Si
6	Imperia SolucionesTecnologicas S.A.C	No
7	Grupo Electrodata S.A.C.	No
8	Tech Solutions Integrated SAC	No
9	Orion Perú S.A.C.	No
10	Information Technology Bussiness SAC	No
11	Cimacom Data S.A.C	No
12	Hant Solutions SAC	No

Empresas	Cantidad
Con Centro de operaciones de seguridad	5
Sin Centro de operaciones de seguridad	7

Fuente: Siscotec del Perú SAC.

Elaboración propia.

En la siguiente figura se observa que hay un 42% de empresas competidoras de Siscotec del PERÚ S.A.C que cuentan con infraestructura de un SOC y un 58% que aún no cuentan. Cabe resaltar que todas las empresas que ocupan una posición superior a Siscotec en el Ranking son las que cuentan con un SOC, por ello si desea ampliar su posicionamiento en el mercado debe de contar con un SOC.



Figura N° 21. Empresas competidores de Siscotec del Perú S.A.C con y sin SOC. Elaboración propia.

1.2. Trabajos Previos

De acuerdo a las investigaciones realizadas no se han encontrado muchas investigaciones similares en el ámbito internacional y local, por lo cual solo se ha considerado cuatro trabajos previos.

Antecedentes Internacionales. En primer lugar, tenemos la investigación realizada por Vásquez (2016), en esta investigación se plantea como objetivo determinar los requerimientos para implementar un SOC en la empresa Anthares IT Services, de acuerdo a sus necesidades.

El método de investigación utilizado fue el de la observación haciendo uso de cuestionarios desarrollados especialmente, así como la realización de entrevista a personal involucrado en el proceso, igualmente desarrollo instrumentos de recopilación y medición estadísticos que permitan una correcta interpretación.

En esta investigación se elaboró una propuesta factible de implementar y acorde a los recursos económicos y financieros con que cuenta la empresa, mejorando su rendimiento y calidad de los servicios ofrecidos.

Para ello se evaluaron los costos beneficios de las diferentes propuestas ofertadas por los proveedores para implementar el SOC, así como la parte técnica de cada una de ellas referidas a por ejemplo al alcance, limite, ubicación, controles, políticas y procedimientos a desarrollar para cada tipo de SOC, a efectos de elegir el más adecuado a la empresa.

La relevancia de esta investigación cualitativa, está en que el tipo de SOC recomendado está acorde a las necesidades de la empresa y se aprovecha la organización con que cuenta.

En cuanto a costos, se establece que es mucho más económico implementar un SOC, que alquilar estos servicios de otras empresas:

SICTUM	BESTEL	SOC PROPIO
\$180,000.00 Mensuales	\$250,000.00 Mensuales	\$600,000.00 Implementación total

Entre las principales conclusiones a las que se llegó en dicha investigación podemos mencionar las siguientes:

1. Es más factible y barato implementar su propio SOC, lo que facilitaría reducir los tiempos de reacción ante una eventualidad, toda vez que estas serían detectadas y atendidas en tiempo real.
2. Las alternativas de un SOC tercerizado es mucho más elevado y con lleva a la reubicación o despido del personal que quedaría excedente, mientras que con el SOC propio se gastaría por una sola vez pequeños montos en capacitaciones y material adicional al SOC.

Luego tenemos la investigación realizada por Montemayor Wong, Virgilio Mosíah (2018), en esta investigación se plantea como objetivo proponer un modelo que haga un mapeo detallado de los procesos específicos llevados a cabo por el SOC con los procesos fundamentales y mejores prácticas de ITIL.

El método de investigación utilizado fue el experimental, estableciendo que un SOC, es una parte o el todo de una plataforma que tiene el propósito de detectar alguna amenaza de seguridad y brindar las medidas correctivas en tiempo real desde una ubicación única y centralizada.

Como resultado del modelo se pretende obtener las bases para una implementación y operación exitosa del SOC basada en ITIL, entendiendo por exitosa una que cumpla con los objetivos y funciones del Security Operation Center, básicamente como indicamos en el párrafo anterior el de detectar amenazas y dar resultados.

Entre las principales conclusiones a las que se llegó en dicha investigación podemos mencionar las siguientes:

1. La gestión de incidentes y de problemas son dos procesos de ITIL que se relacionan directamente, uno a uno, con los procesos específicos del SOC. Éstos forman en sí el corazón del SOC, por lo que su integración constituye una propuesta importante.
2. La aplicación del modelo y de las mejores prácticas de ITIL no asegura por sí solo el éxito del SOC.

En la investigación cualitativa realizada por Carlos Morales, Omar Moreno y Johanna Ortigoza (2014), se plantea como objetivo establecer una propuesta de un SOC para que Fuerza Aérea Colombiana pueda centralizar la seguridad informática en toda su organización.

El método de investigación utilizado fue el lógico deductivo, analizando casos particulares acordes con las necesidades de la organización, para deducir cual es el mejor modelo de SOC para Fuerza Aérea Colombiana.

Como resultado proponen la creación de un SOC propio, a fin de controlar las amenazas contra la seguridad de la información y brindar las medidas

correctivas en tiempo real desde una ubicación única y centralizada a toda la institución.

En cuanto a costos, establecen tres propuestas para implementar el SOC:

PROPUESTA 1	PROPUESTA 2	PROPUESTA 3
\$ 1.301.000,00	\$ 915.000,00	\$ 181,000.00

Se recomendó la propuesta 1, que incluye asesoría, certificación SGSI y elementos de ciberdefensa. Propuesta 2, no incluía asesoría ni certificación para SGSI. Propuesta 3, no incluía asesoría, certificación SGSI ni elementos de ciberdefensa

Entre las principales conclusiones a las que se llegó en dicha investigación podemos mencionar que la tecnología propuesta incluye la ciberseguridad, que le permite a la FAC realizar un seguimiento inteligente y proactivo, mejorando su capacidad de respuesta ante cualquier amenaza.

Antecedentes Nacionales. En la investigación efectuada por Barrantes / Hugo (2012), se plantea como objetivo reducir y mitigar los riesgos de los activos de información de los procesos que se encuentran bajo la gerencia de tecnología de Card Perú S.A. que ponen en peligro los recursos, servicios y continuidad de los procesos tecnológicos.

El método de investigación utilizado fue modelación en el cual se han establecido tres alternativas de implementación, creando abstracciones con vistas a explicar la realidad de implementar un sistema de gestión de seguridad de la información (SGSI), que si bien es cierto no es exactamente un SOC, tiene bastante relación con la investigación que estamos plasmando en la presente tesis.

En dicha investigación se plantea que al implementar un SGSI en la empresa Card Perú S.A. se va a incrementar la seguridad de sus activos de información, disminuyendo los riesgos de ataques.

Sostienen que al implementar el SGSI se obtendrían entre otros, los beneficios siguientes:

1. Dota a la gerencia información valiosa para la gestionar la seguridad de la información, en tiempo real.
2. El análisis y evaluación del riesgo de información se realiza como un sistema.
3. Se reduce el riesgo del error humano.
4. Se aumenta el control a la información.

En la investigación presentan tres alternativas para implementar el SGSI, según detalle siguiente:

- ✓ Alternativa 1: Implementación de Metodologías de Gestión de Riesgos
- ✓ Alternativa 2: Implementación de un SGSI enfocado a la circular N° G-140
- ✓ Alternativa 3: Certificación de un SGSI enfocado a la ISO 27001

Las mismas que fueron analizadas considerando los aspectos siguientes:

Tabla 13. Evaluación cualitativa de las alternativas presentadas:

Criterio	Alternativa 1	Alternativa 2	Alternativa 3
Costo	Bajo	Alto	Muy Alto
Riesgos	Bajo	Bajo	Medio
Tiempo	Muy Bajo	Bajo	Alto
Complejidad	Bajo	Medio	Muy Alto
Competitividad	Muy Bajo	Alto	Muy Alto
Viabilidad	Muy Alto	Muy Alto	Alto
Prioridad	Alto	Muy Alto	Bajo
Regulatorio	Bajo	Muy Alto	Bajo

Fuente: Barrantes / Hugo (2012).
Elaboración Barrantes / Hugo (2012)

Tabla 14. Evaluación cuantitativa de las alternativas presentadas:

Comparación cuantitativa				
Criterio		Alternativa 1	Alternativa 2	Alternativa 3
Costo	20%	40	20	10
Riesgos	10%	40	40	30

Tiempo	18%	50	40	20
Complejidad	5%	50	20	10
Competitividad	12%	10	40	50
Viabilidad	10%	50	50	40
Prioridad	10%	40	50	20
Regulatorio	15%	20	50	20
	100%	36.7	38.5	24.1

Fuente: Barrantes / Hugo (2012).
Elaboración Barrantes / Hugo (2012)

Eligiendo la alternativa 2 por contar con un mayor valor ponderado (38.5)

Entre las principales conclusiones a las que se llegó en dicha investigación podemos mencionar las siguientes:

- 1) Los colaboradores deben de conocer e identificarse con la política de seguridad de la empresa.
- 2) La empresa y sus colaboradores deben estar preparados para enfrentar nuevas vulnerabilidades que se presenten y desarrollen a futuro.

1.3. Teorías Relacionadas al Tema

Empezaremos a analizar las diversas teorías relativas a nuestra variable independiente: Sistema de gestión (del Centro de Operaciones de Seguridad SOC), para luego analizar las teorías relativas a nuestra variable dependiente: Servicio de atención (de Incidencias y/o eventos críticos) en la plataforma de seguridad de la información.

1.3.1. Sistema de gestión.

Según el ISO 9001:2015, 24 “Un sistema de gestión es un conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas, objetivos y procesos para lograr estos objetivos” (sic).

“Los elementos del sistema de gestión establecen la estructura de la organización, los roles y las responsabilidades, la planificación, la

operación, las políticas, las practicas, las reglas, las creencias, los objetivos y los procesos para lograr esos objetivos” (sic).

En tal sentido para fines de la presente investigación se entiende como un sistema de gestión al conjunto de procesos que de acuerdo a una política común, nos va a permitir alcanzar ciertos objetivos, en este caso administrando un SOC que brinde mayor seguridad a la información durante las 24 horas del día y los 7 días de la semana.

1.3.2. Centro de operaciones de seguridad (SOC - security operation center)

Como lo menciona Nathans (2015), un centro de operaciones, es un área de trabajo informático donde se monitorean o vigilan los procesos de información de una empresa, detectando ataques o eventos críticos que puedan afectar los sistemas de la empresa y su funcionamiento normal.

Para efectos de esta investigación, consideramos un SOC como una unidad orgánica de la organización que centralizada las acciones de monitoreo, aseguramiento y defensa de los activos de información, a efectos de realizar o recomendar alguna acción correctiva en un tiempo real, las 24 horas del día y los 7 días de la semana.

Según Muñiz, Alfardan, McIntyre (2015) las amenazas y ataques a la seguridad de la información van evolucionando cada día, por lo que el SOC, tanto en infraestructura, equipos, tecnología y procedimientos, también deben de cambiar a efectos de adecuarse y estar siempre un paso delante de los posibles ataques, hoy estamos en la cuarta generación de los SOC.

Como señalamos en los párrafos anteriores, las funciones más importantes de un SOC son; prevención, detección, análisis y respuesta, en tal sentido para la instalación de de un SOC debemos tener presente lo siguiente:

- a) Procesos: Es necesario contar con toda la información sobre los diferentes procesos que se realiza en el tratamiento de la información a efectos de

establecer cuáles podrían ser las amenazas o ataques que pueda recibir, jerarquizándolas de acuerdo a ciertas prioridades, definir cómo se pueden detectar lo más pronto posible y cuál sería la solución a dichos ataques.

Lógicamente la parte donde los analistas deben de poner mayor atención es la fase de determinar cuál sería el proceso de respuesta más apropiado a cada ataque.

Por lo general se emplea la detección y solución por etapas. La primera etapa, es la inicial o básica, donde se realiza una revisión inicial y se da solución a ataques simples con una respuesta inmediata. Si esta etapa no puede encontrar una solución al ataque, se pasa el caso al segundo nivel o etapa 2, en esta fase el SOC cuenta con personal más calificado y mayores herramientas que le permiten dar una respuesta repuesta a los ataques en un lapso de tiempo prudente. El tercer nivel o etapa 3, está referida a caso complejos que requieren una investigación compleja y que se le da la primera prioridad en su solución. Un Centro de Operaciones de Seguridad (SOC) ante una alerta e incidente utiliza la metodología multicapa.

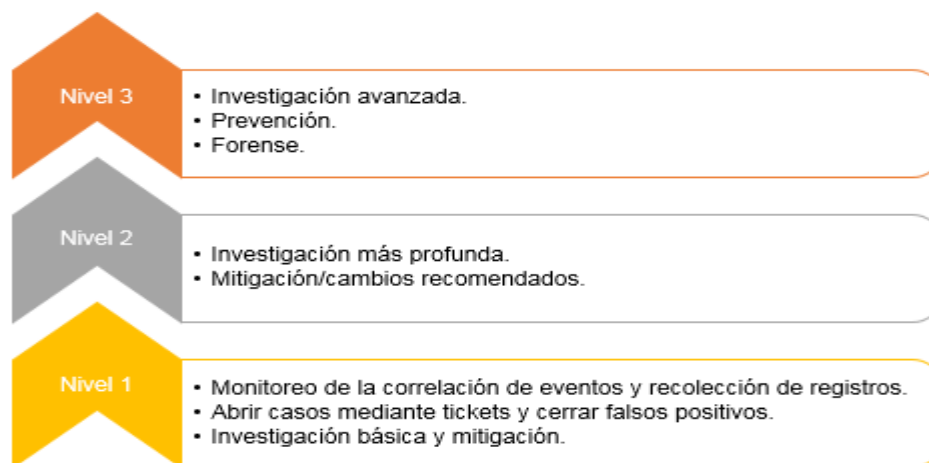


Figura N° 22. Etapas de atención de un SOC.
Elaboración propia.

- b) Personas: Un SOC debe de contar con personal especializado que deben ser capacitados en forma constante a efectos de hacer frente a la evolución de los ataques. Este personal debe ser ubicado en la estructura del SOC, en los diferentes niveles de solución a los ataques, de acuerdo a sus habilidades, destrezas, profesión y capacitación.

- c) Tecnología: Un SOC debe ser implementado con tecnología de vanguardia especializada en inteligencia de seguridad que permita una fácil aplicación por todo el personal involucrado en su uso.

Los servicios que presta el SOC deben estar acorde con los objetivos de cada entidad y este se realiza mediante el monitoreo de los diferentes dispositivos que interviene en cada proceso y en una forma integral las 24 horas en los 7 días de la semana.

Por ello es importante tener en cuenta la estrategia que se va a emplear en la detección, prevención y solución a los ataques, los procesos en el tratamiento de la información y la tecnología con la que se cuenta.

En cuanto a las personas que componen un SOC esto va depender del número de empresas a las que se brinda el servicio y/o casos que se presentan, sin embargo William Quiñonez, Gerente Oficina de Servicios Compartidos BCR & CIEX FOMILENIO II de El Salvador, experto en servicios y tecnologías de la información, en su artículo publicado en lo blog LinkedIn el 4 Dic 2017¹, recomienda lo siguiente:

- ✓ Para el Nivel 1 o Capa 1: Monitorización y análisis. – Recomienda mínimo un especialista y algunos técnicos que van a monitorizar los diferentes procesos, en forma permanente las 24 horas del día, realizando un primer análisis, control y categorización de los incidentes, dándole solución a los incidentes primarios, de lo contrario lo pasan al nivel 2.
- ✓ Para el Nivel 2 o Capa 2: Análisis profundo y respuesta. – Recomienda que este conformado por varios analistas expertos en seguridad y técnicos de seguridad, especializados en diferentes materias a efectos de que puedan realizar un análisis de la ocurrencia comparando distintas fuentes, identificando en qué forma afectan los sistemas críticos y validado los impactos posibles, recomendando las contramedidas que pueden realizarse.

¹ LinkedIn (2017, diciembre, 4). *Centros de Operaciones de Seguridad (SOC) - UNA NECESIDAD CRÍTICA INDISPENSABLE*. Recuperado de <https://www.linkedin.com/pulse/centros-de-operaciones-seguridad-soc-una-necesidad-critica>.

Este personal, también es capaz de realizar análisis forense de los hechos, realizando investigaciones correspondientes a efectos de identificar el atacante y sus motivaciones.

- ✓ Para el Nivel 3 o Capa 3: Expertos y 'hunters'.- Recomienda que esté formado por consultores técnicos, altamente especializados en seguridad a efectos de proponer soluciones a los problemas muy complejos y reducir o mitigar la presentación de ataques, realizan el análisis forense de ataques complejos realizando las auditorías técnicas correspondientes.
- ✓ Un coordinador o administrador del SOC.- Es el encargado de gestionar los recursos de personal, equipos, presupuesto, turnos y acuerdos de nivel de servicio. Es el enlace entre la gerencia y el SOC, así como con las empresas a las cuales se les brinda el servicio.

En un SOC se desempeñan técnicos y profesionales de diferentes especialidades, como por ejemplo: técnicos de seguridad, analistas de seguridad, analista de datos, expertos en ingeniería e integración, especialistas en soluciones de seguridad, expertos en ethical hacking en sistemas y aplicaciones, etc.

Dimensión del SOC.- Para que un SOC preste servicios 24x7 debe contar con una planta de 12 personas mínimo, 1 administrador, 6 analistas para el nivel 1, 2 analistas y 1 ingeniero para el nivel 2 y 2 ingenieros para el nivel 3.

En cuanto a las maquinarias y equipos que componen un SOC, podemos mencionar que se requiere:

1. Infraestructura de red: Compuesta por equipos router y firewall de perímetro, switch core para la segmentación de la red y switches de acceso (donde se encuentran operando las estaciones de trabajo del personal).

Servicio de dedicado primario y otro secundario de internet, de diferentes operadores; ya que es el medio por el cual que permite la gestión y monitoreo de los equipos del cliente.

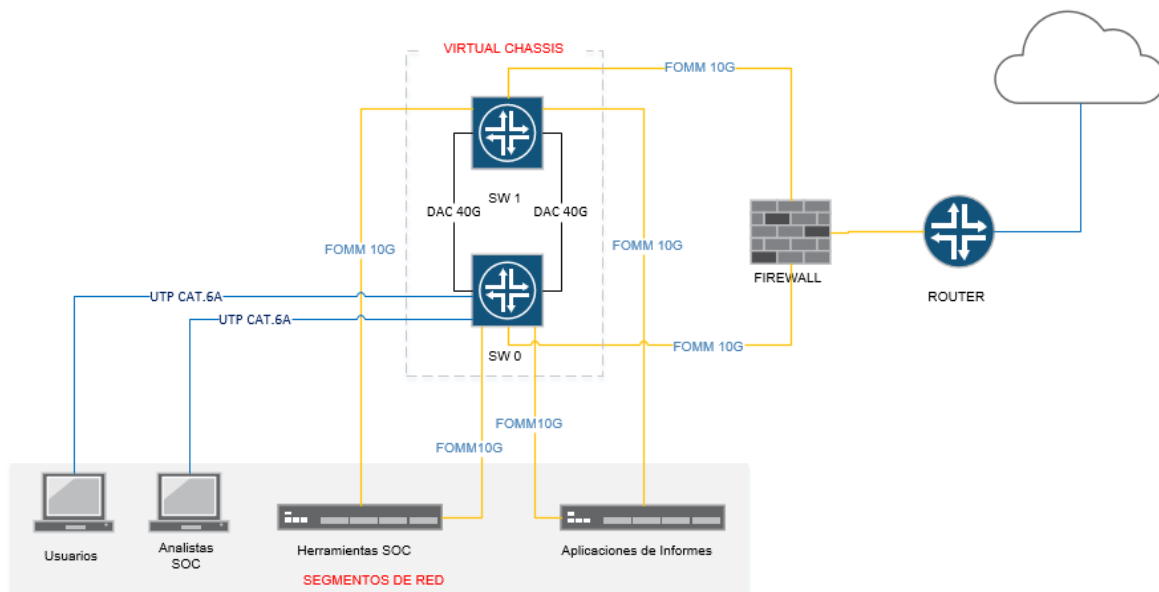


Figura N° 23. Diagrama de infraestructura de red.
Elaboración Propia.

2. Sistema Operativo: EL tipo de sistema operativo a utilizar dependerá del software a utilizar para la recolección, correlación y análisis de data.
3. Almacenamiento: Servidor y storage para el almacenamiento de la data producida por los diversos dispositivos que se estén vigilando. Garantizando que la información esté accesible para el análisis correspondiente.
4. Servidor de colaboración: La relación recíproca, el análisis de la data producida por los equipos vigilados y las resoluciones de casos a posibles ataques, va a generar información valiosa que será empleada posteriormente a fin de solucionar futuros ataques similares.
5. Sistema de Tickets: Para brindar las respuestas a las incidencias, así como administrar el ciclo de vida del mismo. De tal forma que los casos sean categorizados y medibles.
6. Monitoreo: Estaciones de trabajo mobiliario y pantallas; para la observación de acciones producidas por los equipos monitoreados.
7. Herramientas de monitoreo: Para la percibir cualquier acto de inseguridad generados en los diferentes equipos y distribuirlos al personal capacitado para su adecuada respuesta y remediación.



*Figura N° 24. Estación de Monitoreo.
Elaboración: SysLog, y servicio "SOC Prot-On"*

8. Telefonía Ip: Para la comunicación del personal del mismo Centro de Operaciones de Seguridad (SOC) y/o con los clientes.

1.3.3. Problemas de seguridad en el SOC

Los problemas de seguridad que se pueden presentar en un SOC son:

- 1) Carencia de una normativa de seguridad, ya sea políticas, normas y procedimientos de seguridad, por lo que la organización encargada de administrar el SOC debe de establecer ciertas pautas de seguridad y darlas a conocer a sus usuarios.
- 2) La falta de un control de acceso de los usuarios, muchas empresas otorgan acceso común a un grupo de usuarios con lo cual se hace difícil identificar al usuario que realmente realizó la acción que ocasiono el problema, se debe de otorgar acceso individuales.
- 3) La no existencia de un manager de información, encargado de toda la seguridad de la información y quien autorice a cada usuario el acceso a determinada parte de la información.
- 4) La no existencia de planes de continuidad actualizados, debido a que los ataques a la seguridad de la información evolucionan constantemente los planes de contingencia deben ser actualizados permanentemente, no pueden ser algo estático.

- 5) Falta de registros de las acciones seguidas, entre ellas principalmente de los accesos concedidos a que usuario, contraseñas, desde que fecha, tentativas de acceso, modificaciones realizadas, etc.
- 6) Falta de backup o copias de seguridad de la información, esta copia debe de estar en un lugar seguro y en otro servidor totalmente diferente a que donde se procesa normalmente la información.
- 7) La poca o nula capacitación a los usuarios no solo sus responsabilidades y el proceso que debe seguir, sino de las medidas de seguridad que debe tener al hacer uso de los equipos y durante el proceso a seguir.

1.3.4. Principales problemas que se presentan en la operación del SOC

Adicionalmente a la problemática que hemos mencionado en el punto anterior, en el mismo funcionamiento del SOC se pueden presentar algunos problemas derivados del mal desempeño de los trabajadores del SOC, entre ellos tenemos:

- a) La no atención de algunos tickets el mismo día en que fueron generados.
- b) El no monitoreo las 24 horas los 7 días de la semana.
- c) Los dos problemas anteriores ocasionan un no seguimiento permanente de los eventos, que por más simples que sean pueden generar un problema mayor.
- d) Igualmente esto va a ocasionar la presentación de informes y reportes incompletos.

1.3.5. Niveles de servicio

Establecer niveles de servicios acorde a los requerimientos de cada usuario o cliente y dentro de los costos requeridos es una tarea de gran importancia y este proceso es lo que se denomina gestión de niveles de servicios.

La gestión de niveles de servicios, es el área del SOC que se encarga de definir el servicio, negociar con los clientes y supervisar la calidad del servicio prestado a efecto de que el cliente se mantenga satisfechos.

Por ello es fundamental que los niveles de servicio estén claramente definidos y se actualicen constantemente teniendo en cuenta lo siguiente:

- 1) Incluir los nuevos cambios realizados a las configuraciones de la infraestructura de seguridad con que cuenta el cliente y administrados por el SOC.
- 2) Los tiempos de atención de las incidencias presentadas y atendidas por el SOC, para lo cual e debe de tener en cuenta:
 - ✓ El tiempo promedio de generación del ticket correspondiente, considerando el tiempo desde que se comunico el incidente desde cualquier medio de comunicación hasta la generación de ticket.
 - ✓ El tiempo promedio de diagnostico del incidente.
 - ✓ El tiempo promedio de restauración del sistema.
- 3) Seguimiento de actividad sospechosa que incluye toda la infraestructura de seguridad a efectos de verificar cualquier actividad irregular, para ellos se debe tener en cuenta:
 - ✓ El tiempo promedio de comunicar la existencia de una actividad irregular.
 - ✓ El tiempo promedio de entrega del informe con los resultados del análisis de la actividad irregular.
- 4) Gestión de incidentes de seguridad, se debe tener en cuenta:
 - ✓ El tiempo promedio de comunicar los ataques a la seguridad.
 - ✓ El tiempo que se demoro para tomar una acción para evitar que el ataque sea exitoso.
- 5) La entrega de los reportes o informes y el tiempo en que se entregaran, semanal, quincenal o mensual.

Adicionalmente a cada nivel de prestación del servicio, se debe incluir algún tipo de penalidades para ambos contratantes, el prestador del servicio y el cliente.

1.3.6. Calidad en el servicio.

Indudablemente la calidad en el servicio prestado por el SOC, es un factor importante para garantizar la satisfacción del cliente, para ellos se deben de seguir ciertos procedimientos previamente establecidos y serán medidos de acuerdo a unos indicadores definidos.

Para lograr la calidad total en un SOC por lo general se logra mediante la colaboración e intervención activa del personal en la constante detección, análisis y solución a los problemas generados por los diversos ataques a la seguridad.

La calidad total del servicio prestado nos va permitir mantenernos en el mercado, poder crecer, contar con una imagen positiva, ser respetados por nuestros competidores.

1.3.7. Seguridad de la Información

Según Georgem Marakas, “Conforme el uso de la información se va extendiendo con mayor amplitud, proteger dicha información de una manera estructurada y organizada se vuelve un requerimiento cada vez más latente. Las tecnologías de la información, incluyendo los sistemas de la información en Internet, tienen una función vital y creciente en los negocios. La tecnología de la información puede ayudar a todo tipo de negocios a mejorar la eficiencia y el mantenimiento de sus procesos de negocios, a la toma de decisiones de negocios y la colaboración de los grupos de trabajo, mediante el fortalecimiento de sus posiciones competitivas en un mercado rápidamente. -Biante. Esto es evidente, tanto como la tecnología de la información que se utiliza para respaldar los equipos o cualquier otra actividad del negocio. Las tecnologías y sistemas de información de desarrollo de productos, procesos de apoyo al cliente, transacciones de comercio electrónico en Internet se han convertido en un elemento necesario para el éxito de los negocios en el ambiente global dinámico de la actualidad.”²

En si misma línea Cazemier sostiene que la importancia de la seguridad de la información se ha incrementado dramáticamente a causa del movimiento de las redes internas de los negocios hacia sus clientes y socios, así como del traslado

² Marakas, Georgem Sistemas de información gerencial (séptima edición) Editorial Mc Graw Hill 2016

hacia el comercio electrónico y el uso cada vez mayor de redes públicas como la Internet. Conforme el uso de la información se va extendiendo con mayor amplitud, proteger dicha información de una manera estructurada y organizada se vuelve un requerimiento cada vez más latente (Cazemier, 2004).³

Como vemos hoy en día, la información que posee una empresa es uno de sus activos más valiosos, en tal sentido la seguridad de la información es vital para todo tipo de organización, adquiriendo mayor importancia la integridad, disponibilidad y mantener en secreto la información; la misma que debe ser almacenada en un lugar libre de cualquier ataque. Por estas razones cualquier sistema de seguridad debe garantizar estos tres aspectos: confidencialidad, integridad y disponibilidad.

El hecho de no contar con un sistema de seguridad, exponer a la empresa a posibles daños económicos, como son el robo de información estratégica de la empresa, daños a los equipos, incremento de los costos, etc.

Entre los riesgos de no contar con un sistema de seguridad, podemos mencionar entre otros:

- 1º Que la información no esté integrada y se guarde en cada uno de los equipos de los diferentes usuarios, sin embargo esta dispersión de la información, puede ser beneficiosa para la seguridad, si es que se toman algunas medidas, ejemplo de ellos pueden ser los sistemas RAID.
- 2º Robo y pérdida de información
- 3º Fallas en los equipos.

Un ataque a la seguridad de la información o incidente se produce cuando se realiza un acceso o un intento de acceso a la información de la empresa a efectos de apropiarse de la información o afectar el normal funcionamiento de los diferentes procesos de la empresa.

³ Cazemier, Jacques; Overbeek, Paul; Peters, Louk (2004). Best practice for Security Management. Office of Government Commerce: ITIL Services. 8va edición.

Los informes de las incidencias generan un historial que nos permite solucionar incidencias similares de forma rápida y eficiente, evitando la paralización de los procesos y proporcionar información valiosa para mejorar el tratamiento de los incidentes o ataques.

Según Juan Manuel Harán, en su artículo publicado en lo blog welivesecurity el 29 Oct 2018 - 02:21PM⁴, donde realiza un análisis de la situación de seguridad de la información en las empresas de Latioamerica, en el cual sostiene que “el 45% de las grandes empresas en Latinoamérica sufrió una infección por malware en el último año, pese a que para el 52% de las grandes empresas de la región considera al malware entre sus principales preocupaciones en materia de seguridad, la tasa de infecciones es alta”(sic).

1.3.8. Seguridad informática

A. Gomez sostiene que “La seguridad informática está definida como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, integridad y disponibilidad, disminuir el riesgo de los equipos o bloquear el acceso de usuarios no autorizados al sistema”⁵ (Sic).

Como todo sistema de seguridad, en este caso específico, la seguridad de la información, la confidencialidad, la integridad y la disponibilidad, son aspectos vitales en la protección de datos tanto de carácter personal como institucional.

En la Seguridad Informática se entiende por seguridad de hardware, seguridad de software y seguridad en la red. En tal sentido la Universidad

⁴ Harán Juan Manuel (2018) “45% de las grandes empresas en Latinoamérica sufrió una infección por malware en el último año” <https://www.welivesecurity.com/la-es/2018/10/29/45-de-las-grandes-empresas-en-latinoamerica-sufrio-una-infeccion-por-malware-en-el-ultimo-ano/>

⁵ Gómez A. (2011). Enciclopedia de la Seguridad Informática (2da Edición). España: Alfaomega RA-MA.

Internacional de Valencia en su publicación “Lo que debes saber si quieres estudiar seguridad informática”⁶, sostiene lo siguiente:

- 1º La seguridad de hardware a la protección de los equipos informáticos de cualquier daño que puedan sufrir como consecuencia de un ataque o incidente del sistema o a través del tráfico de la red.
- 2º La seguridad de software está referida a los ataques que sufren o puedan sufrir los sistemas informáticos que imposibilita que sigan funcionando correctamente.
- 3º La seguridad de red se refiere a los ataques o amenazas a los sistemas de información provenientes de una red, por ejemplo internet, entre ellos tenemos a los virus, gusanos, caballos de Troya; software espía y publicitario, hackers, robos de información y/o identidad, fraudes, etc.

Un aspecto importante de la seguridad informática es el análisis de riesgos, el cual proporciona herramientas útiles para evaluar el riesgo ya sea en forma cuantitativa o cualitativa, a efectos de tomar las medidas correctivas correspondientes.

Ambos tipos de análisis del riesgo cuantitativo (principalmente en términos monetarios) o cualitativo (en notaciones como alto, bajo, medio) hacen uso de los siguientes elementos interrelacionados: amenazas, vulnerabilidades y controles

1.3.9. Administración de vulnerabilidades

Según Muñiz, Nadhem y McIntyre (2015) la Administración de Vulnerabilidades se refiere al proceso de detectar, identificar, analizar, clasificar, priorizar, tratar y rastrear las fallas en el sistema o vulnerabilidades que se presentan y que puedan afectar la seguridad.

Según los mismos autores, lo más importante es detectar lo más pronto, la posible una vulnerabilidad antes de que ataque un activo y sobre todo brindar las medidas correctivas.

⁶ Universidad Internacional de Valencia (2018). Lo que debes saber si quieres estudiar seguridad informática. España.

1.3.10. Inteligencia de amenazas

La Inteligencia de amenazas consiste en detectar, reconocer y analizar algún posible ataque o amenaza a la seguridad de información para detectar situaciones problemáticas, estableciendo ciertos indicadores que sirvan en la toma de decisiones para implementar un mecanismo de solución a la problemática planteada.

Como podemos ver la inteligencia de amenazas es una parte importante del SOC a efectos de detectar posibles amenazas que pudieren afectar a la empresa.

1.3.11. Servicio al cliente

Como indica Gonzales N. en su libro El Ingeniero y el desarrollo de los negocios: Una Visión Práctica “El servicio al cliente es el servicio o atención que una empresa o negocio brinda a sus clientes al momento de atender sus consultas, pedidos o reclamos, venderle un producto o entregarle el mismo” (González N., 2017, p.67).

Para efectos de la presente investigación servicio al cliente se entiende como servicio de atención de incidencias y/o eventos críticos de la plataforma de seguridad de la información.

1.3.12. Incidencias

“Un incidente es cualquier evento que causa o puede causar una interrupción de un servicio o una reducción de su calidad. Se clasifican en incidentes por hardware (computadora, impresora, etcétera), incidentes por sistemas de información (falla de un sistema de información para un proceso específico), incidentes por software de aplicación (MS Word, MS Excel, etcétera), incidentes en las redes de comunicación (falla en la conectividad). Por otro lado, afirma que los objetivos principales de la

gestión de incidentes es resolver el incidente en el menor tiempo posible, mantener la comunicación entre los gestores de incidentes y el usuario, y evaluar los incidentes para determinar la probabilidad de su recurrencia. (Carillo, 2008, p. 41,86-87).

Según Kolthof, y otros (2008), señalan que un incidente es una acción que interrumpe u obstaculiza un proceso, lo cual implica una disminución en la calidad del mismo.

Según el blog ManageEngine, titulado Gestión de Incidentes “El objetivo de la Gestión de Incidentes es restablecer a su estado normal los servicios de tecnología de la información tan pronto como sea posible, con soluciones temporales o definitivas, asegurándose de que ello no afecte al negocio”.

La gestión de incidentes es un proceso para resolver las interrupciones u obstáculos que se presentan en proceso, restableciéndolo a la brevedad posible y sin perder su calidad.

En la gestión de incidentes se emplea el sistema de ‘tickets’ en el cual se implementa una mesa de ayuda en la que se trabaje las incidencias, según las prioridades del negocio.

La mesa de ayuda o mesa de servicios (Service Desk) tiene como funciones básicas las siguientes:

- 1) Registrar los detalles básicos del usuario.
- 2) Identificar si el usuario informa de una interrupción o está pidiendo un nuevo servicio.
- 3) Determinar cuándo es un Incidente o no mediante un diagnóstico básico.
- 4) Verificar si se puede ayudar con una solución de la base de datos del conocimiento.
- 5) Asignar el incidente al grupo de Especialistas de soporte.
- 6) Trabajar cerca del grupo de especialistas de soporte para ofrecer soluciones al usuario.

7) Cerrar el Incidente con la confirmación del usuario

El problema principal es que en muchos casos las incidencias no son reportadas por los usuarios a través del sistema de tickets para la resolución de los mismos, es decir simplemente no son reportadas. Para solucionar este problema y que la atención sea proactiva y en menor tiempo posible, se debe de implementar un centro de operaciones de seguridad (SOC) y un software que permita buscar, monitorizar y analizar datos (Logs) generados por los servidores, en este caso las consolas antivirus.

Para efectos de la presente investigación consideramos que un incidente es cualquier acto que sucede durante un proceso y que repercute en él, interrumpiendo u obstaculizando el proceso normal de operaciones, lo cual implica una disminución en la calidad del mismo. Por consiguiente, la atención de incidencias cubre todo tipo de actos que interrumpe el proceso normal, incluyendo, preguntas o consultas planteadas por usuarios.

La atención de incidencias y/o eventos críticos, denominado también gestión de incidencias, tiene como objetivos, los siguientes:

1. Detectar y reconocer cualquier interrupción u obstáculo que se presentan en proceso normal de operaciones.
2. Registrar y clasificar estos problemas, otorgando una prioridad para su atención lo más pronto posible.
3. Designar el personal encargado de restaurar el proceso, a la brevedad posible y sin perder su calidad.

Las dimensiones de la atención de casos o incidencias de un nivel de criticidad crítico y alto, no reportados en tiempo real y que son atendidas fueran del tiempo de servicio estimado (SLA) son las siguientes:

1. Registro de Incidencias. - Las incidencias a diario deben ser totalmente registradas en el sistema de ticket de la web, con los datos de la incidencia y lo asigna a Siscotec. El sistema genera el ticket correspondiente informando al usuario vía correo corporativo el número de ticket generado.

El indicador para esta dimensión es número de registro de incidencias, y la fórmula para calcularlo es la sumatoria de todos los registros o incidencias reportadas, generadas por el propio sistema.

2. Generación de reporte de las incidencias no reportadas del último mes. La búsqueda de incidencias no reportadas del último mes se realiza para identificar las incidencias que requieran una acción manual para su solución y que no fueron atendidas en su debida oportunidad en forma integral. Para realizar la búsqueda se tienen que especificar los siguientes aspectos:

- a) Elegir según el criterio de búsqueda. (rango de fecha y tipo de servicio de la consola antivirus)
- b) Ingresar el dato requerido

El indicador para esta dimensión es el número de casos o incidencias no atendidas, y la fórmula para calcularlo es:

$$InA = TIM - IA$$

Donde:

InA: incidencias no atendidas

TIM: Total de incidencias del mes

IA: Incidencias atendidas

3. Porcentaje de cumplimiento del servicio. - Nos proporciona información sobre el grado o porcentaje de cumplimiento del servicio que se está brindado a través de la consola antivirus, o a las limitaciones del software.

