Compañía Nacional del Petróleo

Trabajo Integrador Final (TIF)

Especialización en dirección de proyectos

Proyecto Remediación y optimización infraestructura de red y seguridad informática en una petrolera (CNP)

Autor: James Vallejo Mejia

Ingreso: 2017

Tutor: Daniel Skigin

Introducción

La realización del siguiente TIF, está basado en un proyecto planificado y ejecutado en la vida real en una compañía petrolífera, A la cual por motivos de confidencialidad e integridad, se le ha asignado un nombre ficticio, previamente pertenecí a la compañía como líder de proyectos por lo cual tuve a cargo este proyecto desde su inicio hasta su finalización.

Los documentos se encuentran ordenados con la siguiente nomenclatura:

XXX_ROIRCNP_Alcance_EDT

Fases	**Primeros tres números (Fases)**	**Siglas: Remediación y optimización Infraestructura de red CNP**	**Área Ejemplo:**	**Nombre del documento: Ejemplo**
Inicio	100-x	ROIRCNP		
Planificación	200-x	ROIRCNP	Alcance, tiempo	EDT
Ejecución y seguimiento	300-x	ROIRCNP	Issues	
Cierre	400-x	ROIRCNP	Cierre	Acta de cierre
Anexos	A	ROIRCNP	Adquisiciones	RFP

Contenido

Nombre de archivo	**Proceso**	**Tipo**
101_ROIRCNP_Enfoque y estrategia organizacional	Inicio	Opcional
102_ROIRCNP_PMO	Inicio	Opcional
103_ROIRCNP_Caso de negocio	Inicio	Obligatorio
104_ROIRCNP_Acta constitutiva	Inicio	Obligatorio
200-0_ROIRCNP_Alcance_Plan de gestión	Planificación	Obligatorio
200-1_ROIRCNP_Alcance_Ciclo de vida del proyecto	Planificación	Obligatorio
200-2_ROIRCNP_Alcance_Enunciado	Planificación	Obligatorio
200-3_ROIRCNP_Alcance_EDT	Planificación	Obligatorio
200-4_ROIRCNP_Alcance_Diccionario EDT	Planificación	Obligatorio
201-0_ROIRCNP_Tiempo_Plan de gestión	Planificación	Obligatorio
201-1_ROIRCNP_Tiempo_Linea base	Planificación	Obligatorio

201-2_ROIRCNP_Tiempo_Diagrama de Gantt resumen	Planificación	Obligatorio
201-3_ROIRCNP_Tiempo_Diagrama de Gantt completo	Planificación	Obligatorio
201-4_ROIRCNP_Tiempo_Camino crítico	Planificación	Obligatorio
201-5_ROIRCNP_Tiempo_Hitos	Planificación	Obligatorio
201-6_ROIRCNP_Tiempo_Project	Planificación	Opcional
202-0_ROIRCNP_Costo_Plan de gestión	Planificación	Obligatorio
202-1_ROIRCNP_Costo_Presupuesto	Planificación	Obligatorio
202-2_ROIRCNP_Costo_Distribución del presupuesto	Planificación	Obligatorio
203_ROIRCNP_Riesgos_Plan de gestión	Planificación	Obligatorio
204_ROIRCNP_Calidad_Plan de gestión	Planificación	Obligatorio
205_ROIRCNP_RRHH_OBS y estructura organizacional	Planificación	Obligatorio
205-1_ROIRCNP_RRHH_Roles y responsabilidades	Planificación	Obligatorio
206_ROIRCNP_Análisis de interesados	Planificación	Obligatorio
207_ROIRCNP_Comunicaciones	Planificación	Optativo
301_ROIRCNP_Matriz de riesgos	Ejecución/ Seguimiento	Obligatorio
302-0_ROIRCNP_Informe de avance N°3	Ejecución/ Seguimiento	Obligatorio
302-1_ROIRCNP_Informe de avance N° 3_Diagrama de Gantt	Ejecución/ Seguimiento	Obligatorio
302-2_ROIRCNP_Informe de avance N° 3_Project	Ejecución/ Seguimiento	Obligatorio
303_ROIRCNP_ Log issues	Ejecución/ Seguimiento	Obligatorio
304-0_ROIRCNP_Evento de Cambio_1_RFC	Ejecución/ Seguimiento	Obligatorio
304-1_ROIRCNP_Evento de Cambio 1_Reporte Especial	Ejecución/ Seguimiento	Obligatorio
304-2_ROIRCNP_Evento de Cambio 1_Diagrama de Gantt	Ejecución/ Seguimiento	Obligatorio
304-3_ROIRCNP_Evento de Cambio 1_Hitos	Ejecución/ Seguimiento	Obligatorio
304-4_ROIRCNP_Evento de Cambio 1_Presupuesto	Ejecución/ Seguimiento	Obligatorio
304-5_ROIRCNP_Evento de Cambio 1_Project	Ejecución/ Seguimiento	Obligatorio
305-0_ROIRCNP_Evento de Cambio 2_RFC	Ejecución/ Seguimiento	Obligatorio
305-1_ROIRCNP_Evento de Cambio 2_Reporte especial	Ejecución/ Seguimiento	Obligatorio
305-2_ROIRCNP_Evento de Cambio 2_Project	Ejecución/ Seguimiento	Obligatorio
305-3_ROIRCNP_Evento de Cambio 2_Diagrama de Gantt	Ejecución/ Seguimiento	Obligatorio
400_ROIRCNP_Cierre_Reporte de cierre	Cierre	Obligatorio
401_ROIRCNP_Cierre_Registro de aceptación	Cierre	Obligatorio

402_ROIRCNP_Cierre_Acta de Cierre del proyecto	Cierre	Opcional
403_ROIRCNP_Cierre_Project	Cierre	Opcional
A1_RIRCNP_Informe hallazgos y vulnerabilidades	Cierre	Anexo
A2_ROIRCNP_Adquisiciones_RFP	Cierre	Obligatorio
A3_ROIRCNP_Adquisiciones_Planilla criterios de selección	Cierre	Obligatorio
A4_ROIRCNP_Informe Técnico final	Cierre	Opcional
A5_ROIRCNP_Auditoria CNP_Relevamiento	Inicio	Opcional
A6_ROIRCNP_Diagrama de red	Cierre	Opcional

Compañía Nacional del Petróleo

Enfoque y estrategia organizacional

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Autor: James Vallejo Mejia

Registro de cambios

Fecha	Versión	Descripción	Autor	Aprobación
23/9/2018	1	inicio	PM	

Contenido

Enfoque y plan estratégico de la organización

Identidad Corporativa

CNP (Compañía Nacional del Petróleo) es un actor público clave para el desarrollo energético de Chile y los territorios en los que opera. Posee tres Líneas de Negocio: Exploración y Producción (E&P); Refinación y Comercialización (R&C); y Gas y Energía (G&E). Sus operaciones abarcan activos en Chile, Ecuador, Argentina y Egipto. Con cerca de 3.700 trabajadores en distintos países, su objetivo es contar con equipos comprometidos con la seguridad, la eficiencia y la sostenibilidad en cada uno de los países en los que está presente. [1]

CNP (Compañía Nacional del Petróleo) Argentina es la filial argentina de CNP Chile, compañía dedicada a la exploración y producción de petróleo y gas como brazo internacional de la empresa estatal de hidrocarburos de Chile CNP (Compañía Nacional del Petróleo). Como principal operadora off shore de la Argentina; Se encuentra presente en el país desde 1991, siendo un actor relevante en la actividad hidrocarburífera de la Argentina. Las primeras operaciones fueron en el Área Magallanes, cuando se negoció y acordó con la empresa estatal argentina de hidrocarburos YPF S.E. la asociación de ambas compañías para desarrollar y explotar el yacimiento de petróleo y gas ubicado en la boca oriental del Estrecho de Magallanes. [2]

Modelo de gestión CNP Argentina

La empresa cuenta con un modelo de negocios integrado que se fundamenta sobre la base de un proceso de gestión estratégica y por proyectos, cuyo objetivo final es incrementar el valor de la compañía con seguridad y responsabilidad, contribuyendo a la integración y abastecimiento energético de Argentina y Chile.

Este enfoque permite la unificación de los objetivos de negocio, la cultura y las operaciones en la generación de un plan estratégico, que permite concentrar los esfuerzos de los equipos humanos, optimizar el uso de los recursos productivos para el logro de las metas del negocio, como así también, medir los balances realizados en consecuencia y ejecutar las acciones de mejora continua necesarias. [3]

[1] (Empresa Nacional del Petróleo, 2018)
[2] (ENAP Argentina, 2018)
[3] (ENAP Argentina, 2018)

Misión CNP

Impulsar un futuro energético sostenible para el país y la región, su Propuesta de valor es brindar soluciones energéticas eficientes, innovadoras y sostenibles para favorecer el presente y el futuro energético de todos los territorios donde opera.

Visión CNP

Ser una empresa país articuladora de potentes e innovadoras soluciones energéticas.

Valores CNP

La carta de Valores de CNP es un conjunto de principios que rigen, orientan y motivan la gestión de la empresa y de cada uno de sus trabajadores y trabajadoras como también de sus distintos públicos de interés. Se trata de orientaciones éticas que otorgan un marco de referencia coherente para la definición de acciones y la toma de decisiones a lo largo de toda la cadena del negocio.

CNP ha definido seis valores que son transversales a toda la organización tanto en Chile como en el extranjero. Estos son:

Respeto

Valoramos la diversidad y aceptamos las diferencias de cada persona, propiciando espacios de comunicación con nuestros trabajadores y otros grupos de interés, en un marco de tolerancia.

Honestidad

Expresarnos con la verdad y ser coherentes entre lo que hacemos y decimos, nos permite tener relaciones de confianza al interior de nuestros equipos de trabajo.

Transparencia

Promovemos prácticas organizacionales que permitan la entrega de información y la comunicación veraz con todos nuestros grupos de interés.

Responsabilidad

Trabajamos en equipo con calidad y rigurosidad, haciéndonos cargo de las consecuencias de nuestra labor, buscando ser sostenibles en cada desafío que asumimos al interior y fuera de la organización.

Excelencia

Buscamos agregar valor a la empresa, la sociedad y el medio ambiente, a través de la mejora continua y la innovación en cada una de las acciones que ejecutamos.

Lealtad

Actuamos de forma consecuente, movilizados por el compromiso con los propósitos de nuestra organización y el sentido de nuestro trabajo.

[4]

[4] (Empresa Nacional del Petróleo, 2018)

Referencias

Empresa Nacional del Petróleo. (19 de 09 de 2018). *Enap chile*. Obtenido de https://www.enap.cl/

ENAP Argentina. (19 de 09 de 2018). *ENAP Argentina*. Obtenido de http://www.enap.com.ar/

Compañía Nacional del Petróleo

PMO

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Autor: James Vallejo Mejia

Registro de cambios

Fecha	Versión	Descripción	Autor	Aprobación
23/9/2018	1	PMO	PM	

Contenido

Oficina de gestión de proyectos

Gestion de portfolio, programas y proyectos

Alineándose al marco de referencia del PMbook, PgM y PfMP PMI[1], y siguiendo el modelo de gestión de la compañía, se lleva a cabo la gestión portfolios, programas y proyectos. Agrupando los proyectos de acuerdo al logro de beneficios planeados y la realización de estrategias.

PMO TI

Para la gestión de proyectos relacionados con tecnología la compañía cuenta con una PMO, la cual reporta a la dirección de programas, dónde se colocan los proyectos en contexto explicitando su alineación con los objetivos estratégicos de la Organización.

Funciones

- **Planificación y coordinación y de proyectos:**

A la PMO TI le corresponde planificar y definir las estrategias de coordinación para la ejecución de proyectos TI. Esto incluye la gran responsabilidad de asignar recursos a cada una de los equipos, establecer las prioridades y, decidir cuáles de ellas se ejecutan, cuáles se modifican y cuáles se descartan.

- **Estandarización de procesos:**

Con el objetivo de facilitar el intercambio de recursos, información, herramientas, conocimientos y metodologías empleadas en un proyecto, las PMO se ocupan de poner en un mismo plano todos los procesos que tienen lugar en una organización.

- **Vinculación del proyecto con los objetivos del negocio:**

Al ser un área estratégica, a la PMO también le corresponde lograr que todos los proyectos concebidos y prestos a ejecutarse en el seno de una organización cumplan con los objetivos globales del negocio. No puede haber contradicciones ni fisuras de contenido o de forma. Su labor es hacerlos compatibles.

- **Alineación con objetivos estratégicos:**

De todos los objetivos de las empresas, a los responsables de una PMO les interesan especialmente aquellos de carácter estratégico, pues son éstos los que influyen de forma directa en la ejecución de cualquier proyecto, iniciativa o acción corporativa.

[1] (Project Manager Institute)

Programa Modernización infraestructura informática CNP

Con el propósito de llevar a cabo uno de los objetivos estratégicos trazados, que es la modernización de la compañía, se pone en marcha el siguiente programa:

Modernización infraestructura informática CNP, a cargo de la PMO de la oficina informática de la compañía.

Programa	Programa	Proyectos
Modernización infraestructura informática CNP		**Relevamiento de información infraestructura informática y servicios TI**
	Remediación infraestructura informática y servicios TI	**Remediación y optimización infraestructura de red y seguridad informática**
		Monitoreo operativo
		Monitoreo de seguridad informática
		Remediación entorno Microsoft
		SQL Server
		Remediación entorno virtual
		Remediación Storage
		Remediación Telecomunicaciones
		Control dispositivos móviles

Referencias

Project Manager Institute. (s.f.). *PM, PgMP, PfMP.* Obtenido de https://www.pmi.org/pmbok-guide-standards

Compañía Nacional del Petróleo

Caso de negocio

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Autor: James Vallejo Mejia

Registro de cambios

Fecha	Versión	Descripción	Autor	Aprobación
23/9/2017	1	Caso de negocio	PM	
17/10/2017	2	Caso de negocio		

Contenido

Caso de negocio

1 Resumen ejecutivo

Como modernización de la compañía, después de haber sido adquirida por CNP CL (compañía Nacional del Petróleo Chile), y recientemente haber cambiado su razón social de CIPETROL a CNP Se propone realizar una serie de cambios corporativos entre los cuales está la modernización de la infraestructura TI.

Inicialmente se realiza un proyecto de Relevamiento de toda la infraestructura informática y servicios TI. Durante la finalización del mismo, se entrega un informe de hallazgos, el cual incluye la identificación de desvíos en la organización de la arquitectura TI, detección de desvíos en la Configuración de servicios básicos de red, identificación y cuantificación de riesgos asociados a los desvíos y las alternativas para la corrección de las observaciones y organización de prioridades; Dejando así el punto de partida para la gestión del este proyecto: **Remediación y optimización infraestructura de red y seguridad informática en una petrolera Argentina *CNP Argentina SA***

2 Análisis de la situación

El proyecto de relevamiento se realizó en 4 etapas diferentes:

Etapa I Relevamiento	**Etapa II Mapa y categorización de activos**	**Etapa III Gap análisis**	**Etapa IV Propuestas de mejora**
Tareas	**Tareas**	**Tareas**	**Tareas**
Equipamiento seguridad Informática	Análisis de activos categorizados	Análisis de los puntos de desvíos detectados	Análisis de propuestas de mejora para cada uno de los desvíos identificados
Conectividad WAN/LAN/WIFI	Análisis de recursos/activos relacionados a aplicaciones y servicios de negocio	-Categorización de criticidad y prioridad	
Servicios Básicos de Red	**Entregable**	**Entregable**	**Entregable**
Aplicaciones	Mapa de activos de IT para cada uno de los sitios.	Mapa de activos especificando desvíos para activos críticos	Lista priorizada de vulnerabilidades encontradas, acciones correctivas y recomendaciones.

Infraestructura Servidores Microsoft	Sistemas críticos para el negocio.		Informe de networking, vulnerabilidades en red perimetral, redes internas cableadas e inalámbricas.
Infraestructura de Virtualización	Sistemas fundamentales para realizar tareas diarias		Informe de virtualización, storage y tecnologías de Microsoft
Infraestructura de Storage	Mapa de activos de IT para cada uno de los sitios.		Alternativas de solución para mitigación de riesgos, de tal forma que ES pueda optar por la más conveniente para sus objetivos.
Procedimientos y Compliance	Sistemas críticos para el negocio.		Lista priorizada de vulnerabilidades encontradas, acciones correctivas y recomendaciones.
Entregable	Sistemas fundamentales para realizar tareas diarias		Informe de networking, vulnerabilidades en red perimetral, redes internas cableadas e inalámbricas.
Inventario detallado de equipamiento de red LAN, WIFI, WAN, MAN y seguridad perimetral			Informe de virtualización, storage y tecnologías de Microsoft
			Alternativas de solución para mitigación de riesgos, de tal forma que ES pueda optar por la más conveniente para sus objetivos.

Con esta información el objetivo es realizar un proyecto que ejecute remediación y optimización a la infraestructura de Tecnología informática de CNP, para resolver las configuraciones de los servicios básicos de TI, las vulnerabilidades existentes asociadas a la seguridad informática y alinear las instalaciones a las mejores prácticas recomendadas.

Así mismo, encontrar la propuesta para brindar soporte especializado de la instalación, a ejecutarse con posterioridad de haber finalizado el proyecto mencionado en primer término.

3 Declaración del problema

Según el informe entregado por el proyecto de relevamiento se mencionan a grandes rasgos los dominios y los hallazgos más importantes y en los cuales se centra el proyecto de remediación.

Dominio 1 servidores
Servidores DNS
Servidor de DNS principal expuesto a Internet con todos los ports abiertos, sin sistema de protección de intrusos (IPS) y antivirus (AV)
Un solo registro MX, no hay Mail Server secundario
No se cuenta con servicios DHCP en HA
No se identifica herramienta para gestión de dispositivos móviles
Se identifica un sistema de inventario de activos de IT, pero desactualizado y con alcance incompleto

Dominio 2 protección		
Protección de Borde	**Filtrado de contenido web**	**Antivirus**
Firewall de borde y VPN sin HA	Servicio de WebFiltering no está en HA	La consola de AV no está en HA
No se cuenta con balanceo de Tráfico Saliente a Internet	No se identifican procedimiento de backup de configuración	No se identifican procedimientos de backup de configuración ni control de cambios
FW Fortigate 200B y 110C EoS (End of support)	No hay procedimientos de reportes, desvíos, consumos	Monitoreo: No se cuenta con herramienta de monitoreo
Listas de control de acceso de trafico entrante	No se identifican políticas aplicadas por grupos de usuarios	
No hay monitoreo de servicios		
Servicios publicados en internet sin sistema de protección de intrusos (IPS), ni antivirus (AV) habilitados en el firewall		
El tráfico entre redes interna no pasa a través del firewall, por lo cual no se pueden aplicar políticas de seguridad sobre las mismas.		
El tráfico entre redes LAN-LAN y LAN-WAN no tiene aplicado IPS, AV o restricciones de ancho de banda		

Dominio III Red LAN	
Switches y equipos de fibra óptica	
No hay segmentación de la red	
Equipos conectados en cascada	Servidores sin espacio en Disco
No se cuenta con procedimiento de reportes de consumo / accesos de usuarios	Equipos con puerto quemados
Password de acceso débiles	Falta de etiquetas y documentación de los dispositivos para su identificación
La red WiFi no está segmentada en red corporativa y red de invitados	Equipos no licenciados.

Dominio IV Tecnologias Microsoft
Actualizaciones críticas de seguridad no implementadas
Sitios sin redundancia
No existe redundancia en la solución de correo
Infraestructura virtual
Sisemas operativos fuera de soporte

El informe completo de hallazgos se encuentra dentro de la documentación del proyecto: ***A1_RIRCNP_Informe hallazgos y vulnerabilidades.*** [1]

4 Descripcion del proyecto

El objetivo del proyecto es implementar remediaciones y optimizaciones a la infraestructura de Tecnología Informática (TI) de CNP Argentina S.A. para resolver las configuraciones de los servicios básicos de TI, las vulnerabilidades existentes asociadas a la seguridad informática y alinear las instalaciones a las mejores prácticas recomendadas.

Para ello se deben contratar lo proveedores necesarios para llevar a cabo cada dominio y lograr modernizar la infraestructura adecuadamente.

Realizar la compra de equipamiento necesario para llevar a cabo el proyecto.

[1] (Tycon Technologies, 2017)

5 Justificacion de la necesidad

La finalidad del proyecto es satisfacer las necesidades de los usuarios en el uso de servicios TI, estar a la vanguardia de nuevas tecnologias y luchar contra la obsolecencia tecnologica. Tambier alinear la oficina informatica con la vision y mision de la compañía fundamentadas sobre la base de un proceso de gestión estratégica y por proyectos, con el objetivo de incrementar el valor de la compañía, lograr la unificación de los objetivos de negocio, la cultura y las operaciones en la generación del plan estratégico, que permite concentrar éstos esfuerzos y optimizar el uso de los recursos productivos para el logro de las metas del negocio petrolífero, sobresaliendo y mostrando su capacidad tecnológica frente a los otros competidores.

