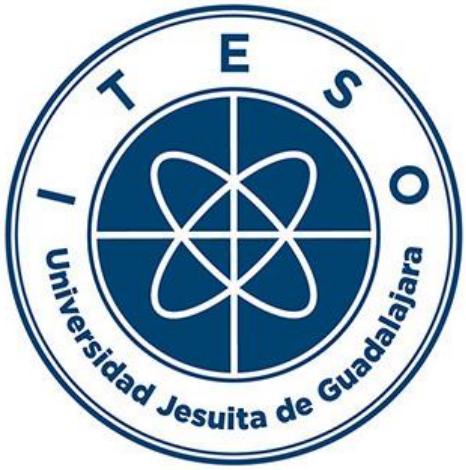
Instituto Tecnológico y de Estudios Superiores de Occidente

Reconocimiento de validez oficial de estudios de nivel superior según acuerdo secretarial 15018, publicado en el Diario Oficial de la Federación del 29 de noviembre de 1976.

Departamento de Electrónica, Sistemas e Informática

MAESTRÍA EN INFORMÁTICA APLICADA



PROCESO DE PREVENCIÓN

TESIS que para obtener el **GRADO** de
MAESTRA EN INFORMÁTICA APLICADA

Presenta: **GRECELY AVILA LÓPEZ**

Asesor **MTRO. RICARDO SALAS MEJÍA**

Tlaquepaque, Jalisco. 18 de julio de 2020

Dedicatoria

Dedicado a mi familia, quienes me apoyaron en todo momento y en todos los aspectos.
A mi hija, para que el ejemplo del estudio y la preparación la acompañen siempre.

I. Contenido

II. Índice de tablas

III. Índice de figuras

Resumen

Este documento trata sobre cómo se llevó a cabo la implementación de un proceso que tiene el objetivo de prevenir. Este concepto que mayormente se utiliza en el sector salud o incluso para evitar accidentes, fue el termino que elegimos para hacer referencia a un proceso que nos ayudaría a prevenir fallas en la red de sistemas informáticos de una filial de América Móvil, el gigante de telecomunicaciones en Latinoamérica, soportado en todo momento por Cisco Systems de México.

Primeramente se abordan en el marco teórico todos los conceptos generales, que si no perteneces al ámbito de las tecnologías de la información, ayudarán a comprender el lenguaje que se maneja en este documento. Se definen términos básicos, desde el significado de "servicio" y su relación con la informática, hasta términos especializados muy enfocados a la operación de procesos en los sistemas computacionales.

Explico lo que para nosotros es un ciclo de prevención, y digo "lo que para nosotros" porque iniciamos definiendo nuestros propios conceptos del tema proactivo, preventivo y predictivo, que sin importar sus definiciones utilizadas en la industria, elegimos lo que únicamente hacia sentido a la operación de nuestro cliente. Definimos lo que sería el proceso de prevención, cuál es su objetivo, bajo los estándares que operaría, cómo se mediría para tomarlo como base y en los subsecuente aplicar la mejora continua, porque como es bien sabido, lo que no se mide no se puede mejorar y finalmente, cómo lo estaríamos evaluando.

En los antecedentes doy detalles de la filial de América móvil en donde se aplicó el proyecto, que por motivos de confidencialidad no me fue posible mencionar su nombre, pero presento datos para familiarizarte en el ambiente de negocio en el que se desenvuelve.

Menciono las metodologías que nos permitieron llevar a cabo el desarrollo e implementación de este proyecto, que si bien no se llevó a cabo un único marco de referencia de principio a fin, fue una combinación de los temas que aplicaron en cuestión de ITIL, PMI, agile & ciclo de Deming, solo aquellos fragmentos que aportaban valor a nuestro proyecto.

Presentamos la descripción de actividades realizadas, cada una con los tiempos en los que se llevaron a cabo y con el detalle de lo que se realizó en cada una de ellas. Nuestro cliente es muy dinámico, siempre en búsqueda de la mejora continua, y al estar en constante cambio, eso hace que tenga ya adquirido el habito de la formalidad para cada una de las tareas que desean implementar, por ende, el resultado es la documentación certera los acuerdos que se llevan a cabo en cada una de las reuniones que tuvimos con

ellos. Esos acuerdos se analizan internamente por cada uno de los equipos de trabajo que intervienen, para posteriormente fijar el acuerdo, documentarlo y anunciarlo a todos los involucrados en el proyecto.

Explicamos los detalles, las negociaciones y las dificultades que se nos presentaron para la definición del proceso y su la implementación. Al inicio presentamos una estrategia de Optimización, la cual, a medida que íbamos avanzando en el tema, se decidía la implementación inmediata de las actividades que se definieron, eso habla del éxito y la aceptación que tuvo nuestro proceso. Ayudó mucho que el cliente tenia toda la disposición, porque supimos manejarlo como un proceso que estaría aportando mucho valor a la operación, así que el reto más grande fue entonces, la definición de los detalles.

Por último reflexiono sobre las lecciones que aprendimos durante la definición y la implementación del proyecto, que a meses de haber arrancado hay detalles muy finos que podemos mejorar, los errores que pudimos haber evitado y que ahora parecieran muy evidentes pero que mientras trabajábamos en ellos no fuimos capaces de identificar, haber reflexionado en ello nos ayudó a tener una propuesta de mejora que también esta incluida en este escrito.

Capítulo I. Marco de Referencia

1.1 Conceptos teóricos aplicables al proyecto

Hoy en día, un gran número de empresas de tecnología no solo se dedican única y exclusivamente a vender e instalar hardware o software innovadores, si no que la gran mayoría además de ofrecer los servicios intrínsecamente ligados a estos productos, como la instalación y la configuración de ellos, están también incursionando en ofrecer en sus portafolios de servicios a sus clientes, servicios de soporte, consultoría o incluso servicios administrados de productos que no forman parte de la propia marca.

Cisco no es la excepción, ya que además de la gran variedad de productos de telecomunicaciones que forman parte de su catalogo, también ofrece: Servicios de Asesoramiento, Implementación, Capacitación, Optimización, de Administración y de Soporte técnico.

De manera general, existe un sin numero de significados para el concepto de servicio, simplemente la Real Academia Española tiene un listado de 19 definiciones para la palabra "Servicio", que para el propósito de este documento nos interesan las definiciones número 16 y 17 que a continuación se describen:

16. m. Organización y personal destinados a cuidar intereses o satisfacer necesidades del público o de alguna entidad oficial o privada. Servicio de correos, de incendios, de reparaciones. (RAE, 2019)

17. m. Función o prestación desempeñadas por organizaciones de servicio y su personal. (RAE, 2019)

Ahora bien, la definición de Servicio en ITIL, que es básicamente el marco de referencia más usado en el ámbito de soporte a las tecnologías de información nos dice lo siguiente:

"Es un medio para habilitar la creación conjunta de valor al facilitar los resultados que los clientes desean alcanzar, sin que el cliente tenga que administrar los costos y riesgos específicos" (AXELOS Limited, 2019)

Cisco también tiene su propia definición de servicio, ya que los servicios de Cisco están siendo cada vez mas una parte importante de sus ingresos:

“Experiencia global, innovación y calidad de servicio que le permiten lograr resultados comerciales extraordinarios” (Cisco Systems, s.f.)

Realmente la definición es muy sencilla, para mi el servicio es una acción que se ofrece con la intención generar valor para ambos, quien da y quien recibe.

Definitivamente existen todo tipo de servicios ligados o no a la venta de un producto, servicios que nos sorprendería saber que existen, pero para efectos de este estudio de caso, nos limitaremos a hablar de los servicios de soporte en el ámbito de las tecnologías de información.

Cada empresa que oferta servicios de soporte técnico puede tener su propia definición, incluso es muy común que se personalicen este tipo de servicios para adecuarse a las necesidades de sus clientes. Básicamente el soporte técnico se refiere al apoyo especializado que las empresas brindan para todo lo relacionado con los componentes tecnológicos, que puede ser desde la reparación, el reemplazo de componentes, apoyo a la configuración, asesoría para la implementación o la implementación misma, etc.

Los temas relacionados a la entrega de servicios de soporte técnico constituyen un amplio espectro, ya que cada cliente requiere de servicios especializados muy particulares, así como hay empresas con altos niveles de especialización que hacen imposible que una sola empresa pueda soportar absolutamente todo componente tecnológico, por lo que nos enfocaremos en definir y hacer referencia a los conceptos que usaremos mas adelante.

Cisco cuenta con cinco centros de servicio de soporte formado por 1300 ingenieros de soporte alrededor del mundo, estos ingenieros están especializados en todos y cada uno de los productos que se ofertan en el portafolio de Cisco.

Cisco además de ofertar los servicios de su portafolio, elabora planes de servicios a la medida, de tal forma que se adapten en su totalidad a lo que los clientes necesitan.

Para nuestro cliente, el servicio ofertado y renovado consecutivamente por los últimos 10 años consiste en el soporte a la infraestructura Cisco, *switches y routers* de diferentes modelos, operado bajo los estándares de ITIL que incluyen Administración de Incidentes y Administración de Problemas.
“ITIL es la directriz más adoptada en el mundo dentro de la gestión de servicios de TI.” (AXELOS Limited, 2019) No es una guía que se tenga que implementar de la A a la Z, ITIL básicamente proporciona la base como un marco de referencia para que las empresas tomen de esta recopilación de

mejores practicas lo que les acomode. ITIL puede ser implementado en todas las empresas en las que trabajen bajo modelos de soporte, no únicamente relacionados con las tecnologías de la información. Y puede ser implementado completamente o solo los procesos que sean convenientes para cada empresa, e incluso puede ser combinado con metodologías como COBIT, ISO2000, Lean, Six Sigma, Agile, entre otras. De hecho, ITIL no fue creado con el objetivo de ordenar el departamento de TI del Gobierno del Reino Unido, si no para hacer a este departamento financieramente rentable.

Ahora bien, “Las mejores practicas son aquellas que se han llevado a cabo de manera eficiente y efectiva, con excelentes resultados en los procesos de TI y en la operación real” (Pabbathi, 2020), y es por ello que ITIL ha tenido tanto éxito, porque ha dado a conocer la manera en que pueden ser implementados sus procesos y se probado su efectividad. ITIL fue concebido a principios de 1980 y hoy en día sigue siendo el marco de referencia mas utilizado en las medianas y grandes empresas.

Con nuestro cliente el proceso más maduro y que fue con el que inicialmente se firmaron los primeros contratos es el Proceso de Administración de Incidentes. Algunos autores o algunas empresas lo manejan como administración de Incidentes o puede encontrarse también como gestión de incidentes, que en realidad se refieren a lo mismo, a cómo manejar los incidentes dentro del departamento de TI.

Para entender mejor lo que comprende el proceso de gestión de incidentes, iniciemos con el concepto de Incidente:

Un incidente es algo que pasa de manera imprevista, que se interpone en la manera de funcionar de las cosas y que por consiguiente hay una consecuencia, casi siempre utilizado para resultados negativos.

La definición que ITIL le da a un incidente es la siguiente: “Incidente se refiere a una interrupción no planificada de un servicio, o reducción en la calidad de un servicio”. (AXELOS Limited, 2019)

En el ámbito de las TI, incidente es un termino muy común, parte de las conversaciones en las áreas de soporte, incluso para los que no están certificados en este marco de referencia.

Los incidentes son clasificados por grados de criticidad, por la urgencia en que es necesario que el servicio vuelva a su normalidad, un incidente no precisamente se refiere a la interrupción total del servicio, puede también aplicarse a la degradación de estos, es decir, que funcionan pero no de manera optima.

Es la misma empresa quien se encarga de definir la prioridad o la severidad de un incidente, ya que una misma situación puede impactar de manera distinta a las empresas de diferente ramo operativo, pongamos un ejemplo, no es lo mismo, que una tienda departamental se quede sin servicio de internet a que una empresa que suministra el servicio de internet deje de hacerlo por causa de un incidente. La tienda departamental su objetivo es vender, y sin internet aun puede hacerlo, aplicando claro soluciones temporales, pero que una empresa que provee de internet deje de hacerlo, significa que la operación total de esta empresa se vio impactado porque no hay servicios que ofrecer, y por consecuencia esta afectación se transmite a sus clientes. Definitivamente hoy en día, el que una empresa no tenga internet constituye un incidente de alta prioridad, en ambos ejemplos, pero el impacto al negocio es en donde puede estar la gran diferencia.

Ahora bien, un incidente menor en esta misma empresa departamental pudiera ser el que algunas de sus impresoras no funcionen, la empresa puede seguir vendiendo, tal vez no pueda imprimir los recibos de venta tan pronto como dictan sus procesos, pero aun la actividad principal de esa empresa no se ve interrumpida.

Con este ejemplo, quiero explicar lo que son las prioridades o las severidades, y que como mencioné anteriormente cada empresa debe definir con certeza y claridad cuales son los incidentes que tienen mayor impacto en los servicios que operan, basados en la combinación de impacto y urgencia para resolver el incidente.

ITIL menciona que pueden establecerse 4 severidades, pueden ser nombradas así como tal, siendo la severidad 1 la de mayor impacto y mayor urgencia hasta la severidad 4 con el menor impacto y la menor urgencia. De nuevo, el impacto y la urgencia pueden ser completamente distintos para cada empresa.

Hay empresas que en lugar de dar números a las severidades, simplemente se refieren a los incidentes como de severidad alta, media o baja.

La correcta definición de las prioridades constituye una mejor practica dentro de la gestión de incidentes, que de hacerse correctamente desde el inicio, y que estas sean dominadas por el personal que se dedica a abrir los incidentes, evitan muchos malentendidos en el proceso por caer en la subjetividad.

Parte importante de un contrato de soporte de servicios es de la definición de las severidades, pero también se complementa con los acuerdos de los niveles de servicio, por sus siglas en ingles conocido como SLA: *Service Level Agreement.*

Un SLA “se define como un compromiso oficial que prevalece entre un proveedor de servicios y un cliente” (Skelton, 2017)

La definición de este autor me parece que lo dice muy simple, es un acuerdo, un compromiso que el proveedor de servicio establece con su cliente.

Y para ello, a cada severidad le corresponde un SLA, es decir, la severidad más alta viene acompañado del SLA más agresivo, o más retador para la empresa que ofrece el servicio. Las empresas que ofrecen el servicio de gestión de incidentes normalmente empaquetan este producto dentro de su portafolio, y por lo que me ha tocado ver, casi siempre se ofrece en tres niveles, cada nivel ligado a tiempos de respuesta distintos y por consiguiente con precios asociados a cada uno de los niveles. Les describo un ejemplo en la tabla 1.

Plan	Severidad 1	Severidad 2	Severidad 3
Platino	• Atención en 15 mins vía telefónica • Restauración de servicios en no mas de 2 horas • Reemplazo de Partes dañadas en no más de 2 horas • Diagnóstico en no más de 3 hrs.	• Atención en 30 mins • Reemplazo de Partes dañadas en no más de 2 horas • Diagnóstico en no más de 3 hrs.	• Atención en menos de 24 horas vía correo electrónico • Reemplazo de Partes dañadas en no más de 2 horas • Diagnóstico en no más de 12 hrs.
Oro	• Atención en 60 mins vía telefónica • Restauración de servicios en no más de 6 horas • Reemplazo de Partes dañadas en no más de 6 horas • Diagnóstico en no más de 6 hrs.	• Atención en 90 mins vía telefónica • Reemplazo de Partes dañadas en no más de 12 horas • Diagnóstico en no mas de 12 hrs.	• Atención en 12 horas correo electrónico • Reemplazo de Partes dañadas en no más de 24 horas • Diagnóstico en no más de 24hrs.
Plata	• Atención en menos de 24 horas vía correo electrónico • Diagnóstico y reemplazo de partes dañadas en 36 hrs.	• Atención en menos de 24 horas vía correo electrónico • Diagnóstico y reemplazo de partes dañadas en 48 hrs.	• Atención en menos de 24 horas vía correo electrónico • Diagnóstico y reemplazo de partes dañadas en 72 hrs.

Tabla 1 Ejemplo de Niveles de Servicio y SLAs

Entre mejores sean los tiempos de respuesta mayor es el precio que tendrá cada plan, y dependiendo del giro del negocio, de la criticidad de cada uno de los servicios que operan, será el plan con los SLAs que necesiten pagar para reestablecer su operación.

“Los incidentes pueden ser diagnosticados y resueltos por personas en muchos grupos diferentes, según la complejidad del problema o el tipo de incidente. Los incidentes pueden ser escalados a un equipo de soporte para su resolución. El enrutamiento se basa típicamente en la categoría de incidente. Es importante que todos estos grupos comprendan el proceso de gestión de incidentes y cómo su contribución a esto ayuda a administrar el valor, los resultados, los costos y los riesgos de los servicios prestados” (AXELOS Limited, 2019)

Ahora bien, “El propósito de gestión de incidentes es minimizar el impacto negativo de los incidentes mediante la restauración del funcionamiento normal del servicio lo más rápido posible”. (AXELOS Limited, 2019)

La gestión de incidentes se ocupa de administrar todos y cada uno de estos incidentes de forma tal que el impacto en los servicios sea minimizado por medio de la restauración, su objetivo principal es restaurar el servicio lo más pronto posible, esto es algo que debe estar siempre en la mente de los que forman parte del proceso de incidentes: “restaurar el servicios tan pronto como sea posible”, la restauración puede ser mediante soluciones definitivas o soluciones temporales, que en el ramo se conocen como *workarounds*.

Un *workaround* no es nada más que una solución que elimina por completo el impacto que genera un incidente. Es muy común que los operadores de los incidentes se enfoquen en esto más que a encontrar la causa raíz del problema, que muchas de las veces, en los sistemas de información, estas soluciones temporales terminan en reiniciar los equipos, y con esta medida, se pierde por completo la oportunidad de llegar a la causa raíz del incidente debido a que con el reinicio se llegan a perder los registros de la falla misma.

“Ningún servicio está exento de errores, fallas o vulnerabilidades, y esto conduce a incidentes. Los errores pueden ocurrir en cualquiera de las cuatro dimensiones de la administración del servicio y aunque muchos de los errores se identifican y resuelven antes de que el servicio esté activo, algunos permanecen sin identificar o sin resolver. Son estos errores los que pueden y supondrán un riesgo para los servicios en operación. En ITIL, estos errores se conocen como problemas y son gestionados por la práctica de gestión de problemas.” (AXELOS Limited, 2019)

Se crea un problema para saber la causa raíz o el origen de los incidentes, ya que si bien, la gestión de incidentes se encarga de restablecer el servicio, el objetivo de la gestión de problemas es saber porqué ocurrió el incidente. La re-ocurrencia de un incidente activa el proceso de gestión de problemas.