El indicador para esta dimensión es el porcentaje de cumplimiento, y se calcula con la fórmula siguiente:

$$CS = ((1-(CRMft/ CRM))*100)$$

Donde:

CS: Cumplimiento del servicio

CRMft : Cantidad de registros mensuales fuera de tiempo de atención

CRM : Cantidad de requerimientos mensuales

Recordemos que se debe de resolver las interrupciones u obstáculos que se presentan en proceso a la brevedad posible y sin perder su calidad, en tal sentido

el tiempo total de atención de incidencias debe ser el más breve posible, así como el número de caso no atendidos debe ser el mínimo posible y el porcentaje de atención debe acercarse al 100%.

1.4. Formulación del problema

¿Cómo la implementación de un Sistema de gestión, específicamente de un Centro de Operaciones de Seguridad (SOC), mejora el servicio de atención de las incidencias y/o eventos críticos en la plataforma de seguridad de la información en la empresa Siscotec del Perú S.A.C.?

1.5. Justificación e importancia

Como se explicó en la situación problemática, el número de amenazas informáticas que buscan realizar un espionaje informático, sabotaje y/o sustraer información de las empresas, a efectos de realizar fraudes, ataques, intromisión o intrusión o de negación de servicio, así como daños ocasionados por virus informáticos que repercuten negativamente en la imagen de la empresa, se ha incrementado considerablemente. En Latinoamérica los ataques a la seguridad de información son principalmente por ransomware (57%), en segundo lugar, por vulnerabilidades (55%) y en tercer lugar por malware (53%).

Es importante resaltar que, Perú es uno de los países de Latinoamérica donde se producen más ataques de robo de información, por consiguiente, la conservación de la información se hace más vulnerable, por lo que se debe tomar medidas que aseguren su integridad, disponibilidad y confidencialidad.

Por eso es vital que, si las acciones de protección informática implementada en cada empresa fallan, es necesario contar el servicio que brinda un Centro de Operaciones de Seguridad (SOC) y un Sistema de comunicaciones adecuado, de tal manera que todos los softwares de seguridad que posean sean gestionados y monitoreado de forma integral en el menor tiempo posible y no se pierda la información de la empresa a efectos de seguir competitivos, asegurando de esta

forma mayores beneficios económicos. De contar con un SOC, las empresas obtendrán mejores resultados en la seguridad de su información, así como reducir el tiempo promedio para resolver incidencias y/o eventos críticos.

Para Siscotec del Perú S.A.C., como empresa sería un gran paso para consolidarse en el mercado nacional y expandirse al mercado internacional, porque se convertiría en la primera empresa, en el Perú, en contar con un Centro de Operaciones de Seguridad (SOC), lo cual le permitiría captar nuevos clientes, especialmente aquellos de mayor envergadura como entidades financieras líderes en el mercado.

La implementación de este proyecto le daría a Siscotec del Perú S.A.C., una mayor rentabilidad, incrementando sus utilidades.

Para las diferentes empresas clientes de Siscotec del Perú S.A.C., sería beneficioso contar con sistema integrado que le permita monitorear y alertar en tiempo real sus softwares de seguridad ante eventos de infección en sus equipos informáticos, correos maliciosos, fuga de información y ataques cibernéticos.

1.6. Hipótesis

En la presente investigación formularemos una hipótesis de tipo de investigación, específicamente de tipo descriptiva, la misma que queda formulada de la siguiente manera:

Si se implementa un sistema de gestión específicamente de un Centro de Operaciones de Seguridad (SOC), en la empresa Siscotec S.A.C. entonces mejorará el nivel de satisfacción de los clientes con respecto al servicio de atención de las incidencias y/o eventos críticos de la plataforma de seguridad de la información.

Lo que queremos demostrar es que implementando un SOC en la empresa Siscotec S.A.C., va a incrementar el nivel satisfacción de los clientes con respecto

al servicio de atención de las incidencias y/o eventos críticos de la plataforma de seguridad de la información.

1.7. Objetivos

1.7.1. Objetivo general

Diseñar de un sistema de gestión para la empresa Siscotec del Perú S.A.C., mejorando el servicio de atención al cliente desde una plataforma de seguridad de la información, específicamente de un Centro de Operaciones de Seguridad (SOC), que le permita un mejor manejo de las incidencias y/o eventos críticos, definiendo los componentes que se requiera para implementar el SOC.

1.7.2. Objetivos específicos

- 1) Realizar la evaluación de los resultados del servicio de atención que se brinda a través de la plataforma de seguridad de la información de la empresa Siscotec del Perú S.A.C., la misma que actualmente no cuenta con SOC implementado.
- 2) Realizar el diagnóstico de los resultados del servicio de atención que se brinda a través del demo de un SOC.
- 3) Realizar una encuesta de satisfacción de los servicios brindados por Siscotec sin SOC y con el demo del SOC
- 4) Desarrollar una propuesta de implementación de un SOC en la empresa Siscotec del Perú S.A.C.

II MATERIAL Y MÉTODO

2.1. Tipo y diseño de la investigación

La presente investigación es de tipo aplicada, considerando que vamos a trabajar algunas incidencias con un demo de un SOC y comparar con los resultados con obtenidos con el proceso normal de Siscotec.

Asimismo, es de diseño cuasi experimental porque el diseño con post prueba y grupos intactos, se ha de realizar las pruebas contando con dos grupos del mismo tamaño y características: uno experimental y uno de control, tal como se muestra en la figura N° 15,

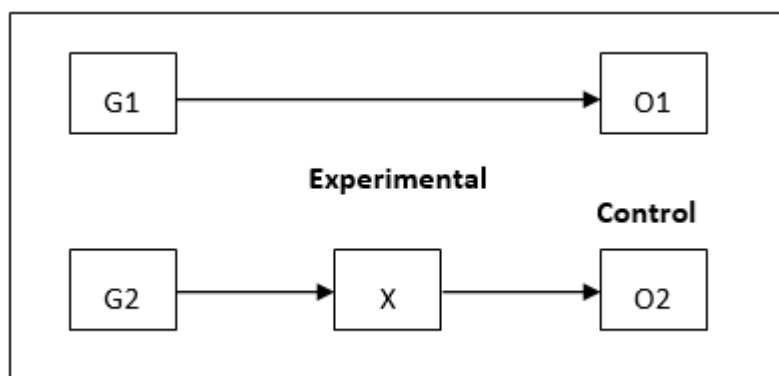


Figura N° 25. Diseño Cuasi - experimental con post prueba y grupos intactos. Elaboración © Carrasco

Donde:

G1: Es el grupo de procesos escogidos como grupo de control

G2: Es el grupo de procesos escogidos como grupo experimental

X: Es la aplicación del Centro de Operaciones de Seguridad (SOC)

O1: Es el resultado de realizar las pruebas con el método tradicional, es decir a través de un sistema de tickets y consola antivirus

O2: Es el resultado de realizar en la gestión de incidencias con el SOC.

2.2. Población y muestra

2.2.1. Población:

En esta investigación consideramos que la población está definida por las incidencias no reportadas y que no que serán atendidas posteriormente.

Como podemos ver en la tabla N° 15 que contiene datos estadísticos de las incidencias no reportadas que se presentaron en el año 2018, el promedio mensual de incidencias no reportadas en ese el año ascienden a 624 incidencias no reportadas (No atendidas en su debida oportunidad). Para efectos de la presente investigación se considera como población 624 incidencias no reportadas.

Tabla N° 15: Promedio de incidencias no reportadas mes a mes 2018

Mes	Equipos sin Agentes Antivirus	Equipos sin Políticas de DLP	Equipos sin Políticas de Firewall de AV	Equipos Infectados con Virus Malware	Equipos Infectados con Spyware Grayware	Total Incidencias
Enero	168	680		398	382	1628
Febrero	157	510		245	163	1075
Marzo	151	405		171	94	821
Abril	130	265		126	85	606
Mayo	122	241		98	75	536
Junio	85	226		83	62	456
Julio	75	225		82	61	443
Agosto	70	221		68	52	411
Setiembre	56	214		56	42	368
Octubre	25	177	170	51	35	458
Noviembre	21	168	119	43	29	380
Diciembre	10	123	104	39	25	301
Total	1070	3455	393	1460	1105	7483
Promedio	89	288	131	122	92	624

Fuente: Siscotec del Perú SAC.
Elaboración propia.

2.2.2. Muestra:

Para calcular la muestra a partir del número de población se utiliza la siguiente fórmula:

$$n = \frac{NZ^2 p q}{(N-1) e^2 + Z^2 p q}$$

Donde:

n = Tamaño de muestra

Z= Nivel de confianza al 95% (1.96) elegido para la investigación

N= Población total de estudio

p = Proporción de éxito en la población, se asume 50% por desconocimiento

q = Complemento de p 50%

e = Error de estimación (5%)

Obteniendo como resultado 238.011676, es decir 238 incidencias como muestra.

Para la composición de la muestra se ha tenido en cuenta el número total de incidencias por tipo de incidencia, de acuerdo al estrato (%), quedando establecida de la siguiente tabla:

Tabla N° 16: Composición de la muestra

Tipo de Incidencia	Incidencias	Porcentaje	Muestra	Muestra Final
Equipos sin Agentes Antivirus	1070	14.30%	34.03	34.00
Equipos sin Políticas de DLP	3455	46.17%	109.89	110.00
Equipos sin Políticas de Firewall de AV	393	5.25%	12.50	13.00
Equipos Infectados con Virus Malware	1460	19.51%	46.44	46.00
Equipos Infectados con Spyware Grayware	1105	14.77%	35.14	35.00
TOTAL	7483	100.00%	238.00	238.00

Fuente: Siscotec del Perú SAC.
Elaboración propia.

2.2.3. Muestreo:

El muestreo aplicado para el presente proyecto fue el Muestreo Aleatorio Simple, donde todos los elementos tienen la misma probabilidad de ser elegidos.

2.3. Variables, operacionalización

Las variables a utilizar son: El servicio de atención de Incidencias y/o eventos críticos de la plataforma de seguridad de la información, como variable dependiente, y el sistema de gestión del Centro de Operaciones de Seguridad (SOC) como variable independiente.

La operacionalización de las variables se efectúa considerando los aspectos de dimensión, indicador, descripción, instrumento, unidad de medida y fórmula, tal como podemos visualizar en la tabla siguiente:

Tabla N° 17: Operacionalización de las variables

VARIABLE	DIMENSIÓN	INDICADOR	DESCRIPCIÓN	INSTRUMENTO DE MEDICIÓN	UNIDAD DE MEDIDA	FÓRMULA
VARIABLE: DEPENDIENTE	Registro de incidencias	I1: Número de registro de incidencias	Es el número de ticket generado por el sistema para el registro de incidencias	Ficha de Observación (Reporte del sistema)	ticket	$RI = ZT$ Donde: RI: Total Registro de Incidencias ZT: Sumatoria de tickets generados.
	Búsqueda de Incidencias	I2: Número de casos o incidencias no atendidas	Es el número de incidencias no reportadas del último mes que no fueron atendidas en su debida oportunidad en forma integral	Ficha de Observación	Incidencia no atendida	$InA = TIM - IA$ Donde: InA: incidencias no atendidas TIM: Total de incidencias del mes IA: Incidencias atendidas
	Cumplimiento del servicio	I3: nivel de satisfacción del cliente	Es el grado o porcentaje de cumplimiento del servicio que se está brindado a través del monitoreo actual y el demo del monitoreo con SOC.	Cuestionario de encuesta	Porcentaje	Procesamiento de los resultados de la encuesta
VARIABLE: INDEPENDIENTE	Sistema de gestión - Centro de Operaciones de Seguridad (SOC).	I4: Implementación del SOC	Se encarga de los aspectos de inteligencia y seguridad de la información, solucionando cualquier incidencia lo más pronto posible.	Lista de cotejo de implementación	Centro de Operaciones	

Fuente: Siscotec del Perú SAC.
Elaboración propia.

2.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad.

Las técnicas e instrumentos de recolección de datos utilizados para el indicador 1: Número de registro de incidencias, se utilizará la técnica de la observación y como instrumento la ficha de observación que es emitido por el sistema web como un Reporte de tickets (ver anexo N° 6). Para el indicador 2:

Número de casos o incidencias no atendida, también se empleará la técnica de la observación y como instrumento la ficha de observación que es emitido por el demo SOC como un registro de casos detectados y reportados (ver anexo N° 7). Para el indicador 3: Nivel de satisfacción del cliente, se utilizará la técnica de la encuesta y como instrumento el cuestionario de la encuesta (ver anexo N°8). Para el indicador 4: Implementación del SOC, se utilizará la técnica de la observación y como instrumento la lista de cotejo (ver anexo N° 9).

La validez y confiabilidad de la información obtenida mediante los instrumentos de recolección de datos, antes descritos son: Ficha de observación, reporte del sistema web de tickets debidamente firmada y sellada por funcionarios de la empresa Siscotec del Peru SAC ver anexo N° 10); para la ficha de observación que es emitido por el demo SOC como un registro de casos detectados y reportados debidamente firmada y sellada por funcionarios de la empresa Siscotec del Peru SAC (ver anexo N° 11). Para validar el instrumento del cuestionario de la encuesta se ha utilizado el Cuestionario de la encuesta debidamente llenado por el usuario y firmada por representantes de la empresa Siscotec del Peru SAC (ver anexo N° 12), el análisis de la confiabilidad de las encuestas sistema web de tickets mediante el coeficiente de Alfa de Crombach (ver anexos N° 13) y el análisis de la confiabilidad de las encuestas sistema Demo SOC mediante el coeficiente de Alfa de Crombach (ver anexos N° 14)

2.5. Procedimiento de análisis de datos.

El procedimiento utilizado para el análisis de los datos es el estadístico descriptivo, donde vamos a analizar comparar los resultados obtenidos en el reporte del sistema web de tickets versus el reporte del registro de casos no reportados emitido por el demo SOC, luego se analizará los resultados estadísticos de la encuesta a fin de determinar el nivel de satisfacción del cliente

2.6. Aspectos éticos.

Los aspectos éticos serán consignados con los datos que la empresa Siscotec del Perú S.A.C. brinde de manera fidedigna. La información obtenida se dio dentro de la operatividad normal de la empresa con el aporte de todos los trabajadores del departamento de soporte técnico de la mencionada empresa, cumplimiento en todo momento con la normatividad establecida por la escuela académica profesional de ingeniería industrial, facultad de ingeniería, arquitectura y urbanismo. Frente a ello, las fuentes bibliográficas primarias y secundarias serán utilizadas bajo el respeto a la autoría.

Asimismo, he respetado la autenticidad de los resultados, garantizando la veracidad de los datos suministrados y estricto respeto a la propiedad intelectual.

En esta investigación hemos empleado el método del contraste de los resultados obtenidos a fin de obtener una interpretación y validez correcta de los resultados

En esta investigación los planteamientos efectuados son identificados como verdaderos tanto por las personas que han colaborado en esta investigación, ya sea personal y clientes de la empresa Siscotec del Perú S.A.C., como por otros profesionales especialistas en la materia investigada, por lo que tiene un alto sentido de credibilidad o valor de la verdad.

En esta investigación tuvimos el compromiso ético de comunicar a la empresa Siscotec de los lugares donde llevaría a cabo el trabajo de campo, las actividades a realizar y los resultados obtenidos, tratando de ser lo más objetivo posible.

2.7. Criterios de rigor científico.

Los criterios de rigor científicos empleados son:

1) Verosimilitud o valor de la verdad.

La verosimilitud implica un indicador de credibilidad, es decir que la investigación puede ser reconocida como creíble o verdadera.

La credibilidad en la presente investigación, se apoya en los siguientes aspectos:

- a) Los hechos presentados son situaciones reales reconocidos y avalados por las personas que participaron en la investigación.
- b) Valoración por expertos de los instrumentos empleados.
- c) Una correcta valorización de los datos e información obtenida.
- d) La amplia experiencia laboral de los sujetos de la investigación.
- e) El cruce de la información obtenida para logara una mejor interpretación y valoración de la información.

2) Transferibilidad o aplicabilidad

En esta investigación se ha efectuado una prolija exposición del entorno en el cual se realizo la investigación. En tal sentido los resultados derivados de la investigación no son generalizables, sino que se pueden aplicar a situaciones similares.

3) Coherencia de la investigación.

En esta investigación existe una coherencia entre los objetivos o propósitos de la investigación el planteamiento de implementación de un SOC en Siscotec.

4) Relevancia

En esta investigación creemos que hemos logrados los objetivos planteados y que existe una correlación entre la justificación de la investigación y los resultados obtenidos.

5) Adecuación o concordancia teórico-epistemológica

El aspecto de adecuación o correspondencia teórico-epistemológica en esta investigación se tomó en cuenta durante toda la investigación, de tal forma que se puso especial interés en que la información y resultados obtenidos estén encuadrados dentro de los supuestos teóricos y enmarcados del aspecto metodológico escogido para la presente investigación.

III RESULTADOS

3.1. Resultados en Tablas y figuras

En lo referente al objetivo específico 1 “Realizar el diagnóstico de los resultados del servicio de atención que se brinda a través de la plataforma de seguridad de la información de la empresa Siscotec”, tenemos los resultados que se presentan en el anexo N° 15.

Siendo lo más resaltante que del estudio realizado, solo 158 casos fueron reportados por el cliente (66%) y 80 casos fueron detectados por el sistema de Siscotec luego del registro, emisión del ticket y análisis pertinente. Este hecho nos demuestra que el 34% de los casos de las incidencias presentadas no son detectadas inicialmente por el cliente, lo que le puede ocasionar grandes perjuicios de seguridad en la información, ver figura N° 26

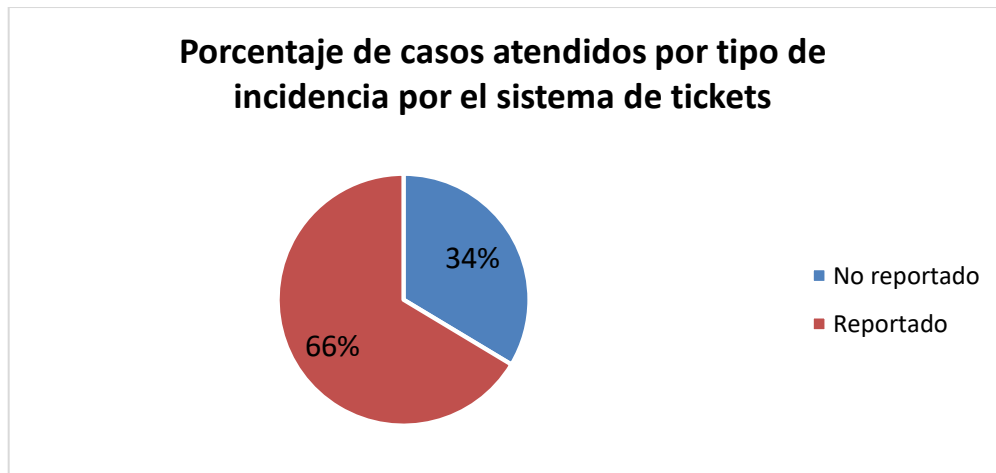


Figura N° 26. Porcentaje de casos atendidos por tipo de incidencia por el sistema de tickets.

Elaboración propia.

Finalmente, si analizamos el tiempo en que se demoró en dar solución a los casos, podemos ver que si bien es cierto que el 82% de los casos el tiempo de atención fue de inmediato (Green), el 12% el tiempo de atención fue alto, por lo que existe una demora considerable en obtener una solución al problema presentado, ver tabla y figura siguiente

Tabla N^a 18: Casos atendidos por SLA de solución por el sistema de tickets

Tipo de casos	Red	Yellow	Green	Total general
DLP	24	11	75	110
Firewall			13	13
Reg. de Agente	2	1	31	34
Spyware Grayware	3	3	29	35
Virus Malware			46	46
Total general	29	15	194	238
Porcentaje	12%	6%	82%	100%

Fuente: Siscotec del Perú SAC.
Elaboración propia.

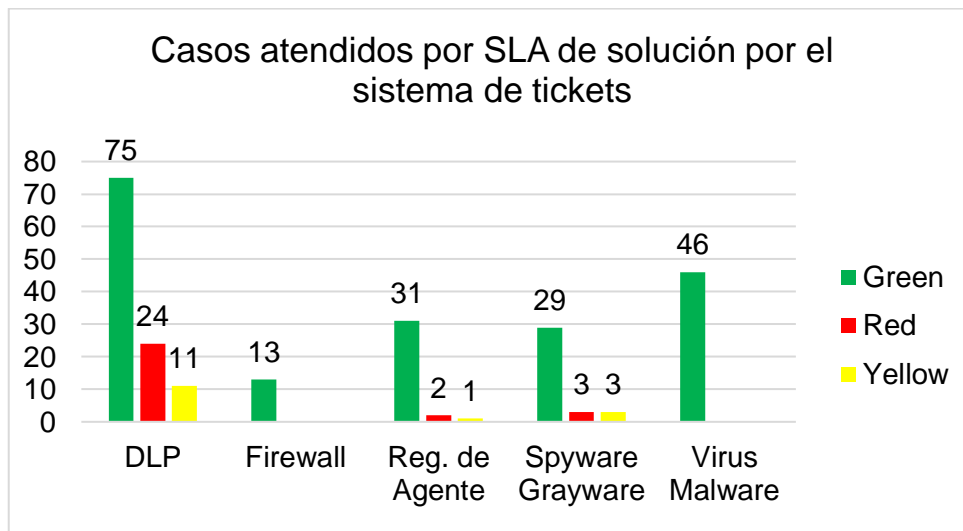


Figura N^o 27. Casos atendidos por SLA de solución por el sistema de tickets.
Elaboración propia.

En cuanto al objetivo específico 2 “Realizar el diagnóstico de los resultados del servicio de atención que se brinda a través del demo de un SOC”, tenemos los resultados que se presentan en el anexo N^o 16.

Lo más importante es que el 100% de los casos presentados son detectados y reportados por el sistema SOC, este hecho es de vital importancia porque a diferencia del sistema de tickets no hay casos reportados por el cliente, tal como lo podemos visualizar en la tabla y figura siguiente:

Tabla N° 19: Casos atendidos por tipo de incidencia por el sistema de Demo SOC.

Tipo de casos	Incidente detectado por el SOC	Porcentaje
DLP	110	46%
Firewall	13	5%
Reg. de Agente	34	14%
Spyware Grayware	35	15%
Virus Malware	46	19%
Total general	238	100%

Fuente: Siscotec del Perú SAC.
Elaboración propia.

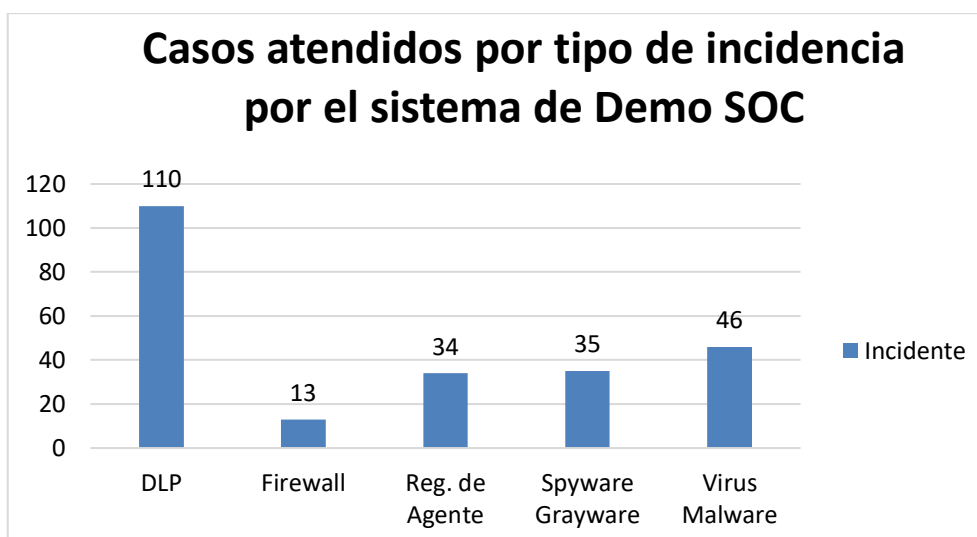


Figura N° 28. Casos atendidos por tipo de incidencia por el sistema de Demo SOC. Elaboración propia.

Finalmente, si analizamos, por nivel de casos atendidos por SLA de solución, es decir por el tiempo en que demoro en dar solución a los casos, podemos ver que el 100% de los casos el tiempo de atención fue de inmediato (Green) en tiempo real, lo que demostraría una mayor eficiencia de seguridad en la información si se cuenta con un SOC.

Tabla N° 20: Casos atendidos por SLA de solución por el sistema de Demo SOC.

Tipo de casos	Verde	Total general
DLP	110	110
Firewall	13	13
Reg. de Agente	34	34
Spyware Grayware	35	35
Virus Malware	46	46
Total general	238	238
Porcentaje	100%	100%

Fuente: Siscotec del Perú SAC.
Elaboración propia.

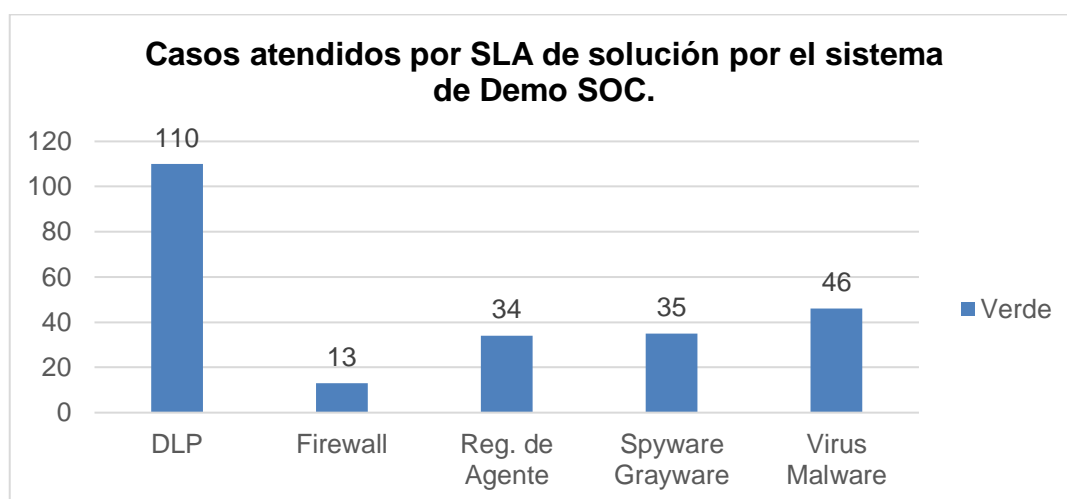


Figura N° 29. Casos atendidos por SLA de solución por el sistema de Demo SOC.
Elaboración propia

En lo relativo al objetivo específico 3 “Realizar una encuesta de satisfacción de los servicios brindados por Siscotec sin SOC y con el demo del SOC”, los resultados se presentan en el anexo N° 17.

En lo referente al tiempo utilizado para la solución del incidente y/o requerimiento, en el sistema actual por tickets los clientes opinan que en el 51.7% de los casos el tiempo empleado en la atención fue regular y el 29.8% que fue bueno. Sin embargo, si la atención fue por el Demo del SOC la mayoría opina que es muy bueno 52.5% y excelente 32.8% y, según podemos observar en las figuras siguientes:

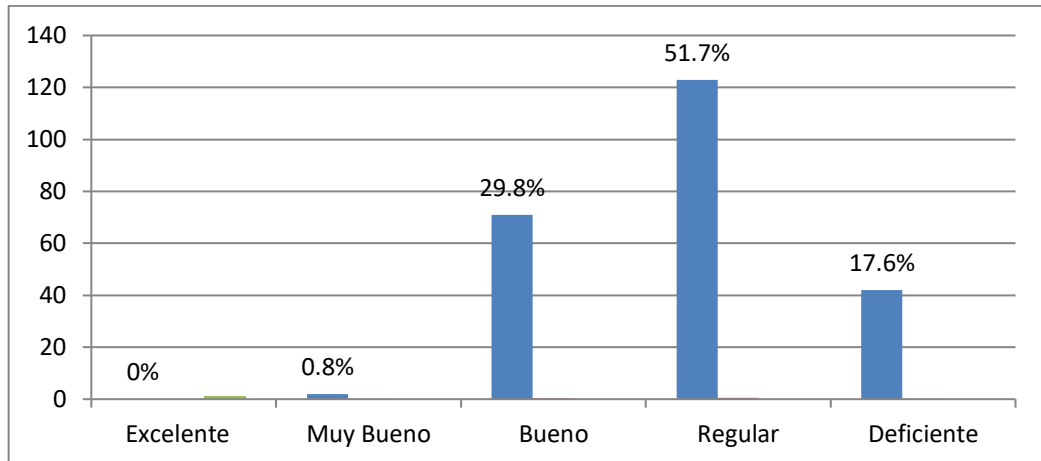


Figura N° 30. Tiempo utilizado para la solución del incidente y/o requerimiento por el sistema de tickets.
Elaboración propia

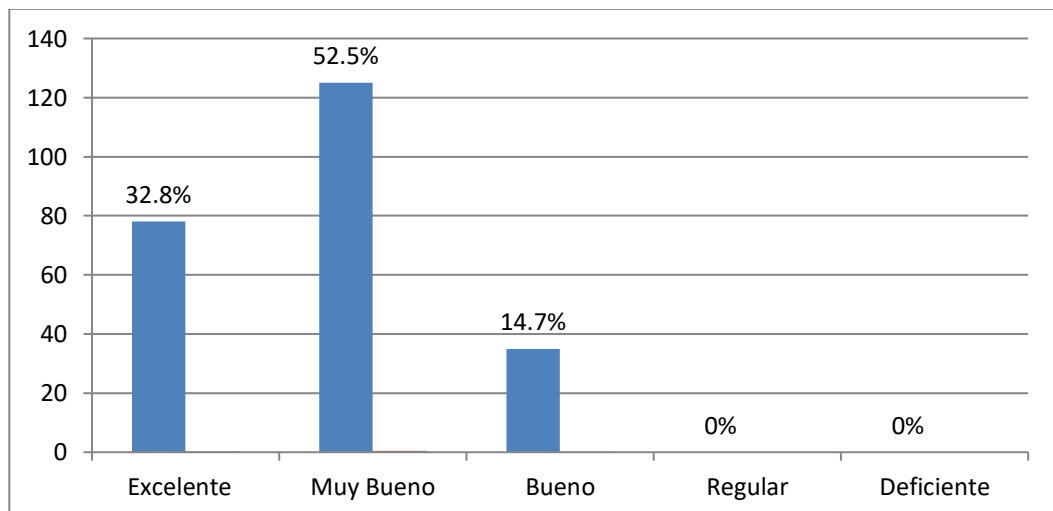


Figura N° 31. Tiempo utilizado para la solución del incidente y/o requerimiento por el sistema de SOC.
Elaboración propia

En relación a que, si se solucionó la incidencia y/o requerimiento en la primera atención, en el servicio brindado a través del sistema actual por tickets el 32.8% sostiene que no se solucionó en la primera atención, y solo el 67.2% opino que sí. Sin embargo, con el Demo del SOC, el 100% de los clientes opinan que, si se solucionó la incidencia y/o requerimiento en la primera atención, lo cual demuestra una mayor eficiencia con el sistema del SOC, según podemos observar en las tablas y figuras siguientes:

Tabla N° 21: Se solucionó su incidencia y/o requerimiento en la primera atención, por el sistema de tickets.

Respuesta	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	160	67.2%	67.2%	67.2%
No	78	32.8%	32.8%	100.0%
Total	238	100.0%	100.0%	

Fuente: Siscotec del Perú SAC.
Elaboración propia.

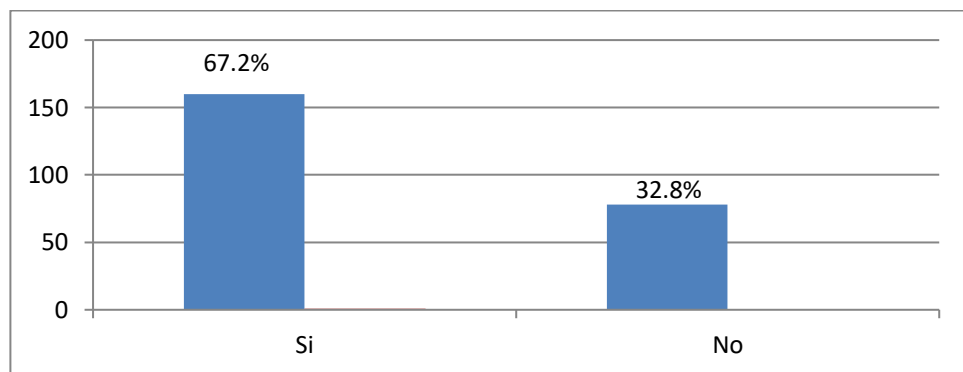


Figura N° 32. Solución de la incidencia y/o requerimiento por el sistema de tickets.
Elaboración propia

Tabla N° 22: Se solucionó su incidencia y/o requerimiento en la primera atención, por el sistema de SOC.

Respuesta	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	238	100.0%	100.0%	100.0%
No	0	0.0%	0.0%	100.0%
Total	238	100.0%	100.0%	

Fuente: Siscotec del Perú SAC.
Elaboración propia.

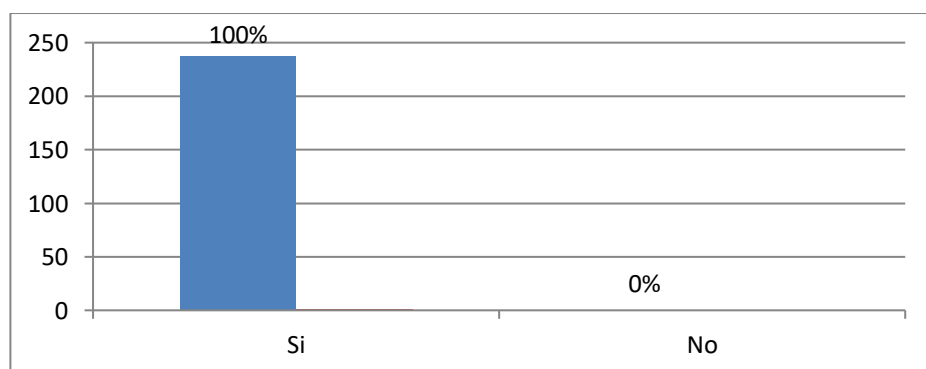


Figura N° 33. Solución de la incidencia y/o requerimiento por el sistema de SOC.
Elaboración propia

En lo que se refiere al objetivo específico 4 “Desarrollar una propuesta de implementación de un SOC en la empresa Siscotec del Perú S.A.C.” que a su vez tiene relación directa con el objetivo general de “Diseño de un sistema de gestión específicamente de un Centro de Operaciones de Seguridad (SOC), en la empresa Siscotec del Perú S.A.C., que permita una mejora del servicio de atención de las incidencias y/o eventos críticos de la plataforma de seguridad de la información que brindan a sus clientes, definiendo los componentes que se requiera para implementar el SOC.”, los resultados se detallan en el punto 3.3 Aporte práctico (propuesta de implementación) de la presente tesis.

3.2. Discusión de resultados

De acuerdo a la entrevista realizada al jefe del departamento de ingeniería y soporte, Juan Manuel Araoz Baca, se detalla el proceso que se realiza a diario con respecto a las incidencias gestionadas el proceso más importante, actualmente es el control de incidencias de los sistemas corporativos que se encuentran en producción y cuya atención y solución son la prioridad diaria del personal. Según esta información se aprecia la importancia de la información que manejan para satisfacer todas y cada una de las necesidades de los usuarios.

Con respecto al diagnóstico de los resultados del servicio de atención que se brinda a través de la plataforma de seguridad de la información de la empresa Siscotec del Perú S.A.C., se demostró que el 34% de las incidencias presentadas no son detectadas inicialmente por el cliente y que la prioridad de atención es determinada por el usuario de acuerdo a su criterio.

Así mismo, se comprobó que del 100% de casos atendidos por SLA de solución por el sistema de tickets, el 12% el tiempo de atención fue alto, por lo que existe una demora considerable en obtener una solución al problema presentado.

Estos hechos pueden ocasionar grandes perjuicios de seguridad en la información de sus empresas, por lo que el sistema de ticket no satisface

plenamente los requerimientos del cliente, en razón de que es complicado satisfacer por completo las necesidades del cliente y a la vez estar completamente seguros.

En cuanto al diagnóstico de los resultados del servicio de atención que se brinda a través del demo de un SOC, vemos que el 100% de los casos presentados son detectados y reportados por el sistema SOC, este hecho es de vital importancia porque a diferencia del sistema de tickets no hay casos no reportados por el cliente, hecho que demostraría una mayor eficiencia de seguridad en la información si se cuenta con un SOC.

En el sistema SOC la prioridad es determinada por el mismo SOC a diferencia del sistema de ticket en el que la prioridad es determinada por el cliente.

En relación al tiempo de atención se demostró que el 100% de los casos atendidos mediante el demo de un SOC, el tiempo de atención fue de inmediato (Green), es decir fueron resueltos en tiempo real, lo que demostraría una mayor eficiencia de seguridad en la información si se cuenta con un SOC.

En estos aspectos nuestra investigación coincide con la investigación realizada por Vásquez (2016), en la cual se sostiene que con la gestión de un SOC se produce una menor presentación de incidentes sin resolver que puedan comprometer la seguridad de la información, coincidiendo también en que existe una mayor eficiencia de seguridad en la información si se cuenta con un SOC.

En lo relativo a la encuesta para medir el grado de satisfacción por el servicio brindado tanto en el sistema actual con ticket, como con el demo SOC, en primer lugar, diré que realizado el análisis de la confiabilidad de las encuestas mediante el coeficiente alfa de Cronbach, (ver anexos N° 13 y 14), este arrojó un aceptable nivel de confiabilidad, tal como podemos visualizar en la siguiente tabla:

Tabla N° 23: Comparativo de los coeficientes de confiabilidad de las encuestas.

NIVEL DEL COEFICIENTE		SISTEMA DE TICKET	SISTEMA DEMO SOC
Muy baja	0.0 a 0.2		
Baja	0.2 a 0.4		
Moderada	0.4 a 0.6		
Buena	0.6 a 0.8	0.701	
Alta	0.8 a 1.0		0.823

Fuente: Siscotec del Perú SAC.
Elaboración propia.