6 Glosario

Tecnología de la información y Comunicaciones (TIC): Son el conjunto de tecnologías que permiten el acceso, producción, tratamiento y comunicación de información presentada en diferentes códigos (texto, imagen, sonido,...) [2]

LAN (Local Área Network): red de área local, vinculan computadoras que se hallan en un mismo espacio físico, como una oficina o edificio [3]

WAN (Redes de área amplia): cubren una zona extensa, a menudo incluso todo un país o continente.[4]

Router: Los routers se utilizan para conectar varias redes. Por ejemplo, puede utilizar un router para conectar sus computadoras en red a Internet y, de esta forma, compartir una conexión de Internet entre varios usuarios [5]

Switch: Los Switches se utilizan para conectar varios dispositivos a través de la misma red dentro de un edificio u oficina[6]

Firewall: Software especializado que examina los datos entrantes y protege la red de su negocio de posibles ataques [7]

Servidor: Un servidor es un ordenador u otro tipo de equipo informático encargado de suministrar información a una serie de clientes, que pueden ser tanto personas como otros dispositivos conectados a él. [8]

Dirección ip: Las direcciones IP, es decir los números del Protocolo Internet (*Internet Protocol - IP*) que identifican en forma unívoca a cada dispositivo que se conecta a la gran red de redes [9]

DHCP: El protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol) es un estándar TCP/IP diseñado para simplificar la administración de la configuración IP de los equipos de nuestra red [10]

DNS: Un servidor DNS (Domain Name System - Sistema de nombres de dominio) es un servidor que traduce nombres de dominio a IPs y viceversa.[11]

---

[2] (Ortí, s.f.)
[3] (appser data engineering S.L, 2015)
[4] (appser data engineering S.L, 2015)
[5] (Cisco Systems, 2012)
[6] (Cisco Systems, 2012)
[7] (Cisco Systems, 2012)
[8] (Infortelecom, 2016)
[9] (LACNIC Argentina, 2017)
[10] (Instituto de tecnologias educativas, s.f.)
[11] (Instituto de tecnologias educativas, s.f.)

Referencias

Cisco Systems. (2012). *Lo que usted necesita saber*. Obtenido de https://www.cisco.com/c/dam/global/es_mx/assets/ofertas/desconectadosanonimos/routing/pdfs/brochure_redes.pdf

appser data engineering S.L. (2015). *Apser.es*. Obtenido de http://www.apser.es/blog/2015/06/20/las-redes-informaticas-que-son-tipos-topologias/

Infortelecom. (26 de 09 de 2016). *Servidor*. Obtenido de https://infortelecom.es/blog/que-es-un-servidor-y-para-que-sirve/

Instituto de tecnologias educativas. (s.f.). *Servidor DHCP y Servidor DNS*. Obtenido de http://formacion.educalab.es/pluginfile.php/37388/mod_resource/content/1/PDF_conlogonuevo/2-Servidor-DHCP-y-DNS.pdf

LACNIC Argentina. (12 de 2017). *¿Cómo se clasifican las direcciones IP?* Obtenido de https://nic.ar/es/enterate/novedades/como-se-clasifican-ip

Ortí, C. B. (s.f.). *LAS TECNOLOGÍAS DE LA INFORMACIÓN Y*. Obtenido de https://www.uv.es/~bellochc/pdf/pwtic1.pdf

Tycon Technologies. (2017). *A1_RIRCNP_Informe hallazgos.* CABA.

Compañía Nacional del Petróleo

Acta Constitutiva

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Autor: James Vallejo Mejia

Registro de cambios

Fecha	Versión	Descripción	Autor	Aprobación
23/3/2017	1	Project charter	PM	
17/04/2017	2	Project charter		

Contenido

Acta constitutiva

1 Resumen ejecutivo

Como modernización de la compañía, después de haber sido adquirida por CNP CL (compañía Nacional del Petróleo Chile), y recientemente haber cambiado su razón social de CIPETROL a CNP Se propone realizar una serie de cambios corporativos entre los cuales está la modernización de la infraestructura TI.

Inicialmente se realiza un proyecto de Relevamiento de toda la infraestructura informática y servicios TI, durante la finalización del mismo, se entrega un informe de hallazgos el cual incluye la identificación de desvíos en la organización de la arquitectura TI, detección de desvíos en la Configuración de servicios básicos de red, identificación y cuantificación de riesgos asociados a los desvíos y las alternativas para la corrección de las observaciones y organización de prioridades. Dejando así el punto de partida para la gestión del este proyecto **Remediación infraestructura de red y seguridad informática en una petrolera Argentina *CNP Argentina SA***

2 Definicion del proyecto

Actualmente CNP Argentina cuenta con un datacenter principal en la oficina de Buenos Aires, allí se aloja la infraestructura de red, Se encuentran equipos fuera de soporte por el fabricante EoS *(End of support),* dispositivos obsoletos, no licenciados, una red wifi antigua y sin protección y una red sin segmentar por lo cual todas las áreas pueden acceder a cualquier servicio aleatoriamente. De igual forma, se tienen otros 3 sites ubicados en Rio Gallegos, Cabo Vírgenes y Pampa Castillo, dentro de los cuales se pretende realizar el proyecto a fin de brindar un servicio tecnológico moderno a los empleados, clientes y demás interesados.

Con la remediación de todas las vulnerabilidades sobre la red halladas en el proyecto de relevamiento[1], se pretende cumplir con los estándares TI, para el funcionamiento de una oficina informática; Implementando una red inalámbrica rápida y accesible, brindando acceso a internet con los filtros adecuados según los perfiles de usuarios y adquirir el equipamiento de última tecnología, con una vida útil de aproximadamente 15 años de funcionamiento.

Se contratará personal con experiencia para brindar soporte, realizar monitoreo y mantener la infraestructura actualizada y funcionando correctamente sin disrupciones

[1] Para mayor detalle ver documento A1_RIRCNP_Informe hallazgos y vulnerabilidades

sobre el servicio por problemas locales. Además se solicitará a los proveedores de redes realizar un esfuerzo para contar con equipos actualizados y mantener redundancia y alta disponibilidad sobre el servicio.

Para llevar a cabo este y otros proyectos del programa será necesario contar con el personal idóneo y con la experiencia suficiente para implementar la nueva red, para ello se trabajará en conjunto con los recursos de la compañía y se realizará un proceso de contratación de personal, además se publicará una licitación para escoger a los proveedores encargados de suministrar el equipamiento y llevar a cabo las actividades dentro del proyecto.

3 Priorización de los objetivos

Se define la siguiente priorización de los objetivos:

	Costo	Plazo	Alcance
Debe lograrse			
Conviene lograrse			
Acepto resultado			

Se debe cumplir el proyecto dentro del tiempo planificado, ya que se deben ejecutar otros proyectos del programa ***Remediación infraestructura informática y servicios TI,*** los cuales tienen fechas pactadas para su inicio; El alcance conviene lograrse, pudiendo cambiar alguna actividad por injerencia de la dirección o proveedores, pactado previamente y registrado correctamente en el control de cambios, El aumento en el costo se acepta si se llega a exceder el presupuesto.

4 Descripción preliminar sobre el Alcance del proyecto

El objetivo principal del proyecto es modernizar la infraestructura de Tecnología Informática (TI) actual de CNP Argentina, optimizando la configuración de los servicios básicos de TI, remediando las vulnerabilidades existentes asociadas a la seguridad informática, adquisición de equipamiento de redes y alineación de las instalaciones con las mejores prácticas recomendadas por la industria.

Asimismo se requiere una propuesta para brindar soporte especializado de la instalación, a ejecutarse con posterioridad de haber finalizado el proyecto mencionado en primer término.

El alcance de la solicitud comprende la realización de todas las tareas según se describe a continuación:

Fases	Descripción
Gestion de contratos	Contratos y proceso de licitación
Servicios DNS externo y DHCP	Configuraciones y recomendaciones para estos servicios
Protección de borde I	implementaciones y ajustes sobre servicios publicados hacia internet, VPN, DMZ
Protección de borde II	Protección IPS (sistema de prevención de intrusos), DDOS (ataque de denegación de servicio distribuido)
Red LAN	Ajustes, configuración e implementación nueva red LAN
Protección de redes internas	Filtrado de tráfico, ancho de banda y permisos de acceso
Filtrado web, anti spam y procedimientos	Filtrado de contenidos web, implementación de procedimientos para la buena gestión de la oficina informática
Red WiFi, MPLS y Backup Satelital	Implementación red Wifi, revisión de enlaces de respaldo con proveedores

5 Entregables

- Equipos configurados y red implementada y probada.
- Documentos de configuración: enumeración del ajuste o configuración realizada, mapa conceptual de la configuración resultante, esquema gráfico, detalle de la versión del software.
- Archivo en formato Microsoft Visio 2010 (o posterior) con el esquema y el detalle de configuración
- Documentos con las directrices para el posterior desarrollo del procedimiento de configuración, control, backup y actuaciones operativas necesarias para el correcto mantenimiento y actualización.
- Definición de un contrato de soporte posterior al proyecto

6 Supuestos

En la planificación del proyecto se asume que se cumplirán los siguientes supuestos:

- La información acerca del equipamiento y servicios actuales de red se encuentran totalmente relavados, previamente en el proyecto de relevamiento de información de la infraestructura TI
- El personal administrativo y operativo es informado de la ejecución del proyecto previo a iniciar.
- Se contará con suministro de energía eléctrica regulada y UPS para la conexión de equipos y disponibilidad.
- Los equipos a instalar son compatibles y pueden negociar entre sí.

7 Restricciones

Las siguientes restricciones son aplicables a este proyecto:

- Tanto procedimientos como proveedores deben ir alineados a las recomendaciones ITIL (nformation Technology Infrastructure Library) marco de trabajo de buenas prácticas aplicables a la Gestión de Servicios de TI. [2]
- Cumplir con los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de Gestión de la información ISO 27001[3]
- Los proveedores deben cumplir con las normas de Seguridad Industrial
- Garantizar el uso de herramientas, software, y equipamiento TI y contar con licenciamiento de ser necesario.
- Restricciones aduaneras para importación y exportación de equipos.

[2] (Axelos, s.f.)

[3] (ISO, s.f.)

8 Riesgos iniciales de alto nivel

Se identifican los siguientes grupos o familias de riesgos, los cuales deberán ser desarrollados oportunamente:

Numero	Riesgo	Causa
1	indisponibilidad en los servicios durante la ejecución de tareas	Falla en alguno de los equipos, configuracion incorrecta
2	Retraso en al ejecucion de tareas	Logistica por parte de proveedores externos, por temas de enlaces de comunicaciones con otros paises.
3	Cambios y mejoras en los dispositivos	Actualizaciones, nuevo firmware, IOS, Parches
4	Intervencion de sindicatos	Resistencia a cambios de tecnologia y permisos de acceso.
5	Cambios en el alcance	Por cambios del cliente, normativas, imposibilidad de conseguir el producto especificado, mayores requerimientos cuando se desarrolle el master-plan, etc.

9 Descripción de interesados (stakeholders)

Se identifican los siguientes interesados, cuya participación directa será requerida durante la gestión de este proyecto:

Interesados	Descripción
Asesores, Equipo de proyecto	Interesados en que el proyecto se lleve a cabo. Son responsables directos de la performance del proyecto. Se considera que estarán altamente alineados con las políticas de gestión y calidad que se propongan.
Contratistas, Subcontratistas, Sindicatos, etc.	Grupo de persona, empresas u organizaciones cuyo aporte es significativo para el proyecto. Tendrán un alto grado de injerencia en la performance del proyecto, sobre todo en las fases de ejecución y cierre. Es muy posible que no se encuentren alineados con las políticas de gestión, por lo cual se deberá tener muy en cuenta cómo puede afectar a las planificaciones.
Empleados administrativos	Son los usuarios finales y quienes usarán los servicios tecnologicos
Empleados TI	Personal de apoyo en el area de tecnologia, estarán involucrados durante todo el proyecto, estan alineados con los objetivos de la organización, brindarán soporte ante cualquier eventualidad.
Fabricantes	Encargados de proveer los equipos y dar soporte por garantía

10 Resumen cronograma e hitos

A continuación se presenta el Resumen del Cronograma de Hitos, que podrá ser modificado a medida que se definan con mayor claridad los requerimientos del proyecto. Cualquier modificación será comunicada por el Director del Proyecto a los Sponsor Interno y Externo del Proyecto en el marco de las reuniones de avance del proyecto.

Nombre de tarea	Comienzo
Gestion de Contratación	jue 20/4/17
Etapa I - Servicios DNS Externo y DHCP	**jue 1/6/17**
Etapa II - Protección de Borde I	**mar 4/7/17**
Etapa III - Protección de Borde II	**vie 18/8/17**
Etapa IV - Switch de LAN	**lun 18/9/17**
Etapa V - Protección de Redes Internas	**jue 2/11/17**
Etapa VI - Webfiltering, Antispam y Procedimientos	**jue 11/1/18**
Etapa VII - RED WiFi, MPLS y Backup Satelital	**mié 21/2/18**

11 Presupuesto

La siguiente tabla contiene un resumen presupuestario basado en los costos planificados y estimados para la consecución exitosa del proyecto:

Presupuesto	
Fase	**Costo**
Etapa I - Servicios DNS Externo y DHCP	$ 1.132.475,00
Etapa II - Protección de Borde I	$ 3.752.144,67
Etapa III - Protección de Borde II	$ 1.249.000,00
Etapa IV - Switch de LAN	$ 2.481.325,00
Etapa V - Protección de Redes Internas	$ 1.717.900,00
Etapa VI - Webfiltering, Antispam y Procedimientos	$ 2.453.427,00
Etapa VII - RED WiFi, MPLS y Backup Satelital	$ 1.090.825,00
Gestión del proyecto	$ 1.800.000,00
Gestion de Contratación	$ 400.000,00
Servicios Públicos	$ 95.600,00
Total del proyecto	$ 16.172.696,67
Reserva de contingencia (15%)	$ 2.425.904,50
Línea base de costos	$ 18.598.601,17
Reserva de gerencia (20%)	$ 3.719.720,23
Presupuesto	**$ 22.318.321,40**

Para la realizacion de este proyecto, la Gerencia corporativa de CNP destino a la Gerencia de informatica de la compañía, un presupuesto de **22.318.321,40** $ Arg, acorde para cumplir todas las expectativas y alinear la infraestructura TI a las mejores prácticas recomendadas y cumplir con el objetivo proyecto.

13 Aprobadores Válidos

Los autorizados a aprobar documentos, procedimientos, modificaciones, cambios y pedidos son:

Por parte de PM|PM: James Vallejo Mejia
Por parte de la dirección CIO: Marcelo cueto

14 Director de proyecto

Para la consecución de los objetivos aquí planteados, se designa a James Vallejo Mejia como Project Manager. Ello no obstante, además de gestionar las tareas operativas, de planificación y comunicación durante la duración del proyecto, también participará operativamente en el desarrollo de los planes de mantenimiento, traspaso a la operación, soporte y garantía.

15 Sponsor

El Sponsor del proyecto es el CIO de CNP AR, actualmente el Ingeniero **Marcelo cueto**

16 Referencias

Axelos. (s.f.). *Itil*. Obtenido de https://www.axelos.com/best-practice-solutions/itil?utm_source=itil.co.uk&utm_medium=redirect&utm_campaign=redirects

ISO. (s.f.). *ISO 27001*. Obtenido de https://www.iso.org/standard/54534.html

Compañía Nacional del Petróleo

Alcance

Plan de gestión

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Autor: James Vallejo Mejia

Registro de cambios

Fecha	Versión	Descripción	Autor	Aprobación
23/3/2017	1	PM Alcance	PM	
17/04/2017	2	PM Alcance	PM	

Contenido

Plan de gestión del alcance

1 Introducción

Mediante la gestión del alcance Se realiza un listado de entregables necesarios para cumplir con el objetivo del proyecto, se establecen los supuestos, restricciones, exclusiones, requerimientos y control de cambios respectivo.

La línea base de alcance se compone de la siguiente manera:

- Ciclo de vida del proyecto
- Enunciado del alcance
- Estructura de Desglose de Trabajo (EDT o WBS en inglés)
- Diccionario de la EDT

2 Ciclo de vida del proyecto

El proyecto se desarrollará por fases, dentro de las cuales se definirá que entregables hacen parte de la misma y el tiempo necesario para su ejecución. El ciclo de vida del proyecto es secuencial, para ir a la siguiente fase, debe estar finalizada la fase previa.

3 Enunciado

El enunciado del proyecto se definirá teniendo claro el objetivo del proyecto y su alineación con los objetivos estratégicos de la organización, Indicando la ubicación que cubre el proyecto y los entregables necesarios.

4 EDT

La EDT del proyecto **Remediación y optimización infraestructura de red y seguridad informática** está desarrollada en forma descendente donde el primer nivel hace referencia o está compuesto por paquetes de trabajo generales, en el segundo nivel se encuentran los entregables necesarios para complementar el primer nivel; Estos paquetes de trabajo identificados por el PM y su equipo, de conformidad con sus conocimientos previos y teniendo en cuenta el proyecto y auditoria de relevamiento, donde se hallaron las vulnerabilidades sobre la infraestructura tecnología. También se contó con la participación de la dirección TI, PMO General de la compañía, PgMP y PfMP, para así alinear los objetivos del proyecto con los objetivos estratégicos de la organización.

5 Diccionario EDT

El Diccionario de la EDT se realizará con la siguiente plantilla, dónde se diligencia a información de cada paquete de trabajo:

<table>
<tr><td>Código EDT</td><td colspan="4"></td></tr>
<tr><td>Nombre del entregable</td><td colspan="4"></td></tr>
<tr><td>Descripción</td><td colspan="4"></td></tr>
<tr><td rowspan="2">Entradas</td><td colspan="2"></td><td>Código EDT</td><td></td></tr>
<tr><td colspan="2"></td><td>Código EDT</td><td></td></tr>
<tr><td>Criterio de verificación y validación</td><td colspan="2"></td><td>Responsable</td><td></td></tr>
<tr><td>Contratistas</td><td colspan="4"></td></tr>
<tr><td rowspan="2">Estimaciones</td><td>Fecha Inicio</td><td></td><td>Fecha fin</td><td></td></tr>
<tr><td>Costo</td><td colspan="3"></td></tr>
<tr><td>Observaciones</td><td colspan="4"></td></tr>
</table>

6 Validación del alcance

Los criterios de aceptación del Alcance se indicarán en el diccionario de la EDT. Para ello se tienen dos resultados:

- Aprobado: se acepta formalmente por escrito que el entregable cumple con los requisitos pedidos
- RFC (Request for Change): Se justifican las observaciones realizadas, dejando por escrito el RFC; Se prepara un modelo para estas solicitudes, en este documento.

7 Solicitudes de cambio RFC

Ante la necesidad de requerir algún cambio sobre el alcance del proyecto, por cualquier motivo, Lo primero que se hará es definir el impacto del RFC en las con relación a las restricciones del proyecto. Además se deben evaluar los beneficios esperados por el cambio

para validar si son justificados en relación a los costos del proyecto, o en los cambios de cronograma.

Él análisis cuantitativo debe contemplar los siguientes puntos:

- Impacto en el equipo de proyecto, en el proyecto mismo y en la organización.
- Influencia del cambio con relaciona los riesgos iniciales
- Evaluación del cambio mediante las diferentes alternativas.

Para aceptar un cambio se debe contemplar lo siguiente:

- Cambios inevitables, por factores externos
- Cambios Que conllevan Beneficio
- Conocimientos y aptitudes del equipo de proyecto para implementar el cambio de manera exitosa.
- El juicio de expertos, postura los stakeholders

Para este proyecto, todo cambio propuesto que afecte al proyecto en cualquiera de sus ámbito, debe ser autorizado por el la dirección TI, mientras que cambios que no afecten al presupuesto, como cambios de cronograma y demás, pueden ser aprobados directamente por el PM.