“Problema: causa de uno o varios incidentes, la causa generalmente no se conoce en el momento en que se crea el registro del problema” (Clydebank Media LLC, 2017)

“Problema se refiere a una causa, o causa potencial, de uno o más incidentes”. (AXELOS Limited, 2019)

Con frecuencia, quienes no están familiarizados con la terminología de ITIL pudieran llamarle problema a un incidente, es muy común que por ejemplo un empleado de una oficina diga que tiene un problema con su impresora cuando no puede imprimir, que le impide continuar con su trabajo, la restauración del servicio de impresión pudo haberse llevado a cabo con el simple reinicio de la impresora. Pero si queremos saber la razón por la que la impresora dejó de imprimir en ese momento, entonces necesitaríamos invocar el proceso de gestión de problemas, iniciando con abrir un problema, que se lleve a cabo una investigación más profunda, un análisis de causa raíz, para saber exactamente el porqué de la falla. Podría ser una falla de comunicación entre dispositivos, podría ser un problema de la red, un problema con el cable, o un problema de hardware, etc. El abrir un caso problema, dependerá también de la criticidad de la falla. El llevar a cabo un análisis de causa raíz pudiera consumir recursos y por ejemplo, si en una ocasión no pudo imprimir y se resolvió con un reinicio, tal vez no sea necesario ir más allá, pero qué tal que esa impresora ya lleva muchos incidentes y necesitamos saber si es necesario el reemplazo de alguna refacción, un cable o la impresora misma, es entonces cuando si vale la pena llegar más profundo en la investigación de la causa raíz.

La diferencia entre un incidente y un problema, según ITIL, radica en que el incidente tiene un impacto en los servicios y el problema es la causa de ese o esos incidentes, en el incidente no precisamente sabemos porqué fallaron las cosas, lo que importa es restablecer el servicio sin importar las causas, los problemas requieren investigación y análisis para identificar la razón de la falla y de esa manera recomendar soluciones a largo plazo.

“identificar las causas de un incidente es una actividad de gestión de problemas que puede llevar a la resolución del incidente, pero también pueden generar conflictos, por ejemplo, investigar la causa de un incidente puede demorar las acciones necesarias para restaurar el servicio.” (AXELOS Limited, 2019)

Frecuentemente nos encontramos con este reto en la operación, en muchas ocasiones la respuesta fácil y rápida a la restauración, es el reinicio de procesos o dispositivos, lo que implica que se pierdan registros de los errores en tiempo real, y por ende, sin estos registros, nos impide llegar a la causa raíz que originó el incidente. Cuando logramos identificar y diagnosticar un problema, esto se tiene que documentar como un error conocido, que debe incluir la causa raíz y la solución a ese problema, de tal manera que

pueda ser consultado por el proceso de incidentes cada vez que se presente un incidente de la misma naturaleza.

La gestión de problemas está estrechamente relacionado a la gestión de incidentes, y según lo que menciona Zitek (2018) en su artículo, muchas de las empresas creen que la gestión de problemas es un simple complemento que puede ser agregado a la gestión de incidentes, cuando en realidad implementar la gestión de problemas va mucho más allá, ya que es un proceso complejo y continuo que no necesariamente tiene que esperar a que pase un incidente para ser activado, de hecho la gestión de problemas siempre esta de alerta.

Dentro del proceso de gestión de problemas existen dos subprocesos, en los que en realidad existe muy poca documentación al respecto:

- Gestión Proactiva de Problemas – PPM por sus siglas en ingles *Proactive Problem Management.*
- Gestión Reactiva de Problemas Reactivo – RPM por sus siglas en ingles *Reactive Problem Management.*

Para los fines de este documento nos enfocaremos en PPM, ya que justo hablaremos de la implementación de un proceso de prevención. Empecemos por definir cada uno de los conceptos relacionados:

Preventivo
“Las actividades preventivas consisten en el análisis de varias fuentes de datos para identificar y corregir problemas que aún no han provocado incidentes.” (Soreanu, 2016)

La definición de preventivo de Soreanu, e incluso la que se describe en la RAE, “Preparación y disposición que se hace anticipadamente para evitar un riesgo o ejecutar algo”, se refiere a situaciones que aun no han sucedido, por lo que el termino sugiere que se lleven a cabo las tareas necesarias para evitar que haya una interrupción en los servicios.

Proactivo
“Las actividades proactivas son las que deben continuar una vez que se obtiene el análisis de la causa raíz, e incluyen:

- Limpieza de la infraestructura: después de que el análisis de la causa raíz identifica y corrige un error de configuración en un dispositivo en particular, todos los demás dispositivos del mismo tipo se analizan en busca de este error y se reparan.

- Lecciones aprendidas: el análisis de la causa raíz puede identificar problemas en el proceso, capacitación, herramientas, etc., que deben resolverse para evitar incidentes similares en el futuro.

Estas actividades son reactivas y proactivas: se desencadenan por incidentes, pero abordan problemas que pueden prevenir futuros incidentes." (Soreanu, 2016)

Es una línea muy delgada la que divide a estos conceptos, pero para efectos prácticos podríamos decir que:

Preventivo: se refiere a las actividades, tareas o análisis que llevamos a cabo para anticiparnos a que suceda un incidente, por ejemplo: se enciende el sensor de la gasolina para prevenir que ésta se acabe y no podamos continuar con nuestro camino.

Proactivo: se refiere a todas esas actividades que llevamos a cabo después de que ya tuvimos una experiencia desagradable con algún incidente, que continuando con el ejemplo anterior, podríamos decir que si ya se nos acabó la gasolina en una ocasión, y tengo dos o más coches en casa, reviso en cada uno de ellos en dónde se encuentra el medidor de la gasolina para evitar que se vuelva a terminar en algún otro coche.

Entonces, de manera muy sencilla la gestión proactiva de problemas tiene como objetivo identificar y resolver problemas, así como proporcionar soluciones adecuadas antes de que ocurran uno o más incidentes.

Como lo comenta Anil Kumar Nandibhatla (2017) en su articulo, implementación de PPM es extremadamente desafiante en un entorno en el que se tienen cientos de servicios, diferentes tecnologías y muchas otras cosas sucediendo al mismo tiempo, y si a esto le agregamos el hecho de que no hay mucha documentación al respecto, lo hace todavía un proyecto de implementación mucho mas retador.

Ciclo de Prevención

Analizando la información de los procesos de ITIL ya implementados con nuestro cliente, Gestión de Incidentes y Gestión de Problemas, encontramos que teníamos ya implementadas tareas que en conjunto con algunas herramientas de Cisco pudieran ser ligadas para generar e implementar un proceso de prevención.

Estas herramientas de Cisco, AFM (*Automatic Fault Management*) & BCI (*Business Critical Services*) ambas son aplicaciones meramente preventivas. AFM identifica en tiempo real mensajes error alimentándose de las fallas ocurridas en la red del cliente o incluso de errores que han ocurrido de manera global con otros clientes que tienen implementados los mismos equipos Cisco, y BCI que por medio de tableros de monitoreo identifica tendencias de falla o umbrales de parámetros que indican que algo pudiera fallar.

Entonces, como se muestra en la figura No. 1, el ciclo de prevención inicia al abrir uno o varios incidentes, que son atendidos aplicando acciones de restauración de los servicios, después se genera un caso problema para obtener la causa raíz, y posteriormente se genera un caso preventivo para identificar el log, alarma, umbral o el parámetro exacto que puede ser convertido en una entrada para AFM o BCI, y de esta manera las herramientas toman ese conocimiento y a partir de ahí, monitorear siempre esa información en la red para que la próxima vez que aparezca sepamos que acciones tomar, ya sea para evitar por completo la interrupción del servicio o en el peor de los casos, cuando las fallas son inminentes, minimizar el tiempo de la afectación al tener ya documentadas las acciones para ello.

Figura 1 Ciclo de Prevención

Prácticamente con el ciclo de prevención, estamos alimentando una base de datos de errores conocidos, que con el paso del tiempo estaríamos enriqueciendo de tal manera que lo que ya nos pasó se pueda evitar o al menos no impacte de la misma manera a la operación de nuestro cliente.

Proceso de Prevención

Prevenir tiene que ver con tomar acciones por adelantado para evitar daños, riesgos, peligros, situaciones desagradables, en el caso de las tecnologías de información, anticiparnos a las fallas que puedan presentar los equipos de cómputo y por ende reducir considerablemente el efecto que pudiera desencadenar su mal funcionamiento.

Sabemos que siempre habrá fallas en los dispositivos, son maquinas, que por defectos de fabrica, el uso, el paso del tiempo, el ambiente, por muchos factores pueden llegar fallar en algún momento. Por lo que para nosotros fue necesario reunirnos con nuestro cliente para tomar acciones y tratar de minimizar la afectación causada por fallas en los equipos.

Si bien, no existe mucha documentación acerca del tema de la prevención en el ámbito de las tecnologías de la información, al menos no tal cual usando el concepto de “Prevención”, este documento se basa en ello, establecer los conceptos que mejor encajan con nuestro cliente y los servicios que ofrecemos,

incluso generando nuestras propias definiciones que van acorde con la operación que ya se encuentra en ejecución hoy en día.

Todos los colaboradores de nuestro cliente que operan los procesos de gestión de incidentes y gestión de problemas están certificados como expertos en ITIL, y es por ello que tratamos de apegarnos lo mas posible a los lineamientos de este marco de referencia, la realidad es que no existe un proceso dentro de ITIL que pudiéramos haber tomado como referencia con fines preventivos. Dentro del portafolio de Servicios que ofrece Cisco tampoco se encuentra algún proceso llamado "Gestión de la prevención" ó algún proceso similar dedicado a prevenir. No encontramos documentación pública disponible sobre procesos para prevenir en la industria de TI, ITIL habla un poco sobre la Gestión Proactiva de problemas pero solo a manera de definición, por lo que si bien tomamos a ITIL como base para crear nuestra propia versión de un proceso de prevención, resaltamos que trabajamos en nuestra propia metodología para llevar a cabo este proyecto, ya que acordamos nuestras definiciones, métricas, KPIs, acciones preventivas, y todo lo que un proceso conlleva, basándonos en las necesidades de nuestro cliente.

El proceso de prevención implementado con nuestro cliente busca minimizar el impacto a los servicios mediante la identificación de riesgos y ejecución de acciones preventivas.

Métricas

Una vez que los procesos han sido implementados es necesario medirlos, se vuelve muy relevante saber si lo que se ha implementado lo estamos haciendo de manera correcta o de la manera en que lo planeamos, porque al principio cuando el proceso es puesto en operación tal vez pueda haber cosas que durante la planeación parecían la mejor manera de hacerlas, pero al ponerlo en practica el resultado es diferente, al inicio los números pudieran no ser los mejores, pero para ello hay que medir, se dice que lo que no se mide no se puede mejorar.

Medir es simplemente capturar los datos necesarios, de tal manera que podamos facilitar la toma de decisiones. Cada empresa decidirá qué datos son los más relevantes para ellos, los que le permitirán alcanzar los objetivos que se han trazado.

No obstante, hay recomendaciones generales que suelen ser un buen punto de partida en la mayoría de los casos, sobre todo tratándose de los principales procesos de ITIL, como la gestión de incidentes y la gestión de problemas.

Las métricas “son mediciones que evalúan cuantitativamente el desempeño de las operaciones de la industria” (Pabbathi, 2020) según ITIL una métrica es “una medición o cálculo que se supervisa o informa para su gestión y mejora” (AXELOS Limited, 2019)

Existen diferentes tipos de métricas:

“Métrica Tecnológica: es una métrica asociada a un componente tecnológico o aplicación, tales como desempeño o disponibilidad (número de transacciones por minuto en una base de datos, consumo de ancho de banda, tiempo en ejecutar una operación de cómputo, etc.).

Métrica de Proceso: Orientadas hacia procesos de la administración o provisión de servicios y nos ayudan a determinar la efectividad general de un proceso a través de 4 características: valor agregado, calidad, desempeño y adhesión.

Métrica de Servicio: Nos permiten medir el desempeño de un servicio End to End” (Romero, 2015)

Las métricas permiten obtener estadísticas bastante detalladas sobre la calidad del servicio y la eficiencia de los procesos de cada empresa.

Algunas de las métricas que pueden medirse en el proceso de gestión de incidentes son las siguientes:

- Número de casos problema cerrados
- Tiempo promedio de diagnóstico
- Número de Casos problema con causa raíz identificada
- Número de incidencias resueltas con *workaround* documentado
- Categorías de incidencias reportadas en el periodo
- Costo total de resolución por problema
- Tiempo promedio de Solución
- Número de cambios creados para solucionar un problema
- Etc.

Reitero, cada empresa decidirá qué es lo importante para ellos y de esta manera elegir las métricas que consideren que van alineados con sus objetivos de negocio. Es necesario identificar muy bien qué es lo que se quiere medir, definir muy bien el concepto, desarrollarlo para que sea claro de identificar, calcular y comprender lo que se quiere obtener.

KPI

Un KPI por sus siglas en ingles *Key Performance Indicator,* está compuesto por métricas que miden el rendimiento de los procesos, y que estarían determinando el éxito o no del proceso mismo. Algunas definiciones para KPI son las siguientes:

KPI: Métricas vitales necesarias para que una organización cumpla con sus objetivos comerciales, lo que refleja los CSF (*Critical Success Factor*) de una organización. (Pabbathi, 2020)

KPI: son valiosos indicadores de rendimiento y proporcionan información crítica para los tomadores de decisiones dentro de los departamentos de TI (Clydebank Media LLC, 2017)

"Un KPI es una métrica importante utilizada para evaluar el éxito en el cumplimiento de un objetivo." (AXELOS Limited, 2019)

Es importante que recalquemos la distinción entre un KPI y una métrica general. Los KPI son métricas (siendo que métricas es el término general para una medición) pero no todas las métricas son KPI. Nuestro proceso o servicio puede tener muchas métricas que nos ayudarán a tomar decisiones y algunas de esas son KPI. Lo ideal es que el número de KPI sea muy limitado y que el resto de las métricas estén asociadas indirectamente a un KPI. (Romero, 2015)
En la siguiente tabla veamos las diferencias entre métrica y KPI:

KPI	Métrica
Miden el progreso hacia un objetivo	Son datos cuantitativos, números, estadísticas.
Crean expectativas y llevan a la acción para conseguir un objetivo	No tienen valor por si mismas.
Los KPIs son métricas	Las métricas no son KPIs
Ejemplo:	Ejemplo:
Incidentes con Impacto < 20%	Numero de Incidentes con Impacto

Tabla 2 Diferencias entre métrica y KPI

Tablero de control

ITIL dice que un tablero de control, también conocido como *dashboard*, es una "Representación gráfica de datos en tiempo real, (AXELOS Limited, 2019), tan simple como eso, Un lugar donde colocas de manera grafica los KPIs que te interesa medir para tomar las decisiones del rumbo de la empresa. Es importante recalcar que el dashboard te permite medir el estado actual de una serie de indicadores y evaluarlos frente a los objetivos que se hayan trazado. Los *dashboards* tienen la ventaja de poder detectar en una sola vista, las desviaciones que se vayan presentando y por ende actuar a tiempo para corregirlas.

Es muy importante saber elegir los KPIs que conformarán el tablero de control, obviamente deberán estar ahí los que son más relevantes para la empresa, optar por los que generan mayor valor y organizarlo de forma tal que sea posible observar toda la información que nos interese de forma clara, deberá ser de fácil comprensión y lectura.

El tablero de control sirve para saber lo que esta sucediendo en el negocio en tiempo real, sin dejar de lado la operación del día a día.

A continuación, en la figura no. 2, un ejemplo del tablero de control de Gestión de problemas, en el cual tenemos en una sola vista el estatus general del proceso durante un mes en específico, el volumen de casos creados y cerrados en el mes, el tiempo transcurrido para encontrar la causa raíz, el tiempo que nos tomó entregar solución la solución final, si hubo reincidencias, y el promedio de la evaluación que tuvieron los problemas del mes, todos ellos con la finalidad de censar el status de cada uno con respecto al objetivo planteado.

Figura 2 Ejemplo de Tablero de control o dashboard mensual del proceso de Gestión de Problemas.

CSAT

La gestión de incidentes esta muy ligada a la satisfacción del cliente, porque justo al reportar un incidente el usuario se encuentra en una situación que, en muchas de las ocasiones, le impide continuar con su trabajo o con la acción que venia realizando, podría estar desesperado, frustrado, podría tratarse incluso que involucra perdida de dinero, cuestiones de vida o muerte, y el hecho de que alguien que lo atienda le haya resuelto o no su problema envuelve muchas emociones que desencadenan en el resultado de la evaluación de un incidente o problema.

Si no es fácil medir la parte racional de la experiencia de un cliente con una compañía o una marca, la cuestión se complica cuando añadimos que sus decisiones tienen un claro componente emocional como es el caso de su experiencia. (Alfaro, 2012)

Existen diferentes formas de saber qué tan felices están los clientes, analicemos las formas más populares de evaluar productos o servicios en el mercado:

"*Net Promoter Score*, NPS es una de las métricas más de moda en relación con la experiencia de cliente. Es una forma sencilla de obtener cierta información mediante una simple pregunta:

¿Recomendaría esta compañía a un amigo o familiar?

Figura 3 Escala de Evaluación del NPS

La pregunta frecuentemente viene acompañada de una imagen con números del 1 al 10 para que la persona elija que tan probable es que haría la recomendación, siendo el 0 el menos probable y el 10 muy probable que recomiende.

En la figura No. 3, aparecen en rojo del 0 al 6, para quienes obtienen los resultados de las evaluaciones, es indica que no recomendarían o que incluso hablarían mal del producto o el servicio, el 7 y el 8 en amarillo porque son personas que tienen una opinión neutral, y el 9 y el 10 en verde, que según el NPS serian las personas que recomienden.

El NPS, no ofrece información sobre cómo y dónde actuar para mejorar. Por otra parte, es un indicador muy cuestionado en algunos círculos y según la comunidad científica no está demostrada su correlación con el crecimiento de las compañías." (Molina, 2012)

Me parece que el NPS es una manera de evaluar muy general, como comenta el autor de esta definición no ayuda en cómo y dónde actuar para mejorar. Entiendo que hoy en día no a todos los usuarios de un producto o un servicio nos gusta emplear tiempo en una encuesta se servicio muy larga, y sobre todo si no tenemos mucho que decir. Es muy común que solo cuando queremos quejarnos contestamos una encuesta de satisfacción, por lo que considero que el NPS, podría usarse cuando queremos saber la lealtad emocional que el cliente siente por la empresa o la marca, solo eso.

"El CES (*Customer Effort Score*) es un indicador muy interesante para todo lo relacionado con las interacciones de servicio al cliente. Según algunos estudios, presenta una mayor correlación que las mediciones tradicionales de satisfacción y que el NPS con los comportamientos y decisiones del cliente como: recompra, incremento del gasto o recomendación.