A continuación, pasamos a demostrar cómo se obtuvo esos resultados:

$$\alpha = \frac{N}{N-1} \left(1 - \frac{\sum V_i}{V_k} \right)$$

Donde:

α = Alfa de Cronbach

N = Número total de ítems

$\sum V_i$ = Sumatoria de las Varianzas individuales

V_k = Varianza total

En el sistema de ticket el coeficiente de confiabilidad fue:

$$N = 4$$

$$\sum V_i = 1.10$$

$$V_k = 2.31$$

Resultado del coeficiente de confiabilidad:

$$\alpha \text{ (Alfa de Cronbach)} = 0.701$$

En el sistema demo SOC el coeficiente de confiabilidad fue:

$$N = 4$$

$$\sum V_i = 0.84003$$

$$V_k = 0.51932$$

Resultado del coeficiente de confiabilidad:

$$\alpha \text{ (Alfa de Cronbach)} = 0.823$$

Los resultados han demostrado que, si se cuenta con un SOC, el 100% de los casos será detectado y reportado por el SOC, los cuales serán atendidos en de

inmediato en tiempo real (se solucionó el incidente o requerimiento en primera atención) a diferencia del sistema de tickets en cual solo el 32.8% de los casos de las incidencias presentadas son solucionadas en la primera atención y el 67.2% pasa a un segundo nivel de soporte, es decir son resueltos en un tiempo mayor de lo normal, hecho que demostraría una mayor eficiencia de seguridad en la información si se cuenta con un SOC. Así mismo de acuerdo a la encuesta realizada se ha podido determinar que los clientes están más satisfechos con el servicio brindado a través del SOC.

Cabe señalar que ninguna de las investigaciones similares que se han realizado y citadas en la parte de antecedentes de esta investigación a incluido el aspecto de satisfacción del cliente con el servicio brindado a través del SOC.

3.3. Aporte práctico (propuesta, si el caso lo amerita)

En la investigación realizada por Vásquez (2016), propone que el SOC se adapte a las necesidades de la empresa, mejorando su sistema de gestión de seguridad de la información.

En tal sentido, debemos tener en cuenta la teoría de del sistema de gestión, así como la teoría relativa al centro de operaciones de seguridad, que se pueden aplicar en una unidad orgánica específica dentro de la organización, centralizando todas las labores de seguridad durante las 24 horas del día y los 7 días de la semana.

Actualmente la empresa Siscotec del Perú S.A.C., se dedica a brindar servicio de implementación y soporte a soluciones de seguridad de información y redes de a través de un sistema web de emisión de Tickets publicado en modalidad 24x7x365. Es importante resaltar que los clientes de Siscotec en muchos casos cuentan además con otras de soluciones de software de seguridad por lo que surge la necesidad de centralizar la gestión de estos mismos en un sistema de gestión integral que monitoree y brinde alertas en tiempo real ante posibles vulnerabilidades

y/o ataques cibernéticos, y permita una correcta toma de decisiones a nivel seguridad de la información, por lo que es necesario la implementación de un SOC.

En la investigación realizada por Montemayor Wong, Virgilio Mosíah (2018), se indica que se debe detallar todos los procesos específicos llevados a cabo por el SOC así como los procesos fundamentales que se realizan, a fin de cumplir con cada uno de los objetivos y requerimientos de un SOC.

Siguiendo estas pautas, nuestra propuesta de implementación de un SOC en Siscotec comprende tres (3) etapas: Planificación, diseño e implementación.

1º Etapa: La primera etapa corresponde a la planificación, en esta etapa destacamos principalmente lo referente a la identificación de metas, la evaluación de las capacidades con que cuenta la empresa, y las estrategias a seguir, básicamente definimos los roles que va a desempeñar el personal y el tiempo de atención del servicio.

a) Identificación de metas.

- 1) Ofrecer servicios de seguridad de acuerdo a los procesos de negocios de cada cliente.
- 2) Garantizar el empleo adecuado de las aplicaciones e información que hagan uso los clientes, brindando soluciones tecnológicas lo mas antes posibles ante cualquier incidente de seguridad.
- 3) Contar con personal especializado, capacitado y altamente calificado.
- 4) Ser una de las mejores organizaciones que brinda el servicio de seguridad de la información, con calidad y eficiencia.

b) Evaluación de Capacidades

- 1) Siscotec no cuenta con un SOC.
- 2) Poseen una estructura de seguridad tipo consola que funciona bajo la modalidad de ticket y no asociada a ningún SOC.
- 3) Siscotec no cuenta con ningún tipo de experiencia en el manejo de un SOC.
- 4) El personal de la Siscotec no cuenta con ningún entrenamiento asociado a la gestión de un SOC.

- 5) El manejo de seguridad por consola, tipo ticket, le ha permitido a su personal contar con alguna experiencia en el manejo de incidentes y sus soluciones.
 - 6) Siscotec dispone de una infraestructura de red que sirve como soporte para todos los procesos y aplicaciones que realiza.
 - 7) Siscotec posee ciertas herramientas para el procesamiento de Datos y monitoreo.
 - 8) Siscotec dispone de controles de seguridad básicos como son los Cortafuegos.
 - 9) Siscotec no dispone de herramientas de almacenamiento de logs.
- c) Estrategia del SOC
- 1) Como señalamos Siscotec, no cuenta con un SOC implementado, pero para efectos de esta investigación se probó un Demos de SOC, con personal de la propia empresa, estableciéndose los roles siguientes:
 - El Jefe del Departamento de Ingeniería de Siscotec, desempeño el rol de Director del SOC.
 - El Gerente General de Siscotec, fue el encargado de tomar las decisiones estratégicas del SOC.
 - El Jefe de Soporte de Siscotec, fue el encargado de brindar apoyo en la implementación de las estrategias del SOC.
 - El Personal técnico del área de soporte de Siscotec, fueron los encargados de apoyar en la ejecución de las labores del SOC.Por consiguiente creemos que dicho personal puede cumplir las mismas funciones cuando se implemente el SOC en la empresa.
 - 2) El SOC, prestara el servicio de seguridad de la información las 24 horas del día los 7 días de la semana, los cual contribuirá a una mejor gestión de la seguridad, para lo cual se deberá contratar nuevo personal para cubrir toda la jornada laboral de 24 horas todos los días.

2º Etapa: La segunda etapa corresponde al diseño. El SOC de Siscotec se implementará en el local de la oficina Central, para ello se deberá tener en cuenta lo siguiente:

- a) Espacio físico, se debe contar con por lo menos 4 espacios físicos:

- 1) Una Sala de Monitoreo, con 6 escritorios equipado cada uno de ellos con una Computadora de escritorio con dos Monitores FHD de al menos 22", un teléfono ip con salida local e Internacional, aire acondicionado y 6 pantallas en alta definición de 55 pulgadas.
 - 2) Una Oficina para el Administrador del SOC, con 1 computadora, 1 teléfono ip con salida local e Internacional, aire acondicionado y 1 pantalla en alta definición de 49 pulgadas.
 - 3) Una Sala de Conferencia, con una mesa de reuniones, 10 sillas giratorias, 1 computadora, 1 teléfono ip con salida local e Internacional, aire acondicionado y 1 pantalla en alta definición de 55 pulgadas, 1 pizarra inteligente.
 - 4) El Data center debe contar por lo menos con, puerta cortafuego, cuarto eléctrico, sistema de aire acondicionado, sistemas de alarma contra incendio, sistema de seguridad, etc.
- b) Seguridad Física, se debe implementar en la Sala de Monitoreo, por lo menos las medidas de seguridad siguientes:
- 1) Restringir el acceso solo al personal autorizado.
 - 2) Implementar una bitácora de registro de acceso.
 - 3) Contar con un sistema de cámaras de vigilancia de circuito cerrado, con grabación continúa las 24 horas del día, todos los días de la semana.
 - 4) Un sistema acústico a prueba de sonidos, para que no se filtre la información que se discuta.
- c) Infraestructura Activa, entre los diferentes elementos tecnológicos con que debe contar el SOC, algunos de los cuales ya cuenta Siscotec, tenemos a:
- 1) Infraestructura de Red, Siscotec cuenta con:
 - ✓ Enrutador de Perímetro,
 - ✓ Cortafuego Perimetral,
 - ✓ Conmutador de Núcleo
 - ✓ Conmutadores de acceso,Sin embargo deberá agregar segmentos de VLANS independiente.
 - 2) Mecanismos de Seguridad a los equipos
 - ✓ Se debe de configurar 3 zonas de seguridad en el cortafuego (Inside, Outside, DMZ).

- ✓ Implementar una red de administración Outband para el monitoreo de equipos.
 - ✓ Realizar el control de acceso a los equipos por medio de un servidor.
- 3) Sistema Operativo va a depender de las herramientas que se utilicen, actualmente Siscotec trabaja con Windows, por lo que puede seguir operando con dicho sistema operativo.
 - 4) Se debe contar con un sistema de almacenamiento a través de un servidor potente que garantice que la información estará disponible para su debido análisis.
 - 5) Actualmente Siscotec cuenta con un sistema de administración de incidencias por medio de tickets, para lo cual emplea la herramienta Click, creemos que se puede seguir usando dicha herramienta en la implementación del SOC.
- d) En la generación y recolección de eventos de seguridad, se deberá utilizar las herramientas siguientes;
- 1) Un gestor de eventos de información de seguridad, empleando la herramienta SIEM (Security Information Event Management) a efectos de administrar la seguridad de la información.
 - 2) Un administrador de eventos de seguridad, utilizando la herramienta Gestión de Eventos de Seguridad (SEM).
 - 3) La herramienta Network Time Protocol (NTP), con un servidor de tiempo.
- e) Administración de Vulnerabilidades
- 1) Actualmente Siscotec cuenta un servicio de evaluación de vulnerabilidades, el cual se puede seguir empleando cuando se instale el SOC.
 - 2) Emplear una herramienta de administración de vulnerabilidades como por ejemplo: Orca Security, Skybox Vulnerability, Topia, Crashtest Security, Centraleyezer o Nessus.
- f) Personas, como señalamos anteriormente para que un SOC preste servicio 24 x 7 debe contar como mínimo 12 personas, 1 administrador, 6 analistas para el nivel 1, 2 analistas y 1 ingeniero para el nivel 2 y 2

ingenieros para el nivel 3. Actualmente Siscotec cuenta con el número de personal requerido, pero tiene que asegurar que su personal rote en los 3 turnos para cubrir el servicio las 24 horas o de lo contrario contratar nuevo personal si al demanda del servicio crece.

En lo referente a los roles a desempeñar, tal como señalamos en la etapa de planificación, estrategia del SOC se requiere cubrir los siguientes roles:

- Director del SOC, que será cubierto por el Jefe del Departamento de Ingeniería de Siscotec.
- Administrador de Monitoreo de Seguridad, será desempeñado por el Jefe de Soporte de Siscotec.
- Analista de Monitoreo N1 o Analista Junior.
- Analista de Monitoreo N2 o Analista Senior.
- Ingeniero de Seguridad N2 o Ingeniero Senior.
- Ingeniero de Seguridad N3 o Ingeniero Master.

Estos últimos 4 roles también serán cubiertos por el personal técnico del área de soporte de Siscotec. Cabe señalar que actualmente están desempeñado esos roles.

g) Procesos y Procedimientos. Los procesos y procedimientos que se llevaran a cabo el SOC de Siscotec, son los típicos procesos y procedimientos que se desarrollan en un SOC, como son:

1) Administración de Eventos. En este proceso se desarrollan 4 procedimientos principales:

- Monitoreo de Eventos a cargo del Analista Junior N1, el cual generara un ticket de incidencia para poder analizarlo y darle una respuesta adecuada a la incidencia.
- Alertas Recurrentes, son trabajadas por el Analista Junior N1 quien las identifica, analiza y toma las acciones correctivas correspondientes.
- Administración de Casos, a cargo del Analista Senior N2, quien se encarga de analizar y resolver los casos de incidentes de seguridad de cierta complejidad.
- Base de Conocimiento, a cargo del Analista Senior N2, quien una vez resuelto el caso de incidentes de seguridad de cierta

complejidad, procederá a registrar la documentación del caso, en las etapas de presentación, análisis y solución.

- 2) Administración de Incidencias, este proceso se ejecuta bajo la responsabilidad del Administrador de Monitoreo de Seguridad en coordinación del Director del SOC.
- 3) Administración de Problemas, está a cargo de los Ingenieros de Seguridad N2 y N3 y consiste en investigar y determinar la causa de origen y las condiciones en que se dio el incidente, a efectos de señalar los defectos que existen en los equipos o en las configuraciones de los mismos.

3º Etapa: La tercera etapa corresponde a la construcción

- a) En lo referente a la infraestructura de Red, para la segmentación de red LAN se empleara un Switch de Capa 3 o Multicapa que nos va a permitir multiplicar los puertos, pero de una forma cableada y segura; y para los conmutadores de acceso se usara un Switch de Capa 2.
- b) En lo relativo a la seguridad de la red, se instalara un equipo cortafuego perimetral, el acceso a internet se hará mediante un web proxy, existirá 3 zonas de seguridad, en los cuales se empleara un sistema de prevención de intrusos. Así mismo se empleará reglas de control de acceso a la red, archivos, equipos, servicios, etc.
- c) En relación a los sistemas, se recomienda la utilización de Windows Server 2012 a 2013 y con relación a los equipos de los usuarios, se debe deshabilitar los software innecesarios, todos deben contar con un antivirus (el mismo antivirus para todos los equipos).

4º Etapa: La cuarta etapa corresponde a la operación. Existen cuatro procedimientos básicos que debe de ejecutar el SOC:

1. Monitoreo de Eventos. Todos los eventos que se generen deben ser enviados al Sistema de Gestión de Eventos e Información de Seguridad (SIEM), quien los relaciona y otorga una prioridad bajo ciertas reglas preestablecidas, automáticamente se establece una alerta y se notifica a los Analistas del SOC. La alerta de seguridad, también puede ser notificada por

los mismos usuarios a los Analistas del SOC a través de correo electrónico, teléfono, mensajería instantánea y el analista se encarga de registrarlos en el SIEM.

2. Alertas Recurrentes y Clasificación. Aperturada y registrada la alerta el Analista N1 del SOC, procede a investigar y recopilar todo tipo de información relacionada a la alerta como: flujo de tráfico, direcciones IP, origen y destino, usuarios asociados, bitácoras de acceso tanto lógico como físico, sistemas afectados, etc. Si considera necesario se contacta con el usuario para recopilar información adicional.

Con toda la información recopilada procede a clasificar la alerta, asignándole una prioridad que puede ser como baja = nivel 0 y como alta = nivel 1.

Las alertas clasificadas como bajo = 0 serán resueltas y documentadas por el Analista N1 de turno y las alertas clasificadas como alta = 1 serán transferidas al Analista N2 para que proceda a analizarlas y sean resueltas y documentadas.

3. Administración de Casos, cuando una alerta es clasificada como alta = 1, el analista N2 hace uso del Sistema de Administración de Incidentes y genera un reporte de incidente que se adjunta a la carpeta generada por el analista N1 con toda la información recopilada. Si el analista N2 puede resolver el caso procede a comunicar la solución, de lo contrario notifica a los Ingenieros de Seguridad N2 y N3 para que precedan a su análisis y solución.
4. Base de Conocimiento y Seguimiento, se debe efectuar un seguimiento constante de los casos y comunicar al administrador del servicio del estado en que se encuentra.

Para verificar si Siscotec del Perú SAC cuenta con los equipos y medios necesarios para implementar un SOC, se empleó la lista de cotejo denominada Implementación del SOC (ver anexo N° 9) la cual después de su proceso arrojo que, de los 17 aspectos o factores a verificar, se comprobó que cuentan con 9 factores y 8 les faltaría cumplir, los mismos que no involucrarían mayores gastos (ver anexo N° 18):

Los factores con los que cuentan son:

1. Oficina para el Administrador del SOC equipada.
2. Sala de Conferencia equipada con el mobiliario necesario.
3. Espacios de trabajos, mínimo 6.
4. Infraestructura de Red.
5. Mecanismos de Seguridad.
6. Sistemas Operativos.
7. Sistemas de Administración de Tickets.
8. Administración de Vulnerabilidades.
9. Personal que estará a cargo del SOC.

Los factores que les faltaría implementar son:

1. Sala de Monitoreo para alojar al menos 6 espacios de trabajos.
2. Data center con los elementos necesarios del mismo.
3. Acceso a la Sala de Monitoreo restringido, solamente al personal autorizado.
4. Bitácora de registros de acceso controlado.
5. Sistema de Cámaras de Monitoreo (Con grabación continua) de Circuito Cerrado.
6. Cuenta con material a prueba de sonidos.
7. Almacenamiento.
8. Generación y Recolección de Eventos de Seguridad.

IV CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

De la evaluación de los resultados del servicio de atención que se brinda a través de la plataforma de seguridad de la información de la empresa Siscotec del Perú S.A.C., podemos concluir que dicha empresa actualmente no cuenta con SOC implementado y que brinda el servicio de implementación y soporte a soluciones de seguridad de información y redes de a través de un sistema web de emisión de Tickets publicado en modalidad 24x7x365. Este servicio no satisface plenamente los requerimientos del cliente, debido a que las incidencias presentadas no son detectadas inicialmente por el cliente y que la prioridad de atención es determinada por el usuario de acuerdo a su criterio y porque el tiempo de atención de solución por el sistema de tickets es alto.

Del diagnóstico de los resultados del servicio de atención que se brinda a través del demo de un SOC, se concluye que, en el sistema de Demo SOC, el 100% de los casos fue detectado y reportado, a diferencia del sistema de tickets en cual el 34% de los casos de las incidencias presentadas no son detectadas inicialmente por el cliente, hecho que demostraría una mayor eficiencia de seguridad en la información si se cuenta con un SOC.

De los resultados de la encuesta de satisfacción de los servicios brindados por Siscotec sin SOC y con el demo del SOC, se concluye que los clientes de la empresa Siscotec del Perú SAC obtienen una mayor satisfacción en la atención de sus casos de incidencias y requerimientos cuando han sido atendidos con el Demo SOC que con el sistema de ticket, tanto en lo que se refiere al tiempo empleado en su solución como en la calidad brindada, Asimismo el nivel de eficiencia del servicio prestado, se elevaría al 100%, al solucionarse la incidencia y/o requerimiento en la primera atención, ya que de esta forma, el tiempo de reacción es más rápido que cuando se brinda el servicio a través del sistema de ticket, toda vez que el proceso sería en tiempo real.

Finalmente se concluye que la propuesta de implementación de un SOC basado en etapas, en la empresa Siscotec del Perú SAC, es factible y viable, toda vez que cuenta con los equipos y medios necesarios para implementar un SOC y que los ocho (8) factores que les faltaría cumplir no involucrarían mayores gastos. Económicamente podemos decir que, si bien es cierto que el costo de implementación del SOC es alto, este se puede recuperar muy pronto con la adquisición de nuevos clientes, toda vez que el nivel de satisfacción de los actuales clientes se eleva al 100% y el prestigio de la empresa crecería.

4.2. Recomendaciones

En el sistema web actual de emisión de Tickets, la empresa Siscotec debe reforzar su accionar a efectos de que las incidencias presentadas sean detectadas y atendidas en un menor tiempo de atención de solución.

Dado que el presente trabajo estuvo limitado a analizar el tiempo y solución otorgado a las incidencias y requerimientos de algunos clientes de la empresa Siscotec del Perú SAC comparando el sistema de tickets con el Demo SOC, en una investigación a futuro, ya no se debe utilizar un Demo sino de un sistema SOC debidamente implementado y operativo.

Para saber con mayor precisión el nivel de satisfacción de los servicios brindados por Siscotec se debe crear de un contenido WEB especialmente vinculada al SOC, para dar a conocer los resultados de los incidentes de seguridad más relevantes en tiempo real y realizar una encuesta de satisfacción en línea.

La empresa Siscotec del Perú S.A.C., cuenta con la mayoría de factores técnicos necesarios para implementar un SOC en sus instalaciones, por lo que debe completar con implementar los 8 factores que le faltan cumplir para contar con su propio SOC.

REFERENCIAS

- Alexander, A. (2012). *Diseño de un Sistema de Gestión de Seguridad de Información*. Segunda Edición. Colombia. Alfaomega.
- Barrantes, C. & Hugo, J. (2012), *Diseño e implementación de un sistema de gestión de seguridad de información en procesos tecnológicos*. Universidad de San Martín de Porres, Lima, Perú.
- Blog LinkedIn (2017). *Centros de Operaciones de Seguridad (SOC) - Una Necesidad Crítica Indispensable*. Recuperado de <https://www.linkedin.com/pulse/centros-de-operaciones-seguridad-soc-una-necesidad-critica>.
- Blog ManageEngine, (2014). *Gestión de Incidentes*. Recuperado de <https://manageengine.com.mx/blog-me-post/gestion-de-incidentes>.
- Blog Universidad de Barcelona (2018). *Seguridad de Información, Un conocimiento imprescindible*. Recuperado de <https://www.obs-edu.com/int/blog-investigacion/sistemas/seguridad-de-la-informacion-un-conocimiento-imprescindible>.
- Camelo, L. (2010). *Seguridad de la Información en Colombia. Marco Normativo (Normas y políticas) de un SGSI* Recuperado de: seguridadinformacioncolombia.blogspot.com.co/2010/03/marco-normativo-normas-y-politicas-de.html.
- Carrillo H. (2008). *Gestión de Incidentes aplicando ITIL en una compañía de telecomunicaciones Contact Center*. Universidad Nacional Mayor de San Marcos, Lima, Perú.
- Cazemier, J., Overbeek, & Peters, L. (2004). *Best practice for Security Management. Office of Government Commerce: ITIL Services*. Londres, Reino Unido, The Stationery Office/Tso.
- Gómez A. (2011). *Enciclopedia de la Seguridad Informática*. Madrid, España: Alfaomega RA- MA.
- Gonzales N. (2017) *El Ingeniero Y El Desarrollo De Los Negocios: Una Visión Práctica*, Estados Unidos; Palibrio.

- Kolthof, A., Jong de, A., Pieper, M., Tjassing, R., Van Der Veen, A., & Verheijen, T. (2008). *Gestión del Servicio Basada en ITIL® V3*. New York Estados Unidos: Van Haren Publishing.
- Montemayor, V. (2018), *Modelo de Implementación y Operación de un Security Operation Center a Partir de sus Procesos Específicos y Basado en ITIL- Edición Única*. Tecnológico de Monterrey, Monterrey, México.
- Morales, C., Moreno O. & Ortigoza J. (2014), *Propuesta de un Modelo de Centro de Operaciones de Seguridad (SOC) para Fuerza Aérea Colombiana*. Universidad Piloto de Colombia, Bogotá, Colombia.
- Muniz Joseph, Alfardan Nadhem, McIntyre Gary. Security Operations Center: Buiding, Operating, and Maintaining your SOC. Estados Unidos: Ciscopress, 2015.
- Nathans, David. Designing and Building a SOC. Estados Unidos: Syngress, 2015.
- O'Brien, J. & Marakas, G. (2006). *Sistemas de información gerencial*. Mexico, Mexico, Editorial Mc Graw Hill.
- Pacheco, F. (2010). *La importancia de un SGSI*. Recuperado de www.welivesecurity.com/la-es/2010/09/10/la-importancia-de-un-sgsi/.
- Universidad Internacional de Valencia. Lo que debes saber si quieres estudiar seguridad informática. España. Editorial de la Universidad Internacional de Valencia, 2018
- Vanguardia.com. (2016). *¿Qué es un SOC y que puede hacer por su empresa?*. Recuperado de <https://www.vanguardia.com/mundo/tecnologia/351799-que-es-un-soc-y-que-puede-hacer-por-su-empresa>.
- Vásquez, G. (2016). *Propuesta de modelos de implementación y gestión para un centro de operaciones de seguridad (SOC)*. Instituto Politécnico Nacional, México, México.
- Universidad Internacional de Valencia (2018). *Lo que debes saber si quieres estudiar informática*. Recuperado de <https://www.universidadviu.com/tres-tipos-seguridad-informatica-debes-conocer/>.

Anexo N° 2

Reporte de incidencias vía correo corporativo

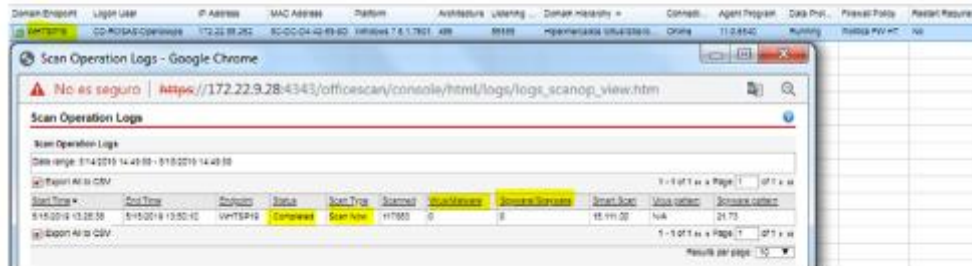
miércoles 15/05/2019 02:52 p.m.
HC Hurtado Christian (Externo)
 AV TCK:ALA39724 - Malware Infection Match R:Bajo - Abierto

Para Claudio Saavedra

CC SOC Falabella; Rafael A Arispe Z; Juan Contreras Muñoz; Seguridad y Comunicaciones Perú; 'soporte'; Seguridad Informática Perú; Soporte Peru;

Hola Claudio;

Favor de cerrar el caso el equipo no registra alertas de virus.



Saludos;

Christian J. Hurtado S.
 INGENIERO DE SOPORTE
 christianhurtado@siscotec.com
 (+51) 989 615 886
 (+51) 226 5483
 christianjhs
 www.siscotec.com

martes 14/05/2019 11:01 a.m.
HC Hurtado Christian (Externo)
 ticket 5206408 - RE: Requisitos tecnológicos

Para De La Cruz Cecilia (Externo)

CC PE_SEGURIDAD_ENDPOINT; Chuchon Angel; Soporte Peru; Juan Manuel Araoz Baca; Chuchon Angel; PE_SEGURIDAD_ENDPOINT

Buenos días;

Para informar que se agrego a la lista blanca el dominio y cuentas de correo indicados; así como el registro de las IPs en la lista de aprobados.

Saludos;

Christian J. Hurtado S.
 INGENIERO DE SOPORTE
 christianhurtado@siscotec.com
 (+51) 989 615 886
 (+51) 226 5483
 christianjhs
 www.siscotec.com

Anexo N° 3

Registro de logs de la consola antivirus de cada cliente

The screenshot shows the ITRAD OfficeScan console interface. The main window displays a list of detected threats under the heading "Data Lake Protection Logs". The table contains the following columns: ID, Date, File Name, Virus Name, File Path, Action, Status, Location, and Action. The table lists several detected threats, including:

ID	Date	File Name	Virus Name	File Path	Action	Status	Location	Action
1770274	21/08/21	IRMSA.MSI	Ransomware:Win32/IRMSA.MSI	\\172.22.22.100\...	Quarantine	Quarantined	C:\Program Files\...	Success
1770275	21/08/21	IRMSA.MSI	Ransomware:Win32/IRMSA.MSI	\\172.22.22.100\...	Quarantine	Quarantined	C:\Program Files\...	Success
1770276	21/08/21	IRMSA.MSI	Ransomware:Win32/IRMSA.MSI	\\172.22.22.100\...	Quarantine	Quarantined	C:\Program Files\...	Success
1770277	21/08/21	IRMSA.MSI	Ransomware:Win32/IRMSA.MSI	\\172.22.22.100\...	Quarantine	Quarantined	C:\Program Files\...	Success
1770278	21/08/21	IRMSA.MSI	Ransomware:Win32/IRMSA.MSI	\\172.22.22.100\...	Quarantine	Quarantined	C:\Program Files\...	Success
1770279	21/08/21	IRMSA.MSI	Ransomware:Win32/IRMSA.MSI	\\172.22.22.100\...	Quarantine	Quarantined	C:\Program Files\...	Success
1770280	21/08/21	IRMSA.MSI	Ransomware:Win32/IRMSA.MSI	\\172.22.22.100\...	Quarantine	Quarantined	C:\Program Files\...	Success
1770281	21/08/21	IRMSA.MSI	Ransomware:Win32/IRMSA.MSI	\\172.22.22.100\...	Quarantine	Quarantined	C:\Program Files\...	Success
1770282	21/08/21	IRMSA.MSI	Ransomware:Win32/IRMSA.MSI	\\172.22.22.100\...	Quarantine	Quarantined	C:\Program Files\...	Success
1770283	21/08/21	IRMSA.MSI	Ransomware:Win32/IRMSA.MSI	\\172.22.22.100\...	Quarantine	Quarantined	C:\Program Files\...	Success
1770284	21/08/21	IRMSA.MSI	Ransomware:Win32/IRMSA.MSI	\\172.22.22.100\...	Quarantine	Quarantined	C:\Program Files\...	Success
1770285	21/08/21	IRMSA.MSI	Ransomware:Win32/IRMSA.MSI	\\172.22.22.100\...	Quarantine	Quarantined	C:\Program Files\...	Success
1770286	21/08/21	IRMSA.MSI	Ransomware:Win32/IRMSA.MSI	\\172.22.22.100\...	Quarantine	Quarantined	C:\Program Files\...	Success
1770287	21/08/21	IRMSA.MSI	Ransomware:Win32/IRMSA.MSI	\\172.22.22.100\...	Quarantine	Quarantined	C:\Program Files\...	Success
1770288	21/08/21	IRMSA.MSI	Ransomware:Win32/IRMSA.MSI	\\172.22.22.100\...	Quarantine	Quarantined	C:\Program Files\...	Success
1770289	21/08/21	IRMSA.MSI	Ransomware:Win32/IRMSA.MSI	\\172.22.22.100\...	Quarantine	Quarantined	C:\Program Files\...	Success
1770290	21/08/21	IRMSA.MSI	Ransomware:Win32/IRMSA.MSI	\\172.22.22.100\...	Quarantine	Quarantined	C:\Program Files\...	Success

The screenshot shows a dashboard with three panels, each displaying a different type of data visualization related to antivirus performance. The panels are titled "SIPSAC REPORTES DE PELIGRO ELABORADO POR...", "SIPSAC REPORTES DE PELIGRO ELABORADO POR...", and "SIPSAC REPORTES DE PELIGRO ELABORADO POR...". Each panel includes a table of data and a line chart showing trends over time. The tables contain columns for "Fecha", "Cantidad", "Porcentaje", and "Estado". The charts show a general upward trend in the data over the period shown.

Anexo N° 4

Entrevista a realizar al Jefe del Departamento de Ingeniería y Soporte

ENTREVISTA



Nombre: Juan Manuel Araoz Baca
Cargo: Jefe del Departamento de Ingeniería y Soporte
Entidad: Siscotec del Perú S.A.C
Ubicación: Jr. Fray Luis de León N° 277 San Borja
Fecha: 12/07/2019

¿Cuál es el proceso más importante en el departamento de Ingeniería y soporte? Por qué

El proceso más importante actualmente es el control de incidencias de los sistemas corporativos que se encuentran en producción y cuya atención y solución son prioridad diaria del personal.

¿Cómo se realiza el proceso de control de incidencias?

Actualmente nuestra empresa se dedica a brindar servicio de implementación y soporte a soluciones de seguridad de información y redes a través de correo corporativo y de un sistema web de emisión de tickets publicado en modalidad 24x7x365. Sin embargo no se mantiene un historial de cómo se desarrollaron los casos y resoluciones. Adicionalmente para entregar mayor valor se pueden monitorear las consolas de las soluciones implementadas en nuestros clientes a través de conexiones remotas.

¿Usted cree que tal como se viene brindando el servicio, satisface los requerimientos del cliente? ¿De ser negativo explique cuál es la problemática que se presenta?

Pienso que no. Es complicado satisfacer por completo las necesidades del cliente y a la vez estar completamente seguros. Parte porque en muchos casos las necesidades del cliente no contemplan la seguridad o una seguridad adecuada y se prioriza sólo la continuidad de las operaciones. Unificar todas las soluciones de seguridad es un tema muy complejo y podría no ser conveniente para los clientes debido a que no todos los fabricantes destacan en todas las verticales de seguridad de la información o redes. Por lo que al proponer una arquitectura de seguridad y redes aplicada al usuario, es necesario involucrar a soluciones de distintos fabricantes y tener todas las habilidades de consultoría y técnicas necesarias para dicho fin.

Nuestro servicio al ser a medida, provee la mejor seguridad que podemos entregar con múltiples fabricantes de los cuales tenemos ingenieros certificados garantizando el soporte post-venta. Hemos visto necesario implementar un servicio de monitoreo en un ambiente específicamente dedicado a ello para lo cual estamos planificando la implementación de un Security Operation Center (SOC).

Por qué los clientes en muchos casos cuentan además con otros de soluciones de software de seguridad y surge la necesidad de centralizar la gestión de estos mismos en un sistema integral que monitoree y brinde alertas en tiempo real ante posibles

¿Ante esta situación de qué forma Siscotec está trabajando cuando se presenta una incidencia y/o problema de esa naturaleza?

Actualmente soportamos todas las incidencias de las soluciones que hemos ofrecido a nuestros clientes de las marcas que representamos. Entendíase por "soportar" el implementar satisfactoriamente una solución y el poder darle soporte post-implementación ante cambios, mal funcionamiento o upgrade de versiones, según se requiera. El proceso de seguir a un ingeniero de soporte lo realiza nuestro sistema web de tickets y lo administra y da seguimiento el Jefe del Departamento de Soporte que mantiene reuniones semanales con los ingenieros de soporte para no disminuir el tiempo de resolución de los casos que se atienden.

Actualmente Siscotec a través del departamento de Soporte designa un ingeniero para cada empresa y/o cliente que hayan contratado el servicio de administración y monitoreo de las conexiones antivirus y antispam, pero no monitoreamos los otros softwares de seguridad de los clientes.

¿Cuál es el tiempo de respuesta para la atención de incidencias reportadas por sus clientes?

El tiempo de respuesta para la atención de incidencia es S1= Crítica (30 Minutos), S2= Alta (1 Hora), S3= Normal (4 Horas), S4= Baja (8 Horas). Es importante mencionar que existen casos o incidencias de un nivel de criticidad crítica y alta que son atendidas fuera del tiempo del servicio estimado(SLA).

¿Cómo definen los niveles de criticidad?

S1 – Crítica: Incidente o defecto muy serio, problema y/o disturbio en el sistema, que está causando que el sistema quede totalmente fuera de servicio, severamente degradado o continuamente fuera de servicio y que puede estar ocasionando: Pérdida de servicio, rendimiento muy degradado del sistema, pérdida de información.

S2 – Alta: Defecto serio, problema y/o disturbio en el sistema que está causando o que es probable que cause un incidente, interrupciones recurrentes, una degradación en el rendimiento, una degradación en el servicio o una pérdida de capacidad importante. Este serio defecto podría también resultar en fallos que impidan la adecuada operación y mantenimiento o que resulte en una baja de rendimiento del Sistema tal que ocasione reclamos de usuarios.

S3 – Normal: Defecto, problema, o disturbio menor en el sistema que no afecta el rendimiento, el servicio o la operación y mantenimiento.

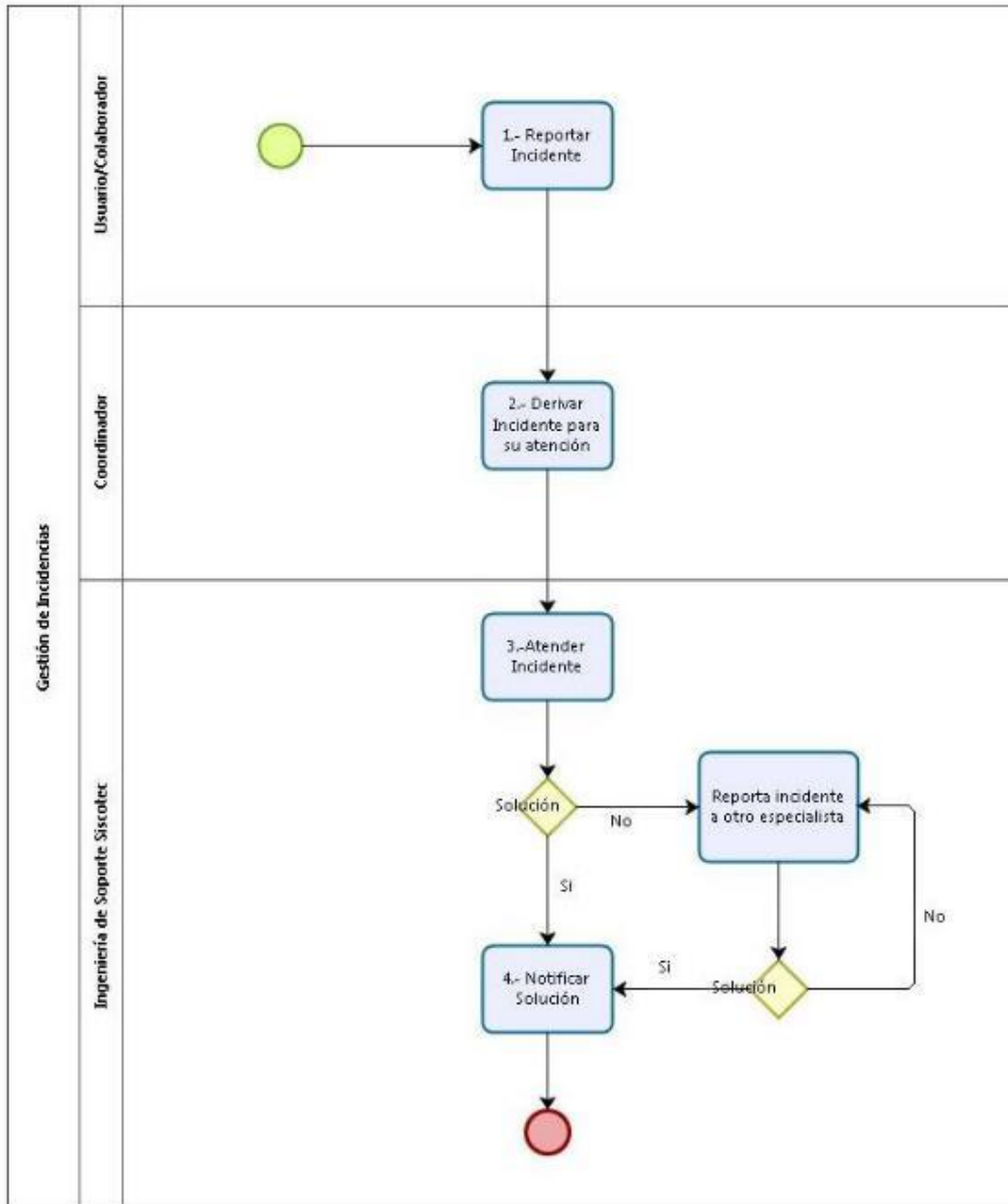
S4 – Baja: Este tipo de severidad está conformado por determinadas acciones de control básico, tales como consultas, planeación de algún cambio, etc.