Plantilla de RFC

GESTION DE PROYECTOS **FORMATO DE GESTIÓN DE RFC A PROYECTO**		
Nombre del proyecto:	**Fecha:**	**Proponente:**
Tipo de cambio a proponer:	**No. De Cambio**	**No. Del proyecto**
Puede anexar todos los documentos que considere necesarios como soporte del cambio y referenciarlos en cada casilla		
Descripción del cambio		
Condiciones actuales del proyecto (en términos del plan global del proyecto)		
Cambio propuesto (precisar actividades que cambian, recursos adicionales, cambios en presupuesto, entre otros)		
Posibles consecuencias del cambio (en resultados del proyecto, económicos, en procesos, en la organización, entre otros)		
Justificación del cambio		
Acciones a desarrollar si se acepta la propuesta de cambio		
Nombre y firma del gerente del proyecto (Solicitante)		Fecha:
Nombre y firma del Coordinador de TI:		Fecha:
Aprobada ( ) Rechazada ( )		No. Acta:
Nombre y firma del Director TI:		Fecha:
Decisiones tomadas frente a la propuesta		

Elaboró:	Fecha:	Código:
Revisó:	Fecha:	Pagina:
Aprobó:	Fecha:	Versión:

Compañía Nacional del Petróleo

Alcance

Ciclo de vida del proyecto

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Autor: James Vallejo Mejia

Registro de cambios

Fecha	Versión	Descripción	Autor	Aprobación
23/03/2017	1	Ciclo de vida	PM	
12/06/2018	2	Ciclo de vida	PM	

Contenido

Ciclo de vida del proyecto

1 Antecedentes y metodología

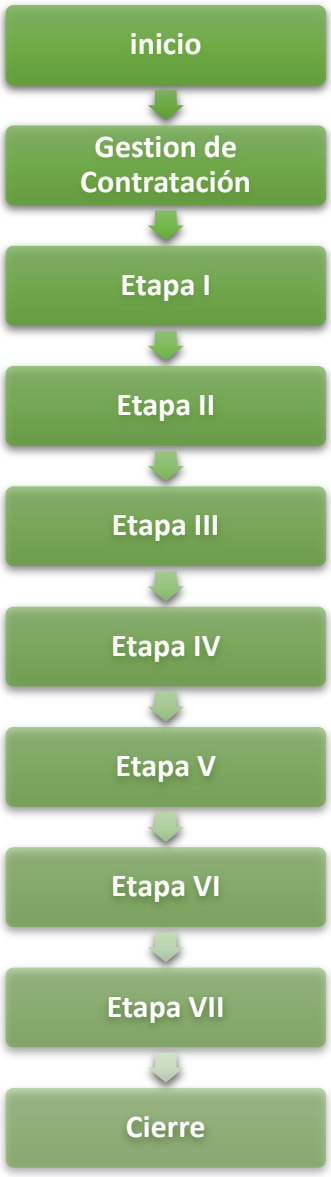
Como se mencionó en el acta constitutiva del proyecto[1] y el caso de negocio[2] El objetivo del presente proyecto es ejecutar remediaciones y optimizaciones a la infraestructura de Tecnología Informática (TI) de CNP (Compañía Nacional del petróleo) Argentina, para resolver las configuración de los servicios básicos de TI, las vulnerabilidades existentes asociadas a la seguridad informática y alinear las instalaciones a las mejores prácticas recomendadas.

Para un correcto seguimiento y control y para evitar generar alto impacto sobre los usuarios, se planifica la ejecución de actividades de manera secuencial

[1] Ver documento 104_ROIRCNP_Acta constitutiva
[2] Ver documento 103_ROIRCNP_Caso de negocio

2 Ciclo de vida del proyecto

Se define el ciclo de vida secuencial agrupando las actividades necesarias para realizar la optimización sobre la infraestructura de red, o remediación de vulnerabilidad requerida, así mismo cada grupo se divide por fases de la siguiente manera:



Detalle ciclo de vida del Proyecto		
Fase	**Nombre**	**Descripción**
Inicio	**Inicio del proyecto**	Inicio del proyecto
Etapa GC	**Gestion de contratos**	Contratos y proceso de licitación
Etapa I	**Servicios DNS externo y DHCP**	Configuraciones y recomendaciones para estos servicios
Etapa II	**Protección de borde I**	Implementaciones y ajustes sobre servicios publicados hacia internet, VPN, DMZ
Etapa III	**Protección de borde II**	Protección IPS (sistema de prevención de intrusos), DDOS (ataque de denegación de servicio distribuido)
Etapa IV	**Red LAN**	Ajustes, configuración e implementación nueva red LAN
Etapa V	**Protección de redes internas**	Filtrado de tráfico, ancho de banda y permisos de acceso
Etapa VI	**Filtrado web, anti spam y procedimientos**	Filtrado de contenidos web, implementación de procedimientos para la buena gestión de la oficina informática
Etapa VII	**Red WiFi, MPLS y Backup Satelital**	Implementación red Wifi, revisión de enlaces de respaldo con proveedores
Cierre		

Compañía Nacional del Petróleo

Alcance

Enunciado

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Autor: James Vallejo Mejia

Registro de cambios

Fecha	Versión	Descripción	Autor	Aprobación
23/03/2017	1	Enunciado	PM	
17/04/2018	2	Enunciado		

Contenido

Enunciado de alcance

1 Objetivo

El objetivo del presente proyecto es ejecutar remediaciones y optimizaciones a la infraestructura de Tecnología Informática (TI) de CNP (Compañía Nacional del petróleo) Argentina, para resolver las configuración de los servicios básicos de TI, las vulnerabilidades existentes asociadas a la seguridad informática y alinear las instalaciones a las mejores prácticas recomendadas.[1]

2 Definición del alcance

El alcance de la solicitud comprende la realización de todas las tareas según se describe a continuación en este documento, incluyendo la oferta de licitación y contratación de los proveedores necesarios para llevar a cabo cada dominio y lograr modernizar la infraestructura adecuadamente.

Se incluye realizar la compra de equipamiento necesario para llevar a cabo el proyecto. Así mismo se requiere una propuesta para brindar soporte especializado de la instalación, a ejecutarse con posterioridad de haber finalizado el proyecto mencionado en primer término.

En los casos donde la actividad requiera de la adquisición de elementos de hardware o software será responsabilidad del proveedor brindar las especificaciones técnicas y requerimientos para los mismos y CNP será el responsable de concretar las adquisiciones.

En los casos donde CNP deba realizar compra de materiales para continuar con la ejecución del proyecto, los plazos que sean requeridos para realizar la gestión de compra hasta la recepción de los mismos no serán contabilizados dentro del cronograma de actividades exigido al proveedor para la concreción de sus actividades.

Las actividades específicas de remediación abarcarán a las siguientes instalaciones de la empresa:

- Central Administrativa – Tucumán 1, CABA (BA)
- Oficina regional en Rio Gallegos - San Juan 641, Rio Gallegos, Santa Cruz (RGL)
- Base Recepción Magallanes – RP1 Km 10, Cabo Vírgenes, Santa Cruz (BRM

[1] Ver mayor detalle de las vulnerabilidades y hallazgos remitirse al documento A1_RIRCNP_Informe hallazgos vulnerabilidades y para antecedentes ver Acta constitutiva del proyecto. 104_ROIRCNP_Acta constitutiva

3 Proyecto de Remediación infraestructura de red y seguridad informática

Las tareas abarcadas en el proyecto son las que se detallan a continuación:

Como primera medida se menciona el hallazgo del informe de relevamiento, del cual se propone el plan de mejora, optimización o remediación de la vulnerabilidad [2]

Luego la tarea propuesta a realizar:

- Contratación de proveedores
  Invitación, Publicación de RFP, Selección y contratación

Servicios DNS Externo

- Servidor de DNS principal expuesto a Internet con todos los ports abiertos, sin sistema de protección de intrusos (IPS) y antivirus (AV)

  Propuesta: En la regla de publicación del servicio configurada en el firewall, habilitar la protección de IPS, el AV y también publicar solo los puertos necesarios para los servicios que brinda el servidor. En el caso del servicio de DNS, puertos tcp/53 y udp/53.

- Ajustar configuración de DNS secundario
  Propuesta: Ajustar la configuración del segundo DNS server para homogeneizar el servicio, según los ajustes que se realicen sobre el DNS primario.

- Un solo registro MX, no hay Mail Server secundario
  Propuesta: Implementar un Mail Server segundario, para que actúe en caso de fallar el principal.

Servicios DHCP

- No se cuenta con servicios DHCP en HA
  Propuesta: Implementar un DHCP Server secundario, para que actúe en caso de fallar el principal.

Protección de Borde

- Firewall de borde y VPN sin HA
  Propuesta: Implementar un clúster de firewall para borde y VPN en clúster de alta disponibilidad.

[2] Ver mayor detalle de las vulnerabilidades y hallazgos remitirse al documento A1_RIRCNP_Informe hallazgos y para antecedentes ver Acta constitutiva del proyecto. 103_ROIRCNP_Acta constitutiva

- ACLs entrantes y red DMZ
  Propuesta: Publicar en internet solo los puertos de los servicios que son necesarios y que se utilizan.

  Todas las aplicaciones y servicios publicados en internet deben estar en la red DMZ.

- Servicio Microsoft TNG esta discontinuado desde el 31/12/2015
  Propuesta: Implementar una alternativa tecnológica diferente al TNG, como por ejemplo un firewall UTM, como lo puede ser FortiGate o Cisco ASA.

- Se identifican publicaciones de servicios a Internet en cadena desde el FW Fortigate 200B y el TNG
  Propuesta: Realizar las adecuaciones para que los servicios sean publicados desde un único equipo y en forma directa.

- Servicios publicados en internet sin sistema de protección de intrusos (IPS), ni antivirus (AV) habilitados en el firewall.
  Propuesta: Realizar las adecuaciones para que todos los servicios publicados en internet cuenten con protección de IPS, AV y Denegación de Servicio.

<u>Protección de redes interna</u>

- El tráfico entre redes interna no pasa a través del firewall, por lo cual no se pueden aplicar políticas de seguridad sobre las mismas.
  Propuesta: Realizar las adecuaciones para que todo el tráfico entre redes de la empresa pase a través del firewall para tener control y poder aplicar políticas de seguridad sobre el mismo.

- El tráfico entre redes LAN-LAN y LAN-WAN no tiene aplicado IPS, AV o restricciones de ancho de banda.
  Propuesta: Aplicar IPS, AV, restricciones de ancho de banda, etc.

- No se cuenta con Protección de acceso a servidores y equipos de infraestructura/networking.
  Propuesta: Realizar las adecuaciones para prohibir el acceso a la infraestructura tecnológica a todas las redes excepto la red de informática. Crear una red exclusiva para los administradores del equipamiento de TI.

<u>WebFilter</u>

- Servicio de WebFiltering no está en HA
  Propuesta: Implementar un esquema de WebFiltering en alta disponibilidad.

- No se identifican procedimiento de backup de configuración
  Propuesta: Desarrollar las directrices de un procedimiento para que se realicen backup y controles periódicos sobre el equipamiento que comprende la infraestructura de TI.

Antivirus

- No se identifican procedimientos de backup de configuración ni control de cambios
  Propuesta: Desarrollar las directrices de un procedimiento para el control de cambios, para que se realicen copias de seguridad y controles periódicos sobre el equipamiento que comprende la infraestructura de TI.

Antispam

- La consola de Antispam no está en HA
  Propuesta: Implementar un esquema de Antispam en alta disponibilidad.

- No se identifican procedimientos de backup de configuración ni control de cambios
  Propuesta: Desarrollar las directrices de un procedimiento para el control de cambios, para que se realicen copias de seguridad y controles periódicos sobre el equipamiento que comprende la infraestructura de TI.

Procedimientos de Seguridad

- ABM cuentas de administrador
  Propuesta: Desarrollar las directrices de un procedimiento diferencial para el ABM de cuentas de administrador de domino.

Switch de red LAN

- No hay segmentación de vlans de para separar y controlar el tráfico entre servidores, servicios y usuarios
  Propuesta: Implementar segmentación por VLANs para red de usuarios y red de servidores. Realizar las adecuaciones para solo la red de administradores pueda ingresar a los servidores.

- Si bien se cuenta con equipos Layer3, no se están aplicando Vlans ni ruteo interno
  Propuesta: Configurar ruteo por capa 3 (nivel de red).

- Se cuenta con Switches L3 en stack, los switches en cascada están conectados solo a un port ethernet.
  Propuesta: Realizar las adecuaciones para utilizar otro puerto de backup en caso de falta en el puerto que está en uso, para evitar cortes de servicios de red.

- Acceso telnet habilitado, passwords no encriptadas en la configuración, acceso directo al “enable” en algunos casos.
  Propuesta: Realizar las adecuaciones para utilizar acceso SSH (secure shell) encriptado.

- Acceso a los equipos habilitado desde todas las redes, red de usuarios compartida con red de gestión de los equipos, IP de administración en la VLan 1 Nativa.
  Propuesta: Realizar las adecuaciones para no utilizar la vlan nativa para tráfico de red.

- Las impresoras están en la misma red que los usuarios y que los equipos de la infraestructura IT.
  Realizar las adecuaciones para asignar una red exclusiva para las impresoras.

- Falta Auditoria de cambios, accesos y backups periódicos
  Propuesta: Desarrollar las directrices de un procedimiento para el control de cambios, para que se realicen copias de seguridad y controles periódicos sobre el equipamiento que comprende la infraestructura de TI.

Red WiFi

- Seguridad WiFi con cifrado WEP vulnerable y obsoleto.
  Propuesta: Implementar cifrado WPA2 o WPA2/Enterprise.

- La red WiFi no está segmentada en red corporativa y red de invitados
  Propuesta: Implementar un SSID WiFi exclusivo para tareas corporativas y un SSID WiFi exclusivo para invitados.

- Desde la red WiFi se puede tener acceso a toda la infraestructura IT (firewalls, switch, servidores, videoconferencia, etc.)
  Propuesta: Implementar una VLAN de sistemas y permitirle solo a ella el acceso a switch, routers, servidores, etc.

Enlaces MPLS / Backup Satélite

- No se identifica claramente un procedimiento de activación/rollback de backup enlaces MPLS/Satelital
  Propuesta: Desarrollar un procedimiento implementar conmutación automática de enlace principal a enlace backup y viceversa.

- No se cuenta con notificación de activación/rollback de uso de enlaces MPLS/Satelital
  Propuesta: Interactuar con el proveedor de telecomunicaciones y coordinar la implementación de una conmutación automática de enlace principal a enlace backup y viceversa.

4 Entregables

Se detalla a continuación una lista mínima de entregables deseados por cada punto de adecuación contenido en este documento:

- Documento de configuración: enumeración del ajuste o configuración realizada, mapa conceptual de la configuración resultante, esquema gráfico, detalle de la versión del software, identificación de las actualizaciones incluidas y/o parches que quedaron instalados al momento de la finalización de la labor.
- Archivo en formato Microsoft Visio 2010 (o posterior) con el esquema y el detalle de configuración, incluyendo identificaciones de los componentes, identificación lógica, detalle de conexiones, rutas lógicas configuradas, interfaces, puertos utilizados, etc.
- Documentos con las directrices para el posterior desarrollo del procedimiento de configuración, control, backup y actuaciones operativas necesarias para el correcto mantenimiento y actualización del estándar.

5 Soporte de incidentes, mantenimiento preventivo y capacitación

Se requiere que el oferente presente una propuesta para brindar soporte, mantenimiento preventivo a la instalación y capacitación a los recursos de ES a partir del período de post-implementación del proyecto “Remediación y Optimización de la Plataforma”.

El alcance de este servicio será por 12 (doce) meses con opción de ser extendido por un período de idéntica duración.

La base de cálculo para el servicio será de 20 horas mensuales, que en el caso de no ser utilizadas se acumularán por 3 (tres) períodos consecutivos.

Las horas incluidas en este servicio podrán ser utilizadas a criterio de CNP para obtener soporte de incidentes, realizar mejoras o actualizaciones sobre el sistema de almacenamiento y obtener capacitación de sus recursos.

Se espera que el oferente brinde capacitación a los recursos de ES para la resolución del nivel 1 de los incidentes que se presenten y demás actividades básicas para la correcta operación de los componentes de la plataforma. Consecuentemente, se reserva para el oferente el servicio de soporte y la resolución de los incidentes que superen el nivel básico y la gestión de solución con el fabricante en los casos que corresponda.

6 Actualización del alcance

Ninguna modificación podrá efectuarse al presente, salvo que fuera hecha por escrito y con el mutuo acuerdo de las partes, en su respectivo control de cambios.

7 Supuestos

Supuesto	Descripción
La información acerca del equipamiento y servicios actuales de red se encuentran totalmente relavados,	previamente en el proyecto de relevamiento de información de la infraestructura TI, se realizó inventario de los equipos pertenecientes a la infraestructura de red
Usuarios informados del proyecto previo a su inicio	El personal administrativo y operativo debe estar informado del proyecto, en una fase previa al inicio
Compatibilidad de equipos	Se espera que todos los equipos sean compatibles y puedan negociar correctamente, los que así lo requieran
Licenciamiento de equipamiento	Con la compra de equipos se debe brindar adquirir su respectiva licencia de acuerdo al fabricante, por lo menos por un año.
Alimentación eléctrica	Se debe contar con red eléctrica regulada y con UPS de Respaldo, para evitar apagados forzados y evitar daños en los equipos.
Entorno de virtualización	Se debe contar con un entorno de virtualización para la creación de máquinas virtuales de los servidores de DNS, DHCP y los que sean requeridos para el proyecto
Invitación a proveedores conocidos	Para la elección de proveedores, se tiene una lista de proveedores conocidos y recomendados por la organización.

8 Restricciones

Restricciones	Descripción
Alineación del proyecto con metodología ITIL	Tanto procedimientos como proveedores deben ir alineados a las recomendaciones ITIL (nformation Technology Infrastructure Library) marco de trabajo de buenas prácticas aplicables a la Gestión de Servicios de TI. [3]
Alineación del proyecto con normas ISO 27001 (Seguridad de la información)	Cumplir con los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de Gestión de la información ISO 27001[4]
Seguridad industrial	Los proveedores deben cumplir con las normas de Seguridad Industrial
Horario	Las tareas se podrán realizar en días hábiles y en horarios de oficina, salvo aquellas actividades que puedan ocasionar alguna disrupción de los servicios de TI. En los casos donde exista riesgo de disrupción de los servicios, se definirá la mejor oportunidad para realizar las actividades fuera de los horarios habituales

9 Requisitos

Requisitos	Descripción
Disponibilidad del personal de proyecto	Como requisitos para la contratación a los proveedores se les solicitará disponibilidad del personal, en caso de cualquier issue, durante la ejecución de alguna tarea
Plazos de entregables	Se reserva un plazo de 5 (cinco) días hábiles para analizar la información y prestar conformidad para dar por finalizada la etapa o hito y sus tareas asociadas y realizar el documento de certificación correspondiente (HES) para el posterior pago de los servicios, en los casos en que corresponda.

[3] (Axelos, s.f.)

[4] (ISO, s.f.)

10 Priorización de los Objetivos

Se define la siguiente priorización de los Objetivos:

	Costo	Plazo	Alcance
Debe lograrse			
Conviene lograrse			
Acepto resultado			

Se debe cumplir el proyecto dentro del tiempo planificado, ya que se deben ejecutar otros proyectos del programa ***Remediación infraestructura informática y servicios TI,*** los cuales tienen fechas pactadas para su inicio; El alcance conviene lograrse, pudiendo cambiar alguna actividad por injerencia de la dirección o proveedores, pactado previamente y registrado correctamente en el control de cambios, El aumento en el costo se acepta si se llega a exceder el presupuesto.

11 Exclusiones

Exclusiones	Descripción
Remediación y optimización en entornos virtuales, monitoreo de las plataformas, entornos Microsoft, SQL server, storage y comunicaciones	Esta remediación hace parte del programa y se gestiona mediante otros proyectos.
Intervención sobre la red eléctrica	Previo a la realización del proyecto se debe asegurar que se cuenta con red eléctrica regulada, planta eléctrica de respaldo y UPS, para protección de los dispositivos de red. No se contempla dentro del alcance ninguna intervención sobre la red eléctrica
Cableado estructurado	CNP cede el contrato de Cableado eléctrico a un proveedor externo, que debe entregar lo relacionado en tiempo para la implementación de red de este proyecto, cualquier actividad relacionada se encuentra fuera del alcance.
Red WAN de proveedores	Los proveedores son stakeholders del proyecto y estarán involucrados en las actividades y requerimientos dentro del alcance del proyecto. Sin embargo no hace parte del proyecto la intervención, configuración y demás de equipos de la red WAN.
Solicitudes TI de otros países	El proyecto solo involucra las actividades mencionadas dentro del alcance, esta fuera cualquier solicitud por parte de directores o cualquier persona de otro país, sin previo registro en control de cambios y con la aprobación de la dirección de TI CNP AR, y la dirección PMO.