El CES se calcula a través de una pregunta: ¿Cuánto esfuerzo personal le ha supuesto gestionar su solicitud? Esta pregunta se responde por parte del cliente en una escala del 1 que corresponde a muy poco esfuerzo, al 5 un gran esfuerzo. (Molina, 2012)

Difiero en que, con una sola pregunta del CES, podamos obtener información que nos lleve a saber si el cliente compraría de nuevo o si nos recomendaría, porque me parece que se queda muy corta en relación

a la experiencia que ha tenido un cliente con la empresa, pero si eso es lo que le interesa saber a la empresa, qué tan leales son sus clientes, me quedaría con el NPS.

Como a nosotros nos interesa tener mucho más detalle del desempeño de los procesos, y sobre todo queremos saber específicamente en dónde tenemos que mejorar elegimos al CSAT como método para evaluar cada uno de los incidentes.

CSAT es el acrónimo de *Customer Satisfaction Score*, es un indicador muy versátil, ya que se le pueden hacer a los usuarios una variedad de preguntas enfocadas a la experiencia que ha tenido un cliente con un producto o servicio. Entonces, dependiendo de lo que a la empresa le interese medir o mejorar, serán las preguntas que se hagan acerca de como fueron atendidos en un requerimiento, es un indicador muy útil para medir a corto plazo la felicidad de los clientes.

“CSAT se mide al interrogar a los clientes mediante una encuesta que generalmente no plantea más de tres a cinco preguntas. La encuesta le pide a cada cliente que califique su satisfacción, a menudo usando una escala de 5 puntos con preguntas y términos como: ¿Qué tan satisfecho está con el servicio que brindamos? Una interpretación popular de la puntuación CSAT utiliza la suma de los encuestados que responden "Satisfecho" o "Muy satisfecho". Esta métrica a menudo se expresa como un porcentaje ". (Jones, 2018)

“El CSAT, o nivel de satisfacción del cliente, es un poco más complicado. Indica qué tan satisfecho está un cliente con un producto, transacción o interacción particular con su empresa utilizando múltiples preguntas” (Hill, 2020)

El siguiente es un ejemplo de las preguntas que se pueden hacer en un CSAT, la idea es calificar del 1 al 5, siendo el 5 la más alta evaluación equivalente a Muy Satisfecho y el 1 al rango más bajo correspondiente a Muy Insatisfecho:

1.Evaluación General
2. Facilidad de Acceso
3. Tiempo de respuesta
4. Estatus del Problema
5. Solución Efectiva
6. Capacidad Técnica
7. Cortesía

Capítulo II. Descripción del proyecto reportado

2.1 Antecedentes del proyecto reportado

América Móvil es la empresa de telecomunicaciones más grande de América Latina y la tercera en el mundo. Sus subsidiarias en México son Telcel, Telmex, Sección Amarilla y Telvista, que ofrecen servicios de telefonía fija y celular, de televisión de paga, de internet y de datos móviles.
De acuerdo con sus estados financieros, el más rentable es el segmento voz celular, seguido del negocio de los datos celulares.

América Móvil tiene presencia en México, Argentina, Brasil, Chile, Colombia, Costa Rica, República Dominicana, Ecuador, El Salvador, Guatemala, Honduras, Nicaragua, Panamá, Paraguay, Perú, Puerto Rico, Uruguay y Estados Unidos, en el continente europeo la compañía tiene presencia en Holanda y Austria.

Telmex es la empresa de telecomunicaciones que ofrece servicios de TI, telefonía fija e internet vía fibra óptica, ADSL y VDSL a los mexicanos. Su infraestructura incluye más de 300,000 km de fibra óptica en México, además de conexiones vía cable submarino con 39 países.
Telmex comenzó a ser proveedor de Internet ISP a través de una de sus filiales.

Nuestro cliente, filial de TELMEX, y por lo tanto parte de América Móvil, fundada en octubre de 1995 se dedica a construir, instalar, mantener, operar y explotar las redes de telecomunicaciones para prestar servicios de conducción de señales de voz, sonidos, datos textos e imágenes a nivel local y de larga distancia nacional e internacional, son integradores globales de redes y tecnología.

Presta servicios de Internet dedicado, servicios de gran ancho de banda. Por ejemplo, redes privadas virtuales (VPN), acceso a multiservicio, internet de alta velocidad (turbo *access*) o internet de acceso normal. En la parte de voz integrar sus servicios de tarjeta prepagada y servicios inteligentes (VPNet). Nuestro cliente administra también la infraestructura de *backbone* hacia las demás filiales de América móvil en Latinoamérica, es decir, es responsable de las principales conexiones troncales de internet, compuesta por un gran número de *routers* interconectados de gran capacidad que llevan los datos a través de fibra óptica.

El 50% de la infraestructura operada por esta empresa, corresponde a la marca Cisco, lo cual hace que el contrato de servicios celebrado entre América Móvil y Cisco Systems de México tome gran relevancia. Existe un contrato máster con América Móvil, que incluye diferentes anexos para cada una de las

filiales, detalla cada uno de los requerimientos para cubrir necesidades distintas de sus clientes, ya que ofrecen ofrece los mejores niveles de servicio, seguridad, y monitoreo 7x24.

Dentro de sus principales clientes destacan: bancos, hospitales, servicios gubernamentales, diversas empresas de iniciativa privada, las mismas subsidiarias de América Móvil como Telmex, Claro, Telcel, entre muchas otras. De ahí la importancia por mantener siempre el más alto grado de disponibilidad de sus redes que exige la actualidad.

La más mínima interrupción del servicio se traduce en perdida para las empresas, por lo que el contrato de servicio de soporte técnico con Cisco cuenta con niveles de servicio muy puntuales. Este contrato se ha venido celebrando consecutivamente desde los últimos 11 años, en un inicio, y hasta antes de este proyecto del Proceso de Prevención, contemplaba únicamente la restauración de los servicios en el menor tiempo posible.

Desde hace ya un par de años, nuestras conversaciones con el cliente iban más allá del análisis de causa raíz, el cliente definitivamente está interesado en saber cuáles son las causas de las fallas que derivan en interrupciones en los equipos Cisco, pero también está preocupado por emplear ese conocimiento adquirido, esas lecciones aprendidas para implementarlas y de esta manera evitar impactos futuros en el servicio a sus clientes.

Dado que el alcance del contrato entre Cisco y nuestro cliente contempla únicamente soporte, y se enfoca básicamente en restaurar los servicios en el menor tiempo posible, todos los recursos estaban puestos en esa tarea. Parte importante de la evolución de la gestión de incidentes, es el saber utilizar la base de conocimiento que nos deja una falla y que ésta sirva prevenir, para evitar que lo mismo suceda en el futuro. Era muy necesario revisar la operación actual, de tal forma que con los mismos recursos pudiéramos dedicarle el tiempo y el esfuerzo que requiere una estrategia de prevención, sin descuidar el soporte y monitoreo que la red demanda.

El Proceso de Prevención contempla desde la unificación de definiciones, el análisis de la operación actual, el rediseño de la operación mediante la creación de un proceso para colectar información que, siendo analizada, nos permitiría emitir una recomendación para que la causa raíz de las interrupciones de servicios no sucedan más en el futuro.

2.2 Objetivo del proyecto reportado

Minimizar el impacto a los servicios que se proporcionan en la red de nuestro cliente, mediante la identificación de riesgos y ejecución de acciones proactivas, así como la disminución de reincidencias por medio de acciones preventivas.

2.3 Descripción de la metodología empleada

Existe una relación de trabajo madura con nuestro cliente, con procesos establecidos y muy comprometidos con la mejora continua. Todos los gerentes y subgerentes de esta empresa están certificados como ITIL *experts*, esto da como resultado el dominio de este *framework* de soporte en la operación del día a día.

El conocer este conjunto de conceptos y buenas prácticas usadas para la gestión de servicios de tecnologías de la información, fue la base para el análisis de la operación que se llevaba en ese momento y a su vez la plataforma que apoyó el rediseño de ésta.

Actualmente se tienen implementados los procesos de Gestión de Incidentes, Gestión de Problemas, Gestión y Evaluación del Cambio.

Nuestro cliente es una de las filiales de América Móvil que cuenta con la independencia del corporativo en cuestión de operación, esto le permite estar siempre ágil y con la libertad de modificar sus formas de trabajo para alinearse y alcanzar sus objetivos las veces que sea necesario, con la única finalidad de la mejora continua. Todos sus procesos siguen el ciclo de Deming, planean, implementan, miden o revisan y actúan en consecuencia.

Finalmente, y como en la mayoría de los proyectos que se implementan por parte de Cisco, este fue debidamente planificado, comunicado, controlado, documentado y está siendo monitoreado a través de un tablero de control mensual para cumplir con procesos de la operación de nuestro cliente y que forman parte de la metodología del PMI.

De manera general no hubo solo una metodología como tal que se implementara de inicio a fin, de hecho al buscar documentación al respecto, esperábamos encontrar experiencias de empresas implementando un proceso de prevención, información que pudiéramos usarla como guía, desafortunadamente no encontramos como tal datos de implementaciones similares por lo que nos tocó sentarnos a planear nuestra propia metodología empleando una combinación de las se mencionaron en los párrafos anteriores, éstas fueron las que se apegaban un poco a la operación actual de nuestro cliente para usarlas como marco de referencia y fueron la base para llegar al objetivo planteado.

2.4 Planeación o Cronología del proyecto llevado a cabo.

Actividad	Fecha
Primera Platica Formal sobre Prevención	22/08/2019
Reunión para establecer alcance de Estrategia de Optimización de Recursos	10/09/2019
Presentación de Propuesta	26/09/2019
Reunión para Confirmación de Acuerdos	03/10/2019
Entrenamiento Cliente	22/10/2019
Entrenamiento Cisco	24/10/2019
Inicio del Nuevo Modelo de Atención de Incidentes	01/11/2019
Definición del Alcance del Proceso Preventivo	06/11/2019
Presentación de Propuesta	19/11/2019
Inicio Proceso Preventivo	01/12/2019
Revisión primer *Service Request* Preventivo	05/12/2019
Ajustes y correcciones al *Service Request* Preventivo	06/12/2019
Transferencia de Conocimiento del Proceso de Prevención	23/12/2019
Kick Off Proceso de Prevención	03/01/2020

Tabla 3 Cronología del proyecto

2.5 Descripción de actividades

Primera Platica Formal sobre Prevención

En diversas reuniones programadas para presentar métricas resultado del contrato de soporte, surgían conversaciones orientadas en todo momento a las acciones que deberían de seguirse para evitar que los incidentes impactaran nuevamente a los servicios. Después de años de revivir los mismos incidentes, Nuestro cliente estaba ya preparado para el siguiente paso, usar todo ese conocimiento adquirido en evitar que sucediera la misma falla una vez más.

Las cláusulas del contrato de servicio están meramente aplicadas al soporte a la operación, no incluía ninguna de estas acciones preventivas, por lo que después de negociar algunas cláusulas se llegó finalmente al acuerdo de incluir este proceso, el cual vendría a mejorar en todo sentido su operación a cambio de algunas tareas que tenían menor prioridad para nuestro cliente.

Se tuvo una primera reunión celebrada en las instalaciones de nuestro cliente, en la que estuvieron presentes el director de Tecnologías de Información de Nuestro cliente y los equipos de trabajo de las Gerencias de Incidentes y Problemas, por parte de Cisco Gerente de Cuenta, Gerente Operativo, Gerentes de Operación y Gerentes Técnicos, todos enfocados a dar paso al Proceso Preventivo. Se habló a muy alto nivel cuáles serían las posibles estrategias, se unificaron los conceptos de tal forma que todos manejáramos el mismo vocabulario preventivo de ahora en adelante, se platicaron las ideas que se tenían en el momento para enfocar los recursos actualmente dedicados al soporte en tareas más preventivas.

Reunión para establecer alcance de Estrategia de Optimización de Recursos

Una vez formalizado el compromiso de iniciar con el Proceso de Prevención, se llevó a cabo la reunión de trabajo con Gerentes y Subgerentes de operación para establecer el alcance y las premisas de la primera tarea: establecer una Estrategia de Optimización de recursos, que como he mencionado con anterioridad, la estrategia vendría a resolver el tema de recursos limitados contemplados en un inicio solo para soporte a la operación, deberíamos organizarnos de tal forma que pudiéramos cubrir la parte preventiva, sin descuidar claro la operación ya implementada de incidentes y problemas.

Se platicaron diferentes puntos de vista, un primer enfoque requería dividir el equipo, nombrando específicamente recursos enfocados a una u otra actividad: reactivo o preventivo. Lo cual no creímos que fuera la solución, dado que pudiéramos tener recursos sin utilización en algunos puntos y la idea aquí era justamente la optimización del equipo de tal forma que no descuidáramos la operación, pero también trabajaríamos sobre aquellos incidentes que afectaron la disponibilidad de gran número de servicios.

Nos costó un poco de trabajo convencer al cliente de no tener ingenieros específicamente asignados para este proceso, en un principio esa fue la petición: elegir a los ingenieros que formarían parte del equipo de prevención. Para Cisco era muy claro que esa no era la solución, por estadísticas, por históricos, sabemos que el mundo de los incidentes es muchas veces impredecible, hay tiempos muertos cuando la operación esta estable, y de repente hay picos de incidentes nunca antes vistos sin que haya alguna tendencia. Para probar esto al cliente, previamente Cisco había analizado el comportamiento del histórico de los incidentes y problemas contemplando registros de un año completo.

Durante ese análisis encontramos también que el 89% de los incidentes correspondían a Incidentes de alta severidad, severidades 1 y 2, lo cual pareciera, si observamos solo estos números, que la red del cliente es muy inestable o que tiene muchísimos problemas críticos. Entendemos que proveen servicios de telefonía e internet a bancos, escuelas, hospitales, residenciales, etc. y que en muchos de los casos se pierde dinero, tiempo y esfuerzo por no tener el servicio activo, pero Nuestro cliente había estado manejando temas como preguntas o consultas de configuraciones como severidades dos, únicamente por la urgencia de alguna configuración que de haberse planeado adecuadamente, pudiera manejarse con el tiempo de respuesta o solución de incidentes severidad 3 o incluso 4, como lo marca ITIL.

En un poco de contexto, el contrato celebrado con nuestro cliente indica que para incidentes severidades 1 y 2, nuestro cliente debe crear un *service request*, ya sea vía telefónica o vía web, y en no más de 15 minutos un ingeniero de soporte dedicado (HTTS) deberá ponerse en contacto con ellos, incluyendo en la llamada un técnico especializado (HTE) más un gerente de operaciones (HTOM), por lo que en la llamada de atención debe siempre haber 3 personas de Cisco en la conferencia con el cliente.

Regresando a los números encontrados resultado del análisis, de ese 89% de *service requests* de alta severidad (1 y 2) el 18% (145) corresponden a casos de severidad 1, el 82% (651) corresponde a severidades 2. El 83% (657) no presentó afectación al servicio, sin embargo, fueron categorizados con alta severidad.

Haciendo referencia a ITIL, las severidades 1 se usan únicamente para cuando hay interrupción en el servicio, actualmente nuestro cliente abría un *service request* severidad 1 solo por considerarlo crítico, sin criterios definidos para ello.

Si bien en esta reunión se platicaron sobre estas ideas de manera general, ambos equipos nos llevamos de tarea elaborar una propuesta de atención basada y apegada a ITIL, que cumpliera también con los compromisos de nuestro cliente hacia sus clientes finales.

Presentación de Propuesta

El día de la reunión, por parte de Cisco habíamos preparado las definiciones de las severidades de manera muy sencilla, puntos específicos para que cualquier operador pudiera identificar la severidad con la que se enfrentaba en cada una las situaciones, como a continuación se detalla:

Severidad 1

Significa que una red operativa está caída, o hubo un impacto crítico (&& o &&&).

- Será utilizada para casos que tengan afectación en servicio en el momento de la apertura
- Para cualquier caso que se presente afectación en sev 2 o 3 se subirá a sev 1

Severidad 2

Significa que no hay servicios impactados en el momento (con excepción de && y &&&) pero existe un riesgo potencial.

- El incidente tuvo afectación, pero éste no fue catalogado como && o &&&
- El incidente fue clasificado como Riesgo Potencial (RP) && o &&&
- Se notificó una alarma critica de la herramienta de BCI y se requiere atención inmediata
- Existe un incidente por una nueva implementación y está clasificado como urgente
- Pérdida de gestión

Severidad 3

Significa que no hay impacto en el servicio ni riesgo potencial

- Consultas y preguntas particulares se abrirán en severidad 3
- Para los errores y *logs* se abrirá como severidad 3
- Casos RIA (*Request in advance*)
- Errores conocidos, KE (*Known Errors*)
- Nuevas implementaciones (eventos o situaciones inesperadas no urgentes)

Apegándonos a ITIL, solo aquellos casos que presentan afectación o interrupción en el servicio deben ser catalogados como severidad 1. Nuestro cliente estuvo de acuerdo en esto, pero además nos pidió agregar aquellos incidentes que presentaron afectación y que además son de clientes críticos para ellos (&& ó &&&). En nuestro contrato con nuestro cliente no tenemos especificados atenciones especiales para sus clientes, por lo que su solicitud no tendría lugar, al menos no con esa justificación, el contrato marca también que el cliente es quien decide la severidad del caso y por ende su tratamiento por lo que accedimos a que los incidentes que no presenten afectación en el momento de que el *service request* fue abierto, pero si lo tuvo en un tiempo inmediato anterior, y además es un cliente clasificado como && ó &&&, podrían entonces abrirse como severidad 1. La definición quedó finalmente como sigue:

Severidad 1

Significa que una red operativa está caída, o hubo un impacto crítico (&& o &&&).

- Será utilizada para casos que tengan afectación en servicio en el momento de la apertura
- Para casos que tuvieron afectación, pero ya no la tienen al momento de la apertura del caso y que estén categorizados como && o &&&
- Para cualquier caso que se presente afectación en sev 2 o 3 se subirá a sev 1

La propuesta también incluía que solamente para *service requests* catalogados como severidad 1 incluirían un HTTS, un HTE y un HTOM, severidades 2 únicamente serían atendidos por HTTS vía telefónica y severidades 3 de igual manera por HTTS vía email.

Definitivamente, el cliente acostumbrado a que la gran mayoría de sus incidentes tenían tiempos de solución muy cortos y atención personalizada, tenia el temor de que las severidades 2 no fueran atendidas adecuadamente. Convencimos al cliente comentando que independientemente de si era una severidad 1 o severidad 2 el diagnóstico estaba comprometido para entregarse en 3 horas, teniendo siempre la puerta abierta para escalar cualquier situación de incidentes en los que ellos notaran algún retraso o alguna desviación.