Jefe del departamento de soporte


Ingeniero de Soporte

Anexo N° 5

Diagrama de Flujo de la gestión de incidencias



Anexo N° 7


Ficha de observación, registro de casos no reportados del Demo SOC.



FICHA DE CASOS NO REPORTADOS DEMO SOC

Item	Medio	Tipo de Caso	Negocio	Plataforma	Tipo de incidencia	Nivel de Prioridad	Usuario Destinatario	Asunto	Fecha de Caso	Mes de creación	Hora de inicio de la atención	Hora de término de la atención	Estado Final	SLA Solución
1														
2														
3														
4														
5														
6														
7														
8														

Anexo N° 8
Cuestionario de la encuesta.

 **siscotec**

Nro:

ENCUESTA DE SASTIFACCIÓN (SIN SOC)

Usuario :

Empresa :

Tipo de Caso :

P1 ¿Cómo califica el tiempo utilizado para la solución del incidente y/o requerimiento con el sistema actual de Siscotec?

Excelente Muy Bueno Bueno Regular Deficiente

P2 ¿Cómo fue la calidad de la atención recibida del personal de Siscotec?

Excelente Muy Bueno Bueno Regular Deficiente

P3 ¿El servicio brindado por el personal de Siscotec, solucionó su incidencia y/o requerimiento en la primera atención?

Si No

P4 ¿La incidencia fue reportado por usted?

Si No

SISCOTEC DEL PERU S.A.C.

.....
Angélica Carrión Quirós Garces
DNI: 45922315
Representante Legal


.....
LARRY BARRETO
LINARES BARRETO
INGENIERO
DE COMPUTACION Y SISTEMAS
Reg. CIP N° 160551



Nro:

ENCUESTA DE SASTIFACCIÓN (CON SOC)

Usuario :

Empresa :

Tipo de Caso :

P1 ¿Cómo califica el tiempo utilizado para la solución del incidente y/o requerimiento con el sistema actual de Siscotec?

Excelente Muy Bueno Bueno Regular Deficiente

P2 ¿Cómo fue la calidad de la atención recibida del personal de Siscotec?

Excelente Muy Bueno Bueno Regular Deficiente

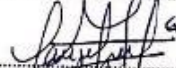
P3 ¿El servicio brindado por el personal de Siscotec, solucionó su incidencia y/o requerimiento en la primera atención?

Si No

P4 ¿La incidencia fue reportado por usted?

Si No

SISCOTEC DEL PERU S.A.C.


Angela del Carmen Quiroz Garcés
DNI: 45922319
Representante Legal


LARRY MANUEL
LINARES BARRETO
INGENIERO
DE COMPUTACION Y SISTEMAS
Reg. CIP Nº 180551

Anexo N° 9

Lista de cotejo de Implementación del SOC

LISTA DE COTEJO IMPLEMENTACIÓN DEL SOC

APECTO O FACTOR	SI	NO
Sala de Monitoreo equipada para alojar al menos 6 espacios de trabajos		
Sala de Conferencia equipada con el mobiliario necesario		
Centro de Datos		
Bitácora de registros de acceso controlado		
Sistema de Cámaras de Monitoreo (Con grabación continua) de Circuito Cerrado		
Cuenta con material a prueba de sonidos		
Espacios de trabajos, mínimo 6		
Infraestructura de Red		
Mecanismos de Seguridad		
Software Licenciado		
Almacenamiento		
Sistemas de Administración de Tickets		
Sistemas de Comunicación		
Generación y Recolección de Eventos de Seguridad		
Administración de Vulnerabilidades		
Personal que estará a cargo del SOC		

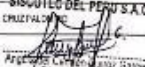
Anexo N° 10

Ficha de observación, reporte del sistema web de tickets debidamente firmada y sellada por representantes de la empresa Siscotec del Perú SAC.



REPORTES DE CASOS ATENDIDO A TRAVES DEL SISTEMA WEB DE TICKETS

Ticket Number	Ticket Type	Opening Date	Solution Date	Support Group	Analyst	Category Level 1	Category Level 2	Category Level 3	Affected User	SLA Solution	Priority
479185	Incidente	03/01/2019 12:21	15/01/2019	Seguridad Endpoint	Christian Hurtado	Banco F.	Oficina	Final	OSORIO ALVARO PERLA ANGELO	Green	Critical
481143	Incidente	02/02/2019 17:42	06/02/2019	Seguridad Endpoint	Christian Hurtado	H. Tallas	Oficina	Final	JUAREZ ANTONIA GISELLA	Green	Critical
483962	Requerimiento	04/02/2019 13:01	03/03/2019	Seguridad Endpoint	Christian Hurtado	Banco F.	Oficina	Final	LECCA ANGELO MELISSA LISETH	Green	Medium
485951	Requerimiento	04/02/2019 13:01	03/03/2019	Seguridad Endpoint	Christian Hurtado	Banco F.	Oficina	Final	LECCA ANGELO MELISSA LISETH	Green	Medium
496471	Requerimiento	13/02/2019 14:32	4/03/2019	Seguridad Endpoint	Christian Hurtado	Banco F.	Oficina	Final	LECCA ANGELO MELISSA LISETH	Green	Medium
527182	Incidente	22/02/2019 15:15	28/02/2019	Seguridad Endpoint	Christian Hurtado	Comodora de Seguros F.	Oficina	Final	CORONEL MEDRANO CARLOS FERNANDO	Green	Critical
524395	Requerimiento	viernes 13/02/2019 16:16	13/02/2019	Seguridad Endpoint	Christian Hurtado	Sig. F.	Oficina	Final	LUJO NEMANUEL ARTURO	Green	Medium
538253	Requerimiento	viernes 27/02/2019 09:10	27/02/2019	Seguridad Endpoint	Christian Hurtado	H. Tallas	Oficina	Final	Dickson Angel	Green	Medium
557473	Requerimiento	viene 08/02/2019 13:38	30/05/2019	Seguridad Endpoint	Christian Hurtado	Comodora de Seguros F.	Oficina	Final	FIGUEROA REYNOSO FERNANDO	Green	Medium
572229	Requerimiento	viene 11/02/2019 10:08	11/02/2019	Seguridad Endpoint	Christian Hurtado	Comodora de Seguros F.	Oficina	Final	Figueroa Fernando	Green	Medium
570704	Requerimiento	viene 11/02/2019 11:21	11/02/2019	Seguridad Endpoint	Christian Hurtado	Banco F.	Oficina	Final	ALVARO JHO CYRILAVANIA@bancoafibella.com.pe	Green	Medium
574712	Requerimiento	viene 11/02/2019 10:41	21/02/2019	Seguridad Endpoint	Christian Hurtado	Sig. F.	Oficina	Final	Manuel Palomares	Green	Medium
498121	Incidente	28/02/2019 12:24	28/02/2019	Seguridad Endpoint	Christian Hurtado	Banco F.	Oficina	Virus Malware	POLO COSTILLA EDUARDO	Green	Critical
478384	Incidente	11/03/2019 18:25	11/03/2019	Seguridad Endpoint	Christian Hurtado	Banco F.	Oficina	Virus Malware	SARAY ROSA VERONICA PATRICIA	Green	Critical
528436	Incidente	22/03/2019 13:53	22/03/2019	Seguridad Endpoint	Christian Hurtado	H. Tallas	Oficina	Virus Malware	CELENA DE LA CRUZ PALOMINO	Green	Critical
528145	Incidente	23/03/2019 11:33	23/03/2019	Seguridad Endpoint	Christian Hurtado	Ofic.	Oficina	Virus Malware	CELENA DE LA CRUZ PALOMINO	Green	Critical
522524	Incidente	31/03/2019 17:44	31/03/2019	Seguridad Endpoint	Christian Hurtado	Carac. Center	Oficina	Virus Malware	CELENA DE LA CRUZ PALOMINO	Green	Critical
527431	Incidente	31/03/2019 13:01	31/03/2019	Seguridad Endpoint	Christian Hurtado	Carac. Center	Oficina	Virus Malware	CELENA DE LA CRUZ PALOMINO	Green	Critical
525959	Incidente	28/03/2019 10:02	28/03/2019	Seguridad Endpoint	Christian Hurtado	Sig. F.	Oficina	Virus Malware	CELENA DE LA CRUZ PALOMINO	Green	Critical
527246	Incidente	31/03/2019 17:40	31/03/2019	Seguridad Endpoint	Christian Hurtado	H. Tallas	Oficina	Virus Malware	CELENA DE LA CRUZ PALOMINO	Green	Critical
527045	Incidente	31/03/2019 17:38	31/03/2019	Seguridad Endpoint	Christian Hurtado	Sig. F.	Oficina	Virus Malware	CELENA DE LA CRUZ PALOMINO	Green	Critical
527046	Incidente	31/03/2019 17:36	31/03/2019	Seguridad Endpoint	Christian Hurtado	Center Center	Oficina	Virus Malware	CELENA DE LA CRUZ PALOMINO	Green	Critical
517235	Incidente	14/03/2019 17:54	04/03/2019	Seguridad Endpoint	Christian Hurtado	Sig. F.	Oficina	Virus Malware	CELENA DE LA CRUZ PALOMINO	Green	Critical


SISCOTEC DEL PERU S.A.C.
 LINARES MARROTO
 INGENIERO
 DE COMPUTACION Y SISTEMAS
 Reg. CIP N° 181551



REPORTE DE CASOS ATENDIDO A TRAVES DEL SISTEMA WEB DE TICKETS

52238	Incidente	31/05/2019 11:52	31/05/2019	Seguridad Endpoint	Christian Hurtado	H. Torres	Oficinas	Viva México	CEOLA DE LA CRUZ PALOMINO	Green	Critical
52232	Incidente	31/05/2019 11:47	31/05/2019	Seguridad Endpoint	Christian Hurtado	H. Torres	Oficinas	Viva México	CEOLA DE LA CRUZ PALOMINO	Green	Critical
52235	Incidente	31/05/2019 11:42	31/05/2019	Seguridad Endpoint	Christian Hurtado	H. Torres	Oficinas	Viva México	CEOLA DE LA CRUZ PALOMINO	Green	Critical
52230	Incidente	31/05/2019 11:37	31/05/2019	Seguridad Endpoint	Christian Hurtado	Orlando Castro	Oficinas	Viva México	CEOLA DE LA CRUZ PALOMINO	Green	Critical
52220	Incidente	31/05/2019 11:32	31/05/2019	Seguridad Endpoint	Christian Hurtado	Silvio	Oficinas	Viva México	CEOLA DE LA CRUZ PALOMINO	Green	Critical
525632	Incidente	28/05/2019 19:12	28/05/2019	Seguridad Endpoint	Christian Hurtado	H. Torres	Oficinas	Viva México	CEOLA DE LA CRUZ PALOMINO	Green	Critical
525602	Incidente	28/05/2019 18:13	28/05/2019	Seguridad Endpoint	Christian Hurtado	H. Torres	Oficinas	Viva México	CEOLA DE LA CRUZ PALOMINO	Green	Critical
525572	Incidente	28/05/2019 18:15	28/05/2019	Seguridad Endpoint	Christian Hurtado	Saga F.	Oficinas	Viva México	CEOLA DE LA CRUZ PALOMINO	Green	Critical
525515	Incidente	28/05/2019 11:17	28/05/2019	Seguridad Endpoint	Christian Hurtado	Saga F.	Oficinas	Viva México	ANGEL MARTIN CHILHORN LUGRE	Green	Critical
525503	Incidente	28/05/2019 11:12	28/05/2019	Seguridad Endpoint	Christian Hurtado	Saga F.	Oficinas	Viva México	CEOLA DE LA CRUZ PALOMINO	Green	Critical
525481	Incidente	28/05/2019 19:18	28/05/2019	Seguridad Endpoint	Christian Hurtado	H. Torres	Oficinas	Viva México	CEOLA DE LA CRUZ PALOMINO	Green	Critical
525436	Incidente	28/05/2019 13:15	28/05/2019	Seguridad Endpoint	Christian Hurtado	Silvio	Oficinas	Viva México	CEOLA DE LA CRUZ PALOMINO	Green	Critical
525412	Incidente	22/05/2019 13:53	22/05/2019	Seguridad Endpoint	Christian Hurtado	Silvio	Oficinas	Viva México	CEOLA DE LA CRUZ PALOMINO	Green	Critical
525322	Incidente	14/05/2019 15:53	14/05/2019	Seguridad Endpoint	Christian Hurtado	Silvio	Oficinas	Viva México	CEOLA DE LA CRUZ PALOMINO	Green	Critical
525298	Incidente	14/05/2019 15:23	14/05/2019	Seguridad Endpoint	Christian Hurtado	Silvio	Oficinas	Viva México	ANGEL MARTIN CHILHORN LUGRE	Green	Critical
525257	Incidente	14/05/2019 15:42	14/05/2019	Seguridad Endpoint	Christian Hurtado	Silvio	Oficinas	Viva México	CEOLA DE LA CRUZ PALOMINO	Green	Critical
5251742	Requerimiento	15/05/2019 13:32	12/05/2019	Seguridad Endpoint	Christian Hurtado	Saga F.	Oficinas	Viva México	GABRIEL ALBERTO BONDARRIA PONZAS	Green	Low
515226	Incidente	05/05/2019 13:41	05/05/2019	Seguridad Endpoint	Christian Hurtado	Saga F.	Oficinas	Viva México	CEOLA DE LA CRUZ PALOMINO	Green	Critical
5151425	Incidente	05/05/2019 11:31	05/05/2019	Seguridad Endpoint	Christian Hurtado	Orlando Castro	Oficinas	Viva México	CEOLA DE LA CRUZ PALOMINO	Green	Critical
517320	Incidente	05/05/2019 17:51	05/05/2019	Seguridad Endpoint	Christian Hurtado	H. Torres	Oficinas	Viva México	CEOLA DE LA CRUZ PALOMINO	Green	Critical
517375	Incidente	05/05/2019 17:46	05/05/2019	Seguridad Endpoint	Christian Hurtado	H. Torres	Oficinas	Viva México	CEOLA DE LA CRUZ PALOMINO	Green	Critical
517358	Incidente	05/05/2019 17:34	05/05/2019	Seguridad Endpoint	Christian Hurtado	Silvio	Oficinas	Viva México	CEOLA DE LA CRUZ PALOMINO	Green	Critical
517334	Incidente	05/05/2019 17:31	05/05/2019	Seguridad Endpoint	Christian Hurtado	Saga F.	Oficinas	Viva México	CEOLA DE LA CRUZ PALOMINO	Green	Critical
526784	Incidente	10/06/2019 21:44	10/06/2019	Seguridad Endpoint	Christian Hurtado	H. Torres	Oficinas	Viva México	CEOLA DE LA CRUZ PALOMINO	Green	Critical

SIGOTEC DELIVERY S.A.C.
 Aligned with the company's values
 P.O. Box 43827215
 Representación Legal

LIANES BARRETO
 INGENIERO
 DE COMPUTACION Y SISTEMAS
 Reg. CP Nº 182551



REPORTE DE CASOS ATENDIDO A TRAVES DEL SISTEMA WEB DE TICKETS

532851	Incidente	16/07/2018 12:25	5670018	Seguridad Encuentro	Directorio Usuarios	Sofar	Oficina	Victor Malave	SECRETARIA DE LA CRUZ PALOMBO	Open	Critical
532815	Incidente	16/07/2018 12:17	5670018	Seguridad Encuentro	Directorio Usuarios	Sofar	Oficina	Victor Malave	SECRETARIA DE LA CRUZ PALOMBO	Open	Critical
532743	Incidente	16/07/2018 12:34	1470018	Seguridad Encuentro	Directorio Usuarios	Carolina de Segura F.	Oficina	Victor Malave	ALICIA VILLALBA MACARONAN@fidelec.com	Open	Critical
532685	Incidente	16/07/2018 12:22	1470018	Seguridad Encuentro	Directorio Usuarios	Carolina de Segura F.	Oficina	Victor Malave	RODRIGUEZ VARGAS CAROLINA MACARONAN@fidelec.com	Open	Critical
532650	Incidente	16/07/2018 12:21	1470018	Seguridad Encuentro	Directorio Usuarios	Carolina de Segura F.	Oficina	Victor Malave	SECRETARIA DE LA CRUZ PALOMBO	Open	Critical
532576	Incidente	16/07/2018 12:32	1470018	Seguridad Encuentro	Directorio Usuarios	Carolina de Segura F.	Oficina	Victor Malave	AGUIAR VALENZUELA DE MUJICA MACARONAN@fidelec.com	Open	Critical
532517	Incidente	16/07/2018 12:26	1470018	Seguridad Encuentro	Directorio Usuarios	Carolina de Segura F.	Oficina	Victor Malave	RODRIGUEZ VARGAS CAROLINA MACARONAN@fidelec.com	Open	Critical
532513	Incidente	16/07/2018 12:07	1470018	Seguridad Encuentro	Directorio Usuarios	Carolina de Segura F.	Oficina	Victor Malave	RODRIGUEZ VARGAS CAROLINA MACARONAN@fidelec.com	Open	Critical
563771	Requerimiento	11/09/2018 11:59	11690018	Seguridad Encuentro	Directorio Usuarios	H. Toluca	Oficina	Victor Malave	CARLOS GUZMAN LOS LECHE ALBARRAN	Open	Low
572872	Incidente	28/10/2018 12:02	5960018	Seguridad Encuentro	Directorio Usuarios	H. Toluca	Oficina	Victor Malave	MATIAS APTEGA	Open	Critical
478275	Incidente	11/01/2019 12:22	11910018	Seguridad Encuentro	Directorio Usuarios	H. Toluca	Oficina	DUP	HUMBERTO MORALES MORALES	Open	Critical
493292	Requerimiento	21/01/2019 16:10	20190018	Seguridad Encuentro	Directorio Usuarios	Caro F.	Oficina	DUP	JAMINEZ ZURRO PAUL MARCO	Open	Critical
475437	Requerimiento	20/12/2018 22:52	26010018	Seguridad Encuentro	Directorio Usuarios	Caro F.	Oficina	DUP	AGUIAR ROMERO JUAN DAVID	Open	Critical
479180	Incidente	11/01/2019 23:15	11670018	Seguridad Encuentro	Directorio Usuarios	Caro F.	Oficina	DUP	WALTER OLIVERA CALVO MAGUI	Open	Critical
493496	Incidente	15/01/2019 17:50	19410018	Seguridad Encuentro	Directorio Usuarios	Caro F.	Oficina	DUP	CHANGA ALARCON MONICA DEBIA	Open	Critical
494259	Requerimiento	26/01/2019 13:47	26710018	Seguridad Encuentro	Directorio Usuarios	Caro F.	Oficina	DUP	RODRIGUEZ RODRIGUEZ OSCAR ORLANDO	Open	Critical
494346	Requerimiento	26/01/2019 18:12	27010018	Seguridad Encuentro	Directorio Usuarios	Caro F.	Oficina	DUP	SARLA LIPARIS JAZHRA ALVARADO	Open	Critical
497185	Incidente	27/01/2019 11:53	27410018	Seguridad Encuentro	Directorio Usuarios	F. Corporativo	Oficina	DUP	SILVANO RODRIGUEZ MARIELLA DELIA	Open	Critical
497018	Incidente	17/01/2019 12:48	17710018	Seguridad Encuentro	Directorio Usuarios	F. Corporativo	Oficina	DUP	PEREZ ACOSTA JORGE ANTONIO	Open	Critical
497013	Requerimiento	17/01/2019 12:35	17700018	Seguridad Encuentro	Directorio Usuarios	Caro F.	Oficina	DUP	FRANCISCA DELIA LUIS ENRIQUE	Open	Critical
497185	Incidente	16/01/2019 12:13	16610018	Seguridad Encuentro	Directorio Usuarios	Caro F.	Oficina	DUP	BEZAR PINO GUSTAVO	Open	Critical
498026	Requerimiento	15/01/2019 13:30	16510018	Seguridad Encuentro	Directorio Usuarios	Caro F.	Oficina	DUP	RODRIGUEZ RODRIGUEZ OSCAR ORLANDO	Open	Critical
498124	Incidente	15/01/2019 10:50	16510018	Seguridad Encuentro	Directorio Usuarios	H. Toluca	Oficina	DUP	ALICIA ESPINOZA JORDY ROYATO	Open	Critical
479225	Requerimiento	14/01/2019 14:14	22010018	Seguridad Encuentro	Directorio Usuarios	Vilma F.	Oficina	DUP	CARLOS ALBERTO ECHENARRA POLO	Open	Critical

SISOTEC DEL PERU S.A.C.

 Carlos Alberto Echenarra Polo

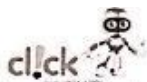
 Representante Legal

LINARES BALLESTER

 INGENIERO

 DE COMPUTACION Y SISTEMAS

 Reg. CIP Nº 18351



REPORTE DE CASOS ATENDIDO A TRAVES DEL SISTEMA WEB DE TICKETS

479598	Incidente	11/01/2019 18:03	19/01/2019	Seguridad Endpoint	Christian Huatazo	Saga F.	Oficoflex	DLP	CACICALTAM RAYO ENMA	Green	Critical
479599	Requerimiento	16/01/2019 18:53	18/01/2019	Seguridad Endpoint	Christian Huatazo	Saga F.	Oficoflex	DLP	Aguilar Rojas Luis Jaime	Green	Critical
479600	Incidente	20/01/2019 17:21	16/01/2019	Seguridad Endpoint	Christian Huatazo	Saga F.	Oficoflex	DLP	Manuel Valverde Galvez	Green	Critical
479596	Requerimiento	08/01/2019 13:22	07/01/2019	Seguridad Endpoint	Christian Huatazo	Saga F.	Oficoflex	DLP	JUAN JOSE RODRIGUEZ CHUMBRERA	Green	Critical
479594	Requerimiento	20/01/2019 13:11	07/01/2019	Seguridad Endpoint	Christian Huatazo	A. Talara	Oficoflex	DLP	GORDONA AGUIE DARAUNA	Green	Critical
479598	Requerimiento	07/01/2019 13:07	07/01/2019	Seguridad Endpoint	Christian Huatazo	F. Servicio Central	Oficoflex	DLP	Jorge Luis Villavicencio Flores	Green	Critical
479590	Requerimiento	07/01/2019 12:43	07/01/2019	Seguridad Endpoint	Christian Huatazo	RAMA F.	Oficoflex	DLP	GARCIA ALBERTO EDOUARDINA FOMARI	Green	Critical
479591	Incidente	20/01/2019 12:42	20/01/2019	Seguridad Endpoint	Christian Huatazo	F. Talara	Oficoflex	DLP	FLORES GARCONES LUIS HENRIQUE	Green	Critical
479597	Requerimiento	20/01/2019 14:25	20/01/2019	Seguridad Endpoint	Christian Huatazo	F. Corporativo	Oficoflex	DLP	LEONARDO GUTIERREZ VICTOR ALBERTO	Green	Critical
480285	Requerimiento	17/01/2019 17:38	14/01/2019	Seguridad Endpoint	Christian Huatazo	F. Talara	Oficoflex	DLP	Orlando Juan Melva Isabel Gonzalez	Green	Critical
481086	Incidente	20/01/2019 11:31	20/01/2019	Seguridad Endpoint	Christian Huatazo	Saga F.	Oficoflex	DLP	ALVARO DE LA CASAS LORIANA MARCELA	Green	Critical
480347	Incidente	05/01/2019 11:38	05/01/2019	Seguridad Endpoint	Christian Huatazo	F. Corporativo	Oficoflex	DLP	SALINAS RODRIGUEZ MARIELLA CELIA	Green	Critical
481042	Requerimiento	20/01/2019 14:58	20/01/2019	Seguridad Endpoint	Christian Huatazo	RAMA F.	Oficoflex	DLP	RODRIGUEZ RODRIGUEZ OSCAR ORLANDO	Yellow	Critical
484515	Requerimiento	28/01/2019 16:01	28/01/2019	Seguridad Endpoint	Christian Huatazo	Saga F.	Oficoflex	DLP	KOCHI JIMMY FERRANDO	Green	Critical
484796	Requerimiento	27/01/2019 18:17	28/01/2019	Seguridad Endpoint	Christian Huatazo	RAMA F.	Oficoflex	DLP	PEGO ARRAGUE MOLINA STEVEN	Green	Critical
485142	Requerimiento	23/01/2019 17:25	20/01/2019	Seguridad Endpoint	Christian Huatazo	RAMA F.	Oficoflex	DLP	RAMIREZ PICHAYQUEZ ALEJANDRO ALBERTO	Green	Critical
490426	Requerimiento	21/01/2019 13:45	21/01/2019	Seguridad Endpoint	Christian Huatazo	RAMA F.	Oficoflex	DLP	MURPHY WILSON MONICA ELENA	Green	Critical
490102	Requerimiento	14/01/2019 05:47	14/01/2019	Seguridad Endpoint	Christian Huatazo	Saga F.	Oficoflex	DLP	PEREZ DE SOLAR YOLA DIEGO IGNACIO JUAN H	Green	Critical
498691	Requerimiento	13/01/2019 20:16	13/01/2019	Seguridad Endpoint	Christian Huatazo	F. Talara	Oficoflex	DLP	TENICO GUTARRA ALBERTO ANAR	Green	Critical
492707	Requerimiento	13/01/2019 18:43	13/01/2019	Seguridad Endpoint	Christian Huatazo	Saga F.	Oficoflex	DLP	MEZA PASCUAL GUAYANO EZEQUIEL	Green	Critical
492112	Incidente	13/01/2019 15:25	13/01/2019	Seguridad Endpoint	Christian Huatazo	F. Corporativo	Oficoflex	DLP	FUENTES RAYRA EDUARDO MARTIN	Green	Critical
492507	Incidente	13/01/2019 14:35	13/01/2019	Seguridad Endpoint	Christian Huatazo	F. Talara	Oficoflex	DLP	RODRIGUEZ PORTUGAL SILVIA	Green	Critical
492849	Requerimiento	11/01/2019 17:31	11/01/2019	Seguridad Endpoint	Christian Huatazo	F. Talara	Oficoflex	DLP	SANCHEZ RISO AGUIRRE ALAN GUILLERMO	Green	Critical
493838	Requerimiento	11/01/2019 05:51	11/01/2019	Seguridad Endpoint	Christian Huatazo	F. Talara	Oficoflex	DLP	POYCE LEACONIA EDWIN VIDAL	Green	Critical

SISCOMTEC DEL PERU S.A.S.
 Av. Jorge Chávez 11000, Puerto Callao
 FON: 45832215
 Representante Legal

[Signature]
 LUIS MARCELO
 INGENIERO
 DE COMPUTACION Y SISTEMAS
 Reg. CIPAP 182951



REPORTE DE CASOS ATENDIDO A TRAVES DEL SISTEMA WEB DE TICKETS

483454	Requerimiento	19/02/2019 17:28	18/02/2019	Seguridad Endpoint	Orlando Hurtado	Sagua F.	Oficina	DLP	MOSQUERA MORA ELENA LISSET	Green	Critical
487732	Requerimiento	19/02/2019 13:22	20/02/2019	Seguridad Endpoint	Orlando Hurtado	Sagua F.	Oficina	DLP	SAVIGNON FERRARI MAFRA JINENA	Green	Critical
487601	Requerimiento	16/02/2019 20:20	16/02/2019	Seguridad Endpoint	Orlando Hurtado	Carolina de Sagua F.	Oficina	DLP	MARGOL VARESBREDA MAYUELA	Green	Critical
486534	Requerimiento	16/02/2019 14:11	16/02/2019	Seguridad Endpoint	Orlando Hurtado	H. Talca	Oficina	DLP	ROSA DE RABALA URIBE	Green	Critical
486196	Requerimiento	16/02/2019 13:43	16/02/2019	Seguridad Endpoint	Orlando Hurtado	Banco F.	Oficina	DLP	ALVARO SALAZAR ELDOROTH	Green	Critical
484150	Requerimiento	30/01/2019 08:57	16/02/2019	Seguridad Endpoint	Orlando Hurtado	Banco F.	Oficina	DLP	ESPANOLLO PALACIOS MILAGROS JACKLINE	Green	Critical
483782	Requerimiento	30/01/2019 10:28	16/02/2019	Seguridad Endpoint	Orlando Hurtado	Sagua F.	Oficina	DLP	RODRIGUEZ GONZALES EVELYN KATHERINE	Green	Critical
501271	Requerimiento	21/01/2019 13:53	21/02/2019	Seguridad Endpoint	Orlando Hurtado	Sagua F.	Oficina	DLP	RODRIGUEZ GONZALEZ ROSA MARTINA	Green	Critical
501430	Requerimiento	20/01/2019 16:35	20/02/2019	Seguridad Endpoint	Orlando Hurtado	Sagua F.	Oficina	DLP	COTRINA HERRERA ALBERTO MARCEL	Green	Critical
524846	Requerimiento	20/01/2019 23:54	20/02/2019	Seguridad Endpoint	Orlando Hurtado	H. Talca	Oficina	DLP	WOLTA VIDAL DANIA VERONICA	Yellow	Critical
530330	Requerimiento	17/02/2019 17:51	17/02/2019	Seguridad Endpoint	Orlando Hurtado	H. Talca	Oficina	DLP	CHOF COCKMELISSA YEN CARLA	Yellow	Critical
53175-4	Requerimiento	23/02/2019 15:47	26/02/2019	Seguridad Endpoint	Orlando Hurtado	Sagua F.	Oficina	DLP	HELAN GARCERAN JACIN WILBERT	Yellow	Critical
543795	Requerimiento	23/02/2019 15:45	26/02/2019	Seguridad Endpoint	Orlando Hurtado	Sagua F.	Oficina	DLP	NEIRA GARCERAN JACIN WILBERT	Yellow	Critical
546334	Requerimiento	20/02/2019 15:57	26/02/2019	Seguridad Endpoint	Orlando Hurtado	H. Talca	Oficina	DLP	SANCHEZ ELVAREZ OSCAR GIANTE	Green	Critical
534269	Requerimiento	20/02/2019 15:24	26/02/2019	Seguridad Endpoint	Orlando Hurtado	H. Talca	Oficina	DLP	CHAVEZ HORNOS MARCELA MIRA	Green	Critical
532012	Requerimiento	07/02/2019 16:17	26/02/2019	Seguridad Endpoint	Orlando Hurtado	Sagua F.	Oficina	DLP	LOPEZ CHILINGANO EDDY ALFONSO	Green	Critical
570510	Requerimiento	16/02/2019 18:03	23/02/2019	Seguridad Endpoint	Orlando Hurtado	Sagua F.	Oficina	DLP	LOPEZ CHILINGANO EDDY ALFONSO	Green	Critical
504201	Requerimiento	18/02/2019 14:04	19/02/2019	Seguridad Endpoint	Orlando Hurtado	H. Talca	Oficina	DLP	SANCHEZ SARMIENTO ALEJANDER ALBERTO	Green	Critical
496362	Requerimiento	14/02/2019 20:15	15/02/2019	Seguridad Endpoint	Orlando Hurtado	Sagua F.	Oficina	DLP	ORTECHO ZUCCHETTI LAURETTE ROSA	Green	Critical
494294	Requerimiento	14/02/2019 15:48	16/02/2019	Seguridad Endpoint	Orlando Hurtado	Sagua F.	Oficina	DLP	REQUENA SANCHEZ OSCAR DAVID	Green	Critical
492030	Requerimiento	13/02/2019 12:34	13/02/2019	Seguridad Endpoint	Orlando Hurtado	Sagua F.	Oficina	DLP	Sagua F. Talca - Talca	Green	Critical
491416	Requerimiento	11/02/2019 17:43	12/02/2019	Seguridad Endpoint	Orlando Hurtado	Sagua F.	Oficina	DLP	LIMBEZ LIZBETH PAOLA MARCELO	Green	Critical
491496	Requerimiento	08/02/2019 21:24	11/02/2019	Seguridad Endpoint	Orlando Hurtado	Compañía de Seguros S.	Oficina	DLP	HUMAR CASAVIROS	Green	Critical
487108	Requerimiento	04/02/2019 12:47	04/02/2019	Seguridad Endpoint	Orlando Hurtado	Banco F.	Oficina	DLP	GONZALEZ HUMAR HERRERA ESTHER	Green	Critical

JUAN CARLOS LLANES BARRETO

 INGENIERO

 DE COMPUTACION Y SISTEMAS

 Reg. CIP Nº 18001



REPORTE DE CASOS ATENDIDO A TRAVES DEL SISTEMA WEB DE TICKETS

508415	Requerimiento	16/02/19 12:49	16/02/19	Seguridad End-user	Christian Harado	Saga F.	OficinaSan	DLP	AGUILAR ULLUSHELBY FISSORA	Green	Critical
508404	Requerimiento	16/02/19 12:47	16/02/19	Seguridad End-user	Christian Harado	Saga F.	OficinaSan	DLP	AGUILAR ULLUSHELBY FISSORA	Red	Critical
508392	Requerimiento	16/02/19 12:32	16/02/19	Seguridad End-user	Christian Harado	Saga F.	OficinaSan	DLP	HEMELCO ESTEBAN ARY JOHANNA	Red	Critical
507828	Requerimiento	16/02/19 11:28	16/02/19	Seguridad End-user	Christian Harado	Saga F.	OficinaSan	DLP	SOLDADES HERMAN MERCEDES VICTORIA	Red	Critical
507818	Requerimiento	16/02/19 11:12	16/02/19	Seguridad End-user	Christian Harado	H. Torres	OficinaSan	DLP	SANABE ULLUS FRANCISCO	Red	Critical
506332	Requerimiento	16/02/19 10:21	16/02/19	Seguridad End-user	Christian Harado	Banco F.	OficinaSan	DLP	MARIPAN VELAZ MORA ELENA	Red	Critical
506215	Requerimiento	16/02/19 10:20	16/02/19	Seguridad End-user	Christian Harado	Comercio (o Seguros F.)	OficinaSan	DLP	Egura Ramos-Jesus David	Red	Critical
506127	Requerimiento	16/02/19 10:14	16/02/19	Seguridad End-user	Christian Harado	F. Contreras	OficinaSan	DLP	FLORES GARRAMBA ELIZABETH DORIS	Red	Critical
504718	Requerimiento	16/02/19 10:47	16/02/19	Seguridad End-user	Christian Harado	Saga F.	OficinaSan	DLP	MELIA DANIELA JON HLOBER	Red	Critical
511817	Requerimiento	16/02/19 11:30	16/02/19	Seguridad End-user	Christian Harado	Open Place	OficinaSan	DLP	MIRALBERTA GARMAN J2	Red	Critical
511805	Requerimiento	16/02/19 11:03	16/02/19	Seguridad End-user	Christian Harado	Banco F.	OficinaSan	DLP	MENDOZA MEGALYN JOHANNA CLODTE	Red	Critical
511814	Requerimiento	16/02/19 11:01	16/02/19	Seguridad End-user	Christian Harado	Saga F.	OficinaSan	DLP	LIDIANA CHIRIYANO EDY ALBIO	Red	Critical
511807	Requerimiento	16/02/19 10:29	16/02/19	Seguridad End-user	Christian Harado	Saga F.	OficinaSan	DLP	DE LA CRUZ PAVES LORDE OFAY	Green	Critical
511798	Requerimiento	16/02/19 10:40	16/02/19	Seguridad End-user	Christian Harado	Saga F.	OficinaSan	DLP	PEDRO CASANOVIA VICTOR MANUEL	Green	Critical
511713	Requerimiento	16/02/19 11:10	16/02/19	Seguridad End-user	Christian Harado	Saga F.	OficinaSan	DLP	SALDAS PAVES YELTON	Green	Critical
511791	Requerimiento	16/02/19 11:45	16/02/19	Seguridad End-user	Christian Harado	Saga F.	OficinaSan	DLP	MELIA DANIELA JON FRANCISCO	Green	Critical
511802	Requerimiento	16/02/19 11:21	16/02/19	Seguridad End-user	Christian Harado	Saga F.	OficinaSan	DLP	SOLDADES HERMAN MERCEDES VICTORIA	Green	Critical
511540	Incidente	11/02/19 10:34	11/02/19	Seguridad End-user	Christian Harado	H. Torres	OficinaSan	DLP	COCLA DE LA CRUZ PALOMBO	Green	Critical
526172	Requerimiento	20/02/19 11:51	20/02/19	Seguridad End-user	Christian Harado	Saga F.	OficinaSan	DLP	MURPHY SQUE VERANEMER ANIBERTO JAVIER	Green	Critical
526494	Incidente	20/02/19 18:43	20/02/19	Seguridad End-user	Christian Harado	H. Torres	OficinaSan	DLP	LEON JESUS ANTONIO MARIANO	Red	Critical
526347	Requerimiento	20/02/19 18:13	20/02/19	Seguridad End-user	Christian Harado	Saga F.	OficinaSan	DLP	MELIA DANIELA JON FRANCISCO	Yellow	Critical
522238	Requerimiento	17/02/19 14:57	17/02/19	Seguridad End-user	Christian Harado	Saga F.	OficinaSan	DLP	AGUILAR RODRIGUEZ MARCELO JESUS	Red	Critical
522136	Requerimiento	14/02/19 12:40	14/02/19	Seguridad End-user	Christian Harado	H. Torres	OficinaSan	DLP	MARCA CUELLAR FELICE	Red	Critical
522121	Requerimiento	13/02/19 11:30	13/02/19	Seguridad End-user	Christian Harado	Algor F.	OficinaSan	DLP	ORE LUAYZA FRANK SALVADO	Red	Critical