Compañía Nacional del Petróleo

Alcance

EDT

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Autor: James Vallejo Mejia

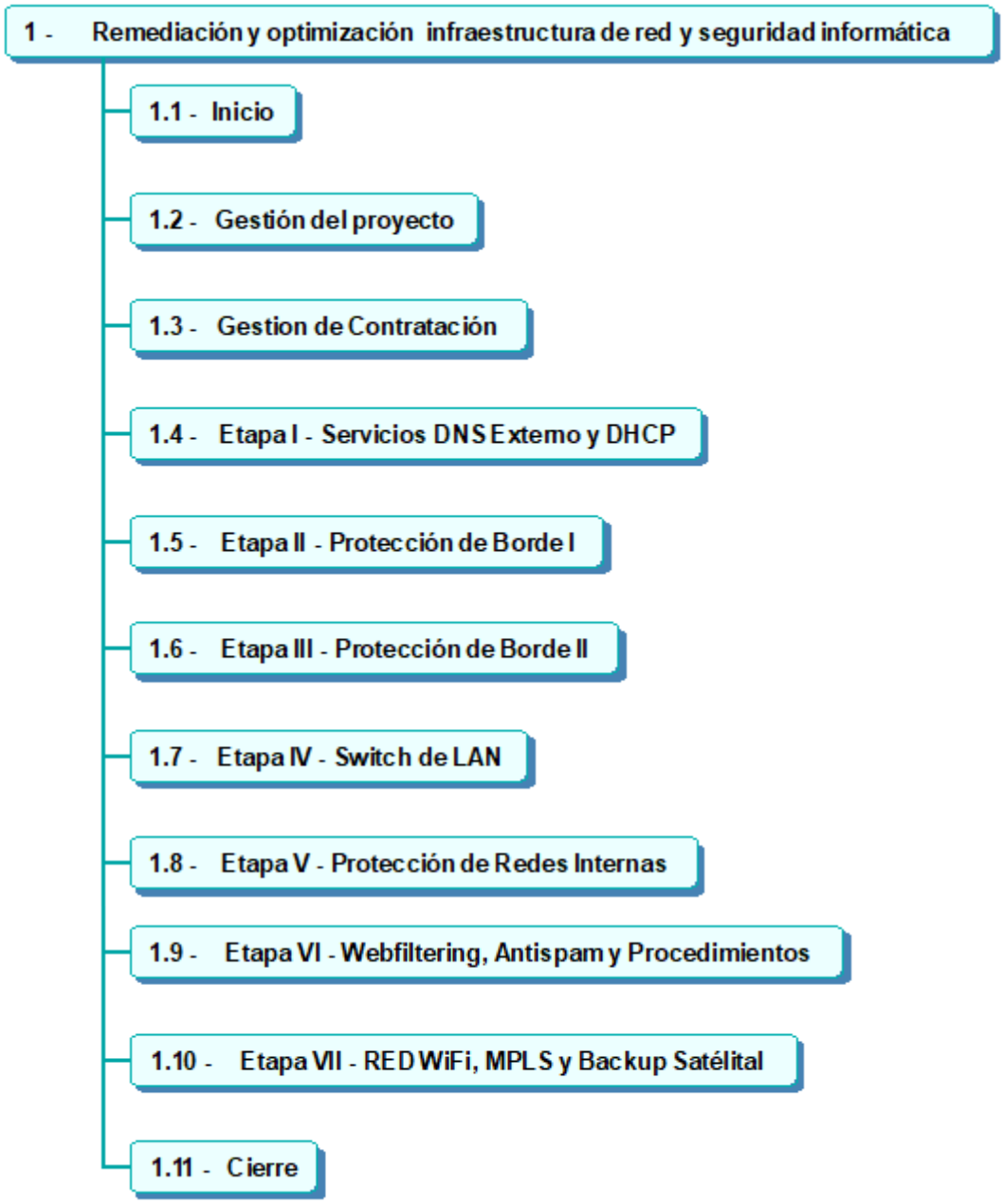
Registro de cambios

Fecha	Versión	Descripción	Autor	Aprobación
23/3/2017	1	EDT	PM	
17/04/2017	2	EDT		

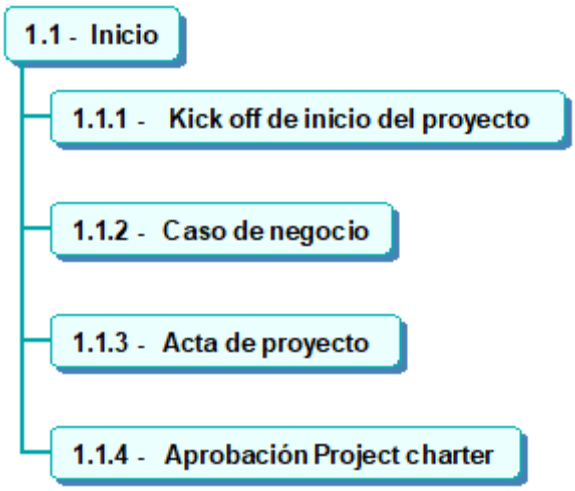
Contenido

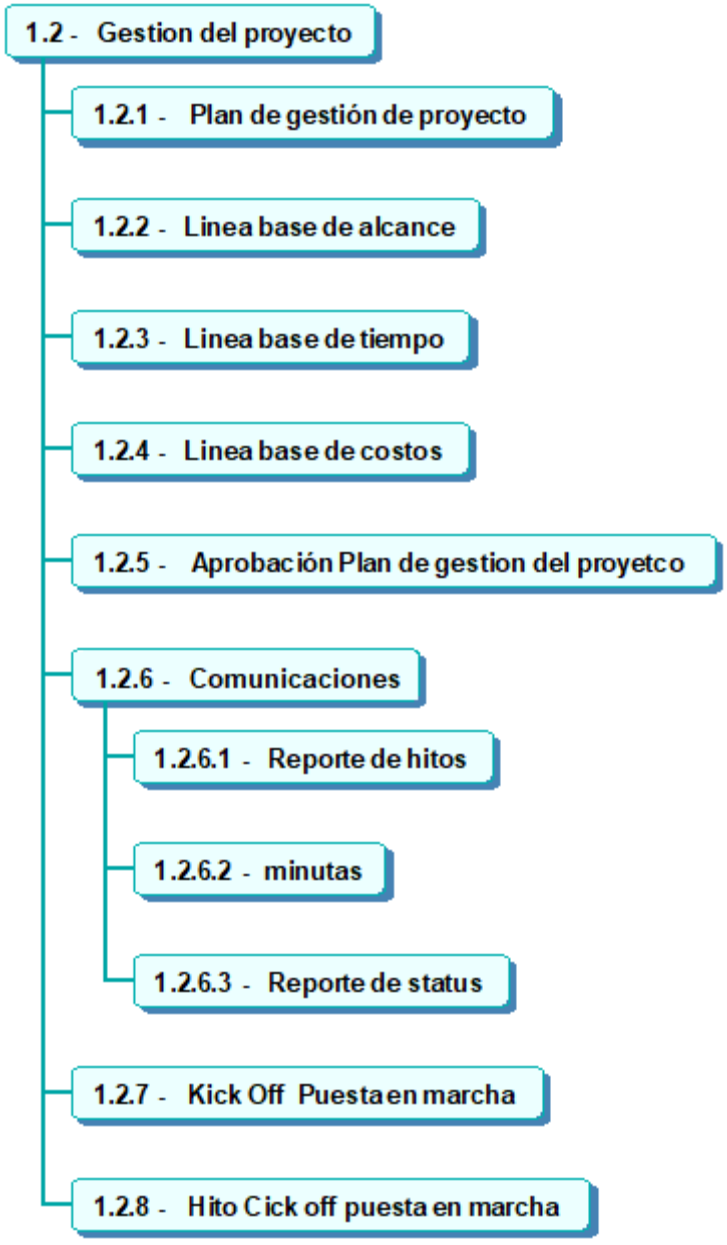
EDT

1 EDT nivel 1

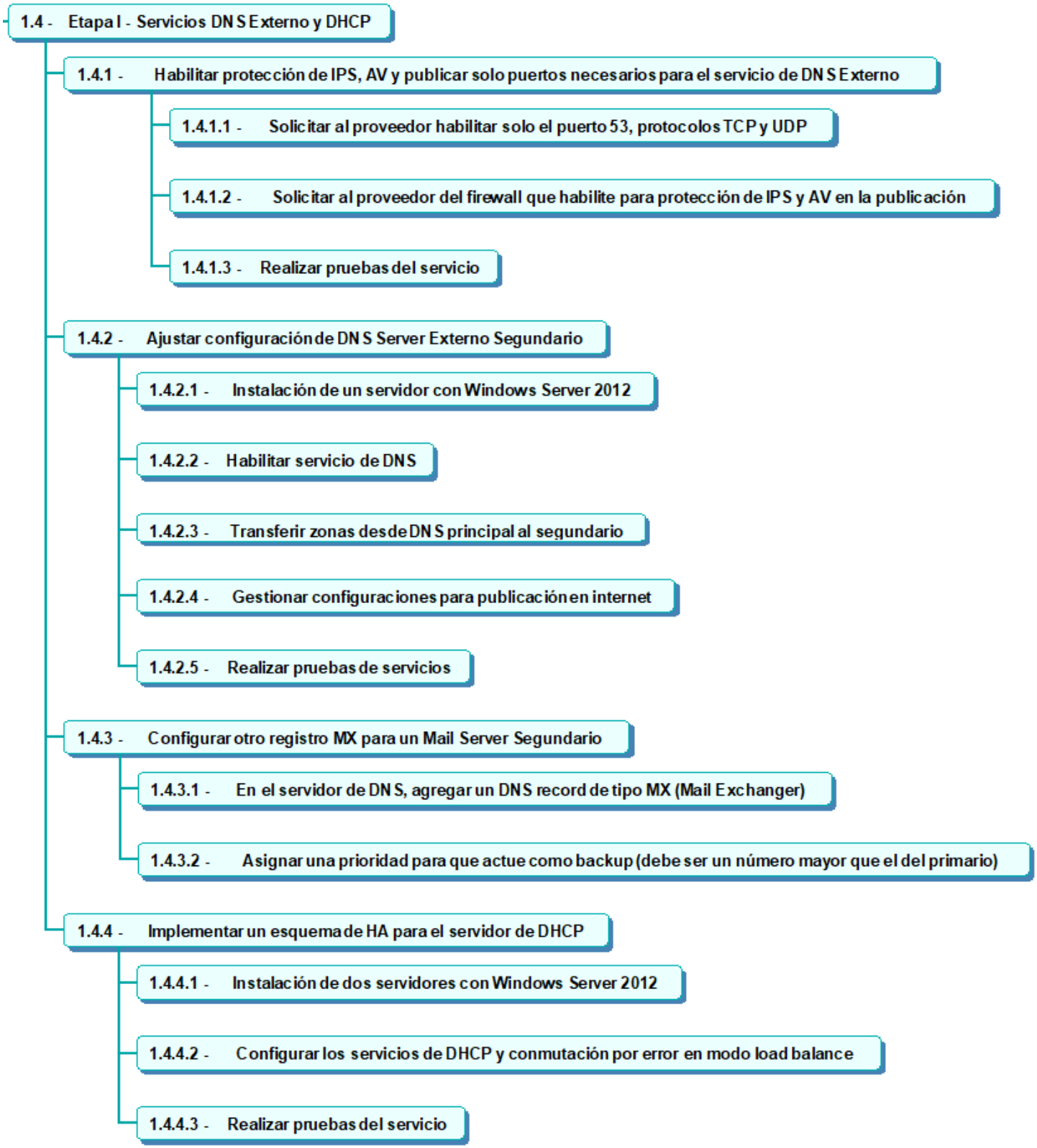


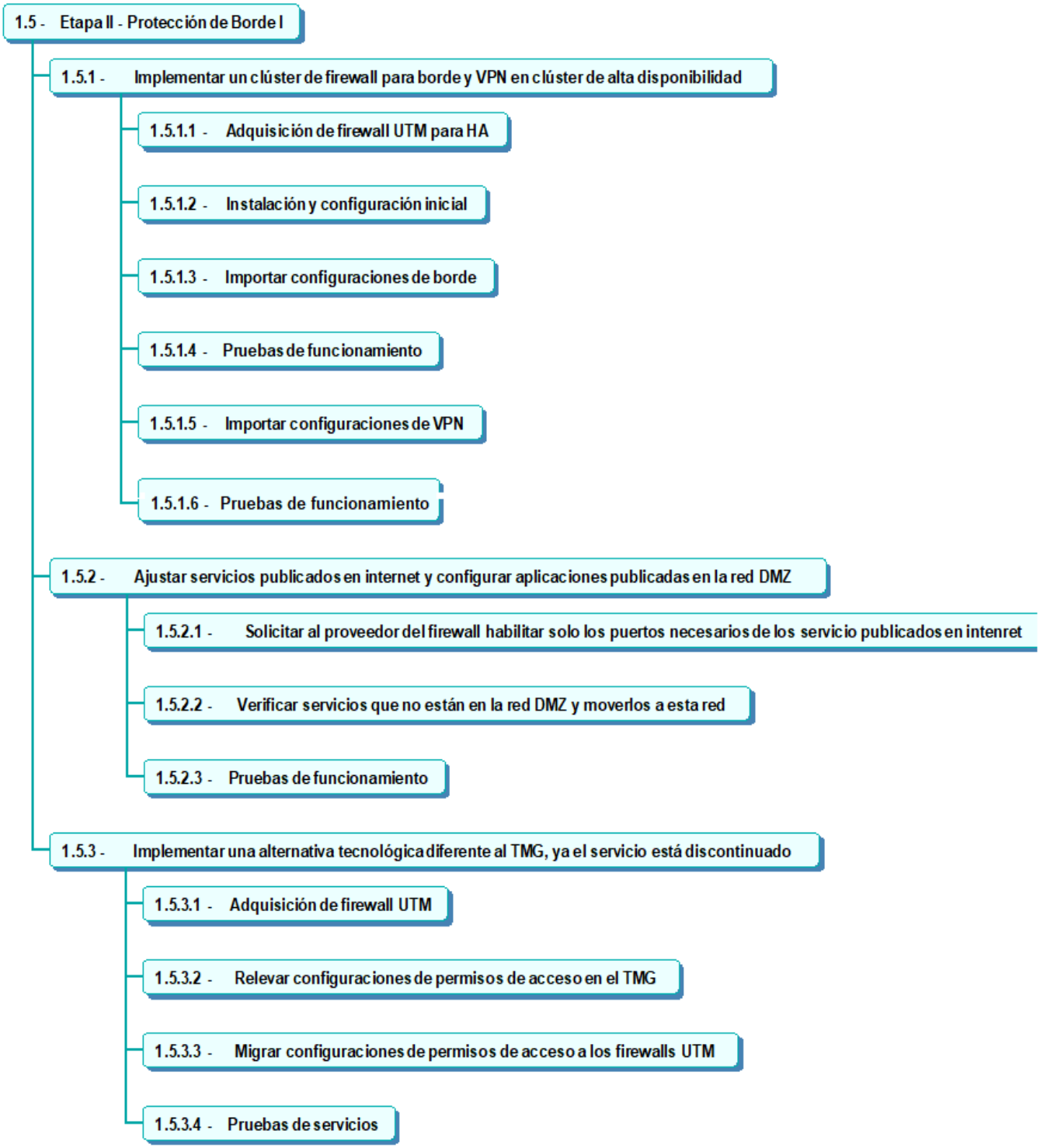
2 EDT Niveles 2 y 3

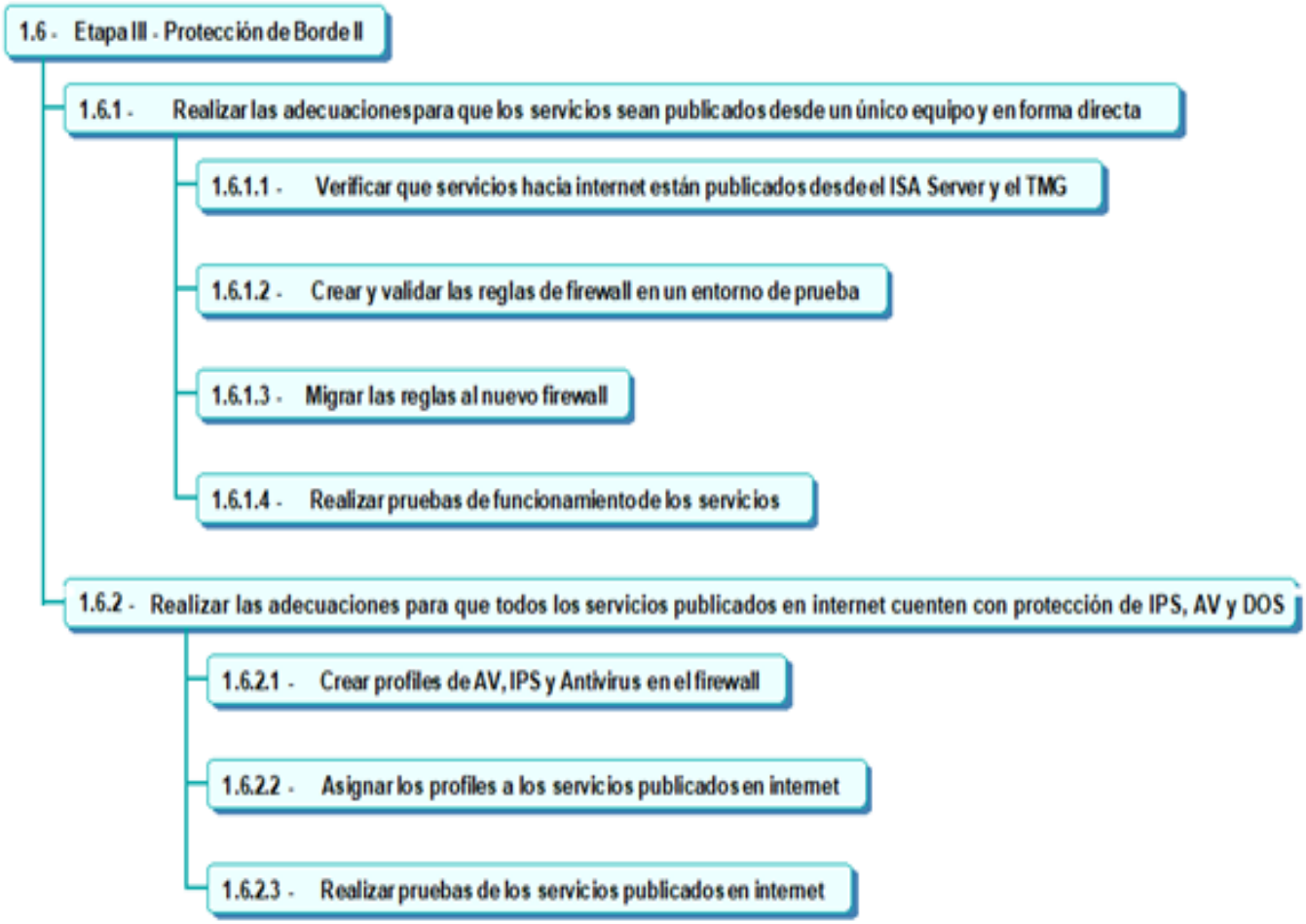


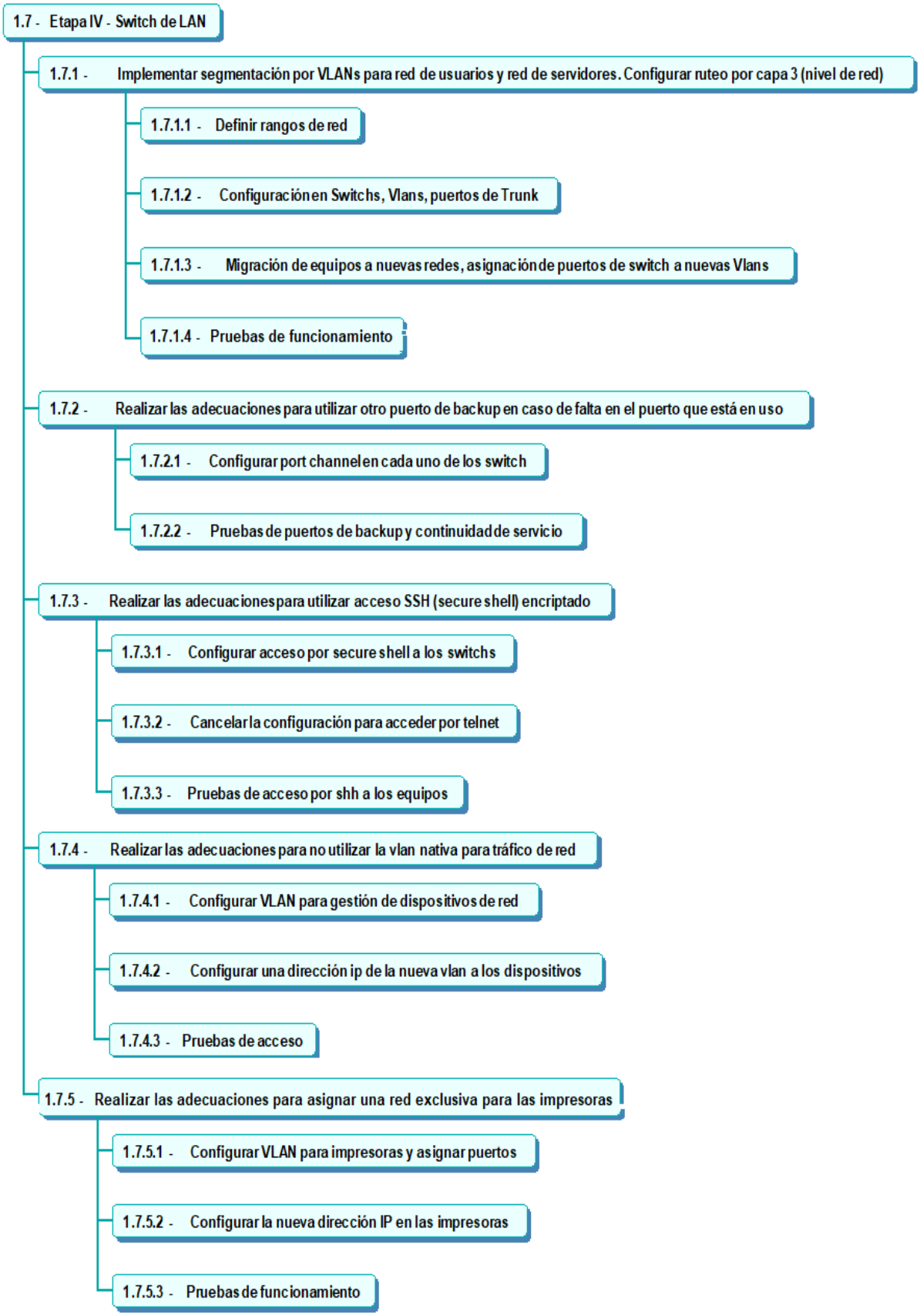

1.2 - Gestion del proyecto
1.2.1 - Plan de gestión de proyecto
1.2.2 - Linea base de alcance
1.2.3 - Linea base de tiempo
1.2.4 - Linea base de costos
1.2.5 - Aprobación Plan de gestion del proyetco
1.2.6 - Comunicaciones
1.2.6.1 - Reporte de hitos
1.2.6.2 - minutas
1.2.6.3 - Reporte de status
1.2.7 - Kick Off Puesta en marcha
1.2.8 - Hito Cick off puesta en marcha