Esta propuesta fue un factor determinante para que pudiéramos avanzar en el proyecto, nuestro cliente accedió de alguna manera a priorizar la operación y que esto nos permitiera hacernos el tiempo para revisar enfocarnos también en el tema preventivo. Los recursos eran limitados, por lo que adicionar actividades era prácticamente imposible, y al aceptar esta propuesta el recurso humano para la implementación de este proyecto prácticamente estaba resuelto.

Comentamos que tendríamos siempre oportunidad de detenernos a lo largo del proceso para revisar de nuevo este punto y ajustarlo las veces que fuera necesario.

Durante la reunión surgió también la idea de realizar un diagrama de flujo que facilitara esta tarea, porque teníamos muchos años manejando estos criterios, y parecía importante tener una referencia que fuera rápida y visual para tomar decisiones en el momento de abrir *service requests*, y como sabemos en situaciones de interrupción de servicios los minutos se vuelven muy valiosos, nuestro cliente se llevó el compromiso de realizarlo para posteriormente revisarlo en conjunto en la siguiente reunión.

Reunión para Confirmación de Acuerdos

La reunión de confirmación de acuerdos tuvo como agenda presentar los acuerdos ya plasmados en un documento, las definiciones de las severidades y el equipo de trabajo que estaría enfocado en cada uno de los *service requests*, de tal manera que tuviéramos únicamente las conclusiones de lo platicado en las reuniones anteriores. La idea era únicamente presentar notas finales o conclusiones.

Pendiente de la reunión anterior teníamos el revisar el diagrama de flujo que sería usado como referencia por los ingenieros para determinar la severidad correcta de acuerdo con las características del *service request*, se platicó en conjunto y quedó aprobado en esta reunión.

La presentación de la estrategia de optimización incluía:

- Antecedentes – Conclusiones del análisis del histórico para dar paso a la estrategia de optimización de recursos.
- Definiciones de Severidades – Descripción de las severidades apegadas a ITIL y que se apegaba a la operación de nuestro cliente, descritas y complementadas entre nuestro cliente y Cisco.
- Atención de *Service Requests* – en base a la definición de las severidades se decidió el equipo de trabajo que estaría enfocándose en cada uno de los *service requests*.
- Diagrama de Flujo – Un diagrama que facilitaría la toma de decisión a los operadores al momento de abrir un *service request.*

El diagrama de flujo de referencia para determinar la severidad de cada uno de los *service requests* quedó aprobado como a continuación se muestra en la figura número 1:

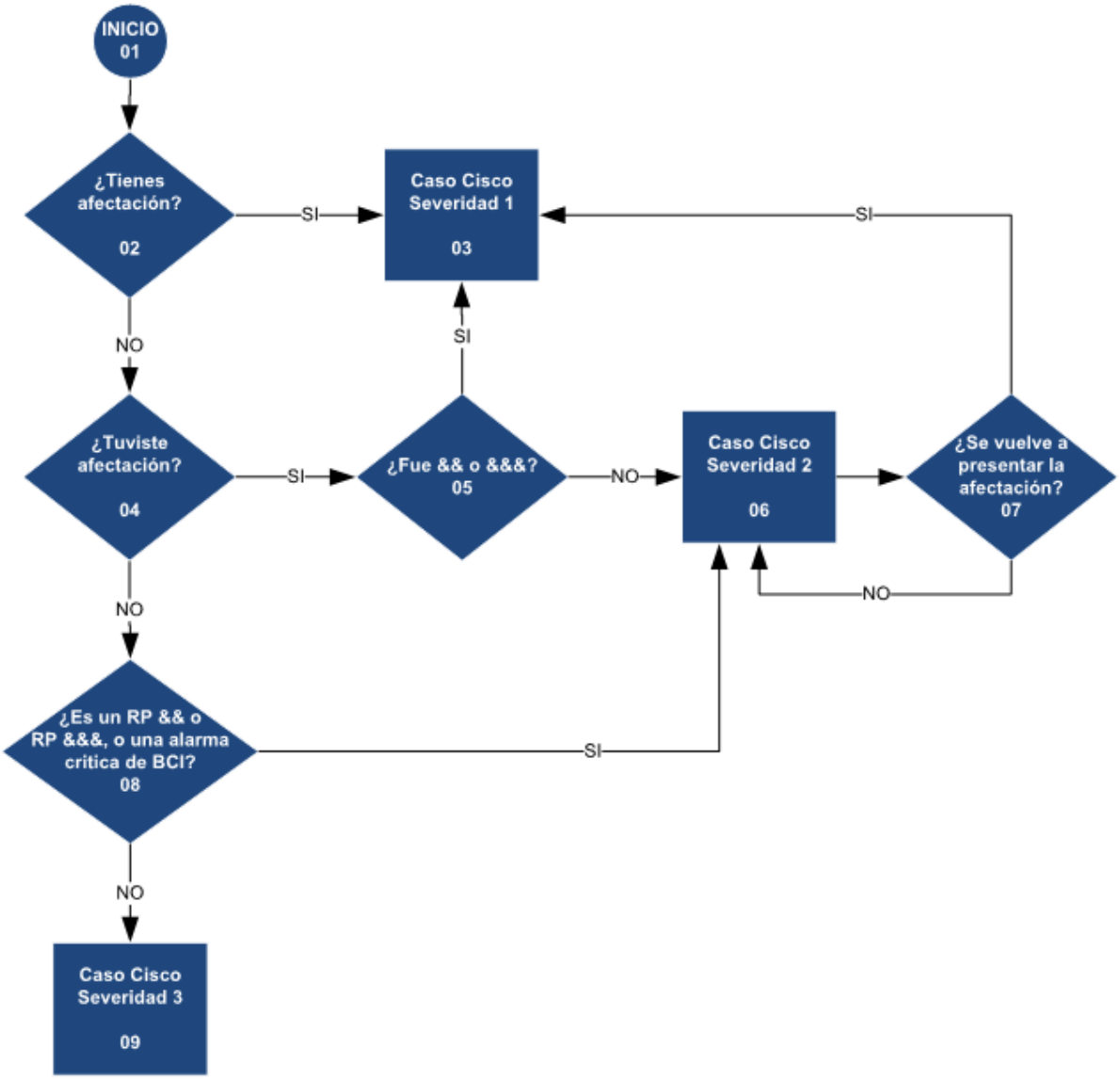


Figura 4 Diagrama de Flujo para determinación de la severidad de un service request

La Estrategia de Optimización presentada tuvo tal aceptación que se decidió en esta reunión, implementarla a partir de noviembre 2019, independientemente del resultado que tendría el Proceso Preventivo.

Entrenamiento

Toda vez que se realiza un cambio en la operación de nuestro cliente, es necesario comunicarlo a los ingenieros de ambos equipos.

Nuestro cliente cuenta con 66 operadores divididos en turnos para cubrir los siete días de la semana las veinticuatro horas del día, por lo que se hicieron dos sesiones presenciales, en las instalaciones de nuestro cliente, y una vía videoconferencia de 1 hora cada una, esta última con la finalidad de ser grabada y distribuida para los operadores que no pudieron asistir a alguna de las sesiones.

Como tal no es un entrenamiento formal, sino una notificación del cambio que incluye los detalles de la nueva forma de trabajar, su objetivo es el de que los ingenieros se familiaricen con el nuevo modelo de categorización y atención de los incidentes en base a sus severidades.

Se utilizó una presentación como guía del entrenamiento que incluía:

1. Antecedentes: Análisis de incidentes y severidades
2. Diagrama de flujo para la apertura y atención de casos
3. Descripción de diagrama de flujo
4. Definición de severidades
5. Consideraciones adicionales
6. Sección para Preguntas y Respuestas

Una sesión adicional fue impartida vía videoconferencia para los ingenieros HTTS de Cisco, contenía la misma información de la presentación guía impartida a nuestro cliente, y ésta también fue grabada para la posterior distribución con los demás integrantes del equipo.

Inicio del Nuevo Modelo de Atención de Incidentes

El 1 de noviembre de 2019 inició entonces el nuevo modelo de atención de servicios utilizando lo establecido en la estrategia de optimización de recursos.

Se estableció que semanalmente se revisaran los *service request* abiertos para analizar si ambos equipos estábamos siguiendo lo acordado en la estrategia. Se llevaría un control de *service requests* abiertos, indicando si la severidad con la que se había abierto el *service requests* fue la adecuada conforme a la definición de severidades y, si el equipo de Cisco estaba atendiendo los casos tal cual fue el compromiso. Estas llamadas serian agendadas de manera serial todos los lunes entre HTOMs de Cisco y los Supervisores de nuestro cliente.

Resultado de estas revisiones semanales se encontraron inconsistencias en la estrategia que fueron revisadas de manera puntual con los operadores que abrieron cada uno los *service requests,* las desviaciones encontradas se muestran en la tabla no. 1:

Concepto	Sem 1	Sem 2	Sem 3	Sem 4	Sem 5	Sem 6	Sem 7	Sem 8
Total *Service Requests*	16	17	24	17	17	23	37	30
SR con desviación	4	4	3	1	1	3	0	3
% Desviación	25%	24%	13%	6%	6%	13%	0%	10%

Tabla 4 Tabla semanal de desviaciones de creación de service requests

Definición del Alcance del Proceso Preventivo

Para iniciar con el alcance del proceso, tendríamos que estar todos de acuerdo en la definición de la palabra Preventivo y lo que esto implicaba, ya que en múltiples ocasiones nos escuchábamos llamando a las tareas que serian parte de este proceso como: proactivas, predictivas, preventivas, por lo que el primer paso fue definir exactamente para nosotros, Cisco y nuestro cliente qué es y qué no es proactivo.

Esta sesión se convirtió en un debate de opiniones, que incluso no pudimos concluir en la primera sesión de 1 hora que habíamos destinado incluso para arrancar con el alcance del proceso, pero que nos pareció a todos muy importante detenernos a exponer todos nuestros puntos de vista y llegar a un concepto que seria el que manejaríamos en adelante.
Teníamos todos muy claro la definición de reactivo y de ahí partimos, algunos opinábamos que la descripción debería estar basada en el impacto al servicio, por parte de nuestro clientela gran mayoría opinaba que debería basarse en el impacto a la infraestructura, lo cual para nosotros no era conveniente, puesto que el diseño y arquitectura de las soluciones estaba diseñada redundantemente de tal manera que si uno de los componentes principales falla, inmediatamente se activa el respaldo y acortamos el tiempo de interrupción de servicio ó incluso en muchas ocasiones puede evitarse. Nuestro cliente comentaba que justamente la redundancia era algo que les había costado a ellos y por ende no debíamos considerarlo de esa manera.

Luego teníamos todos un poco de confusión en la diferencia de una tarea preventiva y una proactiva, muchos coincidían en que eran palabras sinónimas, nos fuimos a buscar definiciones oficiales, tanto en el diccionario como en ITIL, y si bien no satisfacían del todo a los asistentes finalmente entre todos

fuimos construyendo las definiciones que hacían sentido a nuestro cliente y a Cisco, que si bien pueden no apegarse a criterios estandarizados, estas serian las definiciones que definirían las acciones o tareas del proceso preventivo que estábamos por construir. Los conceptos quedaron establecidos como siguen:

> **Proactivo**: tareas o acciones que previenen problemas antes de que ocurran basados en alertas, tendencias o umbrales, son tareas que se ejecutan para evitar interrupciones inesperadas. Que, si bien pudieron haberse presentado en la red, estas nos ayudarían a que no se volvieran a presentar en el futuro.
>
> **Predictivo**: incluye rutinas de inspección de procesos, bitácoras o umbrales que permitan detectar situaciones de alarma en la infraestructura. Serian catalogadas acciones predictivas todas aquellas que ayudarían a evitar el impacto de manera anticipada y que además nunca hayan sucedido o impactado en la red del cliente.
>
> **Preventivo**: Incluiría ambos conceptos, tareas proactivas y predictivas.

Teniendo claro el concepto principal del proceso, continuamos con el objetivo, el cual desde mi punto de vista lo teníamos mucho más claro que incluso las definiciones, y por ende fue mucho más fácil y rápido construirlo con la participación de los asistentes:

> "Minimizar el impacto a los servicios que se proporcionan en la red de nuestro cliente, mediante la identificación de riesgos y ejecución de acciones preventivas, así como la disminución de reincidencias por medio de acciones preventivas"

A partir de la implementación de la estrategia de optimización de recursos, sabríamos identificar perfectamente cuáles serían los *service requests* en los cuales se tendría impacto en los servicios, esto debido a la definición de severidades, la cual indicaba que solamente aquellos que tuvieran afectación en la disponibilidad, únicamente esos, serian identificados como severidad 1. Adicionalmente, todos aquellos que además fueran catalogados como servicios críticos, && ó &&&.

Otro de los temas objeto de debate fue decidir cuáles serían los incidentes que deberían desembocar en preventivos. En un principio nuestro cliente solicitó que todos los incidentes convertidos en Problema, los cuales buscan causa raíz, deberían también complementarse con un *service request* Preventivo, a lo cual Cisco confirmó que se trataba de un numero muy alto de incidentes, y que con seguridad no estábamos preparados para una carga de trabajo tan alta. Algunos opinaron que los incidentes con el mayor tiempo de impacto al servicio, unos otros consideraban que eran más importantes lo que hubieran

tenido el mayor número de servicios impactados y finalmente nuestro cliente accedió a que los incidentes severidad 1 y además que hubieran sido catalogados como && ó &&& serían esos los incidentes objeto de estudio, y que servirían como entradas a al Proceso Preventivo.

Platicamos también de manera general que cada uno de los incidentes tendría un tratamiento diferente, no podríamos establecer actividades específicas para cada uno de los *service request*s, ya que como sabemos, la afectación de servicios puede deberse a problemas de hardware, software, configuraciones, etc. Por lo que quedarían abiertas las técnicas y herramientas utilizadas en el proceso, definitivamente habría muchas que podrían coincidir y entre las más utilizadas serian: la identificación de nemónicos, umbrales, mensajes de error, etc.

Por ende, la salida del proceso sería también diferente de acuerdo con la herramienta ó técnica utilizada, pero coincidiría en que sería una recomendación para prevenir que ese tipo de incidente volviera a afectar de la misma manera la red de nuestro cliente en el futuro.

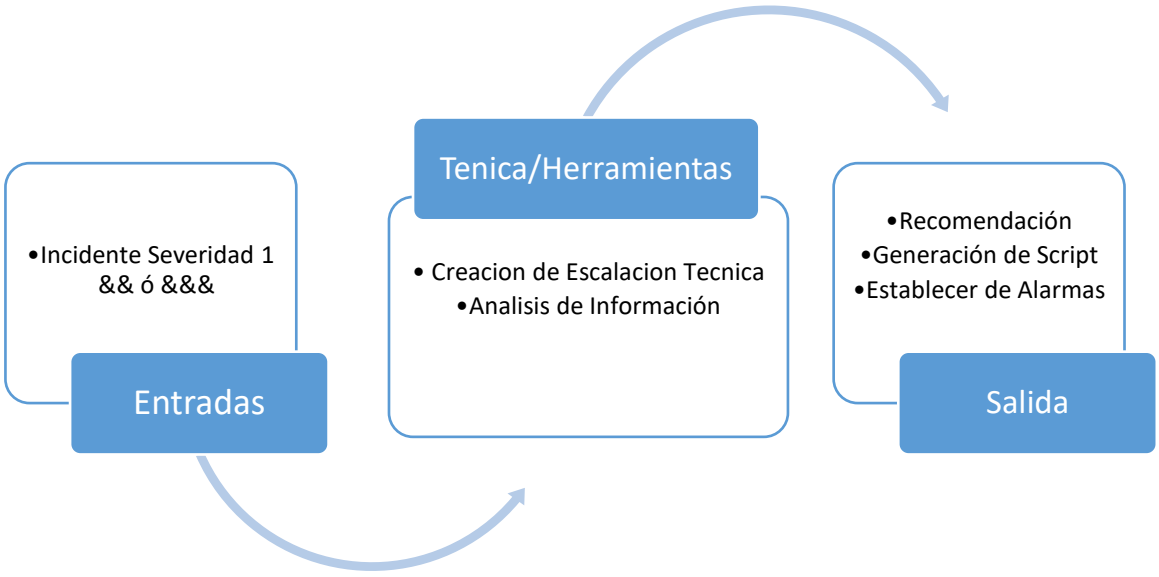


Figura 5 Entradas, Técnicas, Herramientas y Salidas del Proceso Preventivo

Se estableció el ejemplo del tablero de control con las métricas a presentarse de manera mensual:

Figura 6 Formato ejemplo del Tablero de Control mensual del Proceso Preventivo

Definición de las métricas en el tablero de control

Casos Creados

Se refiere al total de *service requests* creados en el mes de análisis, indicando también los *service requests* creados en el mes anterior, con la unica intención de tener una referencia historica.

Esta información es tomada directamente del sistema de gestion y registro de incidentes de Cisco, conciliado previamente con nuestro cliente.

Total de Casos Cerrados

Esta métrica indica *los service requests* cerrados en el mes de análisis, independientemente de su fecha de creación.

El reporte es obtenido por medio de la herramienta de gestion y registro de incidentes de Cisco, que ademas fue validado en conciliación semanal con nuestro cliente.

Clasificación del Output

Se definieron cuatro categorías para los *service requests* preventivos en base al valor que aporta el resultado del análisis.

1. Proactivo: Reduce Tiempo
2. Preventivo: Evita Impacto
3. Proactivo & Preventivo: cumple con ambas
4. No aplica: Aún no es posible determinar si el output es proactiva o preventiva

La métrica muestra el porcentaje de cada uno de los cuatro rubros tomando como universo total el número de *service requests* cerrados en el mes de análisis.

Número de Hits de Firma Preventiva con impacto

Número de veces que la firma preventiva fue invocada para casos con impacto

Número de Hits de Firma Preventiva sin impacto

Número de veces que la firma preventiva fue invocada para casos sin impacto

Número de Hits de Firma Proactiva

Número de veces que la firma proactiva fue invocada

Tiempo Promedio de implementación

Corresponde al tiempo transcurrido entre el cierre del *service request* y la implementación de la firma por parte de nuestro cliente.

Se consideran todos *service requests* cerrados en el mes de analisis, la fecha de cierre de cada uno de los *service requests* se toma directamente del sistema de gestion de incidentes y la implementación de la firma es un dato que se tiene que consultar con nuestro cliente.
Si bien esta métrica no corresponde a la evaluación misma de Cisco, el cliente solicitó verla en el tablero de control para tener la referencia en una sola vista.