Juan Carlos Lopez

 Agente Operativo de Soporte Técnico

 CNI: 45472315

 Representante Legal

Juan Carlos Lopez

 INGENIERO

 INGENIERO

 DE COMPUTACION Y SISTEMAS

 Reg. CIPM 18691



REPORTE DE CASOS ATENDIDO A TRAVES DEL SISTEMA WEB DE TICKETS

420281	Requerimiento	6/17/2019 23:05	6/17/2019	Seguridad Endpoints	Christian Huarcayo	H. Toluca	OficioSca	Reg. de Agente	Dipa_Sca_L2@sis	Green	High
520274	Requerimiento	21/05/2019 13:52	22/05/2019	Seguridad Endpoints	Christian Huarcayo	Sage F.	OficioSca	Reg. de Agente	PAU MADERA RAMON MARQUEL ELIAS	Green	High
520295	Incidente	20/05/2019 17:21	21/05/2019	Seguridad Endpoints	Christian Huarcayo	Sage F.	OficioSca	Reg. de Agente	MIKHO FENIA ERRA BOCALIA	Green	Critical
519584	Incidente	6/05/2019 11:38	6/05/2019	Seguridad Endpoints	Christian Huarcayo	Sage F.	OficioSca	Reg. de Agente	LESIANO MURILLO SANDRINO	Red	Critical
520420	Incidente	27/05/2019 19:40	28/05/2019	Seguridad Endpoints	Christian Huarcayo	Sage F.	OficioSca	Reg. de Agente	CASO D HERRERA CARLOS	Green	Critical
520432	Incidente	12/05/2019 16:34	13/05/2019	Seguridad Endpoints	Christian Huarcayo	Sage F.	OficioSca	Reg. de Agente	ANGELIZ TAPURICOMA ALBERTINA	Red	Critical
520455	Requerimiento de	17/05/2019 16:58	18/05/2019	Seguridad Endpoints	Christian Huarcayo	Sage F.	OficioSca	Reg. de Agente	ANGEL MARTIN DERRONOR LERUJE	Green	High
544360	Requerimiento de	servicio EMC2020 12	19/07/2019	Seguridad Endpoints	Christian Huarcayo	Conecta Center	OficioSca	Reg. de Agente	Melany Diaz cve@sis@sisotec.com.pe	Green	High
558122	Incidente	Junio 20/06/2019 17:32	20/06/2019	Seguridad Endpoints	Christian Huarcayo	H. Toluca	OficioSca	Reg. de Agente	Dipa_Sca_L2@sis	Green	Critical
560842	Requerimiento	Junio 20/06/2019 12:44	20/06/2019	Seguridad Endpoints	Christian Huarcayo	Sage F.	OficioSca	Reg. de Agente	FEMO PAZ ALFREDO RAUL	Green	High
560842	Requerimiento	Junio 20/06/2019 12:44	17/06/2019	Seguridad Endpoints	Christian Huarcayo	Sage F.	OficioSca	Reg. de Agente	FEMO PAZ ALFREDO RAUL	Green	High
560771	Requerimiento	servicio EMC2020 12	19/07/2019	Seguridad Endpoints	Christian Huarcayo	Sage F.	OficioSca	Reg. de Agente	Juan Cesar Espinoza Contreras _jcespinoza@sisotec.com	Green	High
560529	Requerimiento	Junio 22/06/2019 11:22	22/06/2019	Seguridad Endpoints	Christian Huarcayo	Sage F.	OficioSca	Reg. de Agente	Ricard Alvarado _rualvarado@sisotec.com.pe	Green	High
561562	Requerimiento de	servicio 26/07/2019	26/07/2019	Seguridad Endpoints	Christian Huarcayo	H. Toluca	OficioSca	Reg. de Agente	Gulierrez Luis C. _lgulierrez@sisotec.com.pe	Green	High
560458	Requerimiento	servicio 25/07/2019 12:4	25/07/2019	Seguridad Endpoints	Christian Huarcayo	F. Conzales	OficioSca	Reg. de Agente	De La Cruz Cecilia (Esterita) <_cdeacruz@sisotec.com.pe>	Green	High
560575	Incidente	Junio 26/07/2019 08	26/07/2019	Seguridad Endpoints	Christian Huarcayo	H. Toluca	OficioSca	Reg. de Agente	SOC Fideles <sof@sisotec.com>	Yellow	Critical
560580	Requerimiento	servicio 21/07/2019	21/07/2019	Seguridad Endpoints	Christian Huarcayo	Sage F.	OficioSca	Reg. de Agente	Juan Carlos _jcarlos@sisotec.com.pe	Green	High
520261	Requerimiento	servicio 21/07/2019	21/07/2019	Seguridad Endpoints	Christian Huarcayo	H. Toluca	OficioSca	Reg. de Agente	Ricard Alvarado _rualvarado@sisotec.com.pe	Green	High
520427	Requerimiento	servicio 06/02/2019 14:28	06/02/2019	Seguridad Endpoints	Christian Huarcayo	H. Toluca	OficioSca	Reg. de Agente	De La Cruz Cecilia (Esterita) _cdeacruz@sisotec.com.pe	Green	High
520481	Requerimiento	servicio 06/02/2019 02:12	06/02/2019	Seguridad Endpoints	Christian Huarcayo	H. Toluca	OficioSca	Reg. de Agente	Gulierrez Luis C. _lgulierrez@sisotec.com.pe	Green	High
514261	Requerimiento	servicio 06/02/2019 02:12	06/02/2019	Seguridad Endpoints	Christian Huarcayo	H. Toluca	OficioSca	Reg. de Agente	Gulierrez Luis C. _lgulierrez@sisotec.com.pe	Green	High
514296	Requerimiento	servicio 06/02/2019 11:23	06/02/2019	Seguridad Endpoints	Christian Huarcayo	Sage F.	OficioSca	Reg. de Agente	De La Cruz Cecilia (Esterita)	Green	High
514361	Requerimiento	servicio 06/02/2019 16:26	06/02/2019	Seguridad Endpoints	Christian Huarcayo	H. Toluca	OficioSca	Reg. de Agente	Gulierrez Luis	Green	High
514261	Requerimiento	servicio 06/02/2019 11:23	06/02/2019	Seguridad Endpoints	Christian Huarcayo	H. Toluca	OficioSca	Reg. de Agente	Gulierrez Luis C. _lgulierrez@sisotec.com.pe	Green	High

SISOTEC DEL PERU S.A.C.
 Av. José Pizarro 1000 - San Juan de Capatzen
 DNI: 40922219
 Representante Legal

MANUEL BARRERO
 INGENIERO
 DE COMPUTACION Y SISTEMAS
 Reg. CIP N° 180551



REPORTE DE CASOS ATENDIDO A TRAVES DEL SISTEMA WEB DE TICKETS

518740	Requerimiento	Junio 12/05/2019 10:42	12/05/2019	Seguridad Endpoint	Christian Hurtado	H. Torres	OficioSan	Reg. de Agente	Osvaldo Lora - Agenteos@MobiMx.comper	Green	High
518740	Requerimiento	Junio 12/05/2019 10:42	12/05/2019	Seguridad Endpoint	Christian Hurtado	Banco F.	OficioSan	Reg. de Agente	Rodriguez Juan -_rodrujua@MobiMx.comper	Green	High
518743	Requerimiento	Junio 11/05/2019 11:44	11/05/2019	Seguridad Endpoint	Christian Hurtado	Banco F.	OficioSan	Reg. de Agente	De La Cruz Cecilia -Esterini	Green	High
518747	Requerimiento	Junio 11/05/2019 11:44	11/05/2019	Seguridad Endpoint	Christian Hurtado	H. Torres	OficioSan	Reg. de Agente	Osvaldo Lora - Agenteos@MobiMx.comper	Green	High
518749	Requerimiento	Junio 11/05/2019 11:44	11/05/2019	Seguridad Endpoint	Christian Hurtado	Banco F.	OficioSan	Reg. de Agente	De La Cruz Cecilia -Esterini	Green	High
518749	Requerimiento	Junio 11/05/2019 11:44	11/05/2019	Seguridad Endpoint	Christian Hurtado	Sitac	OficioSan	Reg. de Agente	De La Cruz Cecilia -Esterini	Green	High
518752	Requerimiento	Junio 11/05/2019 11:44	11/05/2019	Seguridad Endpoint	Christian Hurtado	Banco F.	OficioSan	Reg. de Agente	De La Cruz Cecilia -Esterini	Green	High
518757	Requerimiento	Junio 14/05/2019 11:34	14/05/2019	Seguridad Endpoint	Christian Hurtado	Banco F.	OficioSan	Reg. de Agente	Zapata Boris	Green	High
518763	Requerimiento	Junio 14/05/2019 11:34	14/05/2019	Seguridad Endpoint	Christian Hurtado	Sitac	OficioSan	Reg. de Agente	De La Cruz Cecilia -Esterini	Green	High
518765	Requerimiento	Junio 17/05/2019 11:44	17/05/2019	Seguridad Endpoint	Christian Hurtado	Sitac	OficioSan	Reg. de Agente	De La Cruz Cecilia -Esterini	Green	High
520349	Incidente	Junio 04/05/2019 11:44	04/05/2019	Seguridad Endpoint	Christian Hurtado	Banco F.	OficioSan	Servicio Grupos	Walter Andres Vargas Cabrera -wvargas@FideMobiMx	Red	Critical
541285	Incidente	Junio 04/05/2019 11:44	04/05/2019	Seguridad Endpoint	Christian Hurtado	Banco F.	OficioSan	Servicio Grupos	Walter Andres Vargas Cabrera -wvargas@FideMobiMx	Yellow	Critical
541292	Incidente	Junio 04/05/2019 11:44	04/05/2019	Seguridad Endpoint	Christian Hurtado	Comercio de Seguros F.	OficioSan	Servicio Grupos	Walter Andres Vargas Cabrera -wvargas@FideMobiMx	Red	Critical
541292	Incidente	Junio 04/05/2019 11:44	04/05/2019	Seguridad Endpoint	Christian Hurtado	F. Servicio De Salud	OficioSan	Servicio Grupos	Walter Andres Vargas Cabrera -wvargas@FideMobiMx	Yellow	Critical
541297	Incidente	Junio 04/05/2019 11:44	04/05/2019	Seguridad Endpoint	Christian Hurtado	Banco F.	OficioSan	Servicio Grupos	Walter Andres Vargas Cabrera -wvargas@FideMobiMx	Red	Critical
541297	Incidente	Junio 04/05/2019 11:44	04/05/2019	Seguridad Endpoint	Christian Hurtado	Banco F.	OficioSan	Servicio Grupos	Walter Andres Vargas Cabrera -wvargas@FideMobiMx	Green	Critical
541300	Incidente	Junio 04/05/2019 11:44	04/05/2019	Seguridad Endpoint	Christian Hurtado	Comercio de Seguros F.	OficioSan	Servicio Grupos	Walter Andres Vargas Cabrera	Yellow	Critical
478063	Requerimiento	05/10/19 13:24	05/10/19	Seguridad Endpoint	Christian Hurtado	Banco F.	OficioSan	Servicio Grupos	FRANCISCA MARCELA ANGEL	Green	Low
480743	Requerimiento	05/10/19 23:03	04/10/19	Seguridad Endpoint	Christian Hurtado	Banco F.	OficioSan	Servicio Grupos	Carolina Benavides Lora Angel	Green	Low
480764	Requerimiento	05/10/19 17:54	04/10/19	Seguridad Endpoint	Christian Hurtado	Banco F.	OficioSan	Servicio Grupos	CAROLINA BENAVIDES LORA ANGEL	Green	Low
487339	Requerimiento	03/02/19 16:41	02/02/19	Seguridad Endpoint	Christian Hurtado	Sitac	OficioSan	Servicio Grupos	Carolina Benavides Lora Angel	Green	Low
487321	Requerimiento	03/02/19 21:29	02/02/19	Seguridad Endpoint	Christian Hurtado	Banco F.	OficioSan	Servicio Grupos	FABIO YAMAGUCHI ROSAMON DEL CARMEN	Green	Low
488086	Requerimiento	08/02/2019 12:39	08/02/19	Seguridad Endpoint	Christian Hurtado	Banco F.	OficioSan	Servicio Grupos	Polan Duran Lora - Polan Duran Lora	Green	Low
517138	Requerimiento	04/05/2019 13:38	04/05/2019	Seguridad Endpoint	Christian Hurtado	Banco F.	OficioSan	Servicio Grupos	RUIZ LIDIANA BRICK JOHANNA	Green	Low

JUAN CARLOS SANCHEZ

 INGENIERO DE SISTEMAS

JUAN CARLOS SANCHEZ

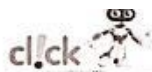
 INGENIERO DE SISTEMAS

SISOTEC DEL PERU S.A.C.

 REPRESENTANTE LEGAL

INGENIERO DE SISTEMAS

 REG. DIP. N° 186551



REPORTE DE CASOS ATENDIDO A TRAVES DEL SISTEMA WEB DE TICKETS

524817	Requerimiento	21/05/2019 13:25	21/05/2019	Seguridad Endpoint	Christian H. Tade	Barco F	Oficina	Sistema Operativo	AMARZ CORRA CLAUDIO CESAR	Green	Low
524835	Requerimiento	23/05/2019 13:55	23/05/2019	Seguridad Endpoint	Christian H. Tade	Barco F	Oficina	Sistema Operativo	MULLI LUIS ENRIQUE JONATHAN	Green	Low
532231	Requerimiento	13/05/2019 12:03	13/05/2019	Seguridad Endpoint	Christian Hurtado	Barco F	Oficina	Sistema Operativo	SARABITO DAMASCOS RAUL ALONSO	Green	Low
531438	Requerimiento	12/05/2019 11:07	12/05/2019	Seguridad Endpoint	Christian Hurtado	Barco F	Oficina	Sistema Operativo	SARABITO DAMASCOS RAUL ALONSO	Green	Low
530572	Requerimiento	11/05/2019 13:30	11/05/2019	Seguridad Endpoint	Christian Hurtado	Barco F	Oficina	Sistema Operativo	Calleros Ediciones Luis Angel	Green	Low
530238	Requerimiento	13/05/2019 14:28	13/05/2019	Seguridad Endpoint	Christian Hurtado	Barco F	Oficina	Sistema Operativo	ANDRA CASTILLO TERRY RONALD	Green	Low
529472	Requerimiento	16/05/2019 15:24	16/05/2019	Seguridad Endpoint	Christian Hurtado	Barco F	Oficina	Sistema Operativo	CASTILLO ANAYA ROBERTO ROBERTO	Green	Low
529358	Requerimiento	15/05/2019 14:53	16/05/2019	Seguridad Endpoint	Christian Hurtado	Barco F	Oficina	Sistema Operativo	CASTILLO ANAYA ROBERTO ROBERTO	Green	Low
528878	Requerimiento	14/05/2019 14:16	20/05/2019	Seguridad Endpoint	Christian Hurtado	Barco F	Oficina	Sistema Operativo	CASTRO YALLESOS EDWIN ANTONIO	Green	Low
543275	Incidente	martes 16/07/2019 12:11	17/07/2019	Seguridad Endpoint	Christian Hurtado	H. Tade	Oficina	Sistema Operativo	CARDENAS PESQUERA KATHERINE (MMA) cardenas@pe	Green	Critical
543287	Requerimiento	viernes 18/07/2019 11:12	18/07/2019	Seguridad Endpoint	Christian Hurtado	Barco F	Oficina	Sistema Operativo	Sanchez Juan Enrique s.juanes@comcast.net	Green	Low
543287	Requerimiento	viernes 18/07/2019 11:12	18/07/2019	Seguridad Endpoint	Christian Hurtado	Barco F	Oficina	Sistema Operativo	BLANCH AYCOBEDA PATRICIA LIZ	Green	Low
543172	Requerimiento	viernes 16/07/2019 14:17	16/07/2019	Seguridad Endpoint	Christian Hurtado	Barco F	Oficina	Sistema Operativo	Coordinacion Soporte Técnico -Coordinacion, Soporte, Técnico	Green	Low
543332	Requerimiento	viernes 23/07/2019 13:20	23/07/2019	Seguridad Endpoint	Christian Hurtado	Barco F	Oficina	Sistema Operativo	DAPIVA MORENO OLIVERA YANIS	Green	Low
543083	Requerimiento	viernes 23/07/2019 13:20	23/07/2019	Seguridad Endpoint	Christian Hurtado	Barco F	Oficina	Sistema Operativo	SCHERO MISTAZA KYTHA ESTHER	Green	Low
543185	Requerimiento	viernes 23/07/2019 13:20	23/07/2019	Seguridad Endpoint	Christian Hurtado	Condic Center	Oficina	Sistema Operativo	José Luis Pinela Sanchez	Green	Low
543555	Incidente	viernes 26/07/2019 13:20	27/07/2019	Seguridad Endpoint	Christian Hurtado	Condic Center	Oficina	Sistema Operativo	José Luis Pinela Sanchez	Green	Critical
542576	Requerimiento	viernes 16/05/2019 14:32	16/05/2019	Seguridad Endpoint	Christian Hurtado	Barco F	Oficina	Sistema Operativo	RAFAEL RAMIREZ ROMANI	Green	Low
541579	Requerimiento	miércoles 23/05/2019 15:53	4/06/2019	Seguridad Endpoint	Christian Hurtado	Barco F	Oficina	Sistema Operativo	DEL CANTO PAREDES ANICHA CARMEN	Green	Low
541144	Requerimiento	viernes 14/05/2019 09:55	11/05/2019	Seguridad Endpoint	Christian Hurtado	H. Tade	Oficina	Sistema Operativo	BONDON BRADY JESUS EMIL	Green	Low
540231	Requerimiento	miércoles 18/05/2019 11:13	18/05/2019	Seguridad Endpoint	Christian Hurtado	Barco F	Oficina	Sistema Operativo	SARABITO DAMASCOS RAUL ALONSO	Green	Low
539494	Requerimiento	viernes 13/05/2019 11:13	14/05/2019	Seguridad Endpoint	Christian Hurtado	Barco F	Oficina	Firewall	FILICION CHAMBITA ALEXANDRO	Green	Medium
539383	Incidente	miércoles 08/05/2019 10:44	09/05/2019	Seguridad Endpoint	Christian Hurtado	H. Tade	Oficina	Web Malware	SISSOTEC DEL PERU S.A.C. DESPTE CUEPE L OLA ENITA	Green	Critical

SISSOTEC DEL PERU S.A.C.
 Calle 100 N° 4123
 República del Perú - Lima
 Representante Legal

INGENIERO EN SISTEMAS
 LUIS MARCELO
 LINARES BARRIETO
 INGENIERO
 DE COMPUTACION Y SISTEMAS
 Reg. CP Nº 18651



REGISTRO DE CASOS DETECTADOS Y REPORTADOS DEL DENSO SOC

26	Corneo	Incidente	Rivero F.	Oficial/Gu	Vista Malena	Mérida	asistencia	SOC Saco - Demaj Colaboración de Impuesto de tránsito en el tipo	15/09/2019	Salavisa	14:22 p.m.	14:34 p.m.	Cerrado	Verde
27	Corneo	Incidente	Silbac	Oficial/Gu	Vista Malena	Mérida	estabilidad	SOC Saco - Demaj Control de VEHICULO JUVENES TAC	24/09/2019	Salavisa	16:00 p.m.	16:22 p.m.	Cerrado	Verde
28	Corneo	Incidente	Correa Garcia	Oficial/Gu	Vista Malena	Mérida	asistencia	SOC Saco - Demaj Control asistencia R. 112 N° 31	21/09/2019	Salavisa	16:00 p.m.	16:04 p.m.	Cerrado	Verde
29	Corneo	Incidente	Alvar	Oficial/Gu	Vista Malena	Mérida	Licenciado	SOC Saco - Demaj Control asistencia R. 112 N° 31	21/09/2019	Salavisa	16:11 p.m.	16:17 p.m.	Cerrado	Verde
30	Corneo	Incidente	Alvar	Oficial/Gu	Vista Malena	Mérida	asistencia	SOC Saco - Demaj Control asistencia R. 112 N° 31	21/09/2019	Salavisa	16:26 p.m.	16:29 p.m.	Cerrado	Verde
31	Corneo	Incidente	Silbac	Oficial/Gu	Vista Malena	Mérida	asistencia	SOC Saco - Demaj Control asistencia R. 112 N° 31	21/09/2019	Salavisa	16:40 p.m.	16:42 p.m.	Cerrado	Verde
32	Corneo	Incidente	Silbac	Oficial/Gu	Vista Malena	Mérida	asistencia	SOC Saco - Demaj Control asistencia R. 112 N° 31	21/09/2019	Salavisa	16:43 p.m.	16:45 p.m.	Cerrado	Verde
33	Corneo	Incidente	Silbac	Oficial/Gu	Vista Malena	Mérida	asistencia	SOC Saco - Demaj Control asistencia R. 112 N° 31	21/09/2019	Salavisa	16:46 p.m.	16:49 p.m.	Cerrado	Verde
34	Corneo	Incidente	Rivero F.	Oficial/Gu	Vista Malena	Mérida	asistencia	SOC Saco - Demaj Control asistencia R. 112 N° 31	21/09/2019	Salavisa	16:46 p.m.	16:49 p.m.	Cerrado	Verde
35	Corneo	Incidente	Rivero F.	Oficial/Gu	Vista Malena	Mérida	asistencia	SOC Saco - Demaj Control asistencia R. 112 N° 31	21/09/2019	Salavisa	16:46 p.m.	16:49 p.m.	Cerrado	Verde
36	Corneo	Incidente	Rivero F.	Oficial/Gu	Vista Malena	Mérida	asistencia	SOC Saco - Demaj Control asistencia R. 112 N° 31	21/09/2019	Salavisa	16:46 p.m.	16:49 p.m.	Cerrado	Verde
37	Corneo	Incidente	Silbac	Oficial/Gu	Vista Malena	Mérida	asistencia	SOC Saco - Demaj Control asistencia R. 112 N° 31	21/09/2019	Salavisa	16:46 p.m.	16:49 p.m.	Cerrado	Verde
38	Corneo	Incidente	Rivero F.	Oficial/Gu	Vista Malena	Mérida	asistencia	SOC Saco - Demaj Control asistencia R. 112 N° 31	21/09/2019	Salavisa	16:46 p.m.	16:49 p.m.	Cerrado	Verde
39	Corneo	Incidente	H. Torres	Oficial/Gu	Vista Malena	Mérida	asistencia	SOC Saco - Demaj Control asistencia R. 112 N° 31	21/09/2019	Salavisa	16:46 p.m.	16:49 p.m.	Cerrado	Verde
40	Corneo	Incidente	Silbac	Oficial/Gu	Vista Malena	Mérida	asistencia	SOC Saco - Demaj Control asistencia R. 112 N° 31	21/09/2019	Salavisa	16:46 p.m.	16:49 p.m.	Cerrado	Verde
41	Corneo	Incidente	H. Torres	Oficial/Gu	Vista Malena	Mérida	asistencia	SOC Saco - Demaj Control asistencia R. 112 N° 31	21/09/2019	Salavisa	16:46 p.m.	16:49 p.m.	Cerrado	Verde
42	Corneo	Incidente	Correa Garcia	Oficial/Gu	Vista Malena	Mérida	asistencia	SOC Saco - Demaj Control asistencia R. 112 N° 31	21/09/2019	Salavisa	16:46 p.m.	16:49 p.m.	Cerrado	Verde
43	Corneo	Incidente	F. Corporado	Oficial/Gu	Vista Malena	Mérida	asistencia	SOC Saco - Demaj Control asistencia R. 112 N° 31	21/09/2019	Salavisa	16:46 p.m.	16:49 p.m.	Cerrado	Verde
44	Corneo	Incidente	Rivero F.	Oficial/Gu	Vista Malena	Mérida	asistencia	SOC Saco - Demaj Control asistencia R. 112 N° 31	21/09/2019	Salavisa	16:46 p.m.	16:49 p.m.	Cerrado	Verde
45	Corneo	Incidente	Correa Garcia	Oficial/Gu	Vista Malena	Mérida	asistencia	SOC Saco - Demaj Control asistencia R. 112 N° 31	21/09/2019	Salavisa	16:46 p.m.	16:49 p.m.	Cerrado	Verde
46	Corneo	Incidente	Rivero F.	Oficial/Gu	DLP	Alto	asistencia	SOC Saco - Demaj Control asistencia R. 112 N° 31	17/07/2019	Alto	16:11 p.m.	16:12 p.m.	Cerrado	Verde
47	Corneo	Incidente	Rivero F.	Oficial/Gu	DLP	Alto	asistencia	SOC Saco - Demaj Control asistencia R. 112 N° 31	18/07/2019	Alto	16:46 p.m.	16:49 p.m.	Cerrado	Verde
48	Corneo	Incidente	Rivero F.	Oficial/Gu	DLP	Alto	asistencia	SOC Saco - Demaj Control asistencia R. 112 N° 31	18/07/2019	Alto	16:46 p.m.	16:49 p.m.	Cerrado	Verde
49	Corneo	Incidente	Rivero F.	Oficial/Gu	DLP	Alto	asistencia	SOC Saco - Demaj Control asistencia R. 112 N° 31	18/07/2019	Alto	16:46 p.m.	16:49 p.m.	Cerrado	Verde
50	Corneo	Incidente	Rivero F.	Oficial/Gu	DLP	Alto	asistencia	SOC Saco - Demaj Control asistencia R. 112 N° 31	18/07/2019	Alto	16:46 p.m.	16:49 p.m.	Cerrado	Verde
51	Corneo	Incidente	Rivero F.	Oficial/Gu	DLP	Alto	asistencia	SOC Saco - Demaj Control asistencia R. 112 N° 31	20/07/2019	Alto	16:46 p.m.	16:49 p.m.	Cerrado	Verde

SIGOTEC DEL PERU S.A.C.

 RUC: 201901010000000000

 Av. 28 de Julio 1011

 Lima 15011

 Teléfono: 445-22319

 www.sigotec.com.pe

 Registro en el M. del Poder Judicial

 DE COMERCIO Y SISTEMAS

 Reg. CIP N° 150551



REGISTRO DE CASOS DETECTADOS Y REPORTADOS DEL DEMO SOC

ID	Categoria	Incidente	Banco F.	Oficina	DUP	Ata	Descripción del caso	SOC	Fecha de inicio	Fecha de fin	Estado	Verde		
52	Credito	Incidente	Banco F.	Oficina	DUP	Ata	Oficina de Cobranza (Banco F.)	SOC Servicio - Dema) Servicio de Equipo por activación de	22/07/2019	Julio	13:07 p.m.	17:35 p.m.	Cerrado	Verde
53	Credito	Incidente	Banco F.	Oficina	DUP	Ata	Oficina de Cobranza (Banco F.)	SOC Servicio - Dema) Servicio de Equipo por activación de	22/07/2019	Julio	16:15 p.m.	18:22 p.m.	Cerrado	Verde
54	Credito	Incidente	Banco F.	Oficina	DUP	Ata	Oficina de Cobranza (Banco F.)	SOC Servicio - Dema) Servicio de Equipo por activación de	22/07/2019	Julio	12:12 p.m.	12:19 p.m.	Cerrado	Verde
55	Credito	Incidente	Banco F.	Oficina	DUP	Ata	Oficina de Cobranza (Banco F.)	SOC Servicio - Dema) Servicio de Equipo por activación de	22/07/2019	Julio	15:07 p.m.	15:19 p.m.	Cerrado	Verde
56	Credito	Incidente	Banco F.	Oficina	DUP	Ata	Oficina de Cobranza (Banco F.)	SOC Servicio - Dema) Servicio de Equipo por activación de	23/07/2019	Julio	15:03 p.m.	15:21 p.m.	Cerrado	Verde
57	Credito	Incidente	Banco F.	Oficina	DUP	Ata	Oficina de Cobranza (Banco F.)	SOC Servicio - Dema) Servicio de Equipo por activación de	24/07/2019	Julio	12:31 p.m.	12:39 p.m.	Cerrado	Verde
58	Credito	Incidente	Banco F.	Oficina	DUP	Ata	Oficina de Cobranza (Banco F.)	SOC Servicio - Dema) Servicio de Equipo por activación de	21/07/2019	Julio	14:34 p.m.	15:32 p.m.	Cerrado	Verde
59	Credito	Incidente	Banco F.	Oficina	DUP	Ata	Oficina de Cobranza (Banco F.)	SOC Servicio - Dema) Servicio de Equipo por activación de	07/08/2019	Agosto	9:21 a.m.	9:27 a.m.	Cerrado	Verde
60	Credito	Incidente	Banco F.	Oficina	DUP	Ata	Oficina de Cobranza (Banco F.)	SOC Servicio - Dema) Servicio de Equipo por activación de	07/08/2019	Agosto	13:30 a.m.	13:31 a.m.	Cerrado	Verde
61	Credito	Incidente	Banco F.	Oficina	DUP	Ata	Oficina de Cobranza (Banco F.)	SOC Servicio - Dema) Servicio de Equipo por activación de	07/08/2019	Agosto	10:22 a.m.	10:36 a.m.	Cerrado	Verde
62	Credito	Incidente	Banco F.	Oficina	DUP	Ata	Oficina de Cobranza (Banco F.)	SOC Servicio - Dema) Servicio de Equipo por activación de	15/07/2019	Julio	16:27 p.m.	16:36 p.m.	Cerrado	Verde
63	Credito	Incidente	Banco F.	Oficina	DUP	Ata	Oficina de Cobranza (Banco F.)	SOC Servicio - Dema) Servicio de Equipo por activación de	09/08/2019	Agosto	16:19 p.m.	17:03 p.m.	Cerrado	Verde
64	Credito	Incidente	Banco F.	Oficina	DUP	Ata	Oficina de Cobranza (Banco F.)	SOC Servicio - Dema) Servicio de Equipo por activación de	15/08/2019	Agosto	16:09 p.m.	16:11 p.m.	Cerrado	Verde
65	Credito	Incidente	Banco F.	Oficina	DUP	Ata	Oficina de Cobranza (Banco F.)	SOC Servicio - Dema) Servicio de Equipo por activación de	14/08/2019	Agosto	17:33 p.m.	17:53 p.m.	Cerrado	Verde
66	Credito	Incidente	Banco F.	Oficina	DUP	Ata	Oficina de Cobranza (Banco F.)	SOC Servicio - Dema) Servicio de Equipo por activación de	10/08/2019	Agosto	14:19 p.m.	14:43 p.m.	Cerrado	Verde
67	Credito	Incidente	Banco F.	Oficina	DUP	Ata	Oficina de Cobranza (Banco F.)	SOC Servicio - Dema) Servicio de Equipo por activación de	06/08/2019	Agosto	20:09 p.m.	20:11 p.m.	Cerrado	Verde
68	Tarjetas	Incidente	Banco F.	Oficina	DUP	Ata	Oficina de Cobranza (Banco F.)	SOC Servicio - Dema) Servicio de Equipo por activación de	15/08/2019	Agosto	16:19 p.m.	16:22 p.m.	Cerrado	Verde
69	Tarjetas	Incidente	Banco F.	Oficina	DUP	Ata	Oficina de Cobranza (Banco F.)	SOC Servicio - Dema) Servicio de Equipo por activación de	14/08/2019	Agosto	21:05 p.m.	21:12 p.m.	Cerrado	Verde
70	Tarjetas	Incidente	Banco F.	Oficina	DUP	Ata	Oficina de Cobranza (Banco F.)	SOC Servicio - Dema) Servicio de Equipo por activación de	15/08/2019	Agosto	11:03 a.m.	11:24 a.m.	Cerrado	Verde
71	Credito	Incidente	Banco F.	Oficina	DUP	Ata	Oficina de Cobranza (Banco F.)	SOC Servicio - Dema) Servicio de Equipo por activación de	09/08/2019	Agosto	17:29 p.m.	20:43 p.m.	Cerrado	Verde
72	Credito	Incidente	Banco F.	Oficina	DUP	Ata	Oficina de Cobranza (Banco F.)	SOC Servicio - Dema) Servicio de Equipo por activación de	23/08/2019	Agosto	15:08 p.m.	16:11 p.m.	Cerrado	Verde
73	Credito	Incidente	Banco F.	Oficina	DUP	Ata	Oficina de Cobranza (Banco F.)	SOC Servicio - Dema) Servicio de Equipo por activación de	29/08/2019	Agosto	10:25 a.m.	10:47 a.m.	Cerrado	Verde
74	Credito	Incidente	Banco F.	Oficina	DUP	Ata	Oficina de Cobranza (Banco F.)	SOC Servicio - Dema) Servicio de Equipo por activación de	29/08/2019	Agosto	11:03 a.m.	11:30 a.m.	Cerrado	Verde
75	Credito	Incidente	Banco F.	Oficina	DUP	Ata	Oficina de Cobranza (Banco F.)	SOC Servicio - Dema) Servicio de Equipo por activación de	28/08/2019	Agosto	14:39 p.m.	16:12 p.m.	Cerrado	Verde
76	Credito	Incidente	Banco F.	Oficina	DUP	Ata	Oficina de Cobranza (Banco F.)	SOC Servicio - Dema) Servicio de Equipo por activación de	14/08/2019	Agosto	17:36 p.m.	17:36 p.m.	Cerrado	Verde
77	Credito	Incidente	Banco F.	Oficina	DUP	Ata	Oficina de Cobranza (Banco F.)	SOC Servicio - Dema) Servicio de Equipo por activación de	14/08/2019	Agosto	17:36 p.m.	17:36 p.m.	Cerrado	Verde


 LUIS ALBERTO LOPEZ
 GERENTE GENERAL
 SISCOMBO S.A.S.
 Calle 100 No. 100-100
 Bogotá, D.C. 110011


 CARLOS ALBERTO LOPEZ
 GERENTE GENERAL
 SISCOMBO S.A.S.
 Calle 100 No. 100-100
 Bogotá, D.C. 110011



REGISTRO DE CASOS DETECTADOS Y REPORTADOS DEL DOWNSOC

Nº	Caso	Incidente	Usuario	Oficina	DUP	Año	Reportado	SOC	Estado	Fecha de inicio	Fecha de fin	Causa	Verde
78	Caso	Incidente	Alfonso F.	Oficina	DUP	Año	Alfonso F. (alfonso.f@)	SOC	Cerrado	12/02/19	12/02/19	Cerrado	Verde
79	Caso	Incidente	Alfonso F.	Oficina	DUP	Año	Jose Vargas	SOC	Cerrado	11/08/19	12/02/19	Cerrado	Verde
80	Caso	Incidente	Alfonso F.	Oficina	DUP	Año	Marvin Velasco	SOC	Cerrado	11/02/19	11/22/19	Cerrado	Verde
81	Caso	Incidente	Alfonso F.	Oficina	DUP	Año	De La Cruz Cecilia (cecilia)	SOC	Cerrado	11/02/19	11/17/19	Cerrado	Verde
82	Caso	Incidente	Alfonso F.	Oficina	DUP	Año	Vargas Jose (jose.vargas@)	SOC	Cerrado	11/02/19	11/20/19	Cerrado	Verde
83	Caso	Incidente	Alfonso F.	Oficina	DUP	Año	Espinosa Mario	SOC	Cerrado	10/20/19	10/27/19	Cerrado	Verde
84	Caso	Incidente	Alfonso F.	Oficina	DUP	Año	Vargas Jose (jose.vargas@)	SOC	Cerrado	10/11/19	11/25/19	Cerrado	Verde
85	Caso	Incidente	Alfonso F.	Oficina	DUP	Año	Alfonso Cabel	SOC	Cerrado	10/02/19	10/08/19	Cerrado	Verde
86	Caso	Incidente	F. Corporativo	Oficina	DUP	Año	MOLINA ROSA ARIADNA	SOC	Cerrado	08/02/19	08/02/19	Cerrado	Verde
87	Caso	Incidente	Alfonso F.	Oficina	DUP	Año	Alfonso Cabel - alfonso@	SOC	Cerrado	06/02/19	06/11/19	Cerrado	Verde
88	Caso	Incidente	Alfonso F.	Oficina	DUP	Año	ALONSO GONZALEZ ALEX	SOC	Cerrado	05/02/19	05/11/19	Cerrado	Verde
89	Caso	Incidente	Alfonso F.	Oficina	DUP	Año	VELAZQUEZ ANDRÉS AD	SOC	Cerrado	04/02/19	04/22/19	Cerrado	Verde
90	Caso	Incidente	Alfonso F.	Oficina	DUP	Año	CALDERON ANDRÉS GUSTAVO	SOC	Cerrado	04/02/19	04/22/19	Cerrado	Verde
91	Caso	Incidente	Alfonso F.	Oficina	DUP	Año	SULLON CHRISTOPHER ALEX	SOC	Cerrado	04/02/19	04/22/19	Cerrado	Verde
92	Caso	Incidente	F. Servicio al Cliente	Oficina	DUP	Año	FRANCO (FRANCO.FRANCO)	SOC	Cerrado	04/02/19	04/22/19	Cerrado	Verde
93	Caso	Incidente	Alfonso F.	Oficina	DUP	Año	VELA GARCIA DEAN PABLO	SOC	Cerrado	03/20/19	03/20/19	Cerrado	Verde
94	Caso	Incidente	Concepción de Soto	Oficina	DUP	Año	ALONSO GONZALEZ ALEX	SOC	Cerrado	03/02/19	03/02/19	Cerrado	Verde
95	Caso	Incidente	H. Talca	Oficina	DUP	Año	VELAZQUEZ ANDRÉS GUSTAVO	SOC	Cerrado	03/02/19	03/02/19	Cerrado	Verde
96	Caso	Incidente	H. Talca	Oficina	DUP	Año	LOPEZ LA FLORES MELI	SOC	Cerrado	03/02/19	03/02/19	Cerrado	Verde
97	Caso	Incidente	Alfonso F.	Oficina	DUP	Año	MARINO ROBERTO GUSTAVO	SOC	Cerrado	03/02/19	03/02/19	Cerrado	Verde
98	Caso	Incidente	H. Talca	Oficina	DUP	Año	Baro Castro pedro carlos	SOC	Cerrado	03/02/19	03/02/19	Cerrado	Verde
99	Caso	Incidente	H. Talca	Oficina	DUP	Año	DE LA CRUZ PABLO GUSTAVO	SOC	Cerrado	03/02/19	03/02/19	Cerrado	Verde
100	Caso	Incidente	H. Talca	Oficina	DUP	Año	LOPEZ LA FLORES MELI	SOC	Cerrado	03/02/19	03/02/19	Cerrado	Verde
101	Caso	Incidente	H. Talca	Oficina	DUP	Año	ALONSO GONZALEZ ALEX	SOC	Cerrado	03/02/19	03/02/19	Cerrado	Verde
102	Caso	Incidente	H. Talca	Oficina	DUP	Año	DE LA CRUZ PABLO GUSTAVO	SOC	Cerrado	03/02/19	03/02/19	Cerrado	Verde
103	Caso	Incidente	Alfonso F.	Oficina	DUP	Año	FERRER YANAGUCHI ADRIAN	SOC	Cerrado	03/02/19	03/02/19	Cerrado	Verde

SISCOG DEL PNP S.A.U.
 LUIS RAMIRO
 LUIS RAMIRO
 DE COMPUTACION Y SISTEMAS
 Reg. CP Nº 180251



REGISTRO DE CASOS DETECTADOS Y REPORTADOS DEL FONDO SOC.