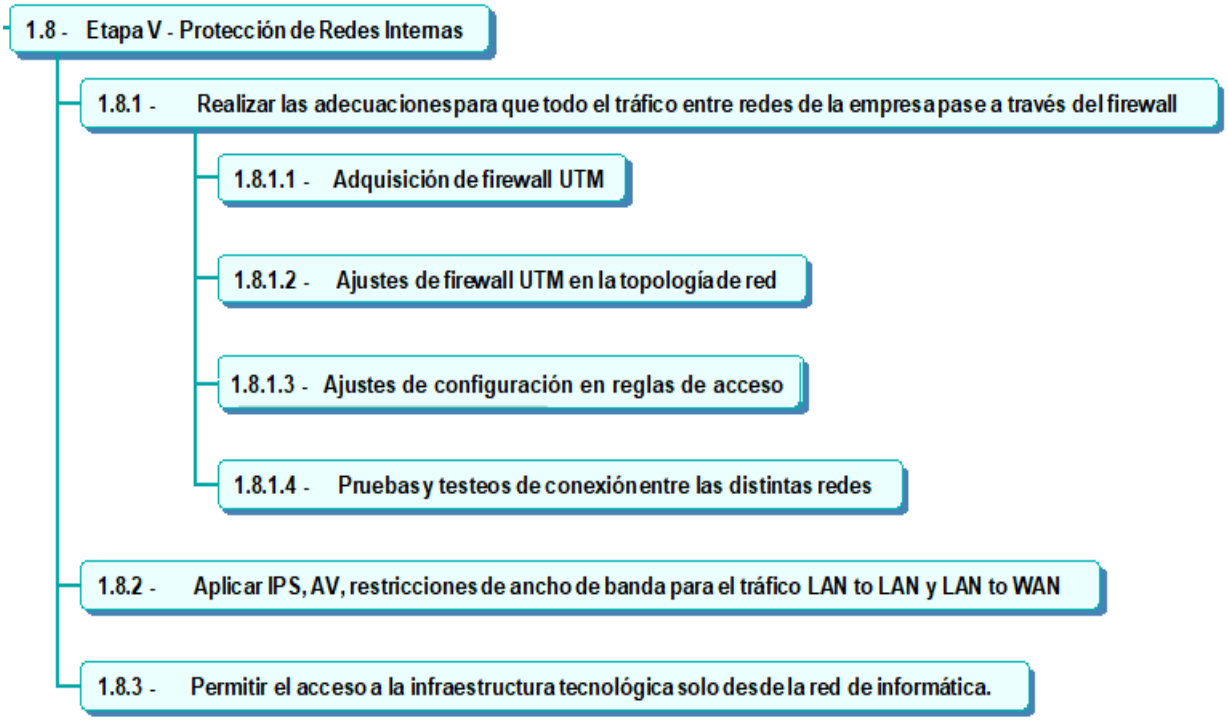

1.3 - Gestion de Contratación
1.3.1 - Búsqueda del proveedor
1.3.1.1 - Invitacion a proveedores
1.3.1.2 - RFP (Request for Proposal)
1.3.1.3 - Análisis y Selección de proveedores
1.3.2 - Contratación

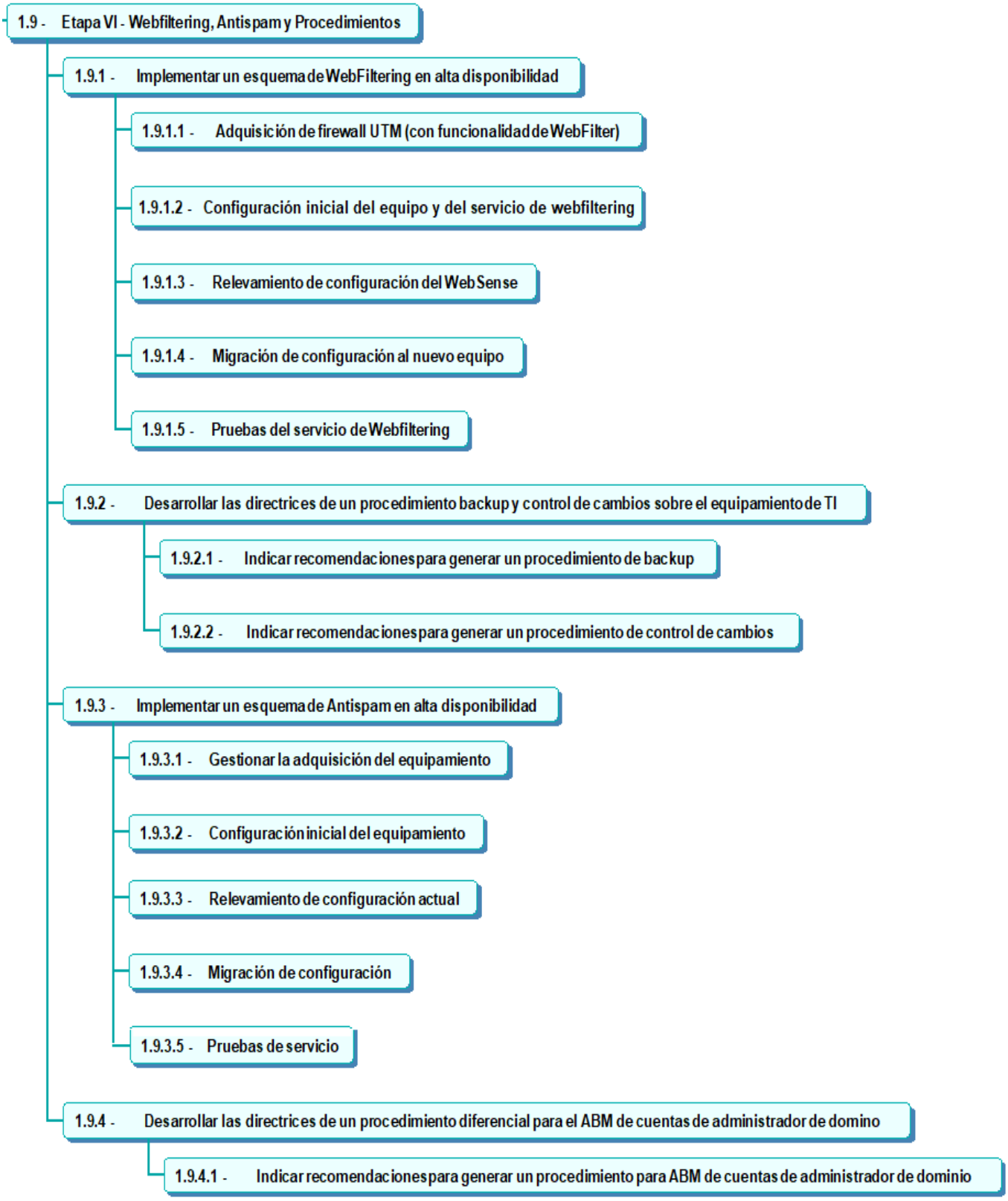

1.4 - Etapa I - Servicios DNS Externo y DHCP
1.4.1 - Habilitar protección de IPS, AV y publicar solo puertos necesarios para el servicio de DNS Externo
1.4.1.1 - Solicitar al proveedor habilitar solo el puerto 53, protocolos TCP y UDP
1.4.1.2 - Solicitar al proveedor del firewall que habilite para protección de IPS y AV en la publicación
1.4.1.3 - Realizar pruebas del servicio
1.4.2 - Ajustar configuración de DNS Server Externo Segundario
1.4.2.1 - Instalación de un servidor con Windows Server 2012
1.4.2.2 - Habilitar servicio de DNS
1.4.2.3 - Transferir zonas desde DNS principal al segundario
1.4.2.4 - Gestionar configuraciones para publicación en internet
1.4.2.5 - Realizar pruebas de servicios
1.4.3 - Configurar otro registro MX para un Mail Server Segundario
1.4.3.1 - En el servidor de DNS, agregar un DNS record de tipo MX (Mail Exchanger)
1.4.3.2 - Asignar una prioridad para que actue como backup (debe ser un número mayor que el del primario)
1.4.4 - Implementar un esquema de HA para el servidor de DHCP
1.4.4.1 - Instalación de dos servidores con Windows Server 2012
1.4.4.2 - Configurar los servicios de DHCP y conmutación por error en modo load balance
1.4.4.3 - Realizar pruebas del servicio

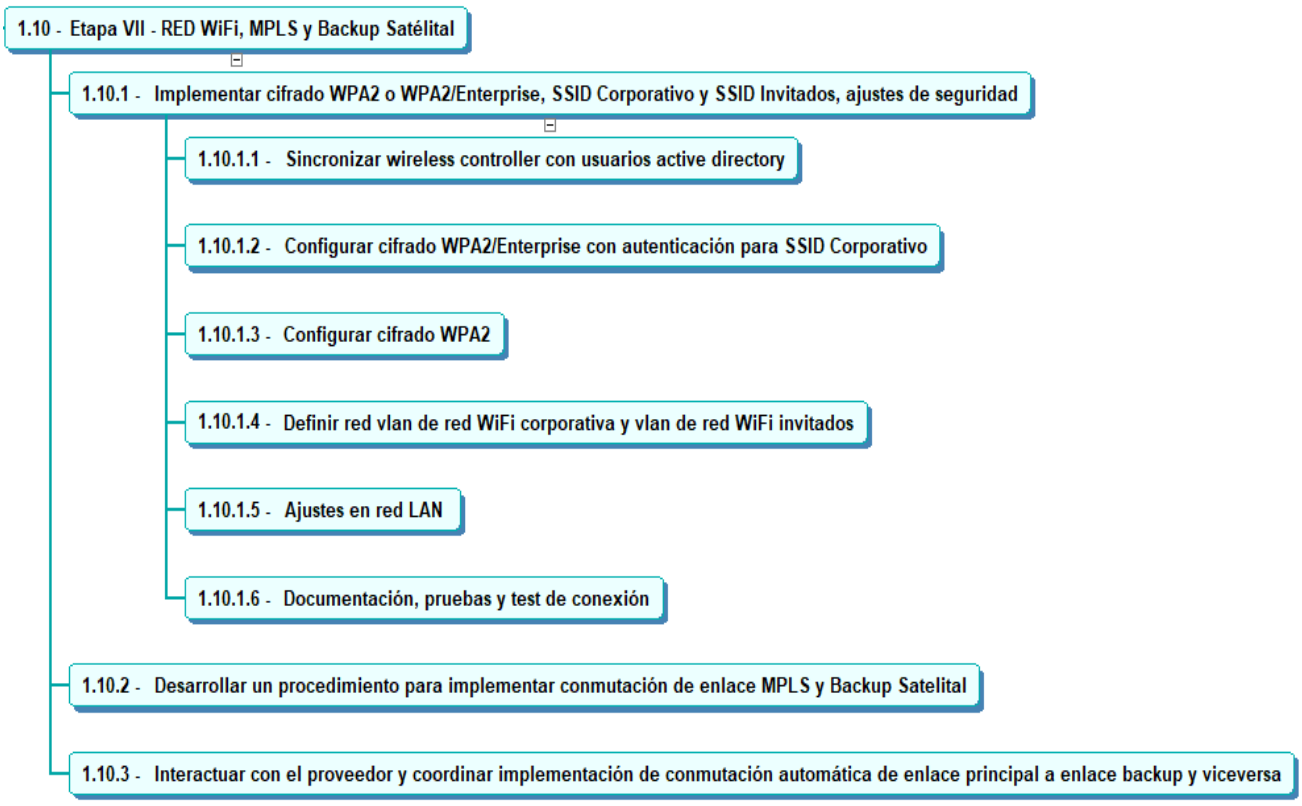

1.5 - Etapa II - Protección de Borde I
1.5.1 - Implementar un clúster de firewall para borde y VPN en clúster de alta disponibilidad
1.5.1.1 - Adquisición de firewall UTM para HA
1.5.1.2 - Instalación y configuración inicial
1.5.1.3 - Importar configuraciones de borde
1.5.1.4 - Pruebas de funcionamiento
1.5.1.5 - Importar configuraciones de VPN
1.5.1.6 - Pruebas de funcionamiento
1.5.2 - Ajustar servicios publicados en internet y configurar aplicaciones publicadas en la red DMZ
1.5.2.1 - Solicitar al proveedor del firewall habilitar solo los puertos necesarios de los servicio publicados en intenret
1.5.2.2 - Verificar servicios que no están en la red DMZ y moverlos a esta red
1.5.2.3 - Pruebas de funcionamiento
1.5.3 - Implementar una alternativa tecnológica diferente al TMG, ya el servicio está discontinuado
1.5.3.1 - Adquisición de firewall UTM
1.5.3.2 - Relevar configuraciones de permisos de acceso en el TMG
1.5.3.3 - Migrar configuraciones de permisos de acceso a los firewalls UTM
1.5.3.4 - Pruebas de servicios

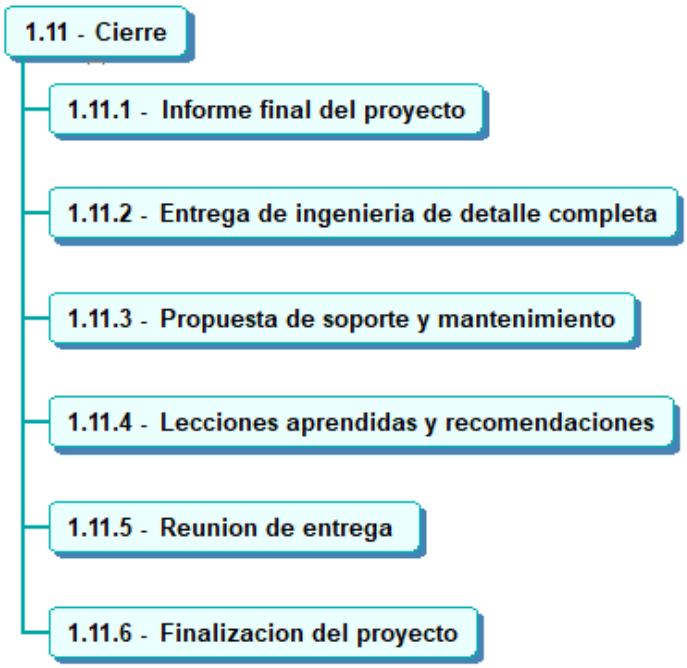

1.6 - Etapa III - Protección de Borde II
1.6.1 - Realizar las adecuaciones para que los servicios sean publicados desde un único equipo y en forma directa
1.6.1.1 - Verificar que servicios hacia internet están publicados desde el ISA Server y el TMG
1.6.1.2 - Crear y validar las reglas de firewall en un entorno de prueba
1.6.1.3 - Migrar las reglas al nuevo firewall
1.6.1.4 - Realizar pruebas de funcionamiento de los servicios
1.6.2 - Realizar las adecuaciones para que todos los servicios publicados en internet cuenten con protección de IPS, AV y DOS
1.6.2.1 - Crear profiles de AV, IPS y Antivirus en el firewall
1.6.2.2 - Asignar los profiles a los servicios publicados en internet
1.6.2.3 - Realizar pruebas de los servicios publicados en internet


1.7 - Etapa IV - Switch de LAN
1.7.1 - Implementar segmentación por VLANs para red de usuarios y red de servidores. Configurar ruteo por capa 3 (nivel de red)
1.7.1.1 - Definir rangos de red
1.7.1.2 - Configuración en Switchs, Vlans, puertos de Trunk
1.7.1.3 - Migración de equipos a nuevas redes, asignación de puertos de switch a nuevas Vlans
1.7.1.4 - Pruebas de funcionamiento
1.7.2 - Realizar las adecuaciones para utilizar otro puerto de backup en caso de falta en el puerto que está en uso
1.7.2.1 - Configurar port channel en cada uno de los switch
1.7.2.2 - Pruebas de puertos de backup y continuidad de servicio
1.7.3 - Realizar las adecuaciones para utilizar acceso SSH (secure shell) encriptado
1.7.3.1 - Configurar acceso por secure shell a los switchs
1.7.3.2 - Cancelar la configuración para acceder por telnet
1.7.3.3 - Pruebas de acceso por shh a los equipos
1.7.4 - Realizar las adecuaciones para no utilizar la vlan nativa para tráfico de red
1.7.4.1 - Configurar VLAN para gestión de dispositivos de red
1.7.4.2 - Configurar una dirección ip de la nueva vlan a los dispositivos
1.7.4.3 - Pruebas de acceso
1.7.5 - Realizar las adecuaciones para asignar una red exclusiva para las impresoras
1.7.5.1 - Configurar VLAN para impresoras y asignar puertos
1.7.5.2 - Configurar la nueva dirección IP en las impresoras
1.7.5.3 - Pruebas de funcionamiento


1.8 - Etapa V - Protección de Redes Internas
1.8.1 - Realizar las adecuaciones para que todo el tráfico entre redes de la empresa pase a través del firewall
1.8.1.1 - Adquisición de firewall UTM
1.8.1.2 - Ajustes de firewall UTM en la topología de red
1.8.1.3 - Ajustes de configuración en reglas de acceso
1.8.1.4 - Pruebas y testeos de conexión entre las distintas redes
1.8.2 - Aplicar IPS, AV, restricciones de ancho de banda para el tráfico LAN to LAN y LAN to WAN
1.8.3 - Permitir el acceso a la infraestructura tecnológica solo desde la red de informática.