Contribución Potencial de Reducción de Tiempo (Proactivo)

Porcentaje de Tiempo de Impacto reducido una vez que la firma es implementada.
Este es el KPI principal, y por el cual podriamos decir que se llevó a cabo todo el proceso, el haber encontrado este indicador fue uno de los puntos que hizo que el proceso haya sido exitoso. Justo es lo que el cliente buscaba desde hace mucho tiempo, tener las herramientas para poder identificar las acciones que reducirían el tiempo del impacto en los servicios, y ademas, medir la cantidad de tiempo que evitó que los servicios se vieran afectados por haber encontrado estas acciones que asegurarían que ese mismo incidente no afectaria mas en su red.

Contribución Potencial de Reducción de Impacto (Preventivo)

Porcentaje de Impacto al Servicio reducido una vez que la firma es implementada.

CSAT

Evaluación de la atención del *service request*, por medio de la encuesta de satisfacción que mide del 1 al 5 los siguientes rubros:

1. Evaluación general de la atención del *service request*
2. Facilidad de acceso a abrir el *service request*
3. Comunicación del estatus del incidente
4. Efectividad de la solución
5. Capacidad técnica del ingeniero que atendió el *service request*
6. Cortesía del ingeniero que atendió el *service request*

Número de Hits de Firma Proactiva
Número de veces que la firma proactiva fue invocada

Si bien, el *dashboard* que se presentaria de manera mensual teoricamente incluíria KPIs para medir el desempeño de Cisco en el proceso, el Director de nuestro cliente nos solicitó que se incluyeran tambien de manera visible ciertos KPIs para tener de primera mano y en una sola vista los indicadores que medirían tambien el desempeño del area Preventiva de nuestro cliente, en un principio Cisco no estuvo de acuerdo, dado que la revision mensual es para Evaluar a Cisco unicamente, el presentador es por parte de Cisco y hace poco sentido que Cisco presente cifras mensuales del desempeño de nuestro cliente. Finalmente serian números que estan fuera de nuestro alcance, tendrian que ser solicitados de manera mensual a nuestro cliente, no tendriamos absolutamente ninguna ingerencia incluso en el calculo de las mismas, pero despues de repetidas ocasiones en que esta solicitud fue realizada, Cisco accedió a incluir en nuestro *dashboard* metricas que dependian totalmente de nuestro cliente. Los KPIs de nuestro cliente que fueron agregados al *dashboard* son los siguientes:

Número de Hits de Firma Preventiva con impacto
Número de Hits de Firma Preventiva sin impacto
Número de Hits de Firma Proactiva
Tiempo Promedio de implementación

Se platicaron también las siguientes premisas que apoyarían al proceso:

- Los Casos Preventivos estarán basados únicamente en incidentes categorizados como && ó &&&.

- Previo a abrir un *service requests* Preventivo se debe de tener un Incidente y un Caso Problema. Se podrá abrir en paralelo al Problema dependiendo de las condiciones del impacto y del diagnóstico causa raíz.

- Se definirán las métricas (*KPIs*) para los Casos Preventivos. Ejemplo: Cantidad de casos preventivos abiertos y cerrados en el mes, Cantidad de reincidencias durante la elaboración de la firma, etc.

- Se definirán si las encuestas de satisfacción seguirán los mismos criterios que un Incidente ó Problema.

- Se llevará a cabo conciliación de *KPIs* todos los jueves. Por cuestiones de auditoria, es necesario realizar esta conciliación de tal manera que nos aseguremos que ambos equipos tenemos los mismos datos en nuestros sistemas.

- Se debe determinar si los Casos preventivos tendrán diferentes prioridades de acuerdo con el impacto y al PM relacionado.

- Definir la nomenclatura de los Casos Preventivos. Ejemplo:

  PREV/S3 | 6.4.2 | ASR9K | ipdsl - mexico10 | 0/0/CPU0 A9K-MOD80-SE state:BR

Presentación de Propuesta

Es costumbre en la operación que lleva Cisco con nuestro cliente, tener juntas presenciales o vía telefónica para exponer nuestras opiniones, lluvia de ideas y defender nuestros puntos de vista para convencer a todo el equipo cuál es la mejor definición, propuesta o procesos. Posteriormente en otra sesión presentamos, en limpio por así decirlo, solo las conclusiones a manera de reforzar los acuerdos, por lo que una vez discutido o expuesto toda la información referente al alcance, regresamos con nuestro cliente para presentar en un documento lo que quedaría establecido como el alcance del proceso preventivo. Ésta presentación incluyó lo siguiente:

1. Objetivo
2. Alcance
3. Ciclo Proceso Preventivo
4. Diagrama del Proceso
5. Premisas
6. Salidas del Ciclo de Prevención
7. Línea de tiempo para compromisos
8. Métricas – Tablero de Control

Inicio Proceso Preventivo

El 1 de diciembre 2019 arranca el proceso Preventivo, tuvimos una llamada corta para decidir cuál sería el primer caso Preventivo que se analizaría, el cual serviría de base para la identificación cómo se presentaría y la información que contendría.

Se acordó también la fecha de la revisión del primer caso preventivo y corroborar que formato y contenido serían los adecuados como entregables o salidas de cada uno de los *service requests*.

Revisión primer *Service Request* Preventivo

Se acordó que como salida de cada uno de los análisis que se llevaran a cabo se realizaría un documento tipo *power point* con la siguiente información:

- Resumen de la descripción del *service request*:
- Logs ó mensajes encontrados

- Alarma que detona la falla
- Condiciones donde se encuentra la falla
- Plan de Acción
- Comandos por capturar en caso de reincidencia

Durante la llamada para revisar este primer *service request* preventivo se pidió corregir y agregar información en la primera sección: "Resumen de la descripción del *service request*", tal como:

- Numero incidente del sistema de gestión de nuestro cliente
- Incluir un número de identificación de la recomendación
- El número de veces en que ese log ó alarma se había presentado antes de fallar

Ajustes y correcciones al *Service Request* Preventivo

Nos llevamos la tarea de incluir la información que nuestro cliente nos había solicitado durante la llamada de la revisión del primer *service request* preventivo, en la presentación formal y se envió vía correo electrónico a todos los equipos involucrados.

Transferencia de Conocimiento del Proceso de Prevención

Se llevó a cabo una sesión presencial en las instalaciones de nuestro cliente para explicar el Proceso de Prevención, tuvimos como guía un documento en *power point* que incluía los siguientes temas:

1. Ciclo de Prevención
2. Proceso Prevención
3. Tablero de Control
4. Definición de Métricas
5. CSAT

Teniendo como base el mismo documento, se llevó a cabo una sesión vía videoconferencia con los ingenieros HTTS de Cisco para notificar sobre este proceso y lo que implicaría la atención de estos por parte de su equipo.

Kick Off Proceso de Prevención

Durante la reunión de revisión trimestral con nuestro cliente, a la cual asisten por parte de Cisco: Equipo de Soporte, Equipo de Servicios Avanzados, Ventas y Gerentes de Servicio. Por parte de nuestro cliente: Director de Tecnologías de Información, Gerentes y Subgerentes de Operaciones, Compras, Logística, Implementaciones, Cambios y Configuraciones, se reservó un espacio para llevar a cabo la presentación ante todos los equipos y arrancar de manera formal la implementación del Proceso Preventivo. Fue presentado por uno de los Gerentes de operaciones y fue recibido y escuchado con mucha aceptación, había en la reunión muchos participantes algunos de ellos muy familiarizados con el proceso por pertenecer al área de operaciones y algunos otros como las áreas de logística, compras y configuraciones que si bien no tienen injerencia directa en el proceso aplaudieron también el esfuerzo realizado por ambos equipos en pro de la alta disponibilidad del servicio a los clientes.

2.6 Resumen de la documentación e información recabada.

Proceso Proactivo

En un principio el proceso lo habíamos llamado Proceso Proactivo, por lo que las primeras presentaciones podrán observarse con ese título, pero después de varias reuniones y de conciliar todas las definiciones relacionadas al tema, incluso consultando la documentación de ITIL, como se ve en la Figura No. 7, acordamos llamar el proceso oficialmente como Proceso Preventivo

Las figuras 4, 5, 6, 7 y 8 muestran la presentación en la que plasmamos las conclusiones de la reunión para establecer las definiciones, y en la cual se definió a alto nivel el proceso proactivo.

Figura 7 Portada de la presentación del Proceso Proactivo (llamado así en un inicio)

Para estar todos de acuerdo con las definiciones que estábamos tratando de conciliar ante los dos equipos, Cisco y nuestro cliente, deberíamos primero concordar con la naturaleza de los eventos, la figura no 5 nos ayudó para mostrar que cualquier evento de falla sucede en el T1= tiempo 1, por lo que todas esas acciones que se hicieran del T1 al T0= tiempo cero, serian todas aquellas en las que nos enfocaríamos en este proceso, todo aquello que podemos hacer antes de que la falla ocurra.

Todas las actividades o incluso eventos que ocurriesen del T1 al T2= tiempo dos, serian todas consideradas como acciones reactivas, es decir, que sucedieron después de algo que falló y que afectó ya sea los servicios productivos o incluso a la infraestructura.

Esta figura fue de gran apoyo para mentalizar a todos, y ubicarnos en todas aquellas situaciones, eventos o acciones en las que nos enfocaríamos, incluso sin tener todavía un nombre oficial.
Con esta imagen todos estuvimos de acuerdo en que nos enfocaríamos, para efectos de este proceso en todo lo que sucediera, o debería suceder desde T0 a T1.

Solo para tener el contexto de toda la figura 5, las acciones reactivas muestran flechas hacia nuestro cliente y Cisco, esto quiere decir que un evento reactivo puede ser identificado tanto por Cisco como por nuestro cliente. Actualmente Cisco cuenta con herramientas de monitoreo en la red de nuestro cliente que nos permiten detectar elementos con falla incluso antes de que el mismo cliente lo note.

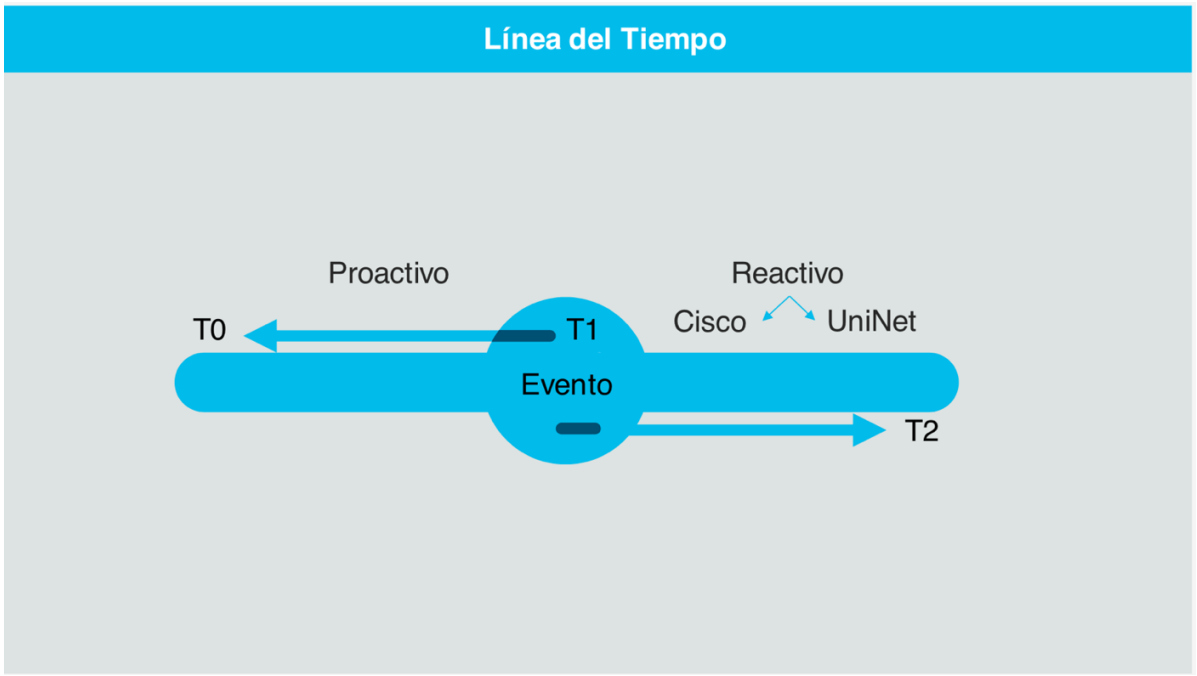


Figura 8 Línea del tiempo de un evento incidente

Todos teníamos en mente tres conceptos, si bien no estaban unificados para Cisco y nuestro cliente, incluso dentro de nuestros mismos equipos, todos sabíamos que trabajaríamos en actividades que ayudarían a prevenir que las fallas ocurrieran.

Preventivo, Proactivo y Predictivo son conceptos que pudieran ser sinónimos para algunas bibliografías, pero acordamos que estas definiciones serian específicas para las actividades que se llevarían a cabo en este proceso, lo importante era definir y estar claros en lo que para Cisco y nuestro cliente comprenderían estos conceptos.

Finalmente convenimos que las tareas preventivas incluirían acciones proactivas y predictivas. Desde este momento surgió la inquietud de cambiarle el nombre al proceso, y llamarlo Preventivo en lugar de Proactivo.

La razón por la que desde un inicio se llamó proactivo es porque dentro de la organización de nuestro cliente existe un área o departamento con ese nombre dedicado a todo aquello que pudiese evitar una falla. En esa reunión no fue oficial el cambio, pero todos nos llevamos esa inquietud en mente.

La figura no. 6 muestra también una separación muy importante basado en si hubo o no impacto en los servicios. Fue una de las discusiones que surgieron en varias ocasiones porque a nuestro cliente le hubiera gustado que se incluyera también la afectación a la infraestructura, finalmente pudimos convencerlos de que aun cuando es nuestro cliente quien decide por criticidad en que equipos invertir en redundancia, esa es justo su función, evitar que la infraestructura se vea afectada y por ende debíamos enfocarnos únicamente en lo que realmente ocasionaba un impacto al negocio, la inoperatividad de los servicios productivos corriendo en esa infraestructura.

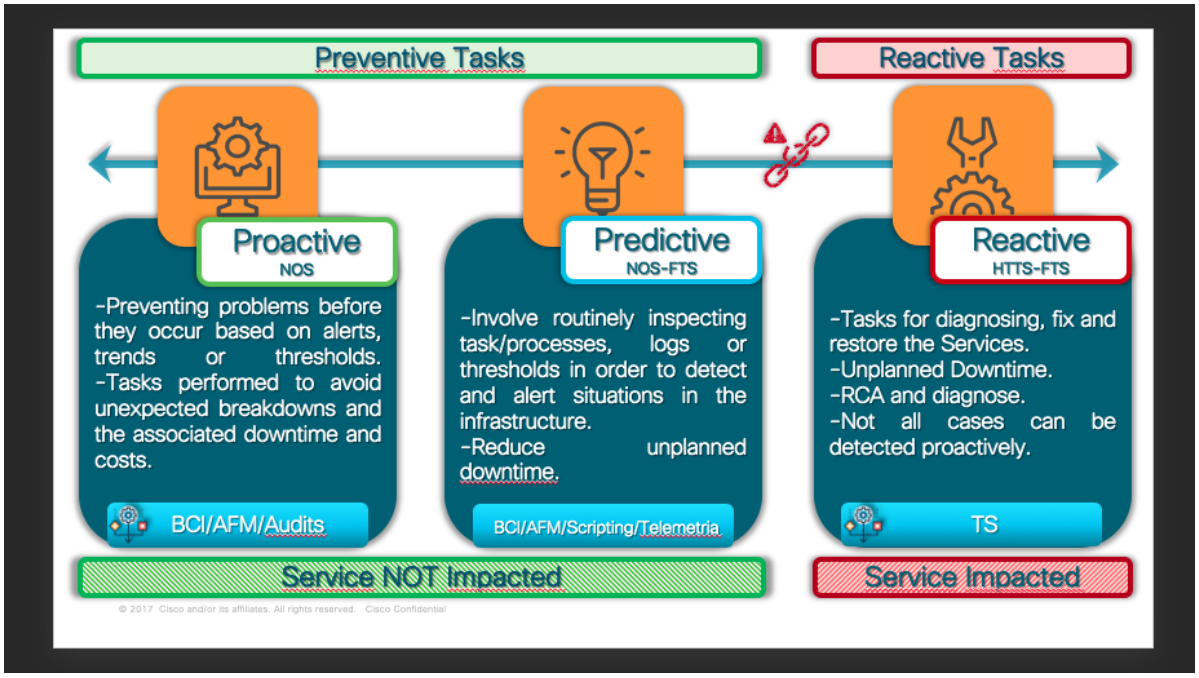


Figura 9 Definiciones de Proactivo, Preventivo, Predictivo y Reactivo

Solo como referencia, y para que todos tuviéramos la definición de “Proactivo” de un ente de mejores prácticas como ITIL, mostramos esta lamina representada por la figura no. 7.

Figura 10 Definición de Proactivo según ITIL

La figura no. 8 ilustra el proceso definido a alto nivel que se trabajó en el inicio, este fue el primer diagrama que se realizó para conceptualizar el proceso.

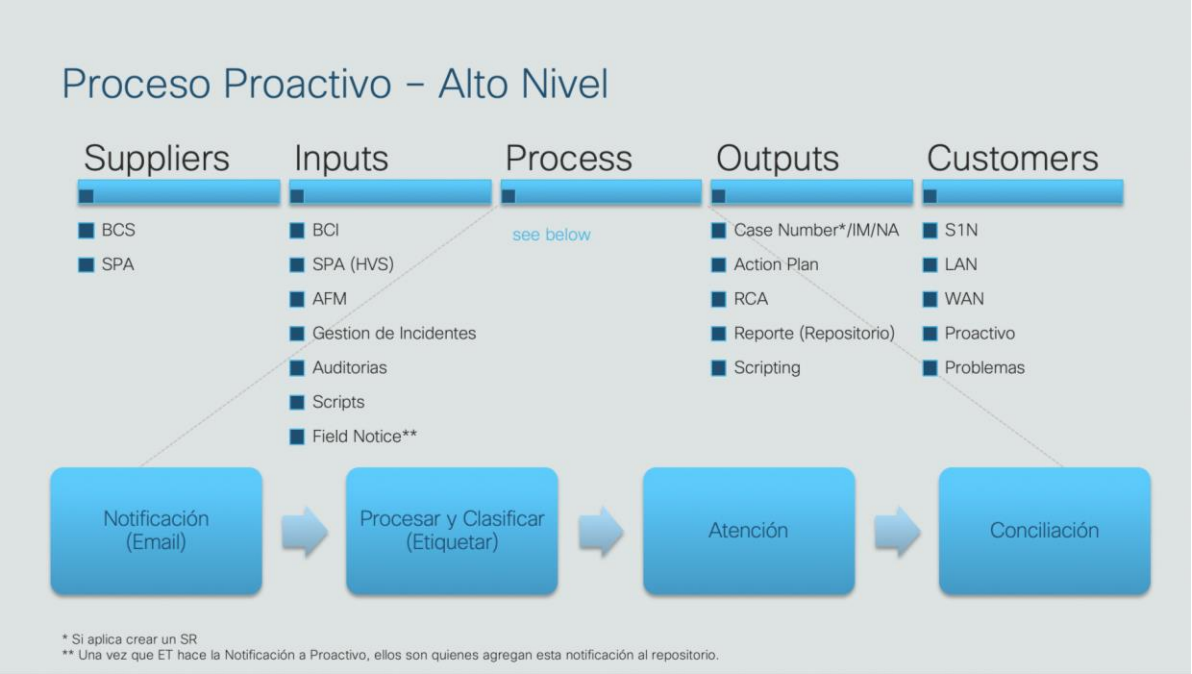


Figura 11 Proceso Proactivo a Alto Nivel

A continuación, la descripción del Proceso Proactivo a alto nivel:

Suppliers (Proveedores)

Corresponde a los equipos de trabajo de Cisco que estarían ofreciendo los servicios proactivos, o por así decirlo, activando y ejecutando el Proceso Proactivo.