Nº	Categoría	Incidente	F. Capacitación	Origen	DLP	Abd	Nombre del Empleado	Descripción del Incidente	Fecha de Detección	Fecha de Reporte	Horas de Trabajo	Gravedad	Verde
104	Casos	Incidente	F. Capacitación	Origen	DLP	Abd	VALLE DOMÍNGUEZ ANTONIO	SOC Sistema - Deneg. Vulnerabilidad DLP presentada en e	8/10/2018	Mayo	7.87 p. m	Grave	Verde
105	Casos	Incidente	Saga F.	Origen	DLP	Abd	LUZENA C. BILLAGANA CECILIA	SOC Sistema - Deneg. Vulnerabilidad DLP presentada en e	8/10/2018	Mayo	1.23 p. m	Grave	Verde
106	Casos	Incidente	Saga F.	Origen	DLP	Abd	LEONEL C. HERNANDEZ	SOC Sistema - Deneg. Servicio de DLP interno	8/10/2018	Mayo	1.30 p. m	Grave	Verde
107	Casos	Incidente	Saga F.	Origen	DLP	Abd	RODRIGUEZ FERRER ANDRÉS	SOC Sistema - Deneg. Vulnerabilidad DLP presentada en e	8/10/2018	Mayo	11.48 p. m	Grave	Verde
108	Casos	Incidente	H. Talca	Origen	DLP	Abd	SANCHEZ DIGNAGUIRELA	SOC Sistema - Deneg. Log de Eventos de dispositivos	24/05/2018	Junio	11.22 p. m	Grave	Verde
109	Casos	Incidente	Comisión de Seg.	Origen	DLP	Abd	Tabares Sal. Efraim Junior	SOC Sistema - Deneg. Log de Eventos de dispositivos	24/05/2018	Junio	4.37 p. m	Grave	Verde
110	Casos	Incidente	H. Talca	Origen	DLP	Abd	GUERRA GILBERTO ERNESTO	SOC Sistema - Deneg. Servicio de DLP interno	24/05/2018	Junio	11.29 p. m	Grave	Verde
111	Casos	Incidente	Saga F.	Origen	DLP	Abd	LUZENA C. BILLAGANA CECILIA	SOC Sistema - Deneg. Servicio de DLP interno	25/05/2018	Junio	11.28 p. m	Grave	Verde
112	Casos	Incidente	Comisión de Seg.	Origen	DLP	Abd	Tabares Sal. Efraim Junior	SOC Sistema - Deneg. Problema de acceso al sistema por parte de usuarios en acceso de datos	25/05/2018	Junio	11.25 p. m	Grave	Verde
113	Casos	Incidente	Saga F.	Origen	DLP	Abd	LUZENA C. BILLAGANA CECILIA	SOC Sistema - Deneg. Vulnerabilidad DLP presentada en e	25/05/2018	Junio	11.34 p. m	Grave	Verde
114	Casos	Incidente	Comisión de Seg.	Origen	DLP	Abd	Tabares Sal. Efraim Junior	SOC Sistema - Deneg. Log de Eventos de dispositivos	27/05/2018	Junio	8.25 p. m	Grave	Verde
115	Casos	Incidente	Saga F.	Origen	DLP	Abd	HERNANDEZ FERRER ANDRÉS	SOC Sistema - Deneg. Vulnerabilidad DLP presentada en e	25/05/2018	Junio	9.44 p. m	Grave	Verde
116	Casos	Incidente	Comisión de Seg.	Origen	DLP	Abd	MARRAS CASARETO OSCAR	SOC Sistema - Deneg. Vulnerabilidad DLP presentada en e	25/05/2018	Junio	4.01 p. m	Grave	Verde
117	Casos	Incidente	Saga F.	Origen	DLP	Abd	HERNANDEZ FERRER ANDRÉS	SOC Sistema - Deneg. Vulnerabilidad DLP presentada en e	25/05/2018	Junio	4.24 p. m	Grave	Verde
118	Casos	Incidente	H. Talca	Origen	DLP	Abd	FERRER QUEROZUCO OSCAR	SOC Sistema - Deneg. Log de Eventos de dispositivos	25/05/2018	Junio	12.45 p. m	Grave	Verde
119	Casos	Incidente	H. Talca	Origen	DLP	Abd	CASARETO GONZALO VICTOR	SOC Sistema - Deneg. Log de Eventos de dispositivos	24/05/2018	Junio	11.27 p. m	Grave	Verde
120	Casos	Incidente	H. Talca	Origen	DLP	Abd	LUZENA C. BILLAGANA CECILIA	SOC Sistema - Deneg. Log de Eventos de dispositivos	24/05/2018	Junio	11.21 p. m	Grave	Verde
121	Casos	Incidente	H. Talca	Origen	DLP	Abd	PEREZ ESCOBAR AGUIRRE ALBERTO	SOC Sistema - Deneg. Log de Eventos de dispositivos	24/05/2018	Junio	11.28 p. m	Grave	Verde
122	Casos	Incidente	F. Capacitación	Origen	DLP	Abd	FERRER ESPINOSA LUIS DOMINGO	SOC Sistema - Deneg. Vulnerabilidad DLP presentada en e	25/05/2018	Junio	5.46 p. m	Grave	Verde
123	Casos	Incidente	Saga F.	Origen	DLP	Abd	Alvarez Cordero Amador Marcelo	SOC Sistema - Deneg. Vulnerabilidad DLP presentada en e	19/05/2018	Junio	2.82 p. m	Grave	Verde
124	Casos	Incidente	Saga F.	Origen	DLP	Abd	RODRIGUEZ FERRER ANDRÉS	SOC Sistema - Deneg. Log de Eventos de dispositivos	19/05/2018	Junio	12.30 p. m	Grave	Verde
125	Casos	Incidente	Saga F.	Origen	DLP	Abd	PAZOS SOTOMAYOR OSCAR	SOC Sistema - Deneg. Vulnerabilidad DLP presentada en e	19/05/2018	Junio	4.22 p. m	Grave	Verde
126	Casos	Incidente	Saga F.	Origen	DLP	Abd	FERRER ESCOBAR AGUIRRE ALBERTO	SOC Sistema - Deneg. Vulnerabilidad DLP presentada en e	17/05/2018	Junio	4.15 p. m	Grave	Verde
127	Casos	Incidente	Saga F.	Origen	DLP	Abd	RODRIGUEZ FERRER ANDRÉS	SOC Sistema - Deneg. Vulnerabilidad DLP presentada en e	17/05/2018	Junio	1.21 p. m	Grave	Verde
128	Casos	Incidente	H. Talca	Origen	DLP	Abd	LOZADA ROSARIO MARCELA	SOC Sistema - Deneg. Log de Eventos de dispositivos	11/05/2018	Junio		Grave	Verde
129	Casos	Incidente	Saga F.	Origen	DLP	Abd	SOTOMAYOR OSWALDO	SOC Sistema - Deneg. Log de Eventos de dispositivos	8/05/2018	Junio		Grave	Verde

SISTEMAS PERU S.A.
 INGENIERO
 LUIS CARLOS
 DE COMERCIO Y SISTEMAS
 REG. CIP Nº 182851



REGISTRO DE CASOS DETECTADOS Y REPORTADOS DEL DEMO SOC

ID	Categoria	Incidente	Procedimiento	Oficina	DEP	Ata	Descripción	SOC	Fecha	Inicio	Fin	Estado	Verificación		
102	Corte	Incidente	F. Servicio Cliente	OficioScan	DLP	Ata	DAROURI CASTAÑO DA	SOC	Severo - Dema/ Vulnerabilidad DLP presentada en	04/02/19	Junio	11:49 p. m.	Cerrado	Verde	
101	Corte	Incidente	Saga F.	OficioScan	DLP	Ata	VALLEJO GUERRA MA	SOC	Severo - Dema/ Servicio de DLP cerrado	04/02/19	Junio	12:25 p. m.	Cerrado	Verde	
103	Corte	Incidente	F. Toluca	OficioScan	DLP	Ata	DE LA ROSA SOTO RAMA	SOC	Severo - Dema/ Servicio de DLP cerrado	04/02/19	Junio	4:39 p. m.	Cerrado	Verde	
104	Corte	Incidente	Finca F.	OficioScan	DLP	Ata	PANDES QUINTO FORCH	SOC	Severo - Dema/ Vulnerabilidad DLP presentada en	04/02/19	Junio	7:12 p. m.	Cerrado	Verde	
104	Corte	Incidente	F. Copacabana	OficioScan	DLP	Ata	RODRIGO VILLAGRA V	SOC	Severo - Dema/ Servicio de DLP cerrado	04/02/19	Junio	8:44 p. m.	Cerrado	Verde	
105	Corte	Incidente	Saga F.	OficioScan	DLP	Ata	CAMACHO P. NICOLA F	SOC	Severo - Dema/ Log de Bloqueo de dispositivos	04/02/19	Julio	02:32 p. m.	Cerrado	Verde	
106	Corte	Incidente	Saga F.	OficioScan	DLP	Ata	LUCENA ORLANDO Z	SOC	Severo - Dema/ Log de Bloqueo de dispositivos	04/02/19	Julio	11:21 p. m.	Cerrado	Verde	
107	Corte	Incidente	M. Toluca	OficioScan	DLP	Ata	DAZ RIBERO CRISTO	SOC	Severo - Dema/ Servicio de DLP cerrado	04/02/19	Julio	12:04 p. m.	1:00 p. m.	Cerrado	Verde
105	Corte	Incidente	Vicent F.	OficioScan	DLP	Ata	ORE LINDA P. MARK A	SOC	Severo - Dema/ Log de Bloqueo de dispositivos	02/02/19	Julio	09:58 p. m.	09:59 p. m.	Cerrado	Verde
108	Corte	Incidente	F. Boremas Conde	OficioScan	DLP	Ata	Carla Aurora Huamani	SOC	Severo - Dema/ Log de Bloqueo de dispositivos	04/02/19	Julio	10:43 p. m.	12:50 p. m.	Cerrado	Verde
109	Corte	Incidente	Comercio de Dep.	OficioScan	DLP	Ata	RODRIGO HUAYTA S	SOC	Severo - Dema/ Vulnerabilidad DLP presentada en	20/02/19	Julio	05:37 p. m.	10:38 p. m.	Cerrado	Verde
111	Corte	Incidente	Saga F.	OficioScan	DLP	Ata	Yusufi Muzuelo V	SOC	Severo - Dema/ Log de Bloqueo de dispositivos	23/02/19	Julio	11:38 p. m.	11:12 p. m.	Cerrado	Verde
112	Corte	Incidente	Saga F.	OficioScan	DLP	Ata	Alexa Gumpen	SOC	Severo - Dema/ Vulnerabilidad DLP presentada en	23/02/19	Julio	11:28 p. m.	08:18 p. m.	Cerrado	Verde
110	Corte	Incidente	Finca F.	OficioScan	DLP	Ata	Juan Carlos Villarreal	SOC	Severo - Dema/ Log de Bloqueo de dispositivos	24/02/19	Julio	11:27 p. m.	11:29 p. m.	Cerrado	Verde
114	Corte	Incidente	Comercio de Dep.	OficioScan	DLP	Ata	Tatiana Sola	SOC	Severo - Dema/ Log de Bloqueo de dispositivos	25/02/19	Julio	11:34 p. m.	11:44 p. m.	Cerrado	Verde
113	Corte	Incidente	F. Boremas Conde	OficioScan	DLP	Ata	JOSE LUIS RAMIREZ M	SOC	Severo - Dema/ Log de Bloqueo de dispositivos	25/02/19	Julio	13:07 p. m.	11:03 p. m.	Cerrado	Verde
116	Corte	Incidente	F. Toluca	OficioScan	DLP	Ata	RODRIGO HERAZA R	SOC	Severo - Dema/ Log de Bloqueo de dispositivos	21/02/19	Julio	19:00 p. m.	19:05 p. m.	Cerrado	Verde
117	Corte	Incidente	F. Toluca	OficioScan	DLP	Ata	HILARIO JAYTA W	SOC	Severo - Dema/ Servicio de DLP cerrado	11/02/19	Julio	04:45 p. m.	10:41 p. m.	Cerrado	Verde
118	Corte	Incidente	Saga F.	OficioScan	DLP	Ata	WALTER FLORES M	SOC	Severo - Dema/ Servicio de DLP cerrado	21/02/19	Julio	05:36 p. m.	05:35 p. m.	Cerrado	Verde
119	Corte	Incidente	Comercio de Dep.	OficioScan	DLP	Ata	Tatiana Sola	SOC	Severo - Dema/ Log de Bloqueo de dispositivos	21/02/19	Julio	11:57 p. m.	11:38 p. m.	Cerrado	Verde
120	Corte	Incidente	Finca F.	OficioScan	DLP	Ata	WALTER FLORES M	SOC	Severo - Dema/ Servicio de DLP cerrado	21/02/19	Julio	15:30 p. m.	15:33 p. m.	Cerrado	Verde
121	Corte	Incidente	Comercio de Dep.	OficioScan	DLP	Ata	Tatiana Sola	SOC	Severo - Dema/ Log de Bloqueo de dispositivos	04/02/19	Agosto	17:34 p. m.	17:29 p. m.	Cerrado	Verde
122	Corte	Incidente	F. Boremas Conde	OficioScan	DLP	Ata	Sofia Rodriguez Man	SOC	Severo - Dema/ Log de Bloqueo de dispositivos	04/02/19	Agosto	11:18 p. m.	11:30 p. m.	Cerrado	Verde
123	Corte	Incidente	Finca F.	OficioScan	DLP	Ata	Umar Castro	SOC	Severo - Dema/ Log de Bloqueo de dispositivos	03/02/19	Agosto	11:28 p. m.	11:31 p. m.	Cerrado	Verde
124	Corte	Incidente	Saga F.	OficioScan	DLP	Ata	Sara Healy Page	SOC	Severo - Dema/ Log de Bloqueo de dispositivos	02/02/19	Agosto	11:26 p. m.	11:26 p. m.	Cerrado	Verde
125	Corte	Incidente	Comercio de Dep.	OficioScan	DLP	Ata	Agustina Jara	SOC	Severo - Dema/ Log de Bloqueo de dispositivos	12/02/19	Agosto	12:08 p. m.	12:08 p. m.	Cerrado	Verde

SIGCODES DEL PERU S.A.C.

 Juan Carlos Villarreal

 Gerente

 LINARES SUAREZ

 ING. EN SISTEMAS


 DE COMPUTACION Y SISTEMAS

 Reg. C.P. Nº 18041



REGISTRO DE CASOS DETECTADOS Y REPORTADOS DEL DEMO SOC

Nº	Categoría	Incidente	Nombre	Oficina	Reg. de Agencia	Ciudad	Descripción	Código	Fecha	Hora Inicial	Hora Final	Ciudad	Verde
152	Casos	Incidente	M. Talara	OficioSan	Reg. de Agencia	Cusco	De La Cruz Cecilia (Externa)	200	2020/09	11:05 a.m.	11:11 a.m.	Cusco	Verde
153	Casos	Incidente	Danco F.	OficioSan	Reg. de Agencia	Cusco	De La Cruz Cecilia (Externa)	200	2020/09	11:36 a.m.	11:38 a.m.	Cusco	Verde
154	Casos	Incidente	Rivero P.	OficioSan	Reg. de Agencia	Cusco	Villar Antonio	200	2020/09	11:56 a.m.	11:52 a.m.	Cusco	Verde
155	Casos	Incidente	Danco F.	OficioSan	Reg. de Agencia	Cusco	Vejez Ana Mercedes	200	2020/09	14:32 a.m.	14:34 p.m.	Cusco	Verde
156	Casos	Incidente	M. Talara	OficioSan	Reg. de Agencia	Cusco	Guatemala Luis	200	2020/09	17:35 p.m.	17:38 p.m.	Cusco	Verde
157	Casos	Incidente	Danco F.	OficioSan	Reg. de Agencia	Cusco	Ando Katerin	200	2020/09	18:28 a.m.	18:21 a.m.	Cusco	Naranja
158	Casos	Incidente	Rivero P.	OficioSan	Reg. de Agencia	Cusco	De La Cruz Cecilia (Externa)	200	2020/09	18:12 a.m.	17:14 a.m.	Cusco	Verde
159	Casos	Incidente	Silbac	OficioSan	Reg. de Agencia	Cusco	De La Cruz Cecilia (Externa)	200	2020/09	18:19 a.m.	18:22 a.m.	Cusco	Verde
160	Casos	Incidente	M. Talara	OficioSan	Reg. de Agencia	Cusco	Guatemala Luis - Agencias	200	2020/09	18:24 a.m.	18:28 a.m.	Cusco	Verde
161	Casos	Incidente	Danco F.	OficioSan	Reg. de Agencia	Cusco	Imenes	200	2020/09	18:36 p.m.	18:38 p.m.	Cusco	Verde
162	Casos	Incidente	Danco F.	OficioSan	Reg. de Agencia	Cusco	Zacarias Ben	200	2020/09	18:52 p.m.	18:53 p.m.	Cusco	Verde
163	Casos	Incidente	F. Corporativo	OficioSan	Reg. de Agencia	Cusco	De La Cruz Cecilia (Externa)	200	2020/09	18:59 p.m.	18:45 p.m.	Cusco	Verde
164	Casos	Incidente	F. Corporativo	OficioSan	Reg. de Agencia	Cusco	Guatemala Luis (Externa)	200	2020/09	18:58 p.m.	18:59 p.m.	Cusco	Verde
165	Casos	Incidente	Rivero P.	OficioSan	Reg. de Agencia	Cusco	De La Cruz Cecilia (Externa)	200	2020/09	19:46 p.m.	19:58 p.m.	Cusco	Verde
166	Casos	Incidente	Danco F.	OficioSan	Reg. de Agencia	Cusco	Villar Antonio	200	2020/09	19:47 a.m.	19:49 a.m.	Cusco	Verde
167	Casos	Incidente	Silbac	OficioSan	Reg. de Agencia	Cusco	De La Cruz Cecilia (Externa)	200	2020/09	19:57 a.m.	19:59 a.m.	Cusco	Verde
168	Casos	Incidente	Danco F.	OficioSan	Reg. de Agencia	Cusco	Vejez Ana Mercedes	200	2020/09	19:58 a.m.	19:59 a.m.	Cusco	Verde
169	Casos	Incidente	Ortiz Gendar	OficioSan	Reg. de Agencia	Cusco	Jose Luis Prado Sanchez	200	2020/09	19:59 a.m.	19:57 p.m.	Cusco	Verde
170	Casos	Incidente	Silbac	OficioSan	Reg. de Agencia	Cusco	Guatemala Luis	200	2020/09	19:59 a.m.	19:58 p.m.	Cusco	Verde
171	Casos	Incidente	M. Talara	OficioSan	Reg. de Agencia	Cusco	Guatemala Luis	200	2020/09	19:59 a.m.	19:59 p.m.	Cusco	Verde
172	Casos	Incidente	Danco F.	OficioSan	Reg. de Agencia	Cusco	De La Cruz Cecilia (Externa)	200	2020/09	19:59 a.m.	19:40 a.m.	Cusco	Verde
173	Casos	Incidente	Danco F.	OficioSan	Reg. de Agencia	Cusco	Vejez Ana Mercedes	200	2020/09	19:59 a.m.	19:40 a.m.	Cusco	Verde
174	Casos	Incidente	Danco F.	OficioSan	Reg. de Agencia	Cusco	Vejez Ana Mercedes	200	2020/09	19:59 a.m.	19:40 a.m.	Cusco	Verde
175	Casos	Incidente	Danco F.	OficioSan	Reg. de Agencia	Cusco	Vejez Ana Mercedes	200	2020/09	19:59 a.m.	19:40 p.m.	Cusco	Verde
176	Casos	Incidente	Danco F.	OficioSan	Reg. de Agencia	Cusco	Vejez Ana Mercedes	200	2020/09	19:59 a.m.	19:40 p.m.	Cusco	Verde
177	Casos	Incidente	Danco F.	OficioSan	Reg. de Agencia	Cusco	Vejez Ana Mercedes	200	2020/09	19:59 a.m.	19:40 p.m.	Cusco	Verde
178	Casos	Incidente	Danco F.	OficioSan	Reg. de Agencia	Cusco	Vejez Ana Mercedes	200	2020/09	19:59 a.m.	19:40 p.m.	Cusco	Verde
179	Casos	Incidente	Danco F.	OficioSan	Reg. de Agencia	Cusco	Vejez Ana Mercedes	200	2020/09	19:59 a.m.	19:40 p.m.	Cusco	Verde
180	Casos	Incidente	Danco F.	OficioSan	Reg. de Agencia	Cusco	Vejez Ana Mercedes	200	2020/09	19:59 a.m.	19:40 p.m.	Cusco	Verde
181	Casos	Incidente	Danco F.	OficioSan	Reg. de Agencia	Cusco	Vejez Ana Mercedes	200	2020/09	19:59 a.m.	19:40 p.m.	Cusco	Verde
182	Casos	Incidente	Danco F.	OficioSan	Reg. de Agencia	Cusco	Vejez Ana Mercedes	200	2020/09	19:59 a.m.	19:40 p.m.	Cusco	Verde
183	Casos	Incidente	Danco F.	OficioSan	Reg. de Agencia	Cusco	Vejez Ana Mercedes	200	2020/09	19:59 a.m.	19:40 p.m.	Cusco	Verde
184	Casos	Incidente	Danco F.	OficioSan	Reg. de Agencia	Cusco	Vejez Ana Mercedes	200	2020/09	19:59 a.m.	19:40 p.m.	Cusco	Verde
185	Casos	Incidente	Danco F.	OficioSan	Reg. de Agencia	Cusco	Vejez Ana Mercedes	200	2020/09	19:59 a.m.	19:40 p.m.	Cusco	Verde
186	Casos	Incidente	Danco F.	OficioSan	Reg. de Agencia	Cusco	Vejez Ana Mercedes	200	2020/09	19:59 a.m.	19:40 p.m.	Cusco	Verde
187	Casos	Incidente	Danco F.	OficioSan	Reg. de Agencia	Cusco	Vejez Ana Mercedes	200	2020/09	19:59 a.m.	19:40 p.m.	Cusco	Verde


 JUAN CARLOS BARRETO
 DIRECTOR GENERAL
 DE COMPUTACION Y SISTEMAS
 Reg. CP Nº 180551




REGISTRO DE CASOS DETECTADOS Y REPORTE DE LOS DEL DEMO SOC

Nº	Caso	Incidente	Nombre	Oficina	Sistema	País	Descripción	Fecha	Hora	Estado	Acción
208	Caso	Incidente	Rosa F.	Oficina	Sistema Operativo	México	CONSEJO SALVADOREÑO	20/08/2014	10:30 p.m.	Cerrado	Verde
209	Caso	Incidente	Rosa F.	Oficina	Sistema Operativo	México	CONSEJO SALVADOREÑO	24/08/2014	11:08 a.m.	Cerrado	Verde
210	Caso	Incidente	Rosa F.	Oficina	Sistema Operativo	México	CONSEJO SALVADOREÑO	26/08/2014	12:38 p.m.	Cerrado	Verde
211	Caso	Incidente	Rosa F.	Oficina	Sistema Operativo	México	CONSEJO SALVADOREÑO	26/08/2014	15:32 p.m.	Cerrado	Verde
212	Caso	Incidente	H. Taluz	Oficina	Sistema Operativo	México	CONSEJO SALVADOREÑO	20/08/2014	16:28 p.m.	Cerrado	Verde
213	Caso	Incidente	H. Taluz	Oficina	Sistema Operativo	México	CONSEJO SALVADOREÑO	18/07/2014	16:36 p.m.	Cerrado	Verde
214	Caso	Incidente	F. Conzatti	Oficina	Sistema Operativo	México	CONSEJO SALVADOREÑO	18/07/2014	17:01 p.m.	Cerrado	Verde
215	Caso	Incidente	Rosa F.	Oficina	Sistema Operativo	México	CONSEJO SALVADOREÑO	24/07/2014	15:35 p.m.	Cerrado	Verde
216	Caso	Incidente	Rosa F.	Oficina	Sistema Operativo	México	CONSEJO SALVADOREÑO	3/08/2014	12:41 p.m.	Cerrado	Verde
217	Caso	Incidente	Rosa F.	Oficina	Sistema Operativo	México	CONSEJO SALVADOREÑO	15/08/2014	18:35 p.m.	Cerrado	Verde
218	Caso	Incidente	Saya F.	Oficina	Sistema Operativo	México	CONSEJO SALVADOREÑO	20/07/2014	11:00 a.m.	Cerrado	Verde
219	Caso	Incidente	Saya F.	Oficina	Sistema Operativo	México	CONSEJO SALVADOREÑO	28/07/2014	12:15 p.m.	Cerrado	Verde
220	Caso	Incidente	H. Taluz	Oficina	Sistema Operativo	México	CONSEJO SALVADOREÑO	6/07/2014	13:13 p.m.	Cerrado	Verde
221	Caso	Incidente	Carolina de Sep.	Oficina	Sistema Operativo	México	CONSEJO SALVADOREÑO	17/07/2014	12:25 p.m.	Cerrado	Verde
222	Caso	Incidente	Saya F.	Oficina	Sistema Operativo	México	CONSEJO SALVADOREÑO	17/08/2014	18:00 p.m.	Cerrado	Verde
223	Caso	Incidente	Carolina de Sep.	Oficina	Sistema Operativo	México	CONSEJO SALVADOREÑO	17/08/2014	10:30 a.m.	Cerrado	Verde
224	Caso	Incidente	Saya F.	Oficina	Sistema Operativo	México	CONSEJO SALVADOREÑO	17/08/2014	19:48 p.m.	Cerrado	Verde
225	Caso	Incidente	Rosa F.	Oficina	Sistema Operativo	México	CONSEJO SALVADOREÑO	17/08/2014	14:55 p.m.	Cerrado	Verde
226	Caso	Incidente	Rosa F.	Oficina	Sistema Operativo	México	CONSEJO SALVADOREÑO	18/08/2014	03:28 a.m.	Cerrado	Verde
227	Caso	Incidente	H. Taluz	Oficina	Sistema Operativo	México	CONSEJO SALVADOREÑO	21/08/2014	09:30 a.m.	Cerrado	Verde
228	Caso	Incidente	Rosa F.	Oficina	Sistema Operativo	México	CONSEJO SALVADOREÑO	21/08/2014	18:45 p.m.	Cerrado	Verde
229	Caso	Incidente	Rosa F.	Oficina	Sistema Operativo	México	CONSEJO SALVADOREÑO	21/08/2014	11:28 a.m.	Cerrado	Verde
230	Caso	Incidente	F. Conzatti	Oficina	Sistema Operativo	México	CONSEJO SALVADOREÑO	23/07/2014	18:47 p.m.	Cerrado	Verde
231	Caso	Incidente	Rosa F.	Oficina	Sistema Operativo	México	CONSEJO SALVADOREÑO	21/08/2014	13:31 p.m.	Cerrado	Verde
232	Caso	Incidente	Rosa F.	Oficina	Sistema Operativo	México	CONSEJO SALVADOREÑO	22/08/2014	18:38 p.m.	Cerrado	Verde
233	Caso	Incidente	Rosa F.	Oficina	Sistema Operativo	México	CONSEJO SALVADOREÑO	23/07/2014	18:38 p.m.	Cerrado	Verde

SICOPEL DEL PERU S.A.C.
 Calle Comercio 1001, Lima 18100
 Telf: 011 422 2222
 www.sicopel.com.pe
 Representante Legal: _____
 Inge. Juan Carlos Barrero
 DE COMPUTACION Y SISTEMAS
 Reg. CIP N° 10510

Anexo N° 12

Cuestionario de la encuesta debidamente llenado por el usuario y firmada por representantes de la empresa Siscotec del Perú SAC.

 **siscotec**

Nro:

ENCUESTA DE SASTIFACCIÓN (SIN SOC)

Usuario :

Empresa :

Tipo de Caso :

P1 ¿Cómo califica el tiempo utilizado para la solución del incidente y/o requerimiento con el sistema actual de Siscotec?

Excelente Muy Bueno Bueno Regular Deficiente

P2 ¿Cómo fue la calidad de la atención recibida del personal de Siscotec?

Excelente Muy Bueno Bueno Regular Deficiente

P3 ¿El servicio brindado por el personal de Siscotec, solucionó su incidencia y/o requerimiento en la primera atención?

Si No

P4 ¿La incidencia fue reportado por usted?

Si No

SISCOTEC DEL PERU S.A.C.

.....
Angélica del Carmel Quinzá Garcés
DNI: 45922315
Representante Legal


.....
LARRY MANIZ
LINARES BARRETO
INGENIERO
DE COMPUTACION Y SISTEMAS
Reg. CIP Nº 180551



Nro:

ENCUESTA DE SASTIFACCIÓN (SIN SOC)

Usuario :
Empresa :
Tipo de Caso :

P1 ¿Cómo califica el tiempo utilizado para la solución del incidente y/o requerimiento con el sistema actual de Siscotec?

Excelente Muy Bueno Bueno Regular Deficiente

P2 ¿Cómo fue la calidad de la atención recibida del personal de Siscotec?

Excelente Muy Bueno Bueno Regular Deficiente

P3 ¿El servicio brindado por el personal de Siscotec, solucionó su incidencia y/o requerimiento en la primera atención?

Si No

P4 ¿La incidencia fue reportado por usted?

Si No

SISCOTEC DEL PERU S.A.C.

Angela Carmel Quiróz Garces
DNI: 45922315
Representante Legal

LARRY MANUEL
LINARES BARRETO
INGENIERO
DE COMPUTACION Y SISTEMAS
Reg. CIP Nº 180551



Nro:

ENCUESTA DE SASTIFACCIÓN (SIN SOC)

Usuario :
Empresa :
Tipo de Caso :

P1 ¿Cómo califica el tiempo utilizado para la solución del incidente y/o requerimiento con el sistema actual de Siscotec?

Excelente Muy Bueno Bueno Regular Deficiente

P2 ¿Cómo fue la calidad de la atención recibida del personal de Siscotec?

Excelente Muy Bueno Bueno Regular Deficiente

P3 ¿El servicio brindado por el personal de Siscotec, solucionó su incidencia y/o requerimiento en la primera atención?

Si No

P4 ¿La incidencia fue reportado por usted?

Si No

SISCOTEC DEL PERU S.A.C.

Angélica del Carmen Muro Garcés
DNI: 45922315
Representante Legal

LARRY MANUEL
LINARES BARRETO
INGENIERO
DE COMPUTACION Y SISTEMAS
Reg. CIP Nº 180551



Nro:

ENCUESTA DE SASTIFACCIÓN (SIN SOC)

Usuario :
Empresa :
Tipo de Caso :

- P1 ¿Cómo califica el tiempo utilizado para la solución del incidente y/o requerimiento con el sistema actual de Siscotec?
Excelente Muy Bueno Bueno Regular Deficiente
- P2 ¿Cómo fue la calidad de la atención recibida del personal de Siscotec?
Excelente Muy Bueno Bueno Regular Deficiente
- P3 ¿El servicio brindado por el personal de Siscotec, solucionó su incidencia y/o requerimiento en la primera atención?
Si No
- P4 ¿La incidencia fue reportado por usted?
Si No

SISCOTEC DEL PERU S.A.C.

Angela de Camacho Garces
DNI: 45922315
Representante Legal

LARRY MANUEL
LINARES BARRETO
INGENIERO
DE COMPUTACION Y SISTEMAS
Reg. CIP Nº 180551



Nro: _____

ENCUESTA DE SASTIFACCIÓN (SIN SOC)

Usuario : Florencia Aucapina Quispe
Empresa : El Supermercado Zottus
Tipo de Caso : Incidente

P1 ¿Cómo califica el tiempo utilizado para la solución del incidente y/o requerimiento con el sistema actual de Siscotec?

Excelente Muy Bueno Bueno Regular Deficiente

P2 ¿Cómo fue la calidad de la atención recibida del personal de Siscotec?

Excelente Muy Bueno Bueno Regular Deficiente


P3 ¿El servicio brindado por el personal de Siscotec, solucionó su incidencia y/o requerimiento en la primera atención?

Si No

P4 ¿La incidencia fue reportado por usted?

Si No

SISCOTEC DEL PERU S.A.C.


Angela Larraín Quiroz Garces
DNI: 45922315
Representante Legal


LARRY MANOS
LINARES BARRETO
INGENIERO
DE COMPUTACION Y SISTEMAS
Reg. CIP Nº 180551



Nro:

ENCUESTA DE SASTIFACCIÓN (CON SOC)

Usuario :
Empresa :
Tipo de Caso :

P1 ¿Cómo califica el tiempo utilizado para la solución del incidente y/o requerimiento con el sistema actual de Siscotec?

Excelente Muy Bueno Bueno Regular Deficiente

P2 ¿Cómo fue la calidad de la atención recibida del personal de Siscotec?

Excelente Muy Bueno Bueno Regular Deficiente


P3 ¿El servicio brindado por el personal de Siscotec, solucionó su incidencia y/o requerimiento en la primera atención?

Si No

P4 ¿La incidencia fue reportado por usted?

Si No

SISCOTEC DEL PERU S.A.C.


Angela del Carmen Juarez Garces
DNI: 45922315
Representante Legal


LARRY MANUEL
LINARES BARRETO
INGENIERO
DE COMPUTACION Y SISTEMAS
Reg. CIP No 180551



Nro:

ENCUESTA DE SASTIFACCIÓN (CON SOC)

Usuario :
Empresa :
Tipo de Caso :

P1 ¿Cómo califica el tiempo utilizado para la solución del incidente y/o requerimiento con el sistema actual de Siscotec?

Excelente Muy Bueno Bueno Regular Deficiente

P2 ¿Cómo fue la calidad de la atención recibida del personal de Siscotec?

Excelente Muy Bueno Bueno Regular Deficiente

P3 ¿El servicio brindado por el personal de Siscotec, solucionó su incidencia y/o requerimiento en la primera atención?

Si No

P4 ¿La incidencia fue reportado por usted?

Si No

SISCOTEC DEL PERU S.A.C.


Angela del Carmen Quirós Garcés
DNI: 45922315
Representante Legal


LARRY MANUEL
LINARES BARRETO
INGENIERO
DE COMPUTACION Y SISTEMAS
Reg. CIP Nº 180551



Nro:

ENCUESTA DE SASTIFACCIÓN (CON SOC)

Usuario :
Empresa :
Tipo de Caso :

P1 ¿Cómo califica el tiempo utilizado para la solución del incidente y/o requerimiento con el sistema actual de Siscotec?

Excelente Muy Bueno Bueno Regular Deficiente

P2 ¿Cómo fue la calidad de la atención recibida del personal de Siscotec?

Excelente Muy Bueno Bueno Regular Deficiente

P3 ¿El servicio brindado por el personal de Siscotec, solucionó su incidencia y/o requerimiento en la primera atención?


Si No

P4 ¿La incidencia fue reportado por usted?

Si No



SISCOTEC DEL PERU S.A.C.


Angela del Carmen Ojeda Garcos
DNI: 45922315
Representante Legal


LARRY MARQUEZ
LINARES BARRETO
INGENIERO
DE COMPUTACION Y SISTEMAS
Reg. CIP Nº 160551



Nro:

ENCUESTA DE SASTIFACCIÓN (CON SOC)

Usuario :
Empresa :
Tipo de Caso :

P1 ¿Cómo califica el tiempo utilizado para la solución del incidente y/o requerimiento con el sistema actual de Siscotec?

Excelente Muy Bueno Bueno Regular Deficiente

P2 ¿Cómo fue la calidad de la atención recibida del personal de Siscotec?

Excelente Muy Bueno Bueno Regular Deficiente

P3 ¿El servicio brindado por el personal de Siscotec, solucionó su incidencia y/o requerimiento en la primera atención?

Si No

P4 ¿La incidencia fue reportado por usted?

Si No



SISCOTEC DEL PERU S.A.C.

Angela del Carmen Quispe Garcés
DNI: 45922315
Representante Legal

LARRY MANUEL
LINARES BARRÉTO
INGENIERO
DE COMPUTACIÓN Y SISTEMAS
Reg. CIP Nº 180551



Nro: _____

ENCUESTA DE SASTIFACCIÓN (CON SOC)

Usuario : Marco Reyes Pardo
Empresa : Saga F.
Tipo de Caso : Incidente

P1 ¿Cómo califica el tiempo utilizado para la solución del incidente y/o requerimiento con el sistema actual de Siscotec?

Excelente Muy Bueno Bueno Regular Deficiente

P2 ¿Cómo fue la calidad de la atención recibida del personal de Siscotec?

Excelente Muy Bueno Bueno Regular Deficiente

P3 ¿El servicio brindado por el personal de Siscotec, solucionó su incidencia y/o requerimiento en la primera atención?

Si No

P4 ¿La incidencia fue reportado por usted?

Si No

SISCOTEC DEL PERU S.A.C.


Angélica del Carmen Duró Garces
DNI: 4592315
Representante Legal


LARRY MANUEL
LINARES BARRETO
INGENIERO
DE COMPUTACION Y SISTEMAS
Reg. CIP Nº 160551

Anexo N° 13

Análisis de la confiabilidad de las encuestas sistema demo SOC mediante el coeficiente de Alfa de Crombach.