1.9 - Etapa VI - Webfiltering, Antispam y Procedimientos
1.9.1 - Implementar un esquema de WebFiltering en alta disponibilidad
1.9.1.1 - Adquisición de firewall UTM (con funcionalidad de WebFilter)
1.9.1.2 - Configuración inicial del equipo y del servicio de webfiltering
1.9.1.3 - Relevamiento de configuración del WebSense
1.9.1.4 - Migración de configuración al nuevo equipo
1.9.1.5 - Pruebas del servicio de Webfiltering
1.9.2 - Desarrollar las directrices de un procedimiento backup y control de cambios sobre el equipamiento de TI
1.9.2.1 - Indicar recomendaciones para generar un procedimiento de backup
1.9.2.2 - Indicar recomendaciones para generar un procedimiento de control de cambios
1.9.3 - Implementar un esquema de Antispam en alta disponibilidad
1.9.3.1 - Gestionar la adquisición del equipamiento
1.9.3.2 - Configuración inicial del equipamiento
1.9.3.3 - Relevamiento de configuración actual
1.9.3.4 - Migración de configuración
1.9.3.5 - Pruebas de servicio
1.9.4 - Desarrollar las directrices de un procedimiento diferencial para el ABM de cuentas de administrador de domino
1.9.4.1 - Indicar recomendaciones para generar un procedimiento para ABM de cuentas de administrador de dominio


1.10 - Etapa VII - RED WiFi, MPLS y Backup Satélital
1.10.1 - Implementar cifrado WPA2 o WPA2/Enterprise, SSID Corporativo y SSID Invitados, ajustes de seguridad
1.10.1.1 - Sincronizar wireless controller con usuarios active directory
1.10.1.2 - Configurar cifrado WPA2/Enterprise con autenticación para SSID Corporativo
1.10.1.3 - Configurar cifrado WPA2
1.10.1.4 - Definir red vlan de red WiFi corporativa y vlan de red WiFi invitados
1.10.1.5 - Ajustes en red LAN
1.10.1.6 - Documentación, pruebas y test de conexión
1.10.2 - Desarrollar un procedimiento para implementar conmutación de enlace MPLS y Backup Satelital
1.10.3 - Interactuar con el proveedor y coordinar implementación de conmutación automática de enlace principal a enlace backup y viceversa


1.11 - Cierre
1.11.1 - Informe final del proyecto
1.11.2 - Entrega de ingenieria de detalle completa
1.11.3 - Propuesta de soporte y mantenimiento
1.11.4 - Lecciones aprendidas y recomendaciones
1.11.5 - Reunion de entrega
1.11.6 - Finalizacion del proyecto

Compañía Nacional del Petróleo

Alcance

Diccionario EDT

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Autor: James Vallejo Mejia

Registro de cambios

Fecha	Versión	Descripción	Autor	Aprobación
23/3/2017	1	Diccionario	PM	
17/04/2017	2	Diccionario		

Contenido

Diccionario EDT

Código EDT	**1.4.4.1**			
Paquete de trabajo	**Instalación de dos servidores con Windows Server 2012**			
Descripción	2 máquinas virtuales con sistema operativo Windows server 2012 de 64 bits con memoria RAM de 128 GB y disco duro de 2 TB.			
Entradas	Gestion de contratación		Código EDT	1.3
Criterio de verificación y validación	Instalación de las máquinas por parte del equipo técnico, verificación de funcionamiento		Responsable	Coordinador TI CNP
Contratistas	Proveedor Softcom			
Estimaciones	Fecha Inicio	30/06/2017	Fecha fin	10/7/2017
	Costo	Ver documento de presupuesto [1]		
Observaciones	Esfuerzo 150 horas			

[1] Ver detalle en el documento 202-1_ROIRCNP_Costo_Presupuesto

Código EDT	**1.5.1.2**			
Paquete de trabajo	**Instalación y configuración inicial**			
Descripción	2 firewalls Marca Cisco referencia Asa 5545, configurados en clúster con su respectivo failover, cableados, instalados en el rack de comunicaciones, conectados al Firewall de root Fortigate 200 D y Core Cisco 3850. Configuración inicial, direccionamiento de gestión preparada para la migración desde el firewall antiguo.			
Entradas	Gestion de contratación		Código EDT	1.3
	Adquisición de firewall UTM para HA		Código EDT	1.5.1.1
Criterio de verificación y validación	Pruebas de funcionalidad y administración local y remota		Responsable	Coordinador TI CNP AR y Coordinador TI CNP CL
Contratistas	Proveedor Tycon technologies			
Estimaciones	Fecha Inicio	10/07/2017	Fecha fin	18/07/2017
	Costo	Ver documento de presupuesto[2]		
Observaciones	Esfuerzo 50 horas			

[2] Ver detalle en el documento 202-1_ROIRCNP_Costo_Presupuesto

Código EDT	**1.6.2.1**			
Paquete de trabajo	**Crear profiles de AV, IPS y Antivirus en el firewall**			
Descripción	Perfiles de acuerdo a los grupos de usuarios definidos en el directorio activo, según el cargo del usuario. Se deben crear 4 grupos de perfiles Alto, medio, bajo y bloqueado. Cada uno con permisos de acuerdo a las necesidades corporativas, restricciones y seguridad informática.			
Entradas	Gestion de contratación y compras		Código EDT	1.3
	Realizar pruebas de funcionamiento de los servicios		Código EDT	1.6.1.4
Criterio de verificación y validación	Aprobación, una vez validadas las pruebas de funcionamiento		Responsable	Coordinador TI CNP
Contratistas	Proveedor Tycon technologies			
Estimaciones	Fecha Inicio	13/09/2017	Fecha fin	22/09/2017
	Costo	Ver documento de presupuesto[3]		
Observaciones	Esfuerzo 92 horas			

[3] Ver detalle en el documento 202-1_ROIRCNP_Costo_Presupuesto

Código EDT	**1.7.1.2**			
Paquete de trabajo	**Configuración en Switchs, Vlans, puertos de Trunk**			
Descripción	Instalación, configuración de los switches adquiridos marca cisco referencia 3850, 8 switches en stack, con sus respectivas troncales hacia equipos de borde, firewall marca fortinet 200D y Cisco ASA 5545; Debe quedar configurada Segmentación y asignación de puertos a las diferentes vlan de acuerdo al diseño realizado.			
Entradas	Gestion de contratación		Código EDT	1.3
	Definir rangos de red		Código EDT	1.7.1.1
Criterio de verificación y validación	Aprobación, una vez validadas las pruebas de funcionamiento		Responsable	Coordinador TI CNP
Contratistas	Proveedor Tycon technologies			
Estimaciones	Fecha Inicio	22/09/2017	Fecha fin	20/10/17
	Costo	Ver documento de presupuesto[4]		
Observaciones	Esfuerzo 41 horas			

[4] Ver detalle en el documento 202-1_ROIRCNP_Costo_Presupuesto

Código EDT	**1.9.2.2**			
Paquete de trabajo	**Indicar recomendaciones para generar un procedimiento de control de cambios**			
Descripción	Documento con la información necesaria para la implementación de un proceso de control de control de cambios en la oficina informática, comité de cambios, personal involucrado, herramientas, procesos y áreas que deberían formar parte.			
Criterio de verificación y validación	Aprobación, conformidad del documento		Responsable	Coordinador TI CNP
Contratistas	Proveedor Tycon technologies			
Estimaciones	Fecha Inicio	19/3/2018	Fecha fin	22/03/18
	Costo	Ver documento de presupuesto[5]		
Observaciones	Esfuerzo 25 horas			

[5] Ver detalle en el documento 202-1_ROIRCNP_Costo_Presupuesto

Compañía Nacional del Petróleo

Tiempo

Plan de gestión

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Autor: James Vallejo Mejia

Registro de cambios

Fecha	Versión	Descripción	Autor	Aprobación
23/3/2017	1	PM Tiempo	PM	
17/04/2017	2	PM Tiempo	PM	

Contenido

Plan de gestión del tiempo

1 Introducción

En el siguiente plan de gestión del tiempo se define la metodología a utilizar para establecer el plazo del proyecto y su cumplimiento, tratando de no afectar las demás variables.

El resultado de este documento tiene como salida principal el cronograma del proyecto; Se establece para comparar el avance proyectado, con el avance real y así controlar si hay desvíos para tomar las medidas necesarias, y que el proyecto culmine en el tiempo deseado.

2 Definición, Secuenciación y duración de actividades

Para la secuenciación de actividades y la definición de duración del cronograma, se tomará como referencia la EDT aprobada del proyecto.

Para la planificación del cronograma se debe tener en cuenta la revisión de los entregables, recursos y la estimación de plazos, así al final se tendrá una línea base con respecto a la cual medir el avance.

Se identificarán los paquetes de trabajo que deben realizarse para completar cada entregable. Las actividades serán secuenciadas con el fin de determinar el orden de los paquetes de trabajo, y para asignar la relación entre las distintas actividades del proyecto.

La duración de las actividades será estimada por analogía (según la técnica top down), y mediante la técnica PERT (Program Evaluation and Review Technique) o estimación de tres valores (valor más probable, valor optimista y valor pesimista). La estimación de las actividades es necesaria con el fin de calcular la duración en horas para completar cada paquete de trabajo. La estimación efectuada contendrá su respectiva reserva de contingencia (buffers), que eventualmente permitirán comprimir la duración de algunas tareas, o solaparlas entre sí a los fines de lograr una reducción en la duración total del proyecto. Sin embargo el Project Manager deberá, analizar cualquier pedido de reducción de la duración del proyecto, de modo de determinar el impacto en la planificación efectuada.

3 Estimación de recursos

Para estimar el tipo y cantidad de recursos y materiales requeridos para ejecutar las actividades se utilizan como herramientas el juicio de expertos, análisis de alternativas y estimación ascendente

En el caso de este proyecto, se tendrán en cuenta los recursos requeridos por cada paquete de trabajo, En general estos son los tipos de recursos que se estiman durante la ejecución del proyecto:

Recurso	
Analista de Comunicaciones Junior	Proveedores e infraestructura TI
Analista de comunicaciones Senior	Proveedores e infraestructura TI
Personal administrativo	Proveedores e infraestructura TI

Los proveedores dispondrán del número de recursos requeridos de acuerdo a las horas asignadas para cada actividad.

4 Herramientas y software de gestión

Para la representación del cronograma y su gestión se usará como modelo de programación la herramienta de MS Project, tanto proveedores, asesores y el equipo del proyecto estarán alineados al trabajo con esta herramienta para lograr un estándar y llevar el correcto control.

Se podrá tener una vista gráfica, mediante un diagrama de Gantt, donde se representan todas las actividades y su duración a lo largo del tiempo. La información mínima para realizar dicha representación es la siguiente: actividad, duración de la actividad, fechas de inicio y fin, recurso, predecesoras.
También será posible ver los hitos y revisar la información detallada de acuerdo a lo requerido.

5 Seguimiento y control

Para determinar la duración del proyecto, se usa el camino crítico, con este método es posible estimar la duración mínima del proyecto; además validar cuales son las tareas a las que se presentará mayor atención por parte de la PMO, y así evitar demoras en el proyecto.

Alguna variación en la ruta crítica tendrá impacto, en la finalización del proyecto, es por ello importante gestionar atentamente las actividades dentro de las rutas críticas.

Otras herramientas a utilizar:

- Revisión del Desempeño (Análisis de tendencias, Método de la Ruta Crítica, Método de la Cadena Critica, Indicadores y Gestión del Valor Ganado)
- Técnicas de Optimización de Recursos
- Compresión del Cronograma

Dependiendo del paquete de trabajo se establecerá el punto de control requerido, estos puntos de control deben estar contemplados en el cronograma (semanal, quincenal y mensual). La variación del cronograma, junto con la revisión de los informes de avance, los resultados de las medidas de desempeño y las modificaciones del cronograma se llevarán a cabo mediante las solicitudes de cambio RFC.

6 Hitos

Se deben definir los puntos de control para la revisión del avance y el cierre de cada fase del proyecto. Se deben ejecutar todas las actividades dentro de las fechas establecidas, ya que de no ser así, se retrasará la finalización del proyecto, Ya que el camino crítico comprende un número importante de actividades secuenciales, que se deben llevar a cabo a tiempo.

Compañía Nacional del Petróleo

Tiempo

Línea base de tiempo

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Autor: James Vallejo Mejia

Registro de cambios

Fecha	Versión	Descripción	Autor	Aprobación
23/3/2017	1	Línea base tiempo	PM	
17/04/2018	2	Línea base tiempo		

Línea base de tiempo

A continuación se presenta la línea base de tiempo que incluye:

- **Cronograma de actividades**
- **Duración de actividades**
- **Recursos**
- **Dependencias**
- **Camino critico (Tareas críticas en color amarillo)**
- **Holgura libre**
- **Hitos (Color Celeste)**

EDT	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Predecesoras EDT	Holgura Total	Nombres de los recursos
1	**Remediación Infraestructura y Seguridad Informática**	**223 días**	**lun 1/5/17**	**mar 3/4/18**			**1 día**	
1.1	Inicio	20 días	mar 2/5/17	mar 30/5/17			0 días	
1.1.1	Kick off de inicio del proyecto	1 día	mar 2/5/17	mar 2/5/17			19 días	
1.1.2	Caso de negocio	8 días	mar 2/5/17	jue 11/5/17			0 días	
1.1.3	Acta de proyecto	12 días	vie 12/5/17	mar 30/5/17	4	1.1.2	0 días	PMO
1.1.4	Aprobación Project charter	0 días	mar 30/5/17	mar 30/5/17	5	1.1.3	0 días	PMO
1.2	Gestion del proyecto	184 días	mar 30/5/17	jue 8/3/18	2	1.1	0 días	
1.2.1	Plan de gestión de proyecto	12 días	mié 31/5/17	jue 15/6/17			220 días	PMO
1.2.2	Línea base de alcance	12 días	mié 31/5/17	jue 15/6/17			220 días	PMO
1.2.3	Línea base de tiempo	12 días	mié 31/5/17	jue 15/6/17			220 días	PMO

1.2.4	Línea base de costos	12 días	mié 31/5/17	jue 15/6/17			220 días	PMO;Direccion General;Finanzas
1.2.5	Aprobación Plan de gestión del proyecto	0 días	mar 30/5/17	mar 30/5/17			232 días	PMO
1.2.6	Comunicaciones	184 días	mié 31/5/17	Lun 30/4/18	5	1.1.3	11 días	
1.2.6.1	Reporte de hitos	221 días	mié 31/5/17	Lun 30/4/18			11 días	PMO
1.2.6.2	minutas	221 días	mié 31/5/17	Lun 30/4/18			11 días	PMO
1.2.6.3	Reporte de status	221 días	mié 31/5/17	Lun 30/4/18			11 días	PMO
1.2.7	Kick Off Puesta en marcha	1 día	mié 31/5/17	mié 31/5/17			0 días	PMO;Direccion General
1.2.8	Hito Cick off puesta en marcha	0 días	mié 31/5/17	mié 31/5/17	17	1.2.7	231 días	PMO
1.3	Gestion de Contratación	31 días	jue 1/6/17	lun 17/7/17	17	1.2.7	0 días	
1.3.1	Búsqueda del proveedor	26 días	jue 1/6/17	lun 10/7/17			0 días	
1.3.1.1	Invitación a proveedores	3 días	jue 1/6/17	lun 5/6/17			0 días	PMO

1.3.1.2	RFP (Request for Proposal)	8 días	mar 6/6/17	jue 15/6/17	21	1.3.1.1	0 días	PMO
1.3.1.3	Análisis y Selección de proveedores	15 días	vie 16/6/17	lun 10/7/17	22	1.3.1.2	0 días	PMO
1.3.2	Contratación	5 días	mar 11/7/17	lun 17/7/17	23	1.3.1.3	0 días	Proveedor Tycon tech;Finanzas; Proveedor Softcom;Proveedor Telefónica
1.4	Etapa I - Servicios DNS Externo y DHCP	24 días	mar 18/7/17	lun 21/8/17	19	1.3	0 días	
1.4.1	Habilitar protección de IPS, AV y publicar solo puertos necesarios para el servicio de DNS Externo	5 días	mar 18/7/17	lun 24/7/17			0 días	
1.4.1.1	Solicitar al proveedor habilitar solo el puerto 53, protocolos TCP y UDP	5 días	mar 18/7/17	lun 24/7/17			0 días	Proveedor Softcom
1.4.1.2	Solicitar al proveedor del firewall que habilite para protección de IPS y AV en la publicación	5 días	mar 18/7/17	lun 24/7/17			0 días	Proveedor Softcom
1.4.1.3	Realizar pruebas del servicio	5 días	mar 18/7/17	lun 24/7/17			0 días	TI CNP; Proveedor Softcom
1.4.2	Ajustar configuración de DNS Server Externo Segundario	6 días	mar 25/7/17	mar 1/8/17	26	1.4.1	0 días	
1.4.2.1	Instalación de un servidor con Windows Server 2012	5 días	mar 25/7/17	lun 31/7/17			1 día	Proveedor Softcom

1.4.2.2	Habilitar servicio de DNS	5 días	mar 25/7/17	lun 31/7/17			1 día	Proveedor Softcom
1.4.2.3	Transferir zonas desde DNS principal al segundario	5 días	mar 25/7/17	lun 31/7/17			1 día	Proveedor Softcom
1.4.2.4	Gestionar configuraciones para publicación en internet	6 días	mar 25/7/17	mar 1/8/17			0 días	Proveedor Softcom
1.4.2.5	Realizar pruebas de servicios	6 días	mar 25/7/17	mar 1/8/17			0 días	Proveedor Softcom;TI CNP
1.4.3	Configurar otro registro MX para un Mail Server Segundario	7 días	mié 2/8/17	jue 10/8/17	30	1.4.2	0 días	
1.4.3.1	En el servidor de DNS, agregar un DNS record de tipo MX (Mail Exchanger)	7 días	mié 2/8/17	jue 10/8/17			0 días	Proveedor Softcom
1.4.3.2	Asignar una prioridad para que actúe como backup (debe ser un número mayor que el del primario)	7 días	mié 2/8/17	jue 10/8/17			0 días	Proveedor Softcom
1.4.4	Implementar un esquema de HA para el servidor de DHCP	6 días	vie 11/8/17	lun 21/8/17	36	1.4.3	0 días	
1.4.4.1	Instalación de dos servidores con Windows Server 2012	6 días	vie 11/8/17	lun 21/8/17			0 días	Proveedor Softcom
1.4.4.2	Configurar los servicios de DHCP y conmutación por error en modo load balance	6 días	vie 11/8/17	lun 21/8/17			0 días	Proveedor Softcom

1.4.4.3	Realizar pruebas del servicio	6 días	vie 11/8/17	lun 21/8/17			0 días	Proveedor Softcom;TI CNP
1.4.5	Finalización Etapa I	0 días	lun 21/8/17	lun 21/8/17	42	1.4.4.3	0 días	PMO
1.5	Etapa II - Protección de Borde I	34 días	mar 22/8/17	vie 6/10/17	25	1.4	0 días	
1.5.1	Implementar un clúster de firewall para borde y VPN en clúster de alta disponibilidad	6 días	mar 22/8/17	mar 29/8/17			0 días	
1.5.1.1	Adquisición de firewall UTM para HA	6 días	mar 22/8/17	mar 29/8/17			0 días	TI CNP;Proveedor Tycon tech
1.5.1.2	Instalación y configuración inicial	6 días	mar 22/8/17	mar 29/8/17			0 días	Proveedor Tycon tech
1.5.1.3	Importar configuraciones de borde	6 días	mar 22/8/17	mar 29/8/17			0 días	Proveedor Tycon tech
1.5.1.4	Pruebas de funcionamiento	6 días	mar 22/8/17	mar 29/8/17			0 días	Proveedor Tycon tech
1.5.1.5	Importar configuraciones de VPN	6 días	mar 22/8/17	mar 29/8/17			0 días	Proveedor Tycon tech
1.5.1.6	Pruebas de funcionamiento	6 días	mar 22/8/17	mar 29/8/17			0 días	Proveedor Tycon tech;TI CNP

1.5.2	Ajustar servicios publicados en internet y configurar aplicaciones publicadas en la red DMZ	11 días	mié 30/8/17	mié 13/9/17	45	1.5.1	0 días	
1.5.2.1	Solicitar al proveedor del firewall habilitar solo los puertos necesarios de los servicio publicados en internet	11 días	mié 30/8/17	mié 13/9/17			0 días	Proveedor Tycon tech;Proveedor Telefónica
1.5.2.2	Verificar servicios que no están en la red DMZ y moverlos a esta red	11 días	mié 30/8/17	mié 13/9/17			0 días	Proveedor Tycon tech
1.5.2.3	Pruebas de funcionamiento	11 días	mié 30/8/17	mié 13/9/17			0 días	Proveedor Tycon tech;TI CNP
1.5.3	Implementar una alternativa tecnológica diferente al TMG, ya el servicio está discontinuado	17 días	jue 14/9/17	vie 6/10/17	52	1.5.2	0 días	
1.5.3.1	Adquisición de firewall UTM	17 días	jue 14/9/17	vie 6/10/17			0 días	PMO;Proveedor Tycon tech
1.5.3.2	Relevar configuraciones de permisos de acceso en el TMG	17 días	jue 14/9/17	vie 6/10/17			0 días	Proveedor Tycon tech
1.5.3.3	Migrar configuraciones de permisos de acceso a los firewalls UTM	17 días	jue 14/9/17	vie 6/10/17			0 días	Proveedor Tycon tech
1.5.3.4	Pruebas de servicios	17 días	jue 14/9/17	vie 6/10/17			0 días	Proveedor Tycon tech;TI CNP
1.5.4	Finalización Etapa II	0 días	vie 6/10/17	vie 6/10/17	56	1.5.3	0 días	PMO
1.6	Etapa III - Protección de Borde II	19 días	mar 10/10/17	vie 3/11/17	44	1.5	0 días	