> *BCS: Business Critical Services*
>
> Equipo de trabajo de Cisco que tiene como responsabilidad ofrecer, recomendar, implementar los servicios profesionales de Cisco.
>
> *SPA: Service Provider Advisors*
>
> Equipo de trabajo de Cisco encargado de soportar el contrato de servicios celebrado con nuestro cliente.

Inputs (Entradas)

Enlista una serie de entradas al proceso, los cuales serian los disparadores para iniciar con el Proceso Proactivo:

BCI

Son las iniciales para *Business Critical Insights*, el cual es una solución de Cisco que proporciona datos en tiempo real del performance de la red de los clientes, que por medio de tableros de control configurables por el cliente puede proporcionar datos de logs, alarmas, alertas arrojados por los equipos. Por lo tanto, esta herramienta sería uno de los principales protagonistas a generar entradas al proceso, dado que estaría aportando mucha información para ser analizada y en caso de aplicar convertirla en poderosa información para evitar impacto a los servicios en un futuro.

SPA

Significa *Service Provider Advisors*, se trata del equipo de trabajo que da soporte a los incidentes de nuestro cliente, y, por ende, otro de los protagonistas para generar entradas a este proceso. Al ser este el equipo que soluciona problemas en la red de nuestro cliente y quien se entera de primera mano de las fallas en los equipos, serian los encargados de buscar esos mismos errores en el resto de los dispositivos para evitar el punto de falla.

AFM

Es otra de las herramientas estrella de Cisco, *Automatic Fault Management*, es un software que cuenta con una base de datos de errores conocidos, y que en el momento en el que estos son detectaos en la red de los clientes, se conecta directamente con la herramienta de administración de incidentes en Cisco para abrir un *service request* de manera automática y que sin la intervención o interacción inicial con el cliente se inicie la investigación de la falla.

Gestión de Incidentes

Es el equipo de operadores que atiende los incidentes por el lado del cliente puede también generar importantes aportaciones al proceso, dado que son ellos quienes manejan los equipos y mantienen el monitoreo 7x24. Ante cualquier error que consideren importante puede ser analizado a profundidad al pasar por el Proceso Preventivo.

Auditorias

El cliente internamente realiza auditorias en su red, incluso es un área dentro de su organización, y de igual manera pudieran someter a análisis cualquier mensaje, error u otra información para ser analizada y pueda convertirse en salidas del Proceso Preventivo.

Scripts

Los scripts son desarrollos de software creados internamente por nuestro cliente para el monitoreo de ciertas variables, alertas, equipos que por limitaciones de las otras aplicaciones usadas para este fin quedan fuera, por lo que el resultado de correr estos scripts pudiera también ser parte de las entradas que alimenten el Proceso Preventivo

Field Notices

Son notificaciones que Cisco publica por problemas importantes, problemas relacionados con la vulnerabilidad de seguridad, que involucran directamente a los productos de Cisco y que generalmente requieren una actualización, solución u otra acción del cliente.

Process (Proceso)

El proceso como tal, a alto nivel, se encargaría de notificar una posible falla, procesarla, clasificarla, atenderla y finalmente conciliarla. Que queremos decir con esto:

Notificación

Todas las entradas deberán ser notificadas vía correo electrónico al equipo de Cisco y a nuestro cliente, pueden venir cualquiera de las herramientas o equipos de trabajo listados en las entradas.

Procesar y Clasificar

Una vez recibida la notificación, el equipo de incidentes nuestro cliente deberá realizar una primera revisión para determinar si la alerta, mensaje, error, variable deberá atenderse inmediatamente dentro del equipo de gestión de incidentes quienes trabajan 7x24 o si la deja pasar al área de Proactivo para que sea analizada con detenimiento.

Atención

Dependiendo de la notificación y del equipo que atienda la alerta, deberá atenderla conforme lo requiera la falla, ya sea programar un reemplazo de hardware, escalar al área de desarrollo, realizar una investigación mas a fondo, etc. según convenga.

Conciliación

La conciliación no es nada mas que asegurarnos ambos equipos de que tenemos registrados los mismos tiempos, los mismos códigos de cierre de los *service requests*, que la atención haya sido la adecuada y que estamos de acuerdo con que el incidente ya fue solucionado.

Outputs (Salidas)

Case Number (Número de Caso)

El grupo de Gestión de Incidentes, en específico el área de soporte primer nivel, encargado de procesar y clasificar la notificación, si decide que será un incidente que requiere acción inmediata, abrirá un caso en su sistema para dar seguimiento con Cisco, por lo que tendremos como salida un numero de caso o un numero de *service request*, pudiera decidir que la notificación ya fue procesada o que no la consideran de importancia como para iniciar una investigación, en esos casos nos regresarán un NA: No aplica.

Action Plan (Plan de Trabajo)

Dependiendo de la notificación, podría necesitarse la investigación de los mensajes, y pudiera ser que resulten acciones a ejecutar, estas acciones o tareas a realizar estarían detalladas en un plan de trabajo.

RCA *(Root Cause Analisis,* Analisis de Causa Raíz*)*

En algunas ocasiones es necesario llegar hasta la causa raíz de alguna falla, normalmente se llevan a cabo investigaciones mas profundas, escalaciones al área de desarrollo para tener como resultado la causa que originó la falla.

Reporte

Se estableció que todas las notificaciones serían registradas en un reporte que estaría en un repositorio de fácil acceso para ambos equipos. Este reporte contendría todos los campos que nos ayudarían a dar seguimiento a las notificaciones.

Scripting

Acordamos que una más de las salidas de este proceso seria la elaboración de scripts que monitorearan ciertas variables y que al llegar a cierto umbral predeterminado, pudiéramos evitar alguna falla. La creación del script sería totalmente responsabilidad de nuestro cliente, Cisco podría apoyar con la determinación de los umbrales o la determinación de las variables a monitorear.

Customers (Clientes)

Los clientes de este proceso serian todos ellos áreas del cliente:

S1N: Soporte Primer Nivel, primera línea de soporte de nuestro cliente.

LAN: Local área *network*, área que atiende incidentes locales.

WAN: es la sigla de Wide Área Network para el área que atiende los incidentes de la red de área amplia de nuestro cliente.

Proactivo: área de nuestro cliente que atiende todo lo que pueda prevenir fallas en el futuro.

Problemas: Área de Gestión de problemas, que acorde a ITIL busca la causa raíz de los incidentes.

Estrategia de Optimización

Las siguientes figuras, de la 9 a la 13, forman parte de la presentación de la Estrategia de Optimización de Recursos, en la cual se presentó el análisis del histórico de como se han presentado los *service requests* durante el 2019.

Figura 12 Portada de la Presentación de la Estrategia de Optimización

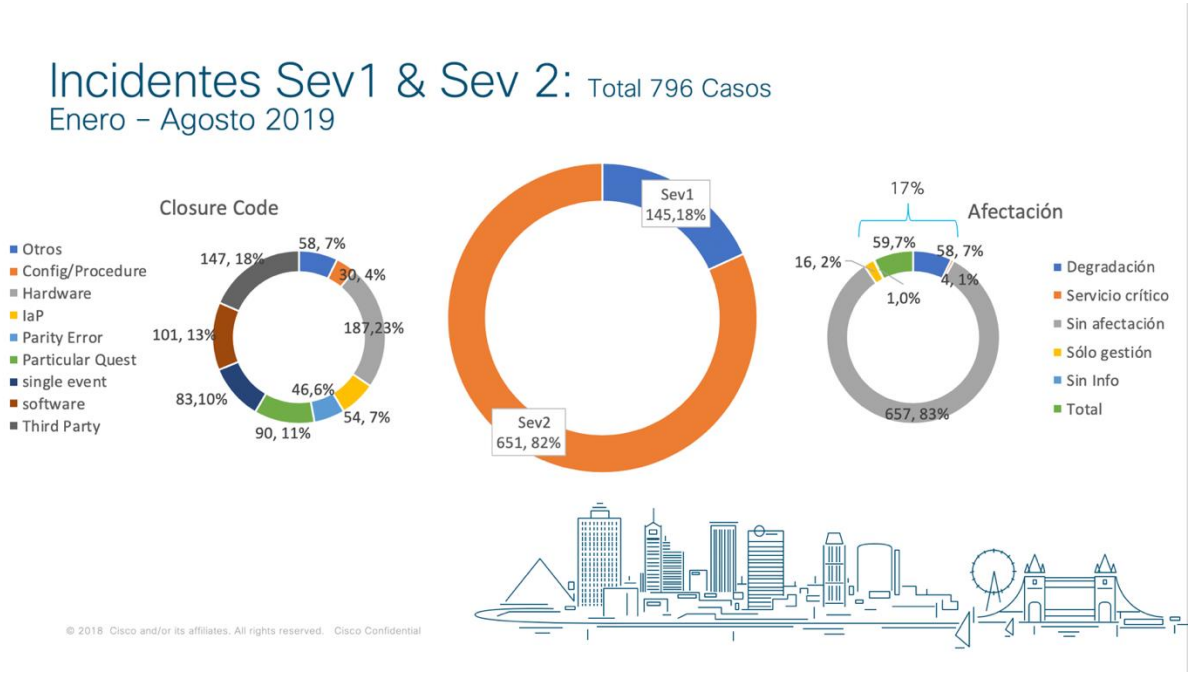


Figura 13 Análisis de los incidentes severidad 1 y severidad 2

El análisis se realizó contemplando los *service requests* reactivos desde enero a agosto 2019, para este análisis fueron descartados *service requests* de implementaciones y de actualizaciones al sistema operativo, que son básicamente actividades programadas basadas en un plan de trabajo establecido y en el cual la gran mayoría de las veces se dan en un ambiente controlado.

Se encontraron un total de 796 *service requests*, de los cuales el 18% (145) fueron severidad 1 y 651, es decir, el 82% fueron severidad 2.

En la grafica de la izquierda se muestra como fueron clasificados los 796 service request, basándonos en el código de cierre, esto es, en el resultado de la investigación. Encontramos que el mayor numero de incidentes, con 23%, corresponde a incidentes de hardware, seguido de 147 (18%) incidentes que fueron cerrados como *Third Party* (Terceros), es decir, que la falla no se encontraba en los equipos Cisco, si no en alguna otra parte de la red y el cliente desde el principio se lo atribuía a Cisco. Este fue un hallazgo muy importante, porque teóricamente el cliente debía realizar primero los componentes de la red para descartar fallas de su lado y si en efecto había un problema con los *routers* o *switches* de Cisco, entonces abrir un *service requests* con nosotros. Así pues, para optimizar recursos, este numero de casos de terceros seria un objetivo a minimizar por parte de nuestro cliente.

En tercer lugar, teníamos los defectos de software, con un 13%, rubro que difícilmente mejoraríamos, puesto que no depende en absoluto de los equipos involucrados en la prestación del servicio a nuestro cliente.

Posteriormente, ocupando el lugar numero cuatro con 11%, 90 Incidentes, cerrados como *Particular Question* (preguntas particulares), los cuales corresponden a *service requests* que el cliente abrió para preguntar sobre dudas ya sea de configuración o de funcionamiento de los equipos. Este rubro también sorprendió, porque hasta este análisis el cliente notó que estaba usando un servicio pensado en atender reactivos, para consultoría. Sobre este punto acordamos que monitorearíamos este tipo de casos de manera semestral para identificar posibles temas de entrenamiento hacia los operadores.

Estos 4 primeros lugares fueron los que consideramos debíamos enfocarnos, para minimizar la carga de trabajo y poder liberar recursos del equipo de Cisco que pudieran enfocarse en el lado preventivo. Posteriormente siguieron temas de errores de paridad, eventos únicos, configuraciones, procedimientos, etcétera con porcentajes mínimos.

En la grafica de la izquierda, se presentó el análisis de esos 796 casos basándonos en la afectación reportada de los servicios.

El 82% de los *service requests* se reportó sin afectación, y tomando en consideración que en este número se encuentran severidades 1 y severidades 2, el dato mismo no nos dice mucho, sobre todo basándonos específicamente en la definición de ITIL, en donde solo incidentes con servicios afectados debe considerarse como severidad 1.

Con 7% tenemos *service requests* con afectación, y tomando en cuenta lo anterior, debieron haber sido estos únicamente los incidentes abiertos como severidad 1. En esto trabajaríamos justamente con esta estrategia para que solamente aquellos incidentes donde los servicios se vean afectados sean registrados con alta severidad.

De igual manera con un 7%, tenemos servicios degradados, donde de nuevo, si no hay afectación estos deben considerarse severidad 2, un punto mas a considerar para monitorear dentro de nuestra estrategia.

Y en mínima representación, service requests con afectación en la gestión, service requests en los que no se registro información de la afectación, y servicios que por ser de clientes finales críticos para nuestro cliente se abrieron con severidad 1 o 2.

Como se puede observar, esta lámina da un panorama general, que ayudó a identificar aquellos incidentes en los que queríamos enfocarnos para reducir de manera significativa la carga de trabajo acumulada en la parte reactiva, ya que sin ser situaciones criticas se estaban evocando los recursos en *service requests* que pudieron seguir un proceso normal de investigación y resolución.

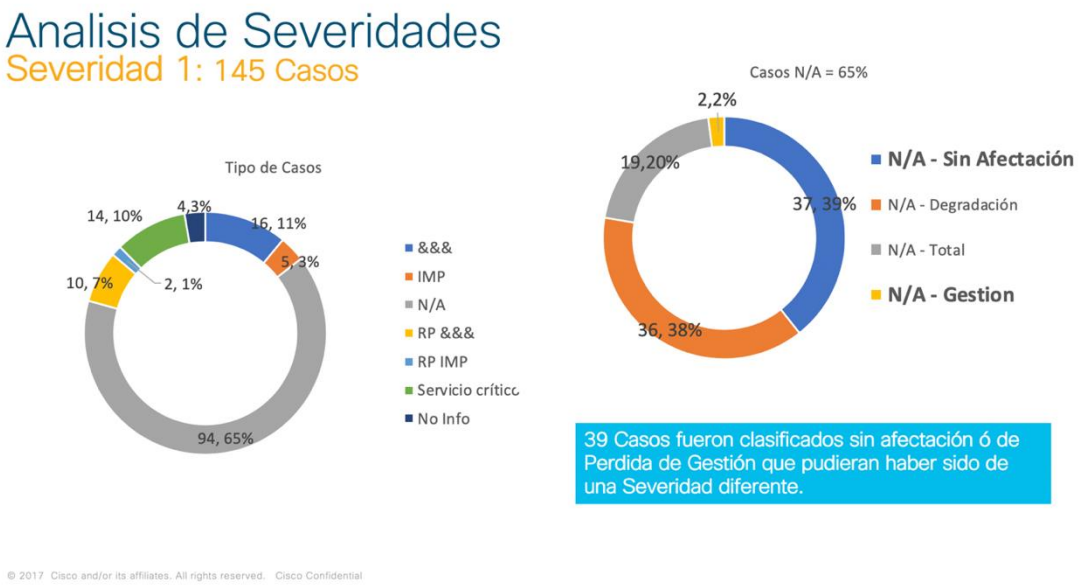


Figura 14 Detalle del análisis de severidades 1

En la figura 11, se mostró el análisis de las severidades 1 basados en afectación y en la clasificación de criticidad de los *service requests*. De los 796 *service requests* analizados, 145 casos fueron severidad 1.

En la grafica de la izquierda, se clasificaron por &&&, IMP (Importantes), RP &&& (Riesgo Potencial &&&), RP IMP (Riesgo Potencial Importante), Servicios críticos etc. Siendo todas éstas, etiquetas que nuestro cliente le agrega a cada uno de los incidentes para identificar la importancia y criticidad de las fallas.

Lo interesante de esto fue, que el 65% de los casos abiertos como severidad 1 no tenían esa clasificación de importancia, y aun así fueron abiertos como urgentes, sin serlo, y en los cuales los recursos de Cisco estuvieron enfocados a resolver la falla como si lo hubieran sido.

El mas alto grado de criticidad se lo da nuestro cliente a la etiqueta &&&, y si vemos en la grafica, solo el 11% de ellos lo fueron, posteriormente esta la etiqueta de IMP con un 3%, y nos seguimos con los riesgos potenciales que ocupan un 7% para los RP &&, y RP IMP con un 1%.

Y solo por ser un cliente critico para nuestro cliente, independientemente de la falla, nuestro cliente abrió el 10% de los casos severidad 1. En estos casos, nuestro cliente nos estaba trasladando un compromiso que tiene con sus clientes, no así, nada estipulado por parte de Cisco para atender a estos clientes con un alto grado de urgencia.

En la grafica de la derecha, se clasificaron los *service requests* severidad 1 de acuerdo con el impacto registrado. El 39% de los incidentes, no tuvo afectación de ningún tipo, por lo que con seguridad este numero de *service requests* debió haber sido abierto con una severidad menor, donde los incidentes siguen un proceso normal de investigación. Este número fue el mas evidente y mas fácil de identificar como incorrecto, y en los cuales estábamos seguros de que este tipo de incidentes debía eliminarse por completo una vez implementada la estrategia.

Con un porcentaje similar, 38%, se encontraron los incidentes con degradación en el servicio, en los cuales, siendo estrictos, tampoco debió haberse abierto como severidad 1.

Solo el 20% de los incidentes tuvo afectación, lo cual quiere decir, que solamente 19 de los 145 debió haber sido abierto como *service requests* severidad 1.

Estos fueron números reveladores que nos dejaron a todos muy claro, que en definitiva necesitábamos de manera urgente la correcta clasificación de los incidentes, de tal manera que pudiéramos enfocar los recursos en aquellos casos que realmente lo necesitaran.