ANÁLISIS DE LA CONFIABILIDAD DE LAS ENCUESTAS DEMO SOC MEDIANTE EL COEFICIENTE ALFA DE CRONBACH

BASE DE DATOS ENCUESTA							
Encuesta	Tipo de Incidencia	Empresa	P1	P2	P3	P4	Total
1	Incidente	Sifsac	5	4	1	1	11
2	Incidente	Saga F.	5	4	1	2	12
3	Incidente	Sifsac	5	4	1	1	11
4	Incidente	Sifsac	5	4	1	2	12
5	Incidente	Sifsac	4	5	1	2	12
6	Incidente	Sifsac	4	5	1	1	11
7	Incidente	Sifsac	4	5	1	2	12
8	Incidente	Viajes F.	4	5	1	1	11
9	Incidente	Saga F.	4	5	1	2	12
10	Incidente	H. Tottus	4	5	1	1	11
11	Incidente	Corredora de S	4	5	1	2	12
12	Incidente	Banco F.	4	5	1	1	11
13	Incidente	Banco F.	4	5	1	1	11
14	Incidente	H. Tottus	4	5	1	1	11
15	Incidente	F. Servicios Ce	4	5	1	1	11
16	Incidente	Saga F.	4	5	1	1	11
17	Incidente	Saga F.	4	5	1	1	11
18	Incidente	Viajes F.	4	5	1	1	11
19	Incidente	H. Tottus	4	5	1	1	11
20	Incidente	F. Corporativo	4	5	1	1	11
21	Incidente	Sifsac	4	5	1	1	11
22	Incidente	Sifsac	4	5	1	1	11
23	Incidente	Contac Center	4	5	1	1	11
24	Incidente	Saga F.	4	5	1	1	11
25	Incidente	H. Tottus	4	5	1	2	12
26	Incidente	Banco F.	4	5	1	1	11
27	Incidente	Sifsac	4	5	1	1	11
28	Incidente	Contac Center	4	5	1	1	11
29	Incidente	Sifsac	4	5	1	2	12
30	Incidente	Sifsac	4	5	1	1	11
31	Incidente	Sifsac	4	5	1	1	11
32	Incidente	Sifsac	4	5	1	1	11
33	Incidente	Sifsac	4	5	1	1	11
34	Incidente	Banco F.	4	5	1	1	11
35	Incidente	Banco F.	4	5	1	1	11
36	Incidente	Sifsac	5	4	1	1	11
37	Incidente	Sifsac	5	4	1	2	12
38	Incidente	Banco F.	5	4	1	2	12
39	Incidente	H. Tottus	5	4	1	2	12
40	Incidente	Saga F.	5	4	1	2	12
41	Incidente	H. Tottus	5	4	1	2	12
42	Incidente	Corredora de S	5	4	1	1	11
43	Incidente	F. Corporativo	5	4	1	1	11
44	Incidente	Banco F.	5	4	1	1	11
45	Incidente	Contac Center	5	4	1	2	12
46	Incidente	Banco F.	3	5	1	2	11
47	Incidente	Banco F.	3	5	1	2	11
48	Incidente	Banco F.	3	5	1	2	11
49	Incidente	Banco F.	3	5	1	2	11
50	Incidente	Banco F.	3	5	1	2	11
51	Incidente	Banco F.	3	5	1	2	11
52	Incidente	Banco F.	3	5	1	2	11
53	Incidente	Banco F.	3	5	1	2	11
54	Incidente	Banco F.	3	5	1	2	11
55	Incidente	Banco F.	3	5	1	2	11
56	Incidente	Banco F.	3	5	1	2	11
57	Incidente	Banco F.	4	4	1	2	11
58	Incidente	Banco F.	4	4	1	2	11
59	Incidente	Banco F.	4	4	1	2	11
60	Incidente	Banco F.	4	4	1	2	11
61	Incidente	Banco F.	4	4	1	2	11

K (Número total de ítems)	4
Vi (Varianza de cada ítem)	0.84003
Vt (Varianza Total)	0.51932

Sección1	1.333
Sección2	-0.618
ABSOLUTO S2	0.618

α (Alfa de Cronbach)	0.823
----------------------	-------


 LARRY MANUEL
 LINARES BARRETO
 INGENIERO
 DE COMPUTACION Y SISTEMAS
 Reg. CIP Nº 180551

SISCOTEC DEL PERU S.A.C.

 Anga del Carmen Quiroz Garces
 DNI: 45922315
 Representante Legal

ANÁLISIS DE LA CONFIABILIDAD DE LAS ENCUESTAS DEMO SOC MEDIANTE EL COEFICIENTE ALFA DE CRONBACH

62	Incidente	Banco F.	4	4	1	2	11
63	Incidente	Banco F.	4	4	1	2	11
64	Incidente	Banco F.	4	4	1	2	11
65	Incidente	Banco F.	4	4	1	2	11
66	Incidente	Banco F.	4	4	1	2	11
67	Incidente	Banco F.	4	4	1	2	11
68	Incidente	Banco F.	4	4	1	2	11
69	Incidente	Banco F.	4	4	1	2	11
70	Incidente	Banco F.	4	5	1	2	12
71	Incidente	Banco F.	4	5	1	2	12
72	Incidente	Banco F.	4	5	1	2	12
73	Incidente	Banco F.	4	5	1	2	12
74	Incidente	F. Corporativo	4	5	1	2	12
75	Incidente	Banco F.	4	5	1	2	12
76	Incidente	Banco F.	4	4	1	2	11
77	Incidente	Banco F.	4	4	1	2	11
78	Incidente	Banco F.	4	4	1	2	11
79	Incidente	Sifisac	4	4	1	2	11
80	Incidente	Sifisac	4	4	1	2	11
81	Incidente	Banco F.	4	4	1	2	11
82	Incidente	Banco F.	4	4	1	2	11
83	Incidente	Banco F.	4	4	1	2	11
84	Incidente	Banco F.	4	4	1	2	11
85	Incidente	Banco F.	4	4	1	2	11
86	Incidente	F. Corporativo	4	4	1	2	11
87	Incidente	Banco F.	4	4	1	2	11
88	Incidente	Banco F.	4	4	1	2	11
89	Incidente	Banco F.	3	5	1	2	11
90	Incidente	Saga F.	3	5	1	2	11
91	Incidente	Banco F.	3	5	1	2	11
92	Incidente	F. Servicios Ce	3	5	1	2	11
93	Incidente	Saga F.	3	5	1	2	11
94	Incidente	Corredora de S	3	5	1	2	11
95	Incidente	H. Totius	3	5	1	2	11
96	Incidente	H. Totius	3	5	1	2	11
97	Incidente	Saga F.	3	5	1	2	11
98	Incidente	H. Totius	3	5	1	2	11
99	Incidente	H. Totius	3	5	1	2	11
100	Incidente	H. Totius	3	5	1	2	11
101	Incidente	H. Totius	3	5	1	2	11
102	Incidente	H. Totius	3	5	1	2	11
103	Incidente	Banco F.	3	5	1	2	11
104	Incidente	F. Corporativo	3	5	1	2	11
105	Incidente	Saga F.	3	5	1	2	11
106	Incidente	Saga F.	5	5	1	2	13
107	Incidente	Banco F.	5	5	1	2	13
108	Incidente	H. Totius	5	5	1	2	13
109	Incidente	Corredora de S	5	5	1	2	13
110	Incidente	H. Totius	5	5	1	2	13
111	Incidente	Saga F.	5	5	1	2	13
112	Incidente	Corredora de S	5	5	1	2	13
113	Incidente	Saga F.	5	5	1	2	13
114	Incidente	Corredora de S	5	5	1	2	13
115	Incidente	Saga F.	5	5	1	2	13
116	Incidente	Corredora de S	5	5	1	2	13
117	Incidente	Banco F.	5	5	1	2	13
118	Incidente	H. Totius	5	5	1	2	13
119	Incidente	H. Totius	5	5	1	2	13
120	Incidente	H. Totius	5	5	1	2	13
121	Incidente	H. Totius	5	5	1	2	13
122	Incidente	F. Corporativo	5	5	1	2	13
123	Incidente	Saga F.	5	5	1	2	13
124	Incidente	Saga F.	5	5	1	2	13
125	Incidente	Saga F.	5	5	1	2	13
126	Incidente	Banco F.	5	5	1	2	13
127	Incidente	Banco F.	5	5	1	2	13
128	Incidente	H. Totius	5	5	1	2	13


LARRY MARIBEL
LINARES BARRETO
INGENIERO
DE COMPUTACION Y SISTEMAS
Reg. CIP Nº 180551


SISCOTEC DEL PERU S.A.C.


Angélica del Carmen Quiroz Garcés
DNI: 45822315
Representante Legal

ANÁLISIS DE LA CONFIABILIDAD DE LAS ENCUESTAS DEMO SOC MEDIANTE EL COEFICIENTE ALFA DE CRONBACH

129	Incidente	Saga F.	5	5	1	2	13
130	Incidente	F. Servicios Ce	5	5	1	2	13
131	Incidente	Saga F.	5	5	1	2	13
132	Incidente	H. Tottus	5	5	1	2	13
133	Incidente	Banco F.	5	5	1	2	13
134	Incidente	F. Corporativo	4	5	1	2	12
135	Incidente	Saga F.	4	5	1	2	12
136	Incidente	Saga F.	4	5	1	2	12
137	Incidente	H. Tottus	4	5	1	2	12
138	Incidente	Viajes F.	4	5	1	2	12
139	Incidente	F. Servicios Ce	4	5	1	2	12
140	Incidente	Corredora de S	4	5	1	2	12
141	Incidente	Saga F.	4	5	1	2	12
142	Incidente	Saga F.	4	5	1	2	12
143	Incidente	Banco F.	4	4	1	2	11
144	Incidente	Corredora de S	4	4	1	2	11
145	Incidente	F. Servicios Ce	4	4	1	2	11
146	Incidente	H. Tottus	4	4	1	2	11
147	Incidente	H. Tottus	4	4	1	2	11
148	Incidente	Banco F.	4	4	1	2	11
149	Incidente	Corredora de S	4	4	1	2	11
150	Incidente	Banco F.	4	4	1	2	11
151	Incidente	Corredora de S	4	4	1	2	11
152	Incidente	F. Servicios Ce	4	4	1	2	11
153	Incidente	Banco F.	4	4	1	2	11
154	Incidente	Saga F.	4	4	1	2	11
155	Incidente	Corredora de S	4	4	1	2	11
156	Incidente	Banco F.	4	5	1	2	12
157	Incidente	Banco F.	5	4	1	2	12
158	Incidente	Banco F.	4	5	1	2	12
159	Incidente	Saga F.	4	5	1	2	12
160	Incidente	Sifsac	5	4	1	2	12
161	Incidente	Corredora de S	4	4	1	2	11
162	Incidente	H. Tottus	4	4	1	2	11
163	Incidente	H. Tottus	3	5	1	2	11
164	Incidente	Corredora de S	4	5	1	2	12
165	Incidente	Saga F.	3	5	1	2	11
166	Incidente	H. Tottus	5	4	1	2	12
167	Incidente	Corredora de S	4	5	1	2	12
168	Incidente	Saga F.	4	5	1	2	12
169	Incidente	Banco F.	5	4	1	2	12
170	Incidente	H. Tottus	5	4	1	2	12
171	Incidente	Banco F.	5	4	1	2	12
172	Incidente	H. Tottus	5	4	1	2	12
173	Incidente	Sifsac	5	4	1	2	12
174	Incidente	H. Tottus	5	4	1	2	12
175	Incidente	Sifsac	5	4	1	2	12
176	Incidente	Banco F.	5	4	1	2	12
177	Incidente	H. Tottus	5	4	1	2	12
178	Incidente	H. Tottus	5	4	1	2	12
179	Incidente	H. Tottus	5	4	1	2	12
180	Incidente	H. Tottus	5	4	1	2	12
181	Incidente	H. Tottus	5	4	1	2	12
182	Incidente	H. Tottus	5	4	1	2	12
183	Incidente	Banco F.	5	4	1	2	12
184	Incidente	Banco F.	5	4	1	2	12
185	Incidente	Banco F.	4	5	1	2	12
186	Incidente	H. Tottus	4	5	1	2	12
187	Incidente	Banco F.	4	4	1	2	11
188	Incidente	Banco F.	4	4	1	2	11
189	Incidente	Sifsac	4	4	1	2	11
190	Incidente	H. Tottus	4	5	1	2	12
191	Incidente	Saga F.	4	5	1	2	12
192	Incidente	Banco F.	5	4	1	2	12
193	Incidente	F. Corporativo	5	4	1	2	12
194	Incidente	F. Corporativo	5	4	1	2	12
195	Incidente	Banco F.	5	4	1	2	12


 LARRY MANUEL
 LINARES BARRETO
 INGENIERO
 DE COMPUTACION Y SISTEMAS
 Reg. CIP N° 180551

SISCOTEC DEL PERU S.A.C.

 Angélica Carrón Quispe Garcos
 DNI: 45922315
 Representante Legal

ANÁLISIS DE LA CONFIABILIDAD DE LAS ENCUESTAS DEMO SOC MEDIANTE EL COEFICIENTE ALFA DE CRONBACH

196	Incidente	Saga F.	5	3	1	2	11
197	Incidente	Sifsac	5	4	1	2	12
198	Incidente	Banco F.	5	4	1	2	12
199	Incidente	Contac Center	5	4	1	2	12
200	Incidente	Sifsac	5	4	1	2	12
201	Incidente	H. Tottus	5	4	1	2	12
202	Incidente	Banco F.	5	4	1	2	12
203	Incidente	Saga F.	4	5	1	2	12
204	Incidente	Saga F.	4	5	1	2	12
205	Incidente	Saga F.	4	5	1	2	12
206	Incidente	Saga F.	4	5	1	2	12
207	Incidente	Banco F.	4	5	1	2	12
208	Incidente	Banco F.	4	5	1	2	12
209	Incidente	Banco F.	4	5	1	2	12
210	Incidente	Banco F.	5	3	1	2	11
211	Incidente	Banco F.	5	4	1	2	12
212	Incidente	H. Tottus	5	4	1	2	12
213	Incidente	H. Tottus	5	4	1	2	12
214	Incidente	F. Corporativo	5	3	1	2	11
215	Incidente	Banco F.	5	3	1	2	11
216	Incidente	Banco F.	4	5	1	2	12
217	Incidente	Banco F.	4	5	1	2	12
218	Incidente	Saga F.	4	5	1	2	12
219	Incidente	Saga F.	4	5	1	2	12
220	Incidente	H. Tottus	4	5	1	2	12
221	Incidente	Corredora de S	3	4	1	2	10
222	Incidente	Saga F.	3	4	1	2	10
223	Incidente	Corredora de S	3	4	1	2	10
224	Incidente	Saga F.	3	4	1	2	10
225	Incidente	Banco F.	3	4	1	2	10
226	Incidente	Banco F.	4	5	1	2	12
227	Incidente	H. Tottus	4	5	1	2	12
228	Incidente	Banco F.	4	5	1	2	12
229	Incidente	Banco F.	4	5	1	2	12
230	Incidente	F. Corporativo	4	5	1	2	12
231	Incidente	Banco F.	4	5	1	2	12
232	Incidente	Banco F.	4	5	1	2	12
233	Incidente	Banco F.	4	5	1	2	12
234	Incidente	Banco F.	4	5	1	2	12
235	Incidente	Banco F.	4	4	1	2	11
236	Incidente	Banco F.	4	4	1	2	11
237	Incidente	Saga F.	4	4	1	2	11
238	Incidente	Banco F.	4	4	1	2	11
			ESTADISTICOS				
VARIANZA			0.44	0.28	0.00	0.11	


 LARRY MANUEL
 LINARES BARRETO
 INGENIERO
 DE COMPUTACION Y SISTEMAS
 Reg. CIP Nº 180551

SISCOTEC DEL PERU S.A.C.

 Angela del Carmen Quiroz Garces
 DNI: 45922315
 Representante Legal

Anexo N° 14

Análisis de la confiabilidad de las encuestas sistema web de tickets mediante el coeficiente de Alfa de Crombach.

ANÁLISIS DE LA CONFIABILIDAD DE LAS ENCUESTAS SISTEMA WEB DE TICKETS MEDIANTE EL COEFICIENTE ALFA DE CRONBACH

BASE DE DATOS ENCUESTA							
Encuesta	Tipo de Incidencia	Empresa	P1	P2	P3	P4	Total
1	Incidente	Banco F.	3	5	2	1	11
2	Incidente	H. Toffus	4	5	2	1	12
3	Requerimiento	Banco F.	3	4	2	1	10
4	Requerimiento	Banco F.	4	5	2	1	12
5	Requerimiento	Banco F.	3	4	2	1	10
6	Incidente	Corredora de S	2	3	1	1	7
7	Requerimiento	Saga F.	2	3	1	1	7
8	Requerimiento	H. Toffus	3	4	2	1	10
9	Requerimiento	Corredora de S	3	5	2	1	11
10	Requerimiento	Corredora de S	3	4	2	1	10
11	Requerimiento	Banco F.	3	5	2	1	11
12	Requerimiento	Saga F.	1	3	1	1	6
13	Incidente	Banco F.	2	3	1	1	7
14	Incidente	Banco F.	2	3	1	1	7
15	Incidente	H. Toffus	1	3	1	1	6
16	Incidente	Sifsac	2	3	1	1	7
17	Incidente	Contac Cente	3	5	2	1	11
18	Incidente	Contac Cente	3	5	2	1	11
19	Incidente	Sifsac	3	4	2	1	10
20	Incidente	H. Toffus	3	5	2	1	11
21	Incidente	Sifsac	1	3	1	1	6
22	Incidente	Contac Cente	1	3	1	1	6
23	Incidente	Sifsac	3	5	2	1	11
24	Incidente	H. Toffus	3	5	2	1	11
25	Incidente	H. Toffus	3	5	2	1	11
26	Incidente	H. Toffus	3	4	2	1	10
27	Incidente	Contac Cente	1	3	1	1	6
28	Incidente	Sifsac	1	3	1	1	6
29	Incidente	H. Toffus	1	3	1	1	6
30	Incidente	H. Toffus	1	3	1	1	6
31	Incidente	Saga F.	3	4	2	1	10
32	Incidente	Saga F.	3	4	2	1	10
33	Incidente	Saga F.	3	4	2	1	10
34	Incidente	H. Toffus	3	4	2	1	10
35	Incidente	Sifsac	3	4	2	1	10
36	Incidente	Sifsac	3	4	2	1	10
37	Incidente	Sifsac	3	3	1	1	8
38	Incidente	Sifsac	3	3	1	1	8
39	Incidente	Sifsac	3	4	1	1	9
40	Requerimiento	Saga F.	3	3	1	1	8
41	Incidente	Saga F.	3	4	1	1	9
42	Incidente	Contac Cente	2	3	1	1	7
43	Incidente	H. Toffus	2	3	1	1	7
44	Incidente	H. Toffus	2	3	1	1	7
45	Incidente	Sifsac	2	3	1	1	7
46	Incidente	Saga F.	3	4	2	1	10
47	Incidente	H. Toffus	3	4	2	1	10
48	Incidente	Sifsac	3	4	2	1	10
49	Incidente	Sifsac	3	4	2	1	10
50	Incidente	Corredora de S	3	4	2	1	10
51	Incidente	Corredora de S	3	4	2	1	10
52	Incidente	Corredora de S	3	4	2	1	10

K (Número total de ítems)	4
Vi (Varianza de cada ítem)	1.10
Vt (Varianza Total)	2.31

Sección 1	1.333
Sección 2	0.526
ABSOLUTO S2	0.526

α (Alfa de Cronbach)	0.701
----------------------	-------


LINARES BARRETO
 INGENIERO
 DE COMPUTACION Y SISTEMAS
 Reg. CIP N° 180551

SISCOTEC DEL PERU S.A.C.

 Angela Quiroz
 DNI: 45922315
 Representante Legal

ANÁLISIS DE LA CONFIABILIDAD DE LAS ENCUESTAS SISTEMA WEB DE TICKETS MEDIANTE EL COEFICIENTE ALFA DE CRONBACH

53	Incidente	Corredora de	3	4	2	1	10
54	Incidente	Corredora de	3	4	2	1	10
55	Incidente	Corredora de	3	4	2	1	10
56	Requerimiento	H. Toltus	3	4	2	1	10
57	Incidente	H. Toltus	2	3	1	1	7
58	Incidente	H. Toltus	1	3	1	1	6
59	Requerimiento	Banco F.	2	3	1	1	7
60	Requerimiento	Corredora de	2	3	1	1	7
61	Incidente	Saga F.	2	3	1	1	7
62	Incidente	Corredora de	2	3	1	1	7
63	Requerimiento	Banco F.	1	3	1	1	6
64	Requerimiento	Banco F.	1	3	1	1	6
65	Incidente	F. Corporativo	1	3	1	1	6
66	Incidente	F. Corporativo	2	3	1	1	7
67	Requerimiento	Banco F.	2	3	1	1	7
68	Incidente	Saga F.	2	3	1	1	7
69	Requerimiento	Banco F.	2	3	1	1	7
70	Incidente	H. Toltus	2	3	1	1	7
71	Requerimiento	Viajes F.	2	3	1	1	7
72	Incidente	Saga F.	2	3	1	1	7
73	Requerimiento	Banco F.	2	3	1	1	7
74	Incidente	Sifsac	2	3	1	1	7
75	Requerimiento	Sifsac	2	3	1	1	7
76	Requerimiento	H. Toltus	1	3	1	1	6
77	Requerimiento	F. Servicios Cer	1	3	1	1	6
78	Requerimiento	Viajes F.	1	3	1	1	6
79	Incidente	H. Toltus	1	3	1	1	6
80	Requerimiento	F. Corporativo	1	3	1	1	6
81	Requerimiento	H. Toltus	1	3	1	1	6
82	Incidente	Saga F.	1	3	1	1	6
83	Incidente	F. Corporativo	1	3	1	1	6
84	Requerimiento	Banco F.	1	3	1	1	6
85	Requerimiento	Saga F.	1	3	1	1	6
86	Requerimiento	Banco F.	1	3	1	1	6
87	Requerimiento	Banco F.	1	3	1	1	6
88	Requerimiento	Banco F.	1	3	1	1	6
89	Requerimiento	Saga F.	1	4	1	1	7
90	Requerimiento	H. Toltus	1	4	1	1	7
91	Requerimiento	Saga F.	1	4	1	1	7
92	Incidente	F. Corporativo	1	4	1	1	7
93	Incidente	H. Toltus	1	4	1	1	7
94	Requerimiento	H. Toltus	1	4	1	1	7
95	Requerimiento	H. Toltus	1	4	1	1	7
96	Requerimiento	Banco F.	1	4	1	1	7
97	Requerimiento	Saga F.	1	4	1	1	7
98	Requerimiento	Corredora de	1	4	1	1	7
99	Requerimiento	H. Toltus	1	4	1	1	7
100	Requerimiento	Banco F.	1	4	1	1	7
101	Requerimiento	Banco F.	1	4	1	1	7
102	Requerimiento	Saga F.	1	4	1	1	7
103	Requerimiento	Banco F.	1	4	1	1	7
104	Requerimiento	Saga F.	1	4	1	1	7
105	Requerimiento	H. Toltus	1	4	1	1	7
106	Requerimiento	H. Toltus	3	4	2	1	10
107	Requerimiento	Saga F.	3	4	2	1	10
108	Requerimiento	Saga F.	3	4	2	1	10


 LARRY MANJAR
 LINARES BARRETO
 INGENIERO
 DE COMPUTACION Y SISTEMAS
 Reg. CIP N° 180551

SISCOTEC DEL PERU S.A.C.

 Angela G. Carmen Juarez Garces
 DNI: 45922315
 Representante Legal

ANÁLISIS DE LA CONFIABILIDAD DE LAS ENCUESTAS SISTEMA WEB DE TICKETS MEDIANTE EL COEFICIENTE ALFA DE CRONBACH

109	Requerimiento	H. Tottus	2	4	1	1	8
110	Requerimiento	H. Tottus	3	4	2	1	10
111	Requerimiento	Saga F.	3	4	2	1	10
112	Requerimiento	Saga F.	2	3	1	1	7
113	Requerimiento	H. Tottus	3	4	2	1	10
114	Requerimiento	Saga F.	2	3	1	1	7
115	Requerimiento	Banco F.	3	4	2	1	10
116	Requerimiento	Saga F.	3	4	2	1	10
117	Requerimiento	Banco F.	2	4	1	1	8
118	Requerimiento	Corredora de S	2	4	1	1	8
119	Requerimiento	Banco F.	2	3	1	1	7
120	Requerimiento	Saga F.	2	3	1	1	7
121	Requerimiento	Saga F.	2	3	1	1	7
122	Requerimiento	Saga F.	2	3	1	1	7
123	Requerimiento	Saga F.	2	3	1	1	7
124	Requerimiento	Saga F.	2	4	1	1	8
125	Requerimiento	H. Tottus	2	3	1	1	7
126	Requerimiento	Banco F.	2	4	1	1	8
127	Requerimiento	Saga F.	2	4	1	1	8
128	Requerimiento	Banco F.	2	3	1	1	7
129	Requerimiento	H. Tottus	3	4	2	1	10
130	Requerimiento	Saga F.	3	4	2	1	10
131	Requerimiento	Corredora de S	2	4	1	1	8
132	Requerimiento	F. Corporativo	3	4	2	1	10
133	Requerimiento	Viajes F.	3	4	2	1	10
134	Requerimiento	H. Tottus	2	4	1	1	8
135	Requerimiento	Saga F.	2	4	1	1	8
136	Requerimiento	Banco F.	2	4	1	1	8
137	Requerimiento	Sifisac	2	4	1	1	8
138	Requerimiento	Corredora de S	2	4	1	1	8
139	Requerimiento	Saga F.	2	4	1	1	8
140	Requerimiento	H. Tottus	2	4	1	1	8
141	Requerimiento	Viajes F.	2	4	1	1	8
142	Requerimiento	Sifisac	2	4	1	1	8
143	Incidente	F. Corporativo	2	4	1	1	8
144	Requerimiento	Saga F.	2	4	1	1	8
145	Requerimiento	Saga F.	2	4	1	1	8
146	Requerimiento	Banco F.	2	4	1	1	8
147	Requerimiento	Banco F.	2	4	1	1	8
148	Requerimiento	H. Tottus	2	4	1	1	8
149	Requerimiento	Banco F.	2	4	1	1	8
150	Requerimiento	Corredora de S	2	4	1	1	8
151	Requerimiento	F. Corporativo	2	4	1	1	8
152	Requerimiento	Saga F.	2	4	1	1	8
153	Requerimiento	Open Plaza	2	4	1	1	8
154	Requerimiento	Banco F.	2	4	1	1	8
155	Requerimiento	Saga F.	2	4	1	1	8
156	Requerimiento	Saga F.	2	3	1	1	7
157	Incidente	Sifisac	3	4	2	1	10
158	Requerimiento	Saga F.	2	3	1	1	7
159	Requerimiento	Saga F.	2	3	1	1	7
160	Requerimiento	Banco F.	3	4	2	1	10
161	Incidente	H. Tottus	2	4	1	1	8
162	Requerimiento	Banco F.	2	4	1	1	8
163	Incidente	H. Tottus	3	4	2	1	10
164	Requerimiento	Saga F.	2	4	1	1	8


LARRY MANUEL
LINARES BARRETO
 INGENIERO
 DE COMPUTACION Y SISTEMAS
 Reg. CIP Nº 180551

SISCOTEC DEL PERU S.A.C.


 Angela Carolina Garces
 DNI: 45622315
 Representante Legal

ANÁLISIS DE LA CONFIABILIDAD DE LAS ENCUESTAS SISTEMA WEB DE TICKETS MEDIANTE EL COEFICIENTE ALFA DE CRONBACH

165	Requerimiento	Saga F.	3	4	2	1	10
166	Requerimiento	H. Toltus	3	4	2	1	10
167	Requerimiento	Viajes F.	2	5	2	1	10
168	Requerimiento	H. Toltus	2	5	2	1	10
169	Requerimiento	Saga F.	2	4	1	1	8
170	Incidente	Saga F.	2	4	1	1	8
171	Incidente	Saga F.	2	4	1	1	8
172	Incidente	Banco F.	3	4	2	1	10
173	Incidente	Saga F.	3	4	2	1	10
174	Requerimiento	Sifsac	2	4	1	1	8
175	Requerimiento	Contac Cente	2	4	1	1	8
176	Incidente	H. Toltus	2	4	1	1	8
177	Requerimiento	Banco F.	2	4	1	1	8
178	Requerimiento	Banco F.	3	4	2	1	10
179	Requerimiento	Banco F.	2	4	1	1	8
180	Requerimiento	Saga F.	3	4	2	1	10
181	Requerimiento	H. Toltus	2	4	1	1	8
182	Requerimiento	F. Corporativo	3	4	2	1	10
183	Incidente	H. Toltus	2	4	1	1	8
184	Requerimiento	Saga F.	3	4	2	1	10
185	Requerimiento	H. Toltus	2	3	1	1	7
186	Requerimiento	H. Toltus	2	3	1	1	7
187	Requerimiento	H. Toltus	2	4	1	1	8
188	Requerimiento	H. Toltus	2	4	1	1	8
189	Requerimiento	Sifsac	2	4	1	1	8
190	Requerimiento	H. Toltus	2	3	1	1	7
191	Requerimiento	H. Toltus	2	3	1	1	7
192	Requerimiento	H. Toltus	3	4	2	1	10
193	Requerimiento	Banco F.	3	4	2	1	10
194	Requerimiento	Banco F.	3	4	2	1	10
195	Requerimiento	H. Toltus	3	4	2	1	10
196	Requerimiento	Saga F.	3	3	1	1	8
197	Requerimiento	Sifsac	3	4	2	1	10
198	Requerimiento	Banco F.	3	4	2	1	10
199	Requerimiento	Banco F.	3	4	2	1	10
200	Requerimiento	Sifsac	3	4	2	1	10
201	Requerimiento	Sifsac	3	4	2	1	10
202	Incidente	Saga F.	3	4	2	1	10
203	Incidente	Banco F.	2	3	1	1	7
204	Incidente	Corredora de S	2	3	1	1	7
205	Incidente	F. Servicios Cen	2	3	1	1	7
206	Incidente	Saga F.	2	3	1	1	7
207	Incidente	Saga F.	2	3	1	1	7
208	Incidente	Corredora de S	2	3	1	1	7
209	Requerimiento	Saga F.	2	3	1	1	7
210	Requerimiento	Banco F.	2	3	1	1	7
211	Requerimiento	Banco F.	2	4	1	1	8
212	Requerimiento	Sifsac	2	4	1	1	8
213	Requerimiento	Banco F.	2	4	1	1	8
214	Requerimiento	Banco F.	2	3	1	1	7
215	Requerimiento	Banco F.	2	3	1	1	7
216	Requerimiento	Banco F.	2	3	1	1	7
217	Requerimiento	Banco F.	2	4	1	1	8
218	Requerimiento	Banco F.	2	4	1	1	8
219	Requerimiento	Banco F.	2	3	1	1	7
220	Requerimiento	Banco F.	2	3	1	1	7


LARRY MANUEL
LINARES BARRERO
INGENIERO
DE COMPUTACION Y SISTEMAS
Reg. CIP N° 180551

SISCOTEC DEL PERU S.A.C.

Angela del Carmen Quiróz Garces
DNI: 45922315
Representante Legal

ANÁLISIS DE LA CONFIABILIDAD DE LAS ENCUESTAS SISTEMA WEB DE TICKETS MEDIANTE EL COEFICIENTE ALFA DE CRONBACH

221	Requerimiento	Banco F.	2	3	1	1	7
222	Requerimiento	Banco F.	2	3	1	1	7
223	Requerimiento	Banco F.	2	3	1	1	7
224	Requerimiento	Banco F.	2	3	1	1	7
225	Incidente	H. Tattus	2	4	1	1	8
226	Requerimiento	Banco F.	2	5	2	1	10
227	Requerimiento	Banco F.	2	5	2	1	10
228	Requerimiento	Banco F.	2	5	2	1	10
229	Requerimiento	Banco F.	2	5	2	1	10
230	Requerimiento	Banco F.	2	5	2	1	10
231	Requerimiento	Contact Center	2	5	2	1	10
232	Incidente	Contact Center	2	5	2	1	10
233	Requerimiento	Banco F.	2	5	2	1	10
234	Requerimiento	Banco F.	2	5	2	1	10
235	Requerimiento	H. Tattus	2	4	1	1	8
236	Requerimiento	Banco F.	2	4	1	1	8
237	Requerimiento	Banco F.	2	4	1	1	8
238	Incidente	H. Tattus	2	4	1	1	8
			ESTADISTICOS				
VARIANZA			0.49	0.38	0.22	0.00	


 LARRY MANJAR
 LINARES BARRETO
 INGENIERO
 DE COMPUTACION Y SISTEMAS
 Reg. CIP Nº 180551

DISCOTEC DEL PERU S.A.C.

 Angel Carlos Saman Diaz Garces
 DNI: 45922315
 Representante Legal

ANEXO N° 15

Resultados en tablas y figuras referente al objetivo específico 1.

Como se puede observar en la ficha de observación Reporte del sistema web de tickets (ver anexo N° 10), nuestra muestra está compuesta por 238 casos que se presentaron en 10 empresas a las cuales Siscotec del Perú SAC les brinda el servicio de implementación y soporte a soluciones de seguridad de información y redes de a través de un sistema web de emisión de Tickets publicado en modalidad 24x7x365, tal como lo podemos visualizar en la tabla y figura siguiente:

Tabla N° 24: Casos presentados en clientes de Sistotec durante el periodo de estudio por el sistema de tickets.

Empresa (Cliente)	Casos presentados
Banco F.	65
Contac Center	8
Corredora de Seguros F.	18
F. Corporativo	9
F. Servicios Centrales	2
H. Tottus	53
Open Plaza	1
Saga F.	53
Sifsac	24
Viajes F.	5
Total general	238

Fuente: Siscotec del Perú SAC.
Elaboración propia.

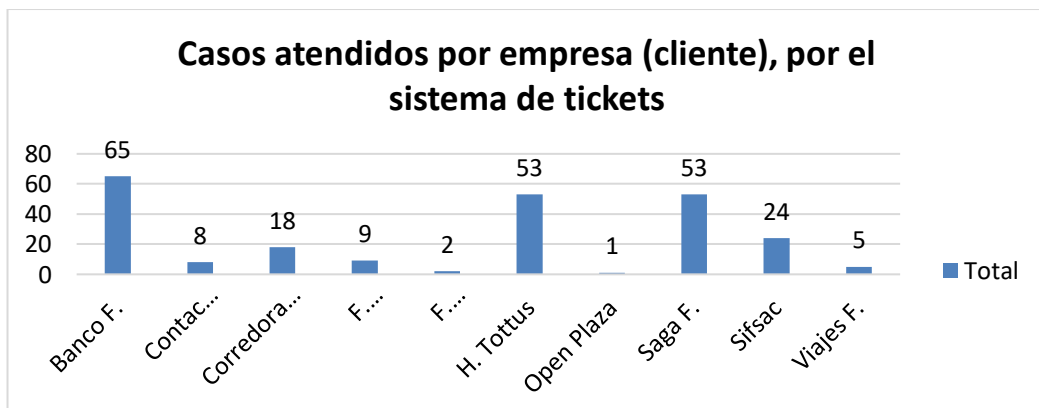


Figura N° 34. Casos atendidos por empresa (cliente) por el sistema de tickets.
Elaboración propia.

Si analizamos la ficha de observación Reporte del sistema web de tickets por casos vemos que el 46% de los casos es por DLP (Data Loss Prevention) luego le sigue Virus Malware 19% Spyware Grayware 15%, Registro de agente (equipos sin antivirus) 14% y finalmente Firewall 5%, tal como lo podemos visualizar en la tabla y figura siguiente:

Tabla N° 25: Casos atendidos por tipo de incidencia, por el sistema de tickets.

Tipo de casos	Reportado	No reportado	Total general	Porcentaje
DLP	92	18	110	46%
Firewall	10	3	13	5%
Reg. de Agente	28	6	34	14%
Spyware Grayware	26	9	35	15%
Virus Malware	2	44	46	19%
Total general	158	80	238	100%

Fuente: Siscotec del Perú SAC.
Elaboración propia.

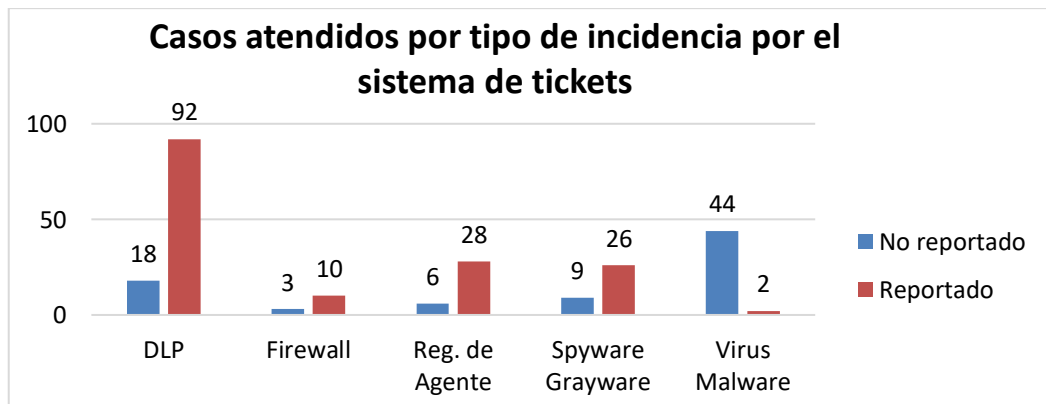


Figura N° 35. Casos atendidos por tipo de incidencia por el sistema de tickets.
Elaboración propia.

Es importante resaltar que de los 238 casos presentados en el periodo de estudio, solo 158 casos fueron reportados por el cliente (66%) y 80 casos fueron detectados por el Siscotec luego del registro, emisión del ticket y análisis pertinente. Este hecho nos demuestra que el 34% de los casos de las incidencias presentadas no son detectadas inicialmente por el cliente, lo que le puede ocasionar grandes perjuicios de seguridad en la información, ver figura siguiente:

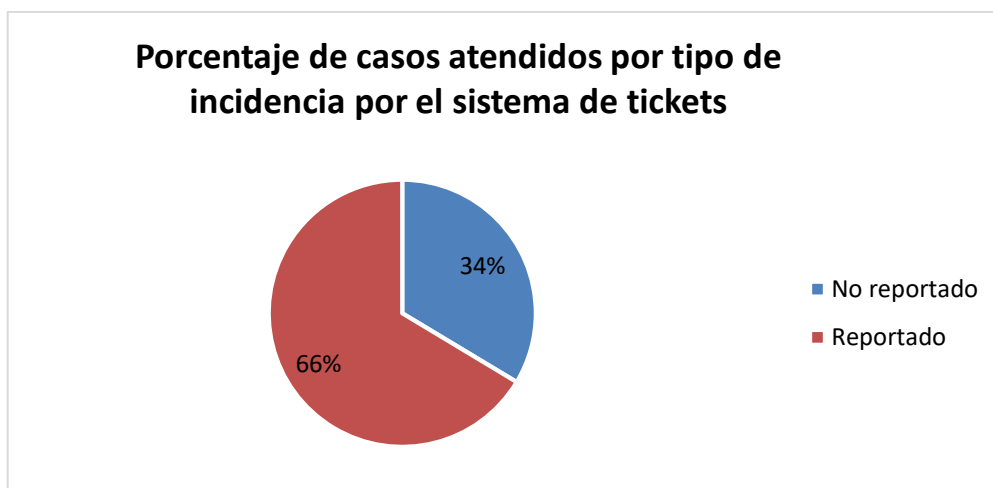


Figura N° 36. Porcentaje de casos atendidos por tipo de incidencia por el sistema de tickets.