1.6.1	Realizar las adecuaciones para que los servicios sean publicados desde un único equipo y en forma directa	12 días	mar 10/10/17	mié 25/10/17			0 días	
1.6.1.1	Verificar que servicios hacia internet están publicados desde el ISA Server y el TMG	12 días	mar 10/10/17	mié 25/10/17			0 días	Proveedor Tycon tech
1.6.1.2	Crear y validar las reglas de firewall en un entorno de prueba	12 días	mar 10/10/17	mié 25/10/17			0 días	Proveedor Tycon tech
1.6.1.3	Migrar las reglas al nuevo firewall	12 días	mar 10/10/17	mié 25/10/17			0 días	Proveedor Tycon tech
1.6.1.4	Realizar pruebas de funcionamiento de los servicios	12 días	mar 10/10/17	mié 25/10/17			0 días	Proveedor Tycon tech;TI CNP
1.6.2	Realizar las adecuaciones para que todos los servicios publicados en internet cuenten con protección de IPS, AV y DOS	7 días	jue 26/10/17	vie 3/11/17	63	1.6.1	0 días	
1.6.2.1	Crear profiles de AV, IPS y Antivirus en el firewall	7 días	jue 26/10/17	vie 3/11/17			0 días	Proveedor Tycon tech
1.6.2.2	Asignar los profiles a los servicios publicados en internet	7 días	jue 26/10/17	vie 3/11/17			0 días	Proveedor Tycon tech
1.6.2.3	Realizar pruebas de los servicios publicados en internet	7 días	jue 26/10/17	vie 3/11/17			0 días	Proveedor Tycon tech;TI CNP
1.6.3	Finalización Etapa III	0 días	vie 3/11/17	vie 3/11/17	68	1.6.2	0 días	PMO

1.7	Etapa IV - Switch de LAN	31 días	lun 6/11/17	vie 5/1/18	62	1.6	0 días	
1.7.1	Implementar segmentación por VLANs para red de usuarios y red de servidores. Configurar ruteo por capa 3 (nivel de red)	19 días	lun 6/11/17	vie 1/12/17			0 días	
1.7.1.1	Definir rangos de red	19 días	lun 6/11/17	vie 1/12/17			0 días	Proveedor Tycon tech
1.7.1.2	Configuración en Switchs, Vlans, puertos de Trunk	19 días	lun 6/11/17	vie 1/12/17			0 días	Proveedor Tycon tech
1.7.1.3	Migración de equipos a nuevas redes, asignación de puertos de switch a nuevas Vlans	19 días	lun 6/11/17	vie 1/12/17			0 días	Proveedor Tycon tech
1.7.1.4	Pruebas de funcionamiento	19 días	lun 6/11/17	vie 1/12/17			0 días	Proveedor Tycon tech;TI CNP
1.7.2	Realizar las adecuaciones para utilizar otro puerto de backup en caso de falta en el puerto que está en uso	8 días	lun 4/12/17	vie 15/12/17	74	1.7.1	0 días	
1.7.2.1	Configurar port channel en cada uno de los switch	8 días	lun 4/12/17	vie 15/12/17			0 días	Proveedor Tycon tech
1.7.2.2	Pruebas de puertos de backup y continuidad de servicio	8 días	lun 4/12/17	vie 15/12/17			0 días	Proveedor Tycon tech
1.7.3	Realizar las adecuaciones para utilizar acceso SSH (secure shell) encriptado	4 días	lun 18/12/17	vie 5/1/18	79	1.7.2	0 días	

1.7.3.1	Configurar acceso por secure shell a los switchs	4 días	lun 18/12/17	vie 5/1/18			0 días	Proveedor Tycon tech
1.7.3.2	Cancelar la configuración para acceder por telnet	4 días	lun 18/12/17	vie 5/1/18			0 días	Proveedor Tycon tech
1.7.3.3	Pruebas de acceso por shh a los equipos	28 horas	lun 18/12/17	vie 5/1/18			4 horas	Proveedor Tycon tech;TI CNP
1.7.4	Realizar las adecuaciones para no utilizar la vlan nativa para tráfico de red	4 días	lun 4/12/17	jue 7/12/17	76	1.7.1.2	8 días	
1.7.4.1	Configurar VLAN para gestión de dispositivos de red	4 días	lun 4/12/17	jue 7/12/17			8 días	Proveedor Tycon tech
1.7.4.2	Configurar una dirección ip de la nueva vlan a los dispositivos	4 días	lun 4/12/17	jue 7/12/17			8 días	Proveedor Tycon tech
1.7.4.3	Pruebas de acceso	4 días	lun 4/12/17	jue 7/12/17			8 días	Proveedor Tycon tech;TI CNP
1.7.5	Realizar las adecuaciones para asignar una red exclusiva para las impresoras	4 días	lun 6/11/17	jue 9/11/17			27 días	
1.7.5.1	Configurar VLAN para impresoras y asignar puertos	4 días	lun 6/11/17	jue 9/11/17			27 días	Proveedor Tycon tech
1.7.5.2	Configurar la nueva dirección IP en las impresoras	4 días	lun 6/11/17	jue 9/11/17			27 días	Proveedor Tycon tech

1.7.5.3	Pruebas de funcionamiento	4 días	lun 6/11/17	jue 9/11/17			27 días	Proveedor Tycon tech;TI CNP
1.7.6	Finalización Etapa IV	0 días	jue 9/11/17	jue 9/11/17	90	1.7.5	27 días	
1.8	Etapa V - Protección de Redes Internas	19 días	lun 8/1/18	jue 1/2/18	73	1.7	0 días	
1.8.1	Realizar las adecuaciones para que todo el tráfico entre redes de la empresa pase a través del firewall	19 días	lun 8/1/18	jue 1/2/18			0 días	
1.8.1.1	Adquisición de firewall UTM	19 días	lun 8/1/18	jue 1/2/18			0 días	Tycon Tech
1.8.1.2	Ajustes de firewall UTM en la topología de red	19 días	lun 8/1/18	jue 1/2/18			0 días	Tycon Tech
1.8.1.3	Ajustes de configuración en reglas de acceso	19 días	lun 8/1/18	jue 1/2/18			0 días	Tycon Tech
1.8.1.4	Pruebas y testeos de conexión entre las distintas redes	19 días	lun 8/1/18	jue 1/2/18			0 días	Tycon Tech
1.8.2	Aplicar IPS, AV, restricciones de ancho de banda para el tráfico LAN to LAN y LAN to WAN	14 días	lun 8/1/18	jue 25/1/18			5 días	Proveedor Tycon tech
1.8.3	Permitir el acceso a la infraestructura tecnológica solo desde la red de informática.	5 días	lun 8/1/18	vie 12/1/18			14 días	Proveedor Tycon tech

1.8.4	Finalización Etapa V	0 días	jue 1/2/18	jue 1/2/18	96	1.8.1	0 días	
1.9	Etapa VI - Webfiltering, Antispam y Procedimientos	39 días	vie 2/2/18	mié 28/3/18	95	1.8	0 días	
1.9.1	Implementar un esquema de WebFiltering en alta disponibilidad	19 días	vie 2/2/18	mié 28/2/18			0 días	
1.9.1.1	Adquisición de firewall UTM (con funcionalidad de WebFilter)	19 días	vie 2/2/18	mié 28/2/18			0 días	PMO;Proveedor Tycon tech
1.9.1.2	Configuración inicial del equipo y del servicio de webfiltering	19 días	vie 2/2/18	mié 28/2/18			0 días	Proveedor Tycon tech
1.9.1.3	Relevamiento de configuración del WebSense	19 días	vie 2/2/18	mié 28/2/18			0 días	Proveedor Tycon tech
1.9.1.4	Migración de configuración al nuevo equipo	19 días	vie 2/2/18	mié 28/2/18			0 días	Proveedor Tycon tech
1.9.1.5	Pruebas del servicio de Webfiltering	19 días	vie 2/2/18	mié 28/2/18			0 días	Proveedor Tycon tech;TI CNP
1.9.2	Desarrollar las directrices de un procedimiento backup y control de cambios sobre el equipamiento de TI	4 días	jue 1/3/18	mar 6/3/18	105	1.9.1	0 días	
1.9.2.1	Indicar recomendaciones para generar un procedimiento de backup	4 días	jue 1/3/18	mar 6/3/18			0 días	Proveedor Tycon tech

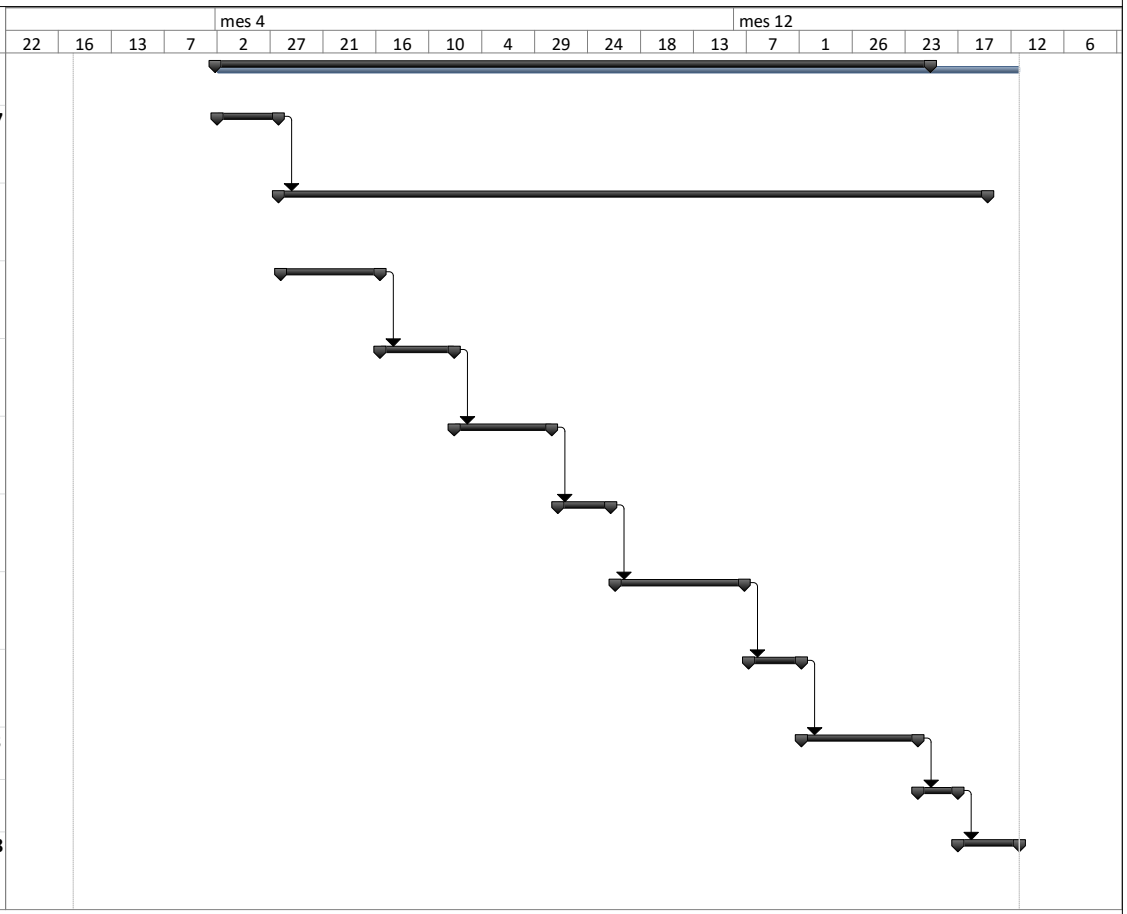
1.9.2.2	Indicar recomendaciones para generar un procedimiento de control de cambios	4 días	jue 1/3/18	mar 6/3/18			0 días	Proveedor Tycon tech
1.9.3	Implementar un esquema de Antispam en alta disponibilidad	6 días	mié 7/3/18	mié 14/3/18	111	1.9.2	0 días	
1.9.3.1	Gestionar la adquisición del equipamiento	6 días	mié 7/3/18	mié 14/3/18			0 días	PMO
1.9.3.2	Configuración inicial del equipamiento	6 días	mié 7/3/18	mié 14/3/18			0 días	Proveedor Tycon tech;TI CNP
1.9.3.3	Relevamiento de configuración actual	6 días	mié 7/3/18	mié 14/3/18			0 días	Proveedor Tycon tech;TI CNP
1.9.3.4	Migración de configuración	6 días	mié 7/3/18	mié 14/3/18			0 días	Proveedor Tycon tech;TI CNP
1.9.3.5	Pruebas de servicio	6 días	mié 7/3/18	mié 14/3/18			0 días	Proveedor Tycon tech;TI CNP
1.9.4	Desarrollar las directrices de un procedimiento diferencial para el ABM de cuentas de administrador de domino	10 días	jue 15/3/18	mié 28/3/18	114	1.9.3	0 días	
1.9.4.1	Indicar recomendaciones para generar un procedimiento para ABM de cuentas de administrador de dominio	10 días	jue 15/3/18	mié 28/3/18			0 días	Proveedor Tycon tech

1.9.5	Finalización Etapa VI	0 días	mié 28/3/18	mié 28/3/18	120	1.9.4	0 días	
1.10	Etapa VII - RED WiFi, MPLS y Backup Satelital	13 días	jue 29/3/18	lun 16/4/18	104	1.9	0 días	
1.10.1	Implementar cifrado WPA2 o WPA2/Enterprise, SSID Corporativo y SSID Invitados, ajustes de seguridad	8 días	jue 29/3/18	lun 9/4/18			0 días	
1.10.1.1	Sincronizar wireless controller con usuarios active directory	8 días	jue 29/3/18	lun 9/4/18			0 días	Proveedor Tycon tech
1.10.1.2	Configurar cifrado WPA2/Enterprise con autenticación para SSID Corporativo	8 días	jue 29/3/18	lun 9/4/18			0 días	Proveedor Tycon tech
1.10.1.3	Configurar cifrado WPA2	8 días	jue 29/3/18	lun 9/4/18			0 días	Proveedor Tycon tech
1.10.1.4	Definir red vlan de red WiFi corporativa y vlan de red WiFi invitados	8 días	jue 29/3/18	lun 9/4/18			0 días	Proveedor Tycon tech
1.10.1.5	Ajustes en red LAN	8 días	jue 29/3/18	lun 9/4/18			0 días	Proveedor Tycon tech
1.10.1.6	Documentación, pruebas y test de conexión	8 días	jue 29/3/18	lun 9/4/18			0 días	Proveedor Tycon tech
1.10.2	Desarrollar un procedimiento para implementar conmutación de enlace MPLS y Backup Satelital	4 días	mar 10/4/18	vie 13/4/18	124	1.10.1	0 días	Proveedor Tycon tech

1.10.3	Interactuar con el proveedor y coordinar implementación de conmutación automática de enlace principal a enlace backup y viceversa	1 día	lun 16/4/18	lun 16/4/18	131	1.10.2	0 días	Proveedor Telefonica;Proveedor Tycon tech
1.10.4	Finalización Etapa VII	0 días	lun 16/4/18	lun 16/4/18	132	1.10.3	0 días	
1.11	Cierre	21 días	mar 17/4/18	mar 15/5/18	123	1.10	0 días	
1.11.1	Informe final del proyecto	20 días	mar 17/4/18	lun 14/5/18			1 día	Proveedor Softcom;Proveedor Telefonica;Proveedor Tycon tech;PMO
1.11.2	Entrega de ingenieria de detalle completa	20 días	mar 17/4/18	lun 14/5/18			0 días	Proveedor Softcom;Proveedor Telefonica;Proveedor Tycon tech;PMO
1.11.3	Propuesta de soporte y mantenimiento	3 días	mar 17/4/18	jue 19/4/18			18 días	Proveedor Tycon tech
1.11.4	Lecciones aprendidas y recomendaciones	10 días	mar 17/4/18	lun 30/4/18			11 días	Proveedor Softcom;Proveedor Telefonica;Proveedor Tycon tech;PMO
1.11.5	Reunión de entrega	1 día	mar 15/5/18	mar 15/5/18	136	1.11.2	0 días	Proveedor Tycon tech;Proveedor Telefónica; Proveedor Softcom;PMO
1.11.6	Finalización del proyecto	0 días	mar 15/5/18	mar 15/5/18	139	1.11.5	0 días	PMO

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	Nombre de tarea	Duración	Comienzo	Fin
1	**Remediación Infraestructura y Seguridad Informática**	**223 días**	**lun 1/5/17**	**mar 3/4/18**
2	**Inicio**	**20 días**	**mar 2/5/17**	**mar 30/5/17**
7	**Gestion del proyecto**	**221 días**	**mié 31/5/17**	**lun 30/4/18**
19	**Gestion de Contratación**	**31 días**	**jue 1/6/17**	**lun 17/7/17**
25	**Etapa I - Servicios DNS Externo y DHCP**	**24 días**	**mar 18/7/17**	**lun 21/8/17**
44	**Etapa II - Protección de Borde I**	**34 días**	**mar 22/8/17**	**vie 6/10/17**
62	**Etapa III - Protección de Borde II**	**19 días**	**mar 10/10/17**	**vie 3/11/17**
73	**Etapa IV - Switch de LAN**	**31 días**	**lun 6/11/17**	**vie 5/1/18**
95	**Etapa V - Protección de Redes Internas**	**19 días**	**lun 8/1/18**	**jue 1/2/18**
104	**Etapa VI - Webfiltering, Antispam y Procedimientos**	**39 días**	**vie 2/2/18**	**mié 28/3/18**
123	**Etapa VII - RED WiFi, MPLS y Backup Satélital**	**13 días**	**jue 29/3/18**	**lun 16/4/18**
134	**Cierre**	**21 días**	**mar 17/4/18**	**mar 15/5/18**

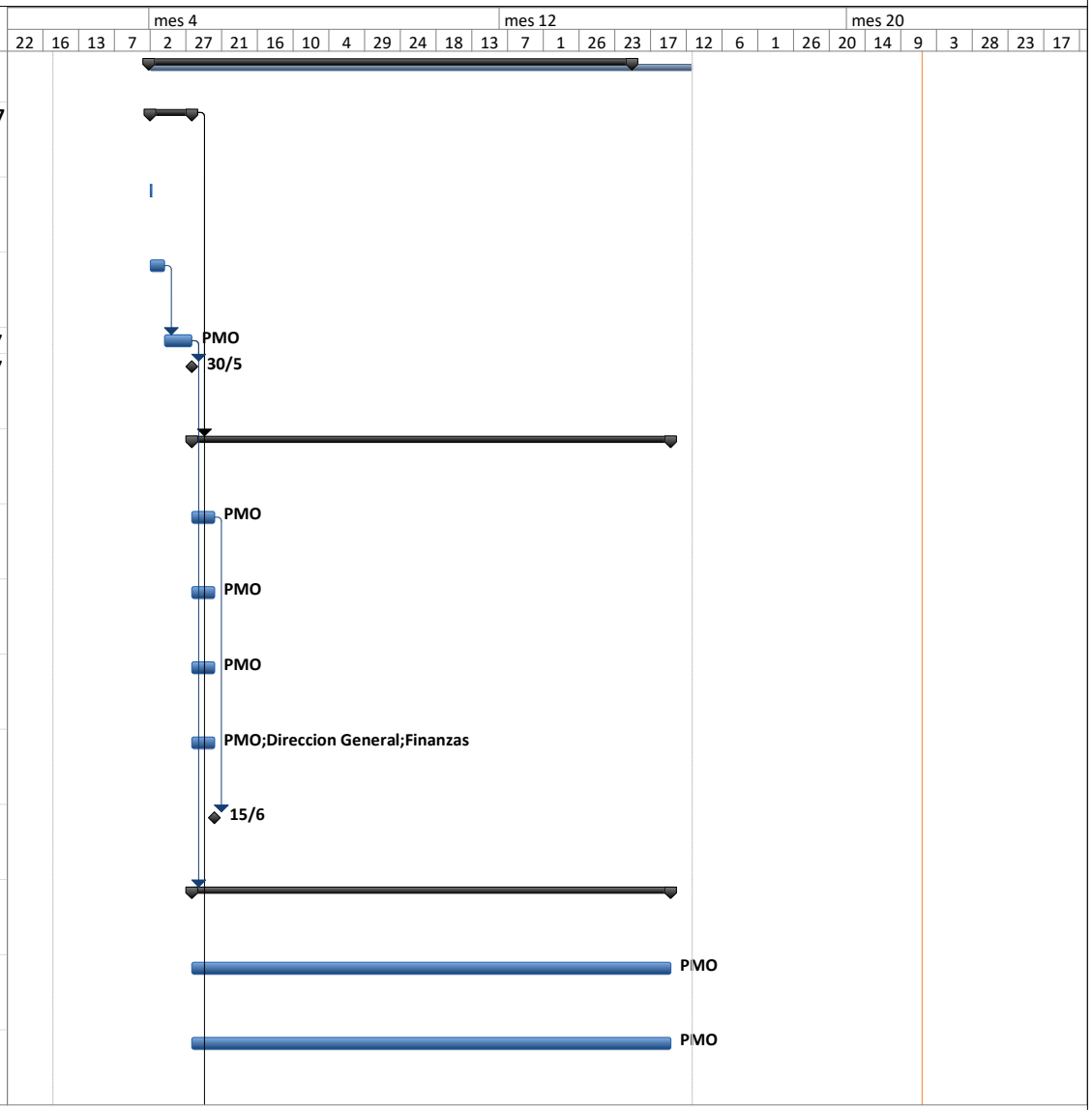


Proyecto: 201-2_ROIRCNP_Tiemp
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin
División	Hito externo	Sólo duración	Fecha límite
Hito	Tarea inactiva	Informe de resumen manual	Progreso
Resumen	Hito inactivo	Resumen manual	
Resumen del proyecto	Resumen inactivo	Sólo el comienzo	