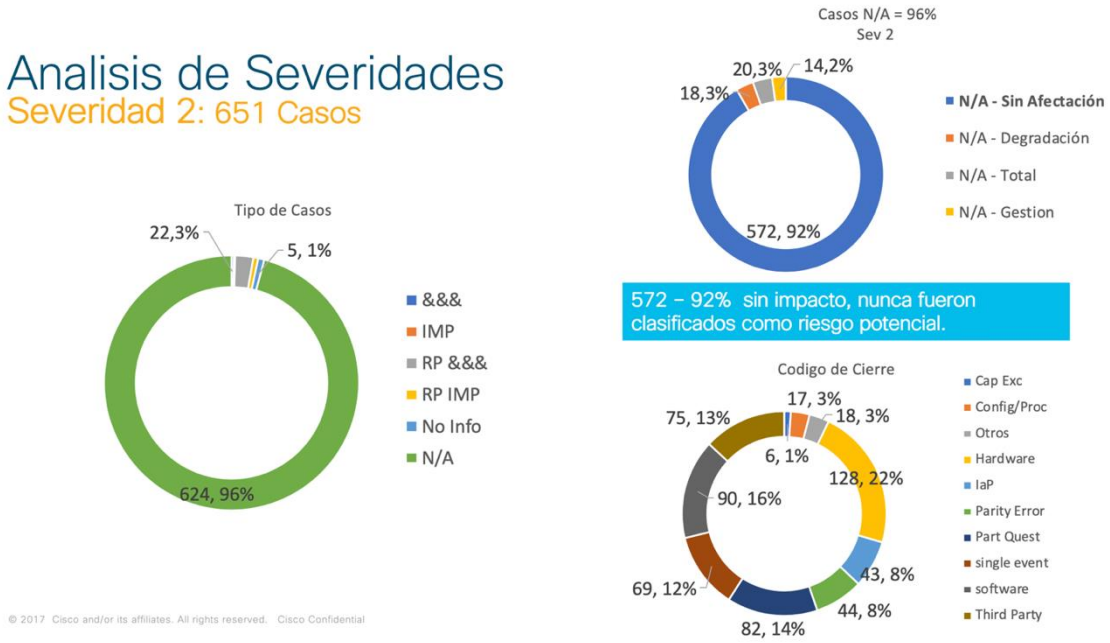


Figura 15 Detalle del análisis de severidades 2

La figura no. 12 muestra el análisis que se realizó a las severidades 2 de enero a agosto de 2019. Del lazo izquierdo en la grafica se puede observar que el 96% de los casos no tuvo ninguna clasificación de caso critico, esto quiere decir que el 4% de los casos, según las practicas que nuestro cliente venia realizando, estuvo mal clasificado a la hora de la creación del *service request* por tratarse de casos &&&, IMP o RP.

La grafica de la izquierda “Casos N/A= 96%”, representa el impacto a los servicios de ese universo de casos que no fueron críticos (624 casos). EL 92% no tuvo afectación, el 2% tuvo afectación en la gestión, y con un 3% de casos (20 casos) tuvo afectación total de los servicios, por lo que estos 20 casos debieron haberse creado con severidad 1 para atender el impacto generado. Un 3% mas fue de casos en los que los servicios presentaron degradación, es decir, si correspondía a *service requests* severidad 2.

De igual manera de lado izquierdo en la grafica de abajo, se encuentra la clasificación de los códigos con los que se cerraron los incidentes severidad 2. Coincidentemente con las Severidades 1 el mayor porcentaje se va a casos en los que fue necesario reemplazar algún componente físico con un 22%, seguido de SW con un16%. En tercer lugar, las preguntas particulares y en cuarto lugar los incidentes de terceros (Third Party) que como ya lo habíamos mencionado en la sección del análisis de las severidades 1, estos dos rubros, terceros y preguntas particulares, serian los incidentes con mayor potencial a ser minimizados si queríamos tener una optimización de recursos.

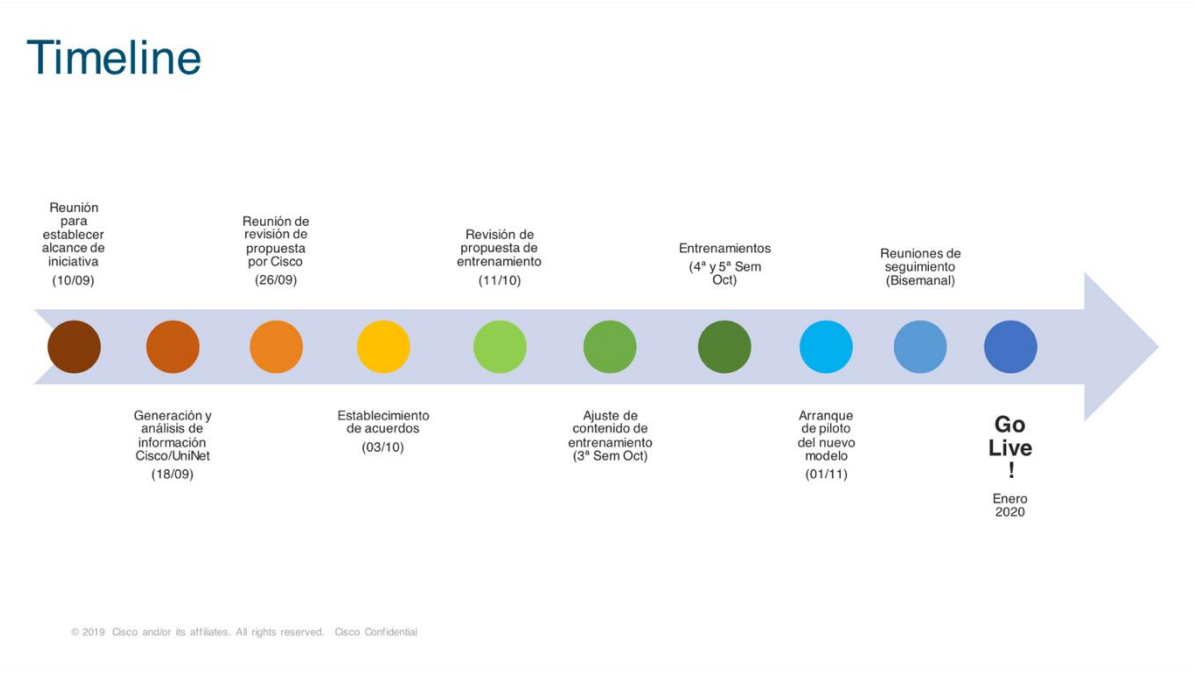


Figura 16 Línea del tiempo de actividades de la implementación de la Estrategia de Optimización

En la lámina dedicada a la línea del tiempo (*Timeline*) de la figura no. 13, presentamos simplemente la cronología en la que plasmamos tanto las fechas de las reuniones que ya habíamos tenido, como las que esperábamos tener para la implementación de esta estrategia.

Presentación de los *service requests* preventivos

La plantilla acordada la presentación de cada uno de los casos preventivos analizados, el ejemplo se ilustra de la figura 14 a la 18.

Figura 17 Formato de la portada de presentación de los SR Preventivos

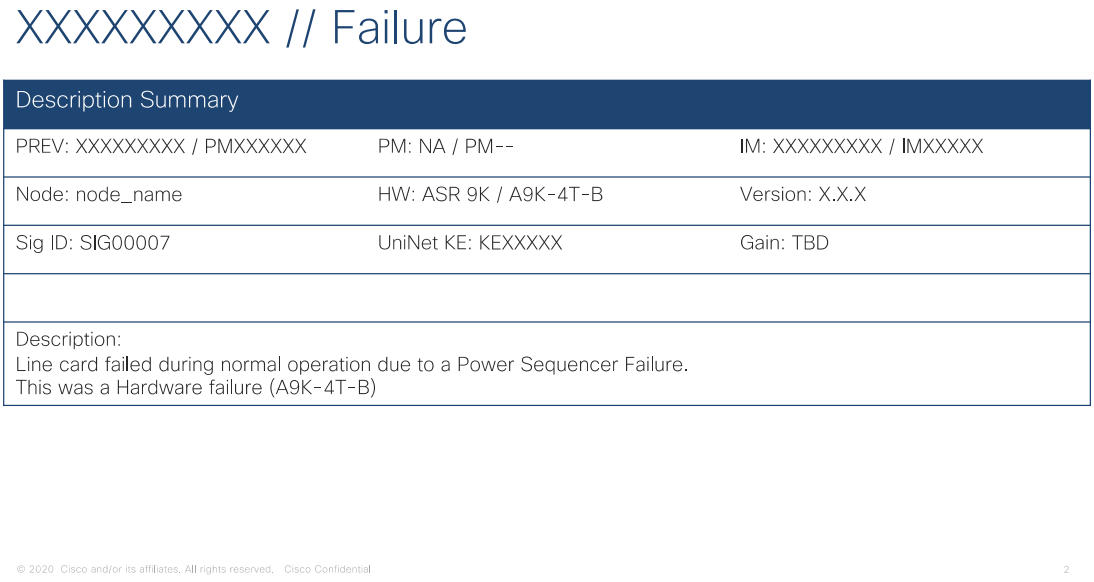


Figura 18 Formato de service request preventivos en la sección para la descripción de la falla

La primera sección de la presentación corresponde a una breve descripción de la falla, así como las características generales del equipo, como el nombre del nodo, la versión del sistema operativo, el modelo del equipo y los números de identificación del *service request* a explicar, tanto del sistema de Cisco (PREV XXXXXXX) como del sistema de registro de incidentes del cliente (PMXXXXX).

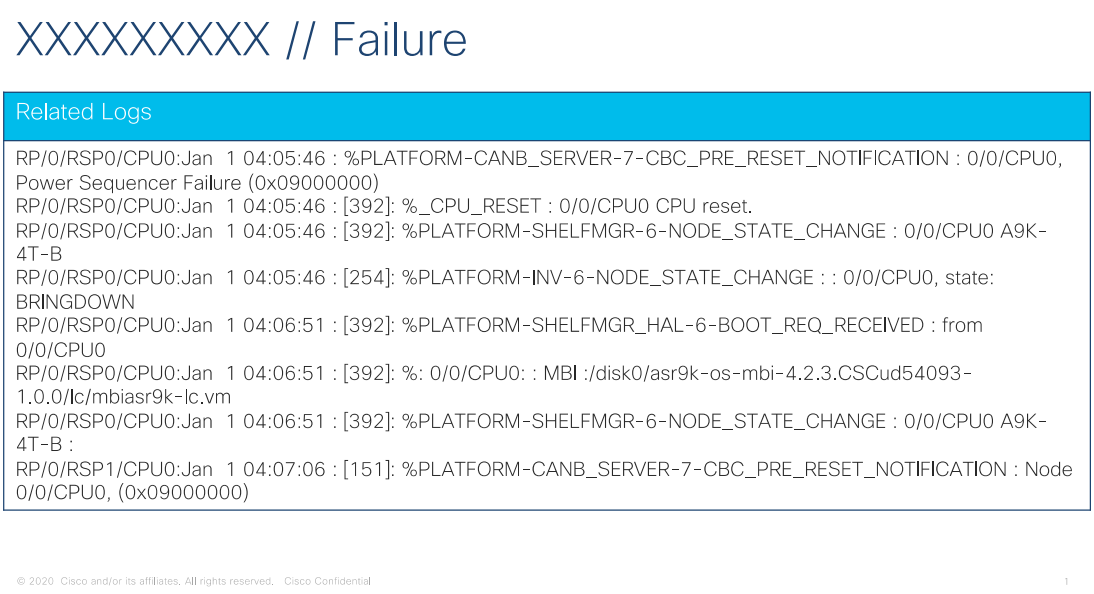


Figura 19 Formato de SR Preventivos en la sección de para los registros de la falla

En la diapositiva dos, representada en la figura no. 16, seria la sección dedicada a mostrar los registros de falla del sistema para su fácil identificación, durante la explicación del *service request*, esta sección toma relevancia para los operadores con perfil técnico, ya que seria el objetivo a identificar para la prevención de incidentes.

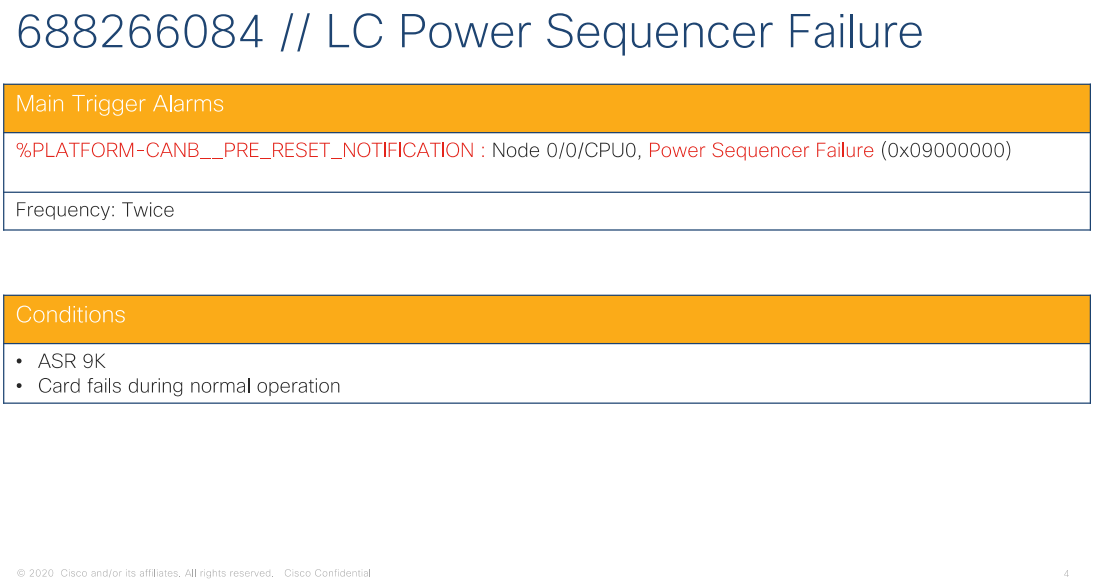


Figura 20 Formato de SR Preventivos en la sección para las alarmas que disparan la falla y las condiciones de falla

En la tercera diapositiva, figura no. 17, estaría la sección para indicar cual es la alarma que sería tomada como disparador de inicio de la falla, es el nemónico preciso que se tiene que buscar para alertar a los operadores de que un incidente está por aparecer.
La frecuencia se usa porque en alguno de los casos es necesario esperar a que este mensaje aparezca en mas de una ocasión para tomar acción.

En las condiciones se pondrían todos aquellos términos que se tendrían que cumplir acompañados del nemónico.

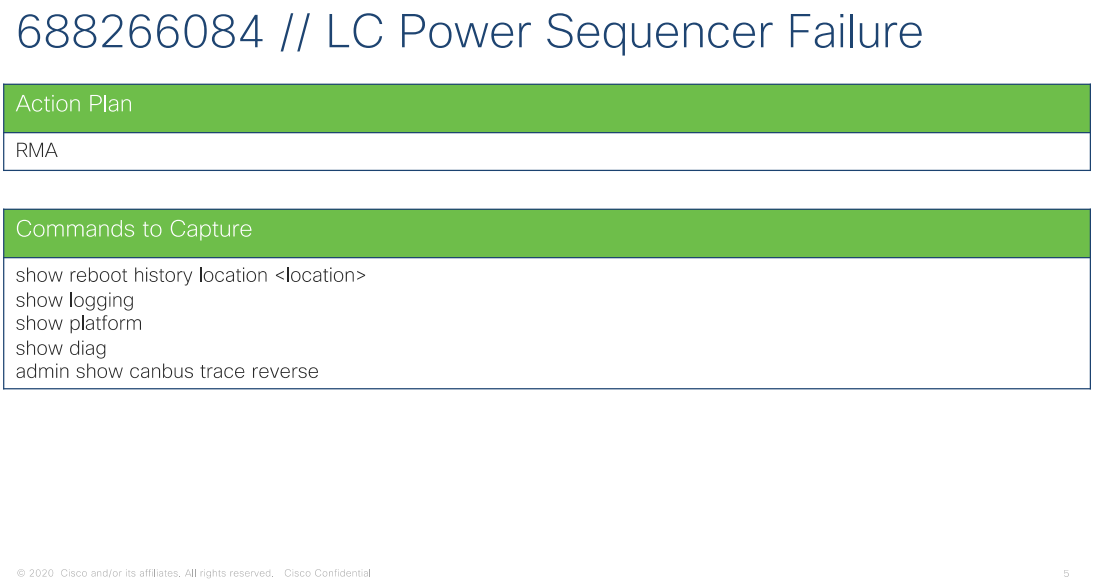


Figura 21 Formato de SR Preventivos en la sección para el plan de trabajo y los comandos a capturar

En la ultima lamina, figura 18, se incluiría el plan de acción a realizar, dependiendo de la salida generada, es decir, podría ser un plan proactivo, preventivo, proactivo y preventivo o pudiera no haberse encontrado algún plan de trabajo para alguna falla.

Finalmente una sección en la que se recomendaria la información a capturar para su analisis.

Por cuestiones de seguridad no podemos mostrar capturas de pantalla del sistema donde se registran los incidentes, ya que este esta catalogado como altamente confidencial.

2.7 Resultados obtenidos en el proyecto reportado

Uno de los grandes cambios en la manera de operar a partir de la implementación del Proceso de Prevención fue sin duda la mejora en la clasificación de los *service requests*. Si bien el cliente estaba acostumbrado a que todos sus incidentes los abría como críticos, y, por ende, Cisco activaba el proceso de Emergencia al incluir en la llamada a un ingeniero dedicado (HTTS), un ingeniero especialista (HTE) y un gerente de operaciones (HTOM) para atenderlos siempre con urgencia, la verdad es que cuando todo es urgente en realidad nada lo es.

Gracias al proceso de Prevención logramos que las severidades los *service requests* estuvieran perfectamente delimitadas, para Cisco, esto es un gran logro, porque además de seguir las mejores practicas de ITIL, los recursos están realmente enfocados en aquellos *service requests* que en realidad lo ameritan, en aquellos en los que realmente son críticos y requieren las tres figuras enfocadas en la atención de la falla. En el equipo se percibía un cierto grado de frustración al estar atendiendo fallas mínimas por medio de un proceso robusto como lo era el proceso de emergencia, y esto también ya fue eliminado, porque ahora sabemos que, si un *service request* severidad 1 es creado, en realidad hay algo critico que atender.

