

Soluciones de Tecnología Pensadas para su Negocio

NETWORK SECURITY OPERATIONS CENTER

**SOLICITUD DE SERVICIOS**

**Sherin Amira Lanao B.**

**Abril**

**2013**

1. **OBJETIVO:**

* Desarrollar procesos que permitan alinear los requerimientos y/o solicitudes con las herramientas de registro y mantener el control de cambios.
* Identificar la prioridad asignada a cada requerimiento.
* Establecer un SLA de prioridad a cada caso.
* Documentar los procedimientos de servicios atendidos.

1. **ALCANCE: (acotado) que cubre**

* Llevar el control de acontecimientos y solicitudes mediante un ticket de atención.
* Interactuar con otros procesos asociados para la oportuna atención de los incidentes y/o solicitudes.
* Monitorizar y realizar el seguimiento respectivo a los tickets de atención, con la finalidad de cumplir con los SLA.

1. **DEFINICIONES:**

* **Cliente:** Son aquellos que tienen un contrato de 1°,2° y 3° nivel con TNP
* **Monitoreo:** el primer operador en los niveles de atención dentro del NSOC de TNP
* **Operador NSOC:** Es el personal del Área del NSOC, que resguarda por la seguridad de los equipos, registrando y reportando todo tipo de alerta e incidencia.
* **Gestión de Requerimientos**: proceso de la orden de servicios.
* **Gestión de incidentes:** Son aquellas alertas que han sido registrados y atendidos en primera instancia, las cuales no comprometen la disponibilidad de los servicios del cliente.
* **Gestión de Cambios:** proceso de transformación de configuración en los servicios brindados.
* **Niveles de Criticidad:** Se mide en base al impacto y la urgencia.
* **Cliente:** Empresa que adquiere el servicio de seguridad gestionada.
* **Servicio:** servicio de seguridad gestionada.
* **SLA:** Acuerdo de nivel de servicio.

1. **DESCRIPCION DEL PROCEDIMIENTO:**

El siguiente procedimiento establece la definición de roles que intervienen en las actividades de Gestión de Requerimientos, que abarca desde la implementación del proyecto hasta el soporte del mismo.

Procedimiento:

* Recepción de requerimiento (canal regularizador), a través de los medios de comunicación establecidos en cada área.
* Registro de requerimientos / solicitud, donde a través de un ticket de atención empieza a correr con el SLA establecido.
* Asignación de prioridad al caso de acuerdo a la orden de configuración bajo demanda del cliente.
* Atención dela solicitud y/o requerimiento, en función del SLA establecido.
* Conformidad satisfactoria de la orden del servicio.
* Cierre de ticket.

**SLA:**

Tiempos de respuesta y solución, de acuerdo a cada prioridad asignada según la criticidad de la solicitud u orden de servicio.

|  |  |  |  |
| --- | --- | --- | --- |
| Prioridad | Respuesta Inicial | Intervalo de Reporte | Notificación del NSOC |
| P1 | Inmediata | Cada 2 horas. | Analista NSOC: Inmediatamente  Ingeniero Especialista: Luego de 2 horas  Soporte de Fabrica: Luego de 3 horas. |
| P2 | < 1 hora | Cada 6 horas | Analista NSOC: Inmediatamente  Ingeniero Especialista: Luego de 6 horas.  Soporte de Fabrica Luego de 8 horas. |
| P3 | < 2 horas | Diariamente | Analista NSOC: Inmediatamente |
| P4 | < 3 horas | Semanalmente | Analista NSOC: Inmediatamente |

**4.1 Implementación**

Forma parte de la fase de diseño, donde se ajustan los recursos y servicios de acuerdo a la necesidad del negocio.

Considerando:

* Soluciones adaptados a la necesidad del negocio
* Arquitectura de infraestructura
* Servicios delimitados

**4.2 NSOC**

Identificación del incidente, a través de a emisión de alertas de las herramientas de monitoreo.

**4.1.2 indisponibilidad de Servicio:**

* Se realiza un ping constante a la dirección pública del equipo.
* Validación de acceso al equipo de seguridad mediante la dirección IP/ Host del equipo.
* Al no tener el acceso al equipo por la dirección IP/Host, procedemos con la comunicación del cliente, informando lo observado y recopilando la información por parte del cliente.
* Registramos la información brindada por el cliente mediante un ticket de atención.
* Comunicación al área del NSOC lo sucedido.
* Se analiza las causas de la caída, escalando el caso al Jefe de soporte, con la información recopilada, para designar al operador que dará la solución al caso en conjunto con el cliente.
* Asignación del ticket al operador que efectuará la solución.
* Monitoreo constante durante la implementación de solución y post solución.
* Registro del cierre del caso, mediante un ticket de atención reportando lo aplicado para la solución, las observaciones analizadas y obteniendo la conformidad del caso por parte del cliente.
* Cierre de ticket