Elaboración propia.

En cuanto al nivel de prioridad de atención de los casos (cabe resaltar que la prioridad es determinada por el usuario de acuerdo a su criterio), en el periodo de estudio se presentaron 172 casos (72%) que fueron reportados como críticos, 28 casos con un nivel alto (12%), 10 casos con un nivel medio (4%) y finalmente 28 casos con un nivel bajo (12%), tal como lo podemos visualizar en la tabla y figura siguiente:

Tabla N° 26: Casos atendidos por nivel de prioridad o criticidad por el sistema de tickets.

Tipo de casos	Critical	High	Medium	Low	Total general
DLP	110				110
Firewall	3		10		13
Reg. de Agente	6	28			34
Spyware Grayware	9			26	35
Virus Malware	44			2	46
Total general	172	28	10	28	238
Porcentaje	72%	12%	4%	12%	100%

Fuente: Siscotec del Perú SAC.

Elaboración propia.

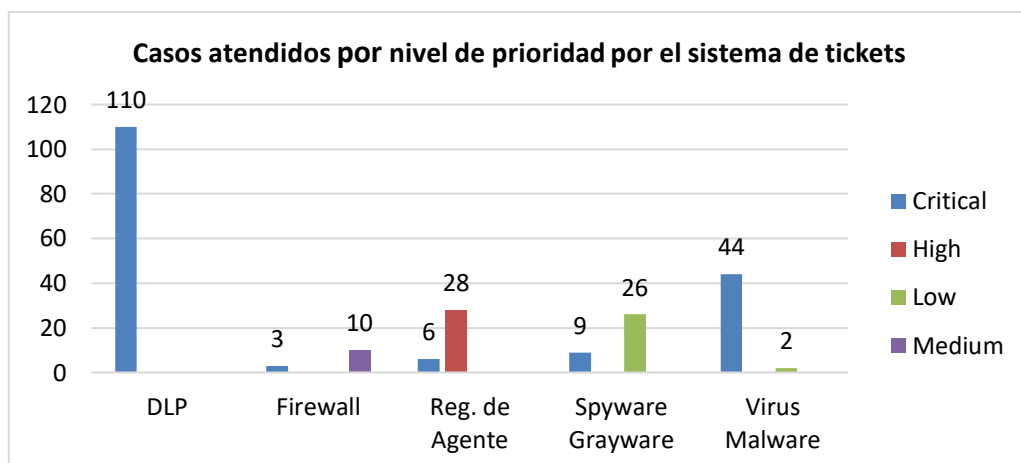


Figura N° 37. Casos atendidos por nivel de prioridad o criticidad por el sistema de tickets. Elaboración propia.

Finalmente, si analizamos la ficha de observación Reporte del sistema web de tickets, por nivel de Casos atendidos por SLA de solución, es decir por el tiempo en que demoro en dar solución a los casos, podemos ver que si bien es cierto que el 82% de los casos el tiempo de atención fue de inmediato (Green) el 12% el tiempo de atención fue alto, por lo que existe una demora considerable en obtener una solución al problema presentado, ver tabla y figura siguiente:

Tabla N° 27: Casos atendidos por SLA de solución por el sistema de tickets.

Tipo de casos	Red	Yellow	Green	Total general
DLP	24	11	75	110
Firewall			13	13
Reg. de Agente	2	1	31	34
Spyware Grayware	3	3	29	35
Virus Malware			46	46
Total general	29	15	194	238
Porcentaje	12%	6%	82%	100%

Fuente: Siscotec del Perú SAC.
Elaboración propia.

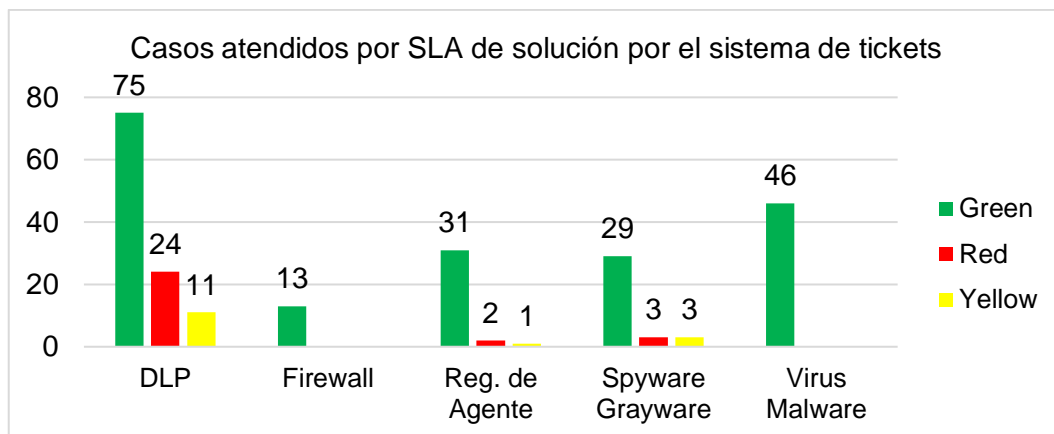


Figura N° 38. Casos atendidos por SLA de solución por el sistema de tickets.
Elaboración propia.

ANEXO N° 16

Resultados en tablas y figuras referente al objetivo específico 2

Como se puede observar en la ficha de observación registro de casos no reportados del Demo SOC (ver anexo N° 11), en forma paralela se trabajó 238 casos que se presentaron en las 10 empresas a las cuales Siscotec del Perú SAC les brinda el servicio de implementación y soporte a soluciones de seguridad de información y redes de a través, pero esta vez los casos fueron atendidos a través de un demo SOC en modalidad 24x7x365, tal como lo podemos visualizar en la tabla y figura siguiente:

Tabla N° 28: Casos presentados en clientes de Siscotec durante el periodo de estudio por el sistema de Demo SOC.

Empresa (Cliente)	Casos presentados
Banco F.	92
Contac Center	4
Corredora de Seguros F.	17
F. Corporativo	11
F. Servicios Centrales	6
H. Tottus	43
Saga F.	38
Sifsac	24
Viajes F.	3
Total general	238

Fuente: Siscotec del Perú SAC.
Elaboración propia.

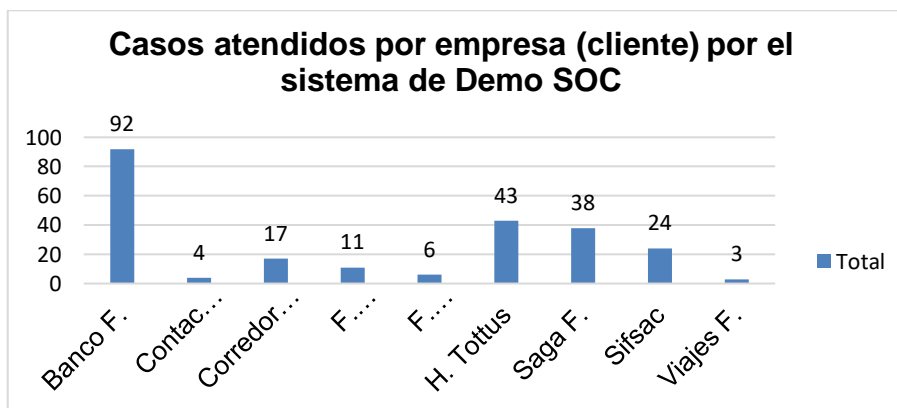


Figura N° 39. Casos atendidos por empresa (cliente) por el sistema de Demo SOC.
Elaboración propia.

Si analizamos la ficha de observación registro de casos detectados y reportados por el Demo SOC por tipo de casos vemos que el 100% de los casos presentados son detectados y reportados por el sistema SOC, este hecho es de vital importancia porque a diferencia del sistema de tickets no hay casos no reportados por el cliente, en esta etapa del estudio se mantuvo las características de la muestra es decir el 46% de los casos es por DLP (Data Loss Prevention) luego le sigue Virus Malware 19% Spyware Grayware 15%, Registro de agente (equipos sin antivirus) 14% y finalmente Firewall 5%, tal como lo podemos visualizar en la tabla y figura siguiente:
 Tabla N° 29: Casos atendidos por tipo de incidencia por el sistema de Demo SOC.

Tipo de casos	Incidente detectado por el SOC	Porcentaje
DLP	110	46%
Firewall	13	5%
Reg. de Agente	34	14%
Spyware Grayware	35	15%
Virus Malware	46	19%
Total general	238	100%

Fuente: Siscotec del Perú SAC.
 Elaboración propia.

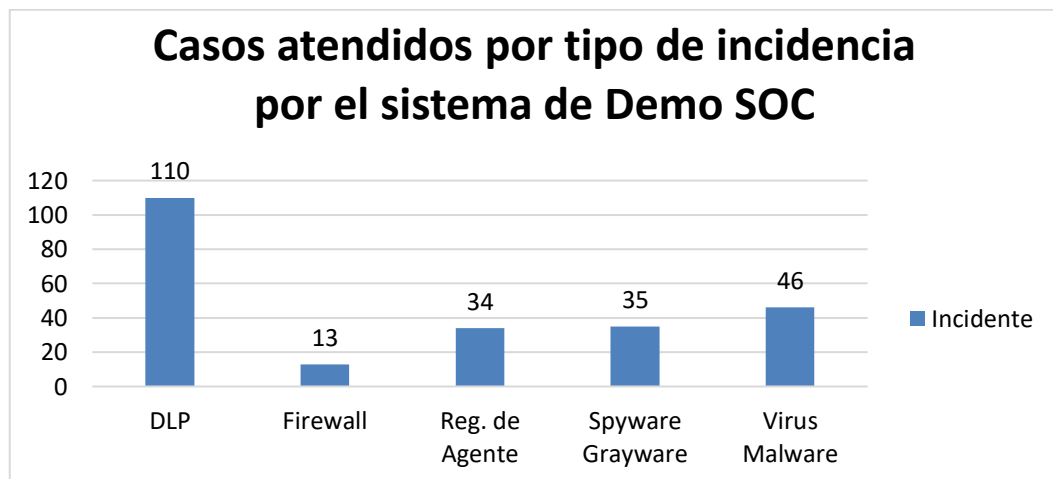


Figura N° 40. Casos atendidos por tipo de incidencia por el sistema de Demo SOC.
 Elaboración propia.

Como mencionamos anteriormente el 100% de los casos fue detectado y reportado por el demo SOC, a diferencia del sistema de tickets

en cual el 34% de los casos de las incidencias presentadas no son detectadas inicialmente por el cliente, hecho que demostraría una mayor eficiencia de seguridad en la información si se cuenta con un SOC.

Si analizamos por nivel de prioridad de atención de los casos presentados (cabe resaltar que en el sistema SOC la prioridad es determinada por el mismo SOC), vemos que solo 34 casos (14%) fueron reportados como críticos, 110 casos como alto (46%), 81 casos como medio (6%) y 13 casos con un nivel de criticidad bajo (6%), tal como lo podemos visualizar en la tabla y figura siguiente:

Tabla N° 30: Casos atendidos por nivel de prioridad o criticidad por el sistema de Demo SOC.

Rótulos de fila	Crítico	Alto	Medio	Bajo	Total
DLP		110			110
Firewall				13	13
Reg. de Agente	34				34
Spyware Grayware			35		35
Virus Malware			46		46
Total general	34	110	81	13	238
Porcentaje	14%	46%	34%	6%	100%

Fuente: Siscotec del Perú SAC.
Elaboración propia.

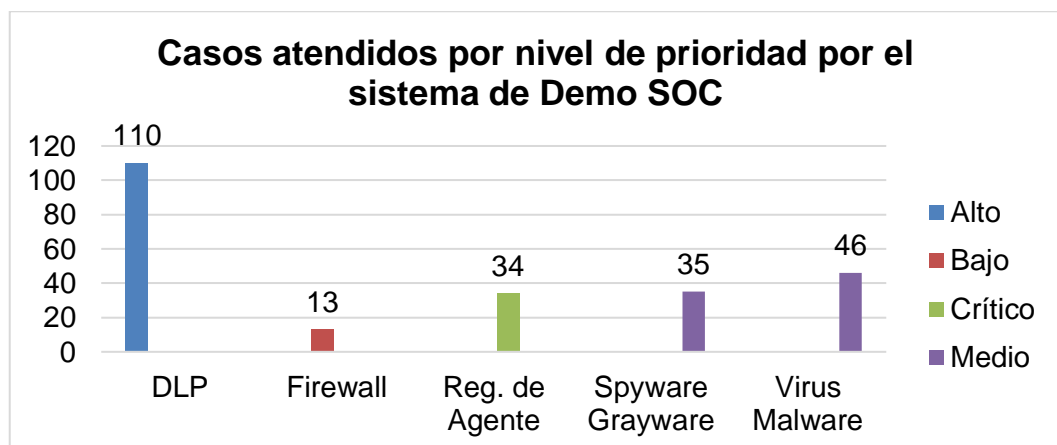


Figura N° 41. Casos atendidos por nivel de prioridad por el sistema de Demo SOC.
Elaboración propia

Finalmente si analizamos, por nivel de casos atendidos por SLA de solución, es decir por el tiempo en que demoro en dar solución a los casos, podemos ver que el 100% de los casos el tiempo de atención fue de inmediato (Green) en tiempo real, lo que demostraría una mayor eficiencia de seguridad en la información si se cuenta con un SOC.

Tabla N° 31: Casos atendidos por SLA de solución por el sistema de Demo SOC.

Tipo de casos	Verde	Total general
DLP	110	110
Firewall	13	13
Reg. de Agente	34	34
Spyware Grayware	35	35
Virus Malware	46	46
Total general	238	238
Porcentaje	100%	100%

Fuente: Siscotec del Perú SAC.
Elaboración propia.

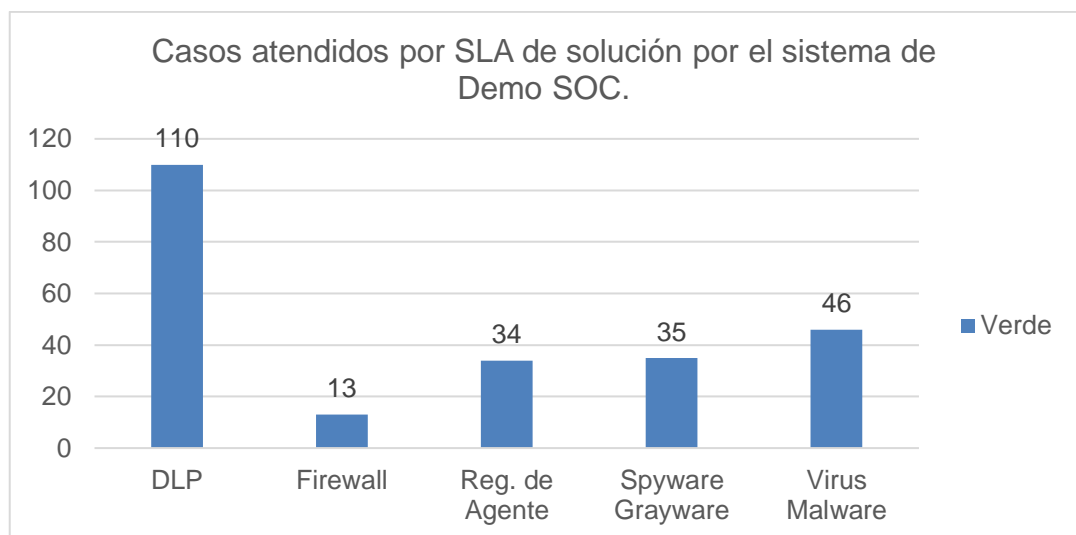


Figura N° 42. Casos atendidos por SLA de solución por el sistema de Demo SOC.
Elaboración propia

ANEXO N° 17
RESULTADOS EN TABLAS Y FIGURAS REFERENTE AL OBJETIVO
ESPECÍFICO 3

En lo relativo al objetivo específico 3 “Realizar una encuesta de satisfacción de los servicios brindados por Siscotec sin SOC y con el demo del SOC” tenemos los siguientes resultados: Se realizó una encuesta para medir el grado de satisfacción por el servicio brindado, entre los 10 clientes de Siscotec del Perú SAC teniendo en cuenta el número total de incidencias presentadas durante el periodo de investigación, es decir por cada incidencia presentada se realizaba la encuesta.

Tabla N° 32: Composición de la encuesta según la muestra

Tipo de Incidencia	Muestra
Equipos sin Agentes Antivirus	34.03
Equipos sin Políticas de DLP	109.89
Equipos sin Políticas de Firewall de AV	12.50
Equipos Infeccionados con Virus Malware	46.44
Equipos Infeccionados con Spyware Grayware	35.14
TOTAL	238.00

Fuente: Siscotec del Perú SAC.
 Elaboración propia.

En lo referente a la pregunta ¿Cómo califica el tiempo utilizado para la solución del incidente y/o requerimiento? Se obtuvo que con el servicio brindado a través del sistema actual por tickets los clientes opinan que en el 51.7% de los casos el tiempo empleado en la atención fue regular y el 29.8% que fue bueno. Sin embargo, si la atención fue por el Demo del SOC la mayoría opina que es muy bueno 52.5% y excelente 32.8% y, según podemos observar en las tablas y figuras siguientes:

Tabla N° 33: Tiempo utilizado para la solución del incidente y/o requerimiento por el sistema de tickets.

Respuesta	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Excelente	0	0.0%	0.0%	0.0%
Muy Bueno	2	0.8%	0.8%	0.8%
Bueno	71	29.8%	29.8%	30.7%
Regular	123	51.7%	51.7%	82.4%
Deficiente	42	17.6%	17.6%	100.0%
Total	238	100.0%	100.0%	

Fuente: Siscotec del Perú SAC.
Elaboración propia.

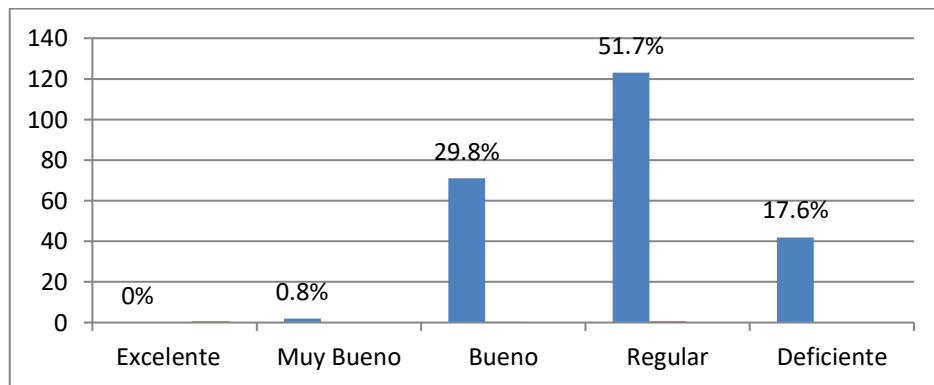


Figura N° 43. Tiempo utilizado para la solución del incidente y/o requerimiento por el sistema de tickets.
Elaboración propia

Tabla N° 34: Tiempo utilizado para la solución del incidente y/o requerimiento por el sistema de SOC.

Respuesta	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Excelente	78	32.8%	32.8%	32.8%
Muy Bueno	125	52.5%	52.5%	85.3%
Bueno	35	14.7%	14.7%	100.0%
Regular	0	0.0%	0.0%	100.0%
Deficiente	0	0.0%	0.0%	100.0%
Total	238	100.0%	100.0%	

Fuente: Siscotec del Perú SAC.
Elaboración propia.

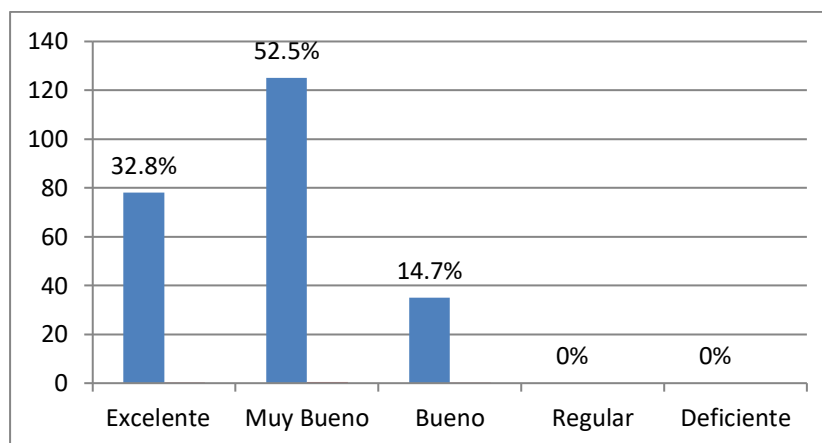


Figura N° 44. Tiempo utilizado para la solución del incidente y/o requerimiento por el sistema de SOC.
Elaboración propia

Con respecto a la pregunta ¿Cómo fue la calidad de la atención recibida del personal de Siscotec? con el servicio brindado a través del sistema actual por tickets los clientes opinan que en el 54.6% la calidad de la atención fue muy bueno y el 36.1% que fue bueno, situación que cambia radicalmente cuando el servicio es brindado a través del Demo del SOC la mayoría opina que es excelente 56.7% y muy bueno 36.1%, según podemos observar en las tablas y figuras siguientes:

Tabla N° 35: Calidad de la atención recibida del personal de Siscotec por el sistema de tickets.

Respuesta	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Excelente	22	9.2%	9.2%	9.2%
Muy Bueno	130	54.6%	54.6%	63.9%
Bueno	86	36.1%	36.1%	100.0%
Regular	0	0.0%	0.0%	100.0%
Deficiente	0	0.0%	0.0%	100.0%
Total	238	100.0%	100.0%	

Fuente: Siscotec del Perú SAC.
Elaboración propia.

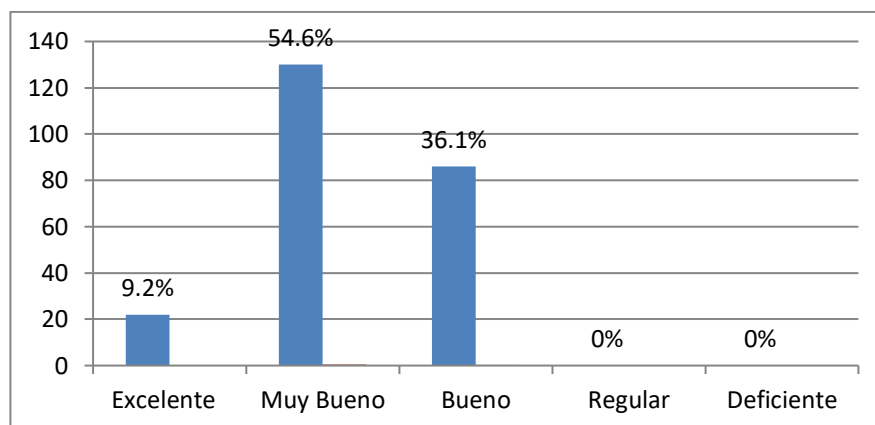


Figura N° 45. Calidad de la atención recibida del personal de Siscotec por el sistema de tickets.
Elaboración propia

Tabla N° 36: Calidad de la atención recibida del personal de Siscotec por el sistema de SOC.

Respuesta	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Excelente	135	56.7%	56.7%	56.7%
Muy Bueno	99	41.6%	41.6%	98.3%
Bueno	4	1.7%	1.7%	100.0%
Regular	0	0.0%	0.0%	100.0%
Deficiente	0	0.0%	0.0%	100.0%
Total	238	100.0%	100.0%	

Fuente: Siscotec del Perú SAC.
Elaboración propia.

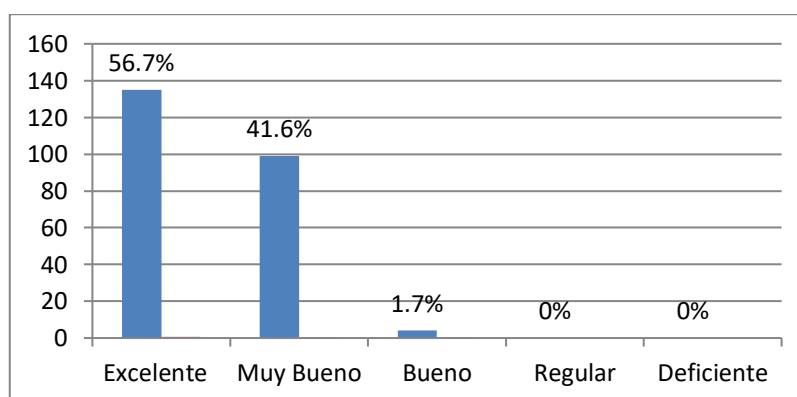


Figura N° 46. Calidad de la atención recibida del personal de Siscotec por el sistema de SOC.
Elaboración propia

En relación a la pregunta ¿El servicio brindado por el personal de Siscotec, solucionó su incidencia y/o requerimiento en la primera atención?

en el servicio brindado a través del sistema actual por tickets el 32.8% sostiene que no se solucionó en la primera atención, es importante mencionar que estos casos se solucionaron cuando pasaron a un siguiente nivel de soporte y solo el 67.2% opino que sí. Sin embargo, con el Demo del SOC, el 100% de los clientes opinan que, si se solucionó la incidencia y/o requerimiento en la primera atención, lo cual demuestra una mayor eficiencia con el sistema del SOC, según podemos observar en las tablas y figuras siguientes:

Tabla N° 37: Se solucionó su incidencia y/o requerimiento en la primera atención, por el sistema de tickets.

Respuesta	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	160	67.2%	67.2%	67.2%
No	78	32.8%	32.8%	100.0%
Total	238	100.0%	100.0%	

Fuente: Siscotec del Perú SAC.
Elaboración propia.

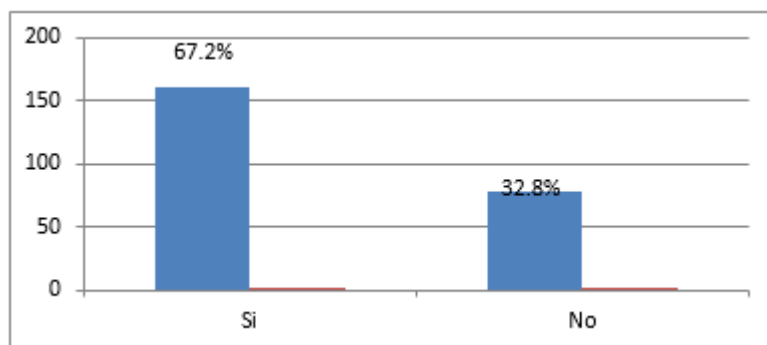


Figura N° 47. Solución de la incidencia y/o requerimiento por el sistema de tickets.
Elaboración propia

Tabla N° 38: Se solucionó su incidencia y/o requerimiento en la primera atención, por el sistema de SOC.

Respuesta	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	238	100.0%	100.0%	100.0%
No	0	0.0%	0.0%	100.0%
Total	238	100.0%	100.0%	

Fuente: Siscotec del Perú SAC.
Elaboración propia.

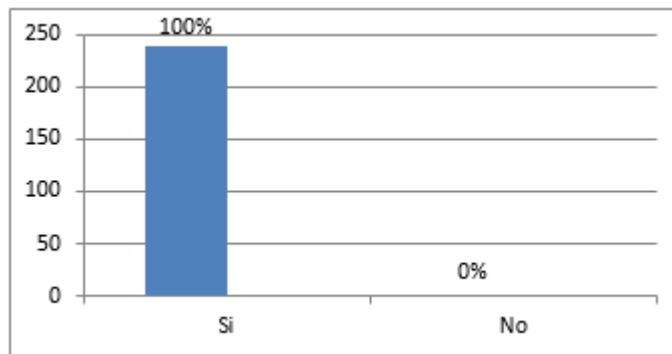


Figura N° 48. Solución de la incidencia y/o requerimiento por el sistema de SOC.
Elaboración propia

Finalmente, en relación a la pregunta ¿La incidencia fue reportado por usted? con el servicio brindado a través del sistema actual por tickets el 100% de los clientes opinan que en si fue reportado por el usuario, situación que cambia radicalmente cuando el servicio es brindado a través del Demo del SOC en el cual el 87% opina que no lo reporto y fue el propio sistema SOC que detecto la incidencia, solo el 13% opino que fueron ellos los que reportaron la incidencia, sin embargo es importante señalar que no se trata de que el SOC no hubiera detectado la incidencia sino que el usuario lo reporto cuando el SOC ya lo había detectado, según podemos observar en las tablas y figuras siguientes:

Tabla N° 39: La incidencia fue reportada por usted, a través del sistema de ticket.

Respuesta	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	238	100.0%	100.0%	100.0%
No	0	0.0%	0.0%	100.0%
Total	238	100.0%	100.0%	

Fuente: Siscotec del Perú SAC.
Elaboración propia.

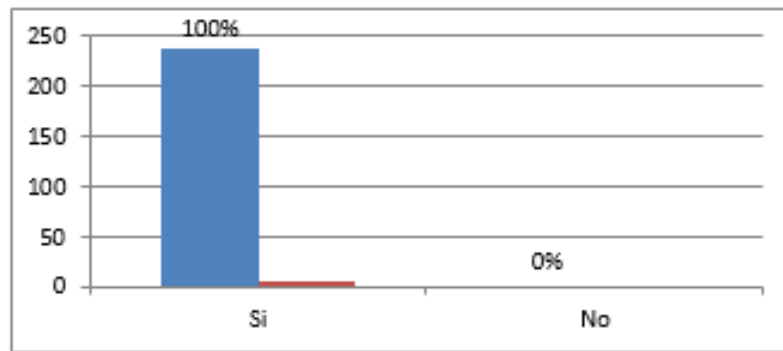


Figura N° 49. La incidencia fue reportada por usted, a través del sistema de ticket.
Elaboración propia

Tabla N° 40: La incidencia fue reportada por usted, a través del sistema de SOC.

Respuesta	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	31	13.0%	13.0%	13.0%
No	207	87.0%	87.0%	100.0%
Total	238	100.0%	100.0%	

Fuente: Siscotec del Perú SAC.
Elaboración propia.

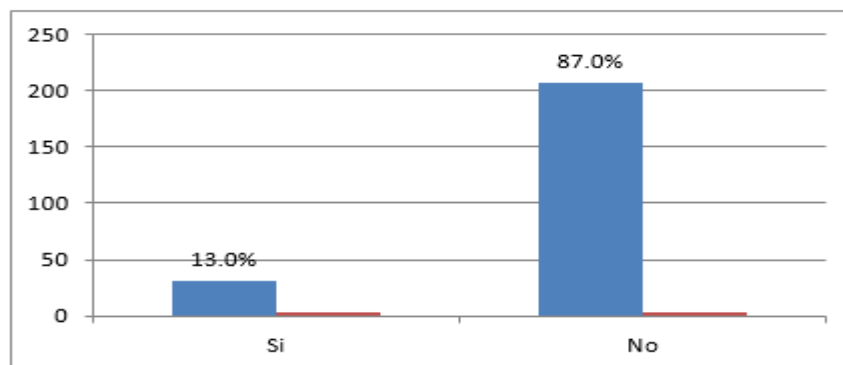


Figura N° 50. La incidencia fue reportada por usted, a través del sistema de SOC.
Elaboración propia

Anexo N° 18

Resultados de la lista de cotejo Implementación del SOC debidamente firmada y sellada por representantes de la empresa Siscotec del Perú SAC

LA LISTA DE COTEJO IMPLEMENTACIÓN DEL SOC

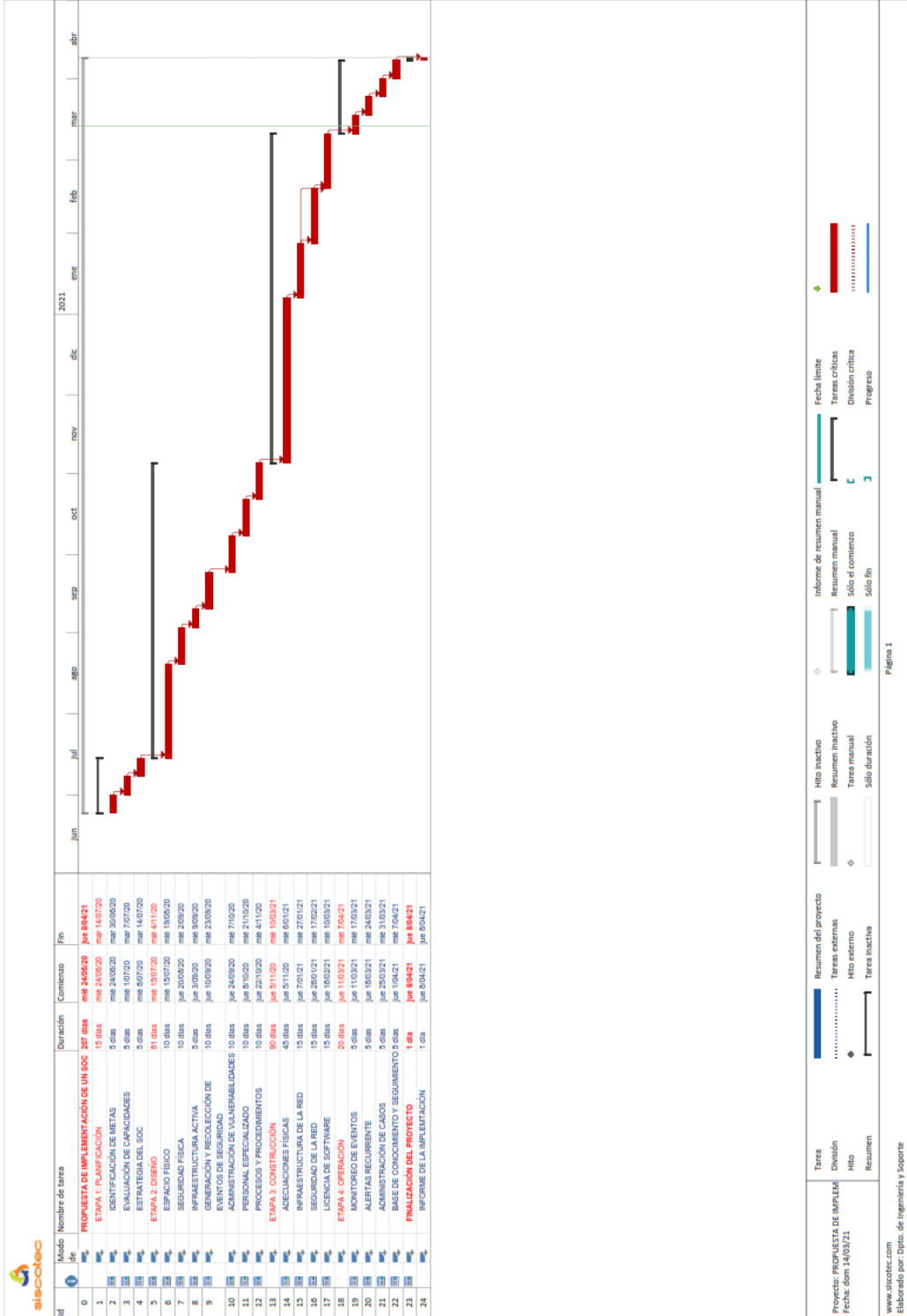
APECTO O FACTOR	SI	NO
Sala de Monitoreo para alojar al menos 6 espacios de trabajos		X
Oficina para el Administrador del SOC equipada	X	
Sala de Conferencia equipada con el mobiliario necesario	X	
Data center con los elementos necesarias del mismo		X
Acceso a la Sala de Monitoreo restringido, solamente al personal autorizado		X
Bitácora de registros de acceso controlado		X
Sistema de Cámaras de Monitoreo (Con grabación continua) de Circuito Cerrado		X
Cuenta con material a prueba de sonidos		X
Espacios de trabajos, mínimo 6	X	
Infraestructura de Red	X	
Mecanismos de Seguridad	X	
Sistemas Operativos	X	
Almacenamiento		X
Sistemas de Administración de Tickets	X	
Generación y Recolección de Eventos de Seguridad		X
Administración de Vulnerabilidades	X	
Personal que estará a cargo del SOC	X	


ANASOLEDAD TORRES GARCOS
 Ana Soledad Torres Garcos
 Cnit: 45922315
 Representante Legal


LARRY BARRETO
 LARRY BARRETO
 INGENIERO
 DE COMPUTACION Y SISTEMAS
 Reg. CIP Nº 180551

Anexo N° 19

Propuesta de la Implementación



Anexo N° 21

Carta de autorización de recolección de información de la empresa Siscotec del Perú S.A.C donde se realizó su investigación.



Lima, 13 de diciembre de 2019

Angela del Carmen Quiroz Garces
Representante Legal – Empresa:


Siscotec Del Perú S.A.C.

AUTORIZA: Permiso para recojo de información pertinente en función del proyecto de investigación, denominado: DISEÑO DE UN SISTEMA DE GESTIÓN PARA MEJORAR EL SERVICIO DE ATENCIÓN EN LA PLATAFORMA DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA SISCOTEC DEL PERÚ S.A.C.

Por el presente, el que suscribe Angela del Carmen Quiroz Garces, representante legal de la empresa: SISCOTEC DEL PERÚ S.A.C con RUC 20538719928, AUTORIZO al alumno Christian Jerson Hurtado Saucedo, identificado con D.N.I. N° 43750584, estudiante de la Escuela Profesional de Ingeniería Industrial de la Universidad Señor de Sipán, y autor de la investigación denominado: DISEÑO DE UN SISTEMA DE GESTIÓN PARA MEJORAR EL SERVICIO DE ATENCIÓN EN LA PLATAFORMA DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA SISCOTEC DEL PERÚ S.A.C; al uso de dicha Información que conforma el expediente técnico así como hojas de memorias, cálculos entre otros como planos para efectos exclusivamente académicos de la elaboración de tesis del alumno Christian Jerson Hurtado Saucedo, enunciado líneas arriba. De quien solicita.

Se garantiza la absoluta confidencialidad de la Información solicitada.

SISCOTEC DEL PERU S.A.C.


Angela del Carmen Quiroz Garces
DNI: 45922315
Representante Legal

ANGELA DEL CARMEN QUIROZ GARCES
DNI 45922315
REPRESENTANTE LEGAL