Adicionalmente, se acordó que las tres figuras de soporte al cliente, HTTS, HTE y HTOM atenderían únicamente las severidades 1, las severidades 2, 3 y 4 serían atendidas únicamente por el equipo de HTTS, por lo que al no estar involucrados todos los elementos, se eliminaron también de las métricas. Cisco estaría siempre abierto para cualquier situación que requiera atención para las severidades menores.

Para nuestra sorpresa, el cliente vio con muy buenos ojos la estrategia de optimización de recursos, que como mencionamos con anterioridad esta fue implementada inmediatamente después de ser presentada.

Ahora bien, si por un lado el cliente estaba cediendo en segregar la atención que hasta el momento siempre había tenido para *service requests* reactivos, de ahora en adelante en *service requests* Preventivos. Si bien es cierto, que parecería que perdía estos beneficios, en realidad estábamos enfocando parte del equipo en disminuir las incidencias a largo plazo, por que al trabajar de manera preventiva evitamos impacto en los servicios de sus clientes finales y por ende evitamos s*ervice requests* severidad 1, por lo que ambos equipos nos vemos beneficiados.

Para el cliente fue muy provechoso también que en Cisco existiera ahora un área como contraparte, esto porque nuestro cliente ya contaba con un área para trabajar con los temas proactivos y en adelante

trabajaríamos en conjunto, teniendo como su aliado a Cisco como proveedor y con esto, toda la experiencia de Cisco, históricos, apoyo de ingenieros, acceso a la información de Cisco, etc.

Uno más de los beneficios del Proceso de Prevención fueron los dos entregables que resultaron del proceso, que ayudarían a registrar, medir y dar seguimiento a todas las acciones preventivas que se generarían a partir de la activación del proceso de prevención:

1. *Dashboard* mensual con el calculo de los indicadores acumulados en el mes a revisar, con el cual podemos ver en una sola vista el estado del proceso, y por ende el impacto que se logró evitar a la red del cliente en el mes en cuestión.

El *dashboard* presentado en Enero se muestra en la figura 22.

Figura 22 Dashboard del Proceso de Prevención presentado en el MBR de Enero

El *dashboard* presentado en Febrero se muestra en la figura 23.

Figura 23 Dashboard del Proceso de Prevención presentado en el MBR de Febrero

2. Cada uno de los incidentes preventivos es analizado con detenimiento, escalado técnicamente si fuera necesario, posteriormente es presentado al equipo del área Preventiva del cliente para entender perfectamente la falla reportada, la solución que se dio en el momento para restaurar los servicios en el menor tiempo posible, la causa raíz en un *service request* tipo problema, y finalmente, identificar en un *service request* preventivo el plan de acción para que este sea a detectado a tiempo, antes de que los servicios se vean afectados.

   El cliente aprecia mucho el tiempo que Cisco emplea no solamente en el análisis, si no en las sesiones en las que se explica cada uno de los *service requests* preventivos, ya que de esta sesión depende el tratamiento que internamente nuestro cliente le dará a esta recomendación, el tipo de implementación que necesita realizar y los recursos que empleará para que esta sea una medida aplicada en toda su red.

Capítulo III. Conclusiones

3.1 Lecciones aprendidas

Se ha mencionado anteriormente que en las conversaciones del cliente estaban los temas proactivos y preventivos desde algunos años atrás, se había quedado ahí siempre, solo en conversaciones. Por parte de Cisco estaba el tema de no estar incluido en el contrato, y si bien profesamos que debemos escuchar al cliente e incluso interpretar lo que no se dice, en este tema simplemente no habíamos avanzado por temor a que el cliente exigiera compromisos que no habían sido firmados en un contrato.
Siento que dejamos pasar mucho tiempo en sentarnos con el cliente y negociar, efectivamente, es otro proceso, otra forma de operar, en efecto, no estaba vendido, pero pudimos haberlo escuchado antes, ver la manera en cómo si se pueden hacer las cosas, por que al final de cuentas el hecho de que trabajemos proactivamente en la red del cliente nos evita también a nosotros incidentes con impacto y con esto, todo el estrés, escalaciones, tiempo y recursos invertidos en investigaciones, pruebas de laboratorio, quejas, largas llamadas telefónicas y por parte del cliente interrupciones en servicios de telefonía e internet que le generan penalizaciones financieras.

En esta ocasión, cuando el tema se volvió realmente serio, nos sirvió mucho que nos preparamos, tuvimos una serie de reuniones internas, donde revisamos una y otra vez lo que era importante para nosotros, en todo aquello que no podríamos aceptar, es decir, que se sumará este nuevo proceso a la operación que ya teníamos, y en aquello que, si íbamos a integrar un nuevo proceso en nuestra operación, tendríamos que dejar de hacer, como por ejemplo: incrementar el KPI para la entrega del diagnóstico de 3 – 6 hrs, o eliminar por completo el seguimiento por parte de los HTEs y HTOMs en todas las severidades 3, entre otras. Porque de algo si estábamos seguros, con los recursos que contábamos actualmente nos resultaba imposible operar ambos procesos.

Trabajando en equipo surgieron muchas ideas, teníamos por así decirlo: Plan A y Plan B, en donde el plan A seria lo ideal, desde el inicio solicitaríamos todo aquello que seria lo mejor para nosotros poder integrar a la operación todas las actividades preventivas que habíamos escuchado al cliente decir que requería integrar. Y como plan B, todo aquello que como mínimo necesitaríamos para operar reactiva y proactivamente. Realmente estuvimos preparados para lo que nosotros consideramos todos los posibles escenarios, y la estrategia de todas las reuniones con el cliente fue ir a escuchar, no decidir en el momento con ellos, sino reunirnos para ver todas las posibilidades internamente y luego regresar con una respuesta. Definitivamente creo que ayudó mucho a no precipitarnos y tomar decisiones presionados por el cliente.

Debo confesar que la propuesta de sacar de las métricas las severidades 2 fue algo que jamás pensé que el cliente aceptaría, de hecho, desde mi punto de vista yo ni siquiera me hubiera atrevido a ponerlo sobre la mesa. Todo el tiempo pensé que como estaban acostumbrados a que las severidades 2 se trataban también como urgentes, en los cuales el compromiso para entregar el diagnóstico era de 3 horas, no dejarían este beneficio tan fácilmente. Definitivamente este fue un punto crucial para lograr que las cosas sucedieran, el proponer una nueva forma de trabajar para dedicarle el tiempo al tema preventivo, aun pensando que el cliente no aceptaría, nos preparamos para ello y lo logramos todos como equipo, mencionamos que no dejaríamos de lado las severidades dos por completo, que estaríamos ahí para cualquier severidad dos que ellos consideraran de importancia, que nos involucraríamos sin cuestionarlos cuando ellos escalaran algún punto relacionado con estos incidentes y que estaríamos monitoreando los diagnósticos realizados por los ingenieros HTTS, para que no se salieran de control. Comentamos también que si queríamos tener los recursos para enfocarnos en el lado preventivo necesitábamos hacer el tiempo y el espacio para llevarlo a cabo y fue así como logramos que el cliente aceptara esta propuesta.

Un sentimiento muy frecuente de las áreas operacionales es que las áreas de ventas dicen que si a todos los requerimientos del cliente con tal de asegurar las renovaciones del contrato y que el cliente permanezca el mayor tiempo posible con un proveedor. Me ha tocado en muchas ocasiones ver cómo desde el lado de ventas se aprueban solicitudes del cliente sin que estas sean consultadas con el área de operación y éstas simplemente no cubren la expectativa de cliente porque se aceptaron para quedar satistechos en una negociación sin haber considerado todas las aristas, algunas veces ni siquiera es viable. Por lo que este fue otro de los puntos cruciales para que esto se llevara a cabo, que en esta ocasión, nos dejaron como área operativa tomar la decisión, y fue muy gratificante, porque nosotros que seriamos los que operaríamos ese contrato sabíamos de primera mano qué tanto más trabajo podíamos aceptar.

Al ser nosotros quienes decidimos totalmente sobre la integración de este nuevo proceso a la operación nos olvidamos un poco de la parte legal. Una vez que los acuerdos fueron establecidos con el cliente, regresamos con los ejecutivos de cuenta de Cisco a cargo de nuestro cliente a presentarles nuestro proyecto y les gustó, nos felicitaron por haber tenido una negociación exitosa al dejar algunos compromisos para adquirir unos nuevos, y no solamente que se agregaran nuevos procesos saturando a los recursos limitados con los que contaba el equipo, pero además surgió un comentario muy valido de uno de los ejecutivos, nos expresaba que prácticamente al proveer todas las acciones preventivas para evitar fallas, pudiéramos estar revelando experiencia profesional de Cisco, así como información confidencial que en un mundo ideal nos llevaría a desaparecer las fallas en la red del cliente y por ende el cliente pudiera pensar que ya no necesita un contrato con Cisco. Si bien, sabemos que la tecnología no

para, tenemos nuevos modelos cada año, siempre hay mejoras en los equipos, tanto en hardware como actualizaciones de software, diferentes diseños en la red que cambian por completo los flujos de información. Nos habíamos olvidado por completo de revisar la parte de los derechos de la información que podíamos o no revelar al cliente. Nos dimos a la tarea de consultar los estatutos legales de lo que estaba permitido compartir con los clientes, en nuestro caso se trataba de realizar investigaciones para anticiparnos a las fallas y no había problema con ello, salimos bien librados, pero definitivamente aprendimos la lección de considerar no solo la parte operativa y financiera, si no también la legal.

Durante nuestras revisiones para presentar una propuesta del proyecto, intentamos acercarnos al área de BCI directamente, el área de Cisco que administra esta herramienta y no tuvimos la respuesta que esperábamos. Considerábamos a BCI una de las entradas principales al proceso de prevención, tratamos de exponer nuestro punto para integrarlos a nuestro proceso, tal vez no supimos expresar la importancia y lo mucho que se beneficiaría el cliente al integrarnos para que todas las salidas de BCI se consideraran dentro del proceso de prevención, pero debido a la carga de trabajo de los integrantes del equipo no fue posible que nos integráramos de manera transparente, lo interesante fue que logramos cruzar algunas actividades que aportarían gran valor al proceso de prevención.

3.2 Propuesta de mejora

En la parte financiera, el Proceso de Prevención definitivamente tendrá que ser incluido en la próxima renovación de contrato, y muy seguramente nos tocará apoyar el costeo del proceso. Lo ideal sería que todos los integrantes del equipo que nos vemos involucrados en ambos procesos empecemos a registrar los tiempos que le dedicamos a cada uno de los procesos, para que cuando llegue el momento podamos tener por lo menos una idea de la utilización de los recursos y sea mucho más fácil poderle poner un precio.

Como he mencionado con anterioridad, la integración total de las herramientas BCI & AFM, definitivamente forman parte de las mejoras que podemos realizar al proceso, ya que al analizar todas las alertas que BCI arroja, podríamos generar valor de manera automática y a su vez, integrando todas las salidas del proceso en AFM, podríamos cerrar completamente el proceso utilizando en todo momento herramientas de Cisco. Las platicas con los equipos de estas herramientas aun continúan y si bien no pudieron ser integradas del todo en esta primera fase muy seguramente conseguiremos el patrocinio para que lo llevemos a cabo en las siguientes etapas, conforme vaya madurando este proceso.

De manera personal, aun sigo analizando la idea de tener un equipo separado del equipo reactivo, recursos dedicados a toda la parte preventiva, o por lo menos organizados de diferente manera. Actualmente hay un ingeniero dedicado al proceso de prevención, que es un hibrido entre un HTOM y un HTE, y el resto del equipo de HTEs apoya cuando este ingeniero necesita ayuda con los análisis de los *service requests*. Mi idea es que pudiéramos tener un equipo de ingenieros en el lado preventivo y que estos apoyen al reactivo cuando fuera necesario. Siento que es más fácil que de lo preventivo se puedan pasar al reactivo, ya que lo preventivo puede esperar, lo reactivo no.

Aunque en un principio nos faltó delimitar perfectamente las responsabilidades del cada uno en el equipo en relación al proceso, la realidad es que somos un equipo muy dinámico y abierto, que en el momento que sea necesario un cambio, que veamos que no funciona la manera en como estamos organizados al día de hoy, nos reunimos y hacemos los cambios que sean necesarios, en verdad somos un equipo en el que todos sumamos y aportamos en pro de la operación.

En cuanto al número de *service requests* analizados mensualmente por medio del proceso de prevención creo que deberíamos ponerle un límite, tal vez este número deberá concordar con el precio, porque el número pudiera variar muchísimo, actualmente está supeditado al número de *service requests* al mes clasificado como &&&. Un mes pudiéramos no tener ninguno o tener 20, creo que eso lo hace complicado, otra opción pudiera ser que se analizaran solo aquellos en los que se requiere el análisis de

causa raíz. Para este punto tendremos que esperar el comportamiento en los próximos meses, y si es necesario revisarlo para llegar a nuevos acuerdos.

Podríamos revisar también cuáles son los *service requests* que sin ser críticos e importantes tienen la mayor reincidencia, o incluso cuáles son relativamente sencillos de resolver pero que nos toman mucho tiempo de diagnóstico, de tal manera que se hiciera un plan genérico que el cliente pueda aplicar proactivamente.

Necesitamos también encontrar la manera de asegurarnos de que los planes preventivos que resultan de la salida de este proceso, están siendo utilizados y debemos estar seguros de que estos aportan el valor para el que fueron propuestos, podríamos estar proponiendo en un futuro alguna métrica que mida la reincidencia de una falla para la cual ya se proporcionó un plan y que las acciones preventivas no fueran ejecutadas, en esta ocasión nosotros le pondríamos uno o más KPIs al cliente, según lo veamos conveniente.

Y por ultimo, documentar este proceso de tal manera que pueda ser agregado al portafolio de servicios que ofrece Cisco para las empresas del giro de proveedores de servicios como lo es nuestro cliente, actualmente somos pioneros en la creación e implementación de temas preventivos y considero que nuestra experiencia puede ayudar a muchos otros clientes a implementarlo, tomando como referencia nuestro proceso.

3.3 Conclusiones

Tanto Cisco como nuestro cliente, nos encontramos muy satisfechos con la implementación de este proceso, aun quedan cosas por afinar y sobre todo por mejorar, considero que este fue el inicio de un gran reto. Estamos consientes de que las falla en los equipos siempre van a existir, pero hemos evolucionado, ahora estamos preparados para aprender de esas fallas, tenemos el proceso que nos ayudará a identificar cuáles podemos evitar por completo, y para aquellas en las que la afectación es inminente estaremos preparados para que la afectación sea lo menos dolorosa posible.

Estoy segura de que éste no es un proceso que se definió y se documentó para ser operado repetitivamente sin ser analizado, como he mencionado con anterioridad, tanto como Cisco como nuestro cliente somos un equipo muy dinámico, que siempre estamos buscando la manera de mejorar e integrar nuevas herramientas, proceso, tareas que agreguen valor a la operación.

Me siento muy orgullosa de haber formado parte de la definición e implementación de este proceso, ya que incluso en Cisco a Nivel Latinoamérica estamos siendo punta de lanza en el tema proactivo, porque muy seguramente, gracias a que ya estamos operándolo, podremos servir de referencia para que este sea un servicio mas dentro del portafolio de servicios ofrecidos por Cisco.

La jornada de trabajo fue una experiencia enriquecedora, ya que el simple hecho de verbalizar nuestro proyecto nos sirve para escucharnos a nosotros mismos y podemos darnos cuenta de que es necesario desarrollar aun más alguna idea que de manera escrita no la tenemos tan clara o que incluso podamos haber tomado por obvia. El que nuestros compañeros escuchen, propongan y den su opinión desde un enfoque de alguien que no precisamente tiene la experiencia del área donde se desarrolla nuestro proyecto agrega gran valor para que podamos complementar nuestro documento.

Bibliografía

Clydebank Media LLC. (2017). *ITIL For Beginners: The Complete Beginners' Guide to ITIL.*

Cisco Systems. (s.f.). Obtenido de Cisco.com: https://www.cisco.com/c/es_pa/services/overview.html

Alfaro, E. (2012). *Customer Experience: Una visión multidimensional del marketing de experiencias.*

Anil Kumar Nandibhatla, P. (4 de January de 2017). *Best Practices in Proactive Problem Management (PPM)*. Obtenido de linkedin.com: https://www.linkedin.com/pulse/best-practices-proactive-problem-management-ppm-anil-nandibhatla-/

AXELOS Limited. (2019). *ITIL 4th edition - Foundation.* Glumin Networks SC.

Hill, A. (1 de March de 2020). *Getting Customer Feedback (NPS vs. CSAT)*. Obtenido de Bysubess 2 Community: https://www.business2community.com/customer-experience/getting-customer-feedback-nps-vs-csat-02288381

ISACA. (2019). *COBIT 2019 Framework - Governance and Management Objectives* . ILL.

Jones, E. (12 de August de 2018). *How Effective Is the Customer Satisfaction (CSAT) Metric?* Obtenido de Business 2 Community: https://www.business2community.com/customer-experience/how-effective-is-the-customer-satisfaction-csat-metric-02104902

Molina, C. (2012). *Customer Experience: Una visión multidimensional del marketing de experiencias.*

Pabbathi, K. K. (2020). *Guidance for Continual Improvement in ITSM.*

RAE. (2019). *Real Academia Española*. Obtenido de https://dle.rae.es/servicio

Romero, A. (10 de June de 2015). *Hablemos de Metricas (ITIL)*. Obtenido de Openservice.mx: https://www.openservice.mx/blog/hablemos-de-metricas-itil/

Skelton, C. (2017). *Major Incident Management for IT Operations.*

Soreanu, G. (26 de May de 2016). *Proactive Problem Management: What ITIL Didn't Teach You.* Obtenido de Thinkhdi.com: https://www.thinkhdi.com/library/supportworld/2014/proactive-problem-management.aspx

Zitek, N. (2018). *ITIL Reactive and Proactive Problem Management: Two sides of the same coin.* Obtenido de advisera.com: https://advisera.com/20000academy/knowledgebase/itil-reactive-proactive-problem-management-two-sides-coin/

Glosario

HTE

High Touch Engineer: Personal técnico especializado

HTOM

High Touch Operations Manager: Gerente de Operaciones

HTTS

Hight Touch Technical Support: Personal técnico dedicado

&&

Clasificación de criticidad que nuestro cliente le da a un *service request* basado en los servicios impactados. Un *service request* clasificado como && significa que tiene mas de 10 servicios afectados y menos de 100.

&&&

Clasificación de criticidad que nuestro cliente le da a un *service request* basado en los servicios impactados. Un *service request* clasificado como &&& significa que tiene mas de 100 servicios afectados.

BCI

Son las iniciales para *Business Critical Insights,* el cual es una solución de Cisco que proporciona datos en tiempo real del performance de la red de los clientes, que por medio de tableros de control configurables por el cliente puede proporcionar datos de logs, alarmas, alertas arrojados por los equipos.