**4.1.2 Uso de CPU y Memoria:**

* El personal de monitoreo, valida el acceso al equipo de seguridad, mediante la dirección IP/Host.
* verificación del proceso de mayor uso, como los recursos de CPU y Memoria, donde el umbral no debe sobrepasar el 80% de uso.
* Verificación de alto consumo de ancho de banda y tráfico generado a lo largo del día.
* Identificación del tipo de tráfico de mayor consumo.
* Comunicación telefónica con el cliente, indicando lo observado y dejando el registro de lo conversado por correo.
* Análisis de la principal aplicación de mayor consumo, mediante un reporte de tráfico en el horario que reporto la alerta.
* Envío del reporte, indicando las recomendaciones correspondientes para solucionar el caso.
* Proceso de escalamiento al Jefe del NSOC, designando al operador que aplicará la solución, de acuerdo a la información recopilada por el operador de monitoreo.
* Monitoreo constante del uso de los recursos.
* Conformidad del cliente.
* Registro de lo observado en el archivo que se maneja a nivel del área.
  + 1. **Detección de Ataques:**
  + Se evalua el nivel de criticidad del ataque recibido y la accion tomada por el equipo.
  + Se establece la comunicación con el cliente, informando lo observado indicando las soluciones para mejorar el caso.
  + Generacion de ticket de atencion, registrando la incidencia presentada.
  + Generacion de un reporte en referencia a los ataques presentados en dichos horarios, definiendo el contenido de:
* Principales fuentes de ataque
* Principales destinos atacados
* Principales servicios o puertos
  + Proceso de escalamiento al supérvisor del Area, con la informacion recopilada, para proceder con la pronta atencion .
  + Registro de lo observado y analizado en el archivo que se maneja en el area.
  + Conformidad del cliente.
  + Cierre de ticket de atencion.

1. **CONTROL DE REGISTRO**

Manejo de plantillas de seguridad, donde se reporta las incidencias reportadas, por hora y fecha del suceso, asi mismoo de mantiene el registro de los acontecimientos y soluciones aplicadas de acuerdo al tipo de incidencia, como respaldo de los acontecimientos mas frecuentes. Informacion relevante a registrar:

* Nombre del operador que reporto la alerta
* Nombre de la empresa Cliente
* Fecha y hora de reporte de incidente
* Nombre del contacto del cliente
* Fecha y hora de operatividad del servicio
* Registro del tipo de incidencia concurrida
* Observacion adicional
* Conclusion final

1. **REGISTRO DE INCIDENTE**

Manejo de las guías de incidentes de modo individual, donde se mantiene el registro de incidencias por tipo, fecha y hora de inoperatividad/ operatividad, contacto, marca y modelo de equipo de manera independiente.

Como parte del procedimiento, se mantiene un historial de los diferentes tipos de incidentes, con el fin de asegurar el manejo de los tiempos de solucion frente a la problemas ya conocidos, optimizando la calidad de servicio.

Mediante la gestion de generacion de ticket’s de atencion, donde se registra la informacion del incidente y el operador asignado para la atencion cambia el estado del ticket , de acuerdo al seguimiento durante la atención, hasta el momento del cierre del caso.

1. **GESTION DE ESCALAMIENTO**

Existen 3 niveles de esccalamiento, de acuerdo a la criticidad del incidente cumpliendo con los tiempos de rspuesta establecidas en el SLA del contrato con **Think Networks.**

|  |  |
| --- | --- |
| Soporte Nivel 1 | Información del producto, consultas sobre configuración de hardware y software, instalación y actualizaciones. Problemas básicos, reemplazos de hardware. |
| Soporte Nivel 2 | Problemas no tan complejos que pueden ser solucionados vía un análisis de los Logs, traces, diagnósticos remotos, etc. |
| Soporte Nivel 3 | Problemas complejos que requieren generar una simulación en los laboratorios del NSOC o ser escalados al soporte de la marca. |

1. **PROCESO DE CONFORMIDAD DEL SERVICIO**

El servicio de monitoreo, abarca una gama de pruebas en conjunto con el cliente, una vez aplicada la solucion al incidente. Con el fin de asegurar el correcto funcionamiento de los servicios, dando un seguimiento continuo durante un tiempo estimado, hasta la obtencion de la conformidad del cliente y el cierre del caso.

Asegurando que los cambios aplicados no afectarán servicios complementarios y no compementarios al incidente concurrido.

El registro de la conformidad del incidente resuelto, puede ser por medio de una llamada telefonica, correo o documento formal.

1. **GESTION DE DOCUMENTACION E INFORMACION**

La obtencion de la conformidad del caso, se plasma en un acta de conformidad del servicio por parte del cliente, donde claramente obtendremos informacion del estatus final del servicio, una vez aplicada la solucion y las pruebas a las que fue sometido en conjunto con el cliente, donde el seguimiento post solucion cuenta con un respaldo de un tiempo estimado, resguardando de esta manera que los demas servicios no se vean afectados.

Donde obtendremos la informacion de lo observado, las recomendaciones para la mejora continua del servicio y conclusiones finales, donde se detalla el estatus final del servicio contribuyendo a la mejora en cuanto a la calidad de servicio, abiertos frente a una oportunidad de mejora.