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	Nombre de tarea	Duración	Comienzo	Fin
1	**Remediación Infraestructura y Seguridad Informática**	**223 días**	**lun 1/5/17**	**mar 3/4/18**
2	**Inicio**	**20 días**	**mar 2/5/17**	**mar 30/5/17**
3	Kick off de inicio del proyecto	1 día	mar 2/5/17	mar 2/5/17
4	Caso de negocio	8 días	mar 2/5/17	jue 11/5/17
5	Acta de proyecto	12 días	vie 12/5/17	mar 30/5/17
6	Aprobación Project charter	0 días	mar 30/5/17	mar 30/5/17
7	**Gestion del proyecto**	**221 días**	**mié 31/5/17**	**lun 30/4/18**
8	Plan de gestión de proyecto	12 días	mié 31/5/17	jue 15/6/17
9	Linea base de alcance	12 días	mié 31/5/17	jue 15/6/17
10	Linea base de tiempo	12 días	mié 31/5/17	jue 15/6/17
11	Linea base de costos	12 días	mié 31/5/17	jue 15/6/17
12	Aprobación Plan de gestion del proyetco	0 días	jue 15/6/17	jue 15/6/17
13	**Comunicaciones**	**221 días**	**mié 31/5/17**	**lun 30/4/18**
14	Reporte de hitos	221 días	mié 31/5/17	lun 30/4/18
15	minutas	221 días	mié 31/5/17	lun 30/4/18

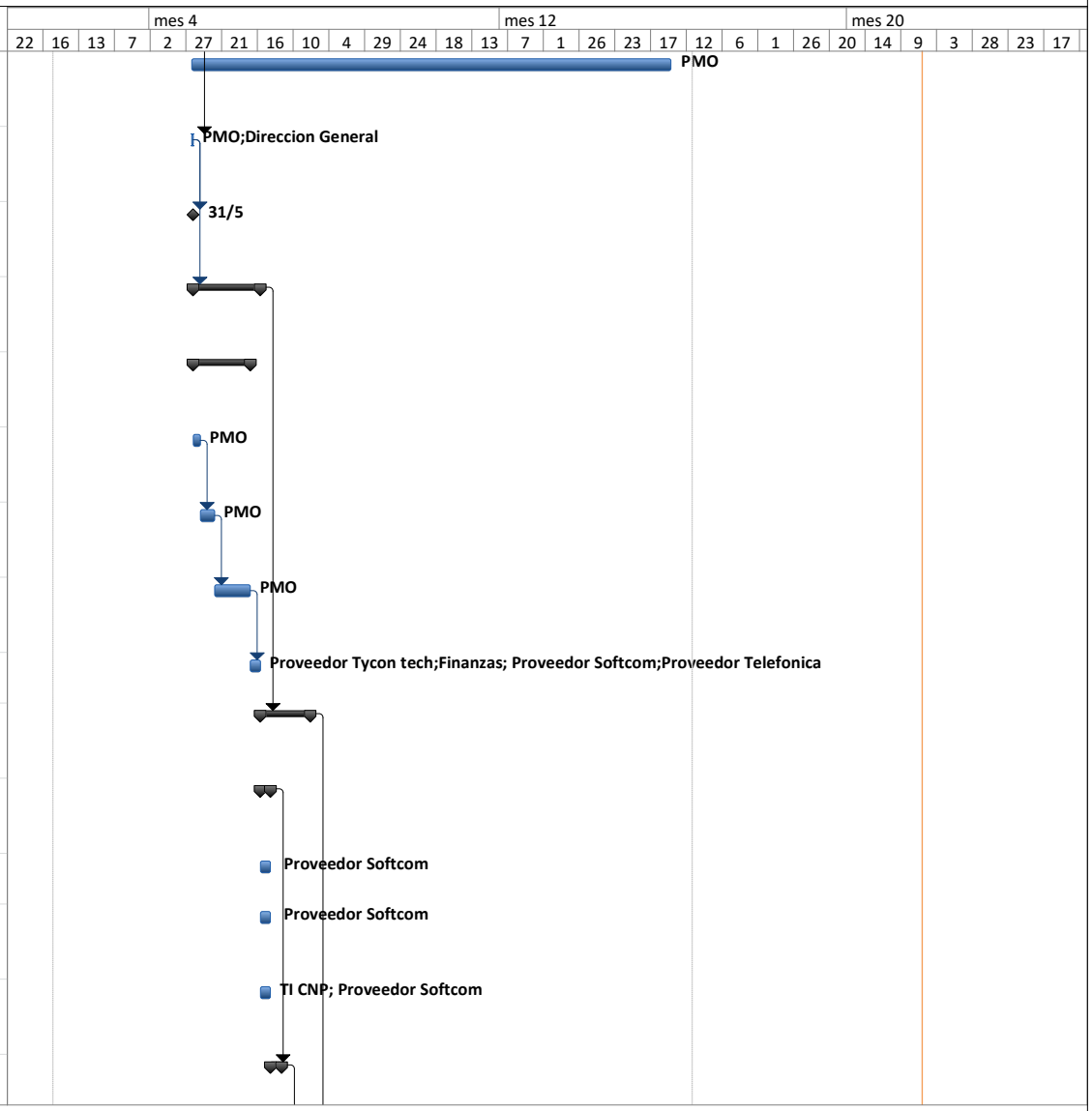


Proyecto: 201-2_ROIRCNP_Tiemp
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin		
División	Hito externo	Sólo duración	Fecha límite		
Hito	Tarea inactiva	Informe de resumen manual	Progreso		
Resumen	Hito inactivo	Resumen manual			
Resumen del proyecto	Resumen inactivo	Sólo el comienzo			

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	Nombre de tarea	Duración	Comienzo	Fin
16	Reporte de status	221 días	mié 31/5/17	lun 30/4/18
17	Kick Off Puesta en marcha	1 día	mié 31/5/17	mié 31/5/17
18	Hito Cick off puesta en marcha	0 días	mié 31/5/17	mié 31/5/17
19	**Gestion de Contratación**	**31 días**	**jue 1/6/17**	**lun 17/7/17**
20	**Búsqueda del proveedor**	**26 días**	**jue 1/6/17**	**lun 10/7/17**
21	Invitacion a proveedores	3 días	jue 1/6/17	lun 5/6/17
22	RFP (Request for Proposal)	8 días	mar 6/6/17	jue 15/6/17
23	Análisis y Selección de proveedores	15 días	vie 16/6/17	lun 10/7/17
24	Contratación	5 días	mar 11/7/17	lun 17/7/17
25	**Etapa I - Servicios DNS Externo y DHCP**	**24 días**	**mar 18/7/17**	**lun 21/8/17**
26	**Habilitar protección de IPS, AV y publicar solo puertos necesarios para el servicio de DNS Externo**	**5 días**	**mar 18/7/17**	**lun 24/7/17**
27	Solicitar al proveedor habilitar solo el puerto 53, protocolos TCP y UDP	5 días	mar 18/7/17	lun 24/7/17
28	Solicitar al proveedor del firewall que habilite para protección de IPS y AV en la publicación	5 días	mar 18/7/17	lun 24/7/17
29	Realizar pruebas del servicio	5 días	mar 18/7/17	lun 24/7/17
30	**Ajustar configuración de DNS Server Externo Segundario**	**6 días**	**mar 25/7/17**	**mar 1/8/17**

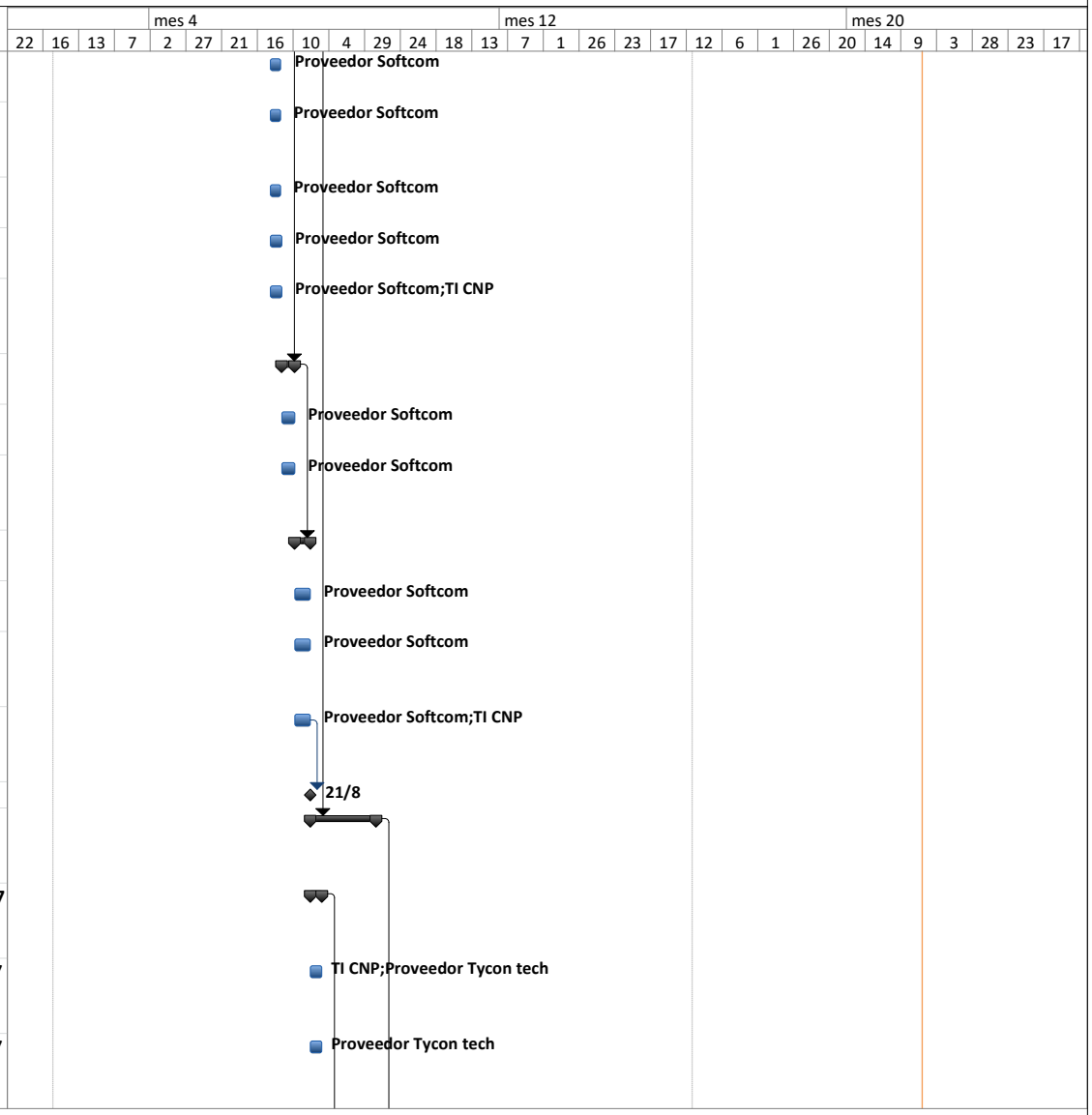


Proyecto: 201-2_ROIRCNP_Tiemp
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin		
División	Hito externo	Sólo duración	Fecha límite		
Hito	Tarea inactiva	Informe de resumen manual	Progreso		
Resumen	Hito inactivo	Resumen manual			
Resumen del proyecto	Resumen inactivo	Sólo el comienzo			

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	Nombre de tarea	Duración	Comienzo	Fin
31	Instalación de un servidor con Windows Server 2012	5 días	mar 25/7/17	lun 31/7/17
32	Habilitar servicio de DNS	5 días	mar 25/7/17	lun 31/7/17
33	Transferir zonas desde DNS principal al segundario	5 días	mar 25/7/17	lun 31/7/17
34	Gestionar configuraciones para publicación en internet	6 días	mar 25/7/17	mar 1/8/17
35	Realizar pruebas de servicios	6 días	mar 25/7/17	mar 1/8/17
36	**Configurar otro registro MX para un Mail Server Segundario**	**7 días**	**mié 2/8/17**	**jue 10/8/17**
37	En el servidor de DNS, agregar un DNS record de tipo MX (Mail Exchanger)	7 días	mié 2/8/17	jue 10/8/17
38	Asignar una prioridad para que actue como backup (debe ser un número mayor que el del primario)	7 días	mié 2/8/17	jue 10/8/17
39	**Implementar un esquema de HA para el servidor de DHCP**	**6 días**	**vie 11/8/17**	**lun 21/8/17**
40	Instalación de dos servidores con Windows Server 2012	6 días	vie 11/8/17	lun 21/8/17
41	Configurar los servicios de DHCP y conmutación por error en modo load balance	6 días	vie 11/8/17	lun 21/8/17
42	Realizar pruebas del servicio	6 días	vie 11/8/17	lun 21/8/17
43	Finalizacion Etapa I	0 días	**lun 21/8/17**	lun 21/8/17
44	**Etapa II - Protección de Borde I**	**34 días**	**mar 22/8/17**	**vie 6/10/17**
45	**Implementar un clúster de firewall para borde y VPN en clúster de alta disponibilidad**	**6 días**	**mar 22/8/17**	**mar 29/8/17**
46	Adquisición de firewall UTM para HA	6 días	mar 22/8/17	mar 29/8/17
47	Instalación y configuración inicial	6 días	mar 22/8/17	mar 29/8/17

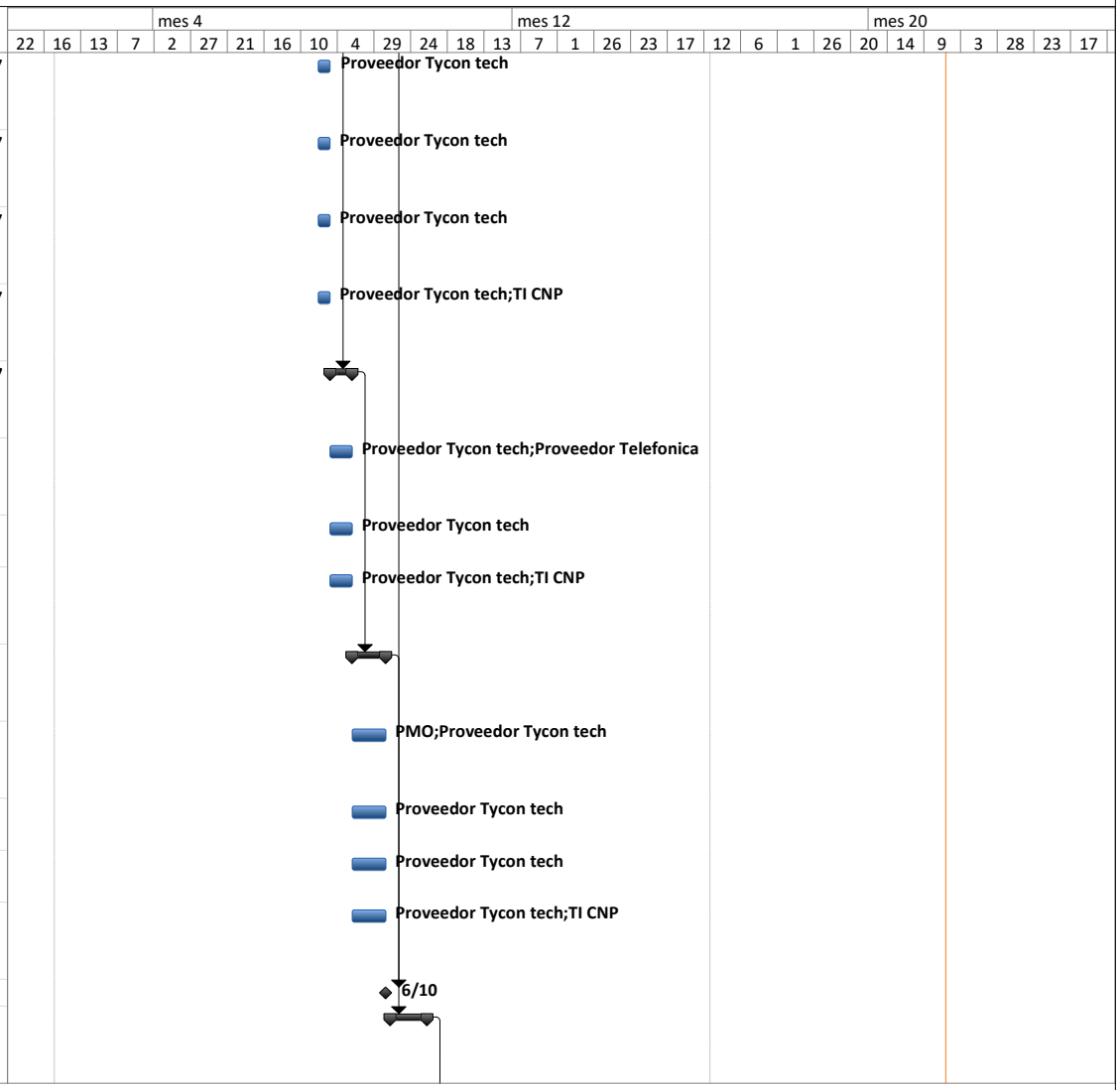


Proyecto: 201-2_ROIRCNP_Tiemp
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin		
División	Hito externo	Sólo duración	Fecha límite		
Hito	Tarea inactiva	Informe de resumen manual	Progreso		
Resumen	Hito inactivo	Resumen manual			
Resumen del proyecto	Resumen inactivo	Sólo el comienzo			

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	Nombre de tarea	Duración	Comienzo	Fin
48	Importar configuraciones de borde	6 días	mar 22/8/17	mar 29/8/17
49	Pruebas de funcionamiento	6 días	mar 22/8/17	mar 29/8/17
50	Importar configuraciones de VPN	6 días	mar 22/8/17	mar 29/8/17
51	Pruebas de funcionamiento	6 días	mar 22/8/17	mar 29/8/17
52	**Ajustar servicios publicados en internet y configurar aplicaciones publicadas en la red DMZ**	**11 días**	**mié 30/8/17**	**mié 13/9/17**
53	Solicitar al proveedor del firewall habilitar solo los puertos necesarios de los servicio publicados en intenret	11 días	mié 30/8/17	mié 13/9/17
54	Verificar servicios que no están en la red DMZ y moverlos a esta red	11 días	mié 30/8/17	mié 13/9/17
55	Pruebas de funcionamiento	11 días	mié 30/8/17	mié 13/9/17
56	**Implementar una alternativa tecnológica diferente al TMG, ya el servicio está discontinuado**	**17 días**	**jue 14/9/17**	**vie 6/10/17**
57	Adquisición de firewall UTM	17 días	jue 14/9/17	vie 6/10/17
58	Relevar configuraciones de permisos de acceso en el TMG	17 días	jue 14/9/17	vie 6/10/17
59	Migrar configuraciones de permisos de acceso a los firewalls UTM	17 días	jue 14/9/17	vie 6/10/17
60	Pruebas de servicios	17 días	jue 14/9/17	vie 6/10/17
61	Finalizacion Etapa II	0 días	**vie 6/10/17**	vie 6/10/17
62	**Etapa III - Protección de Borde II**	**19 días**	**mar 10/10/**	**vie 3/11/17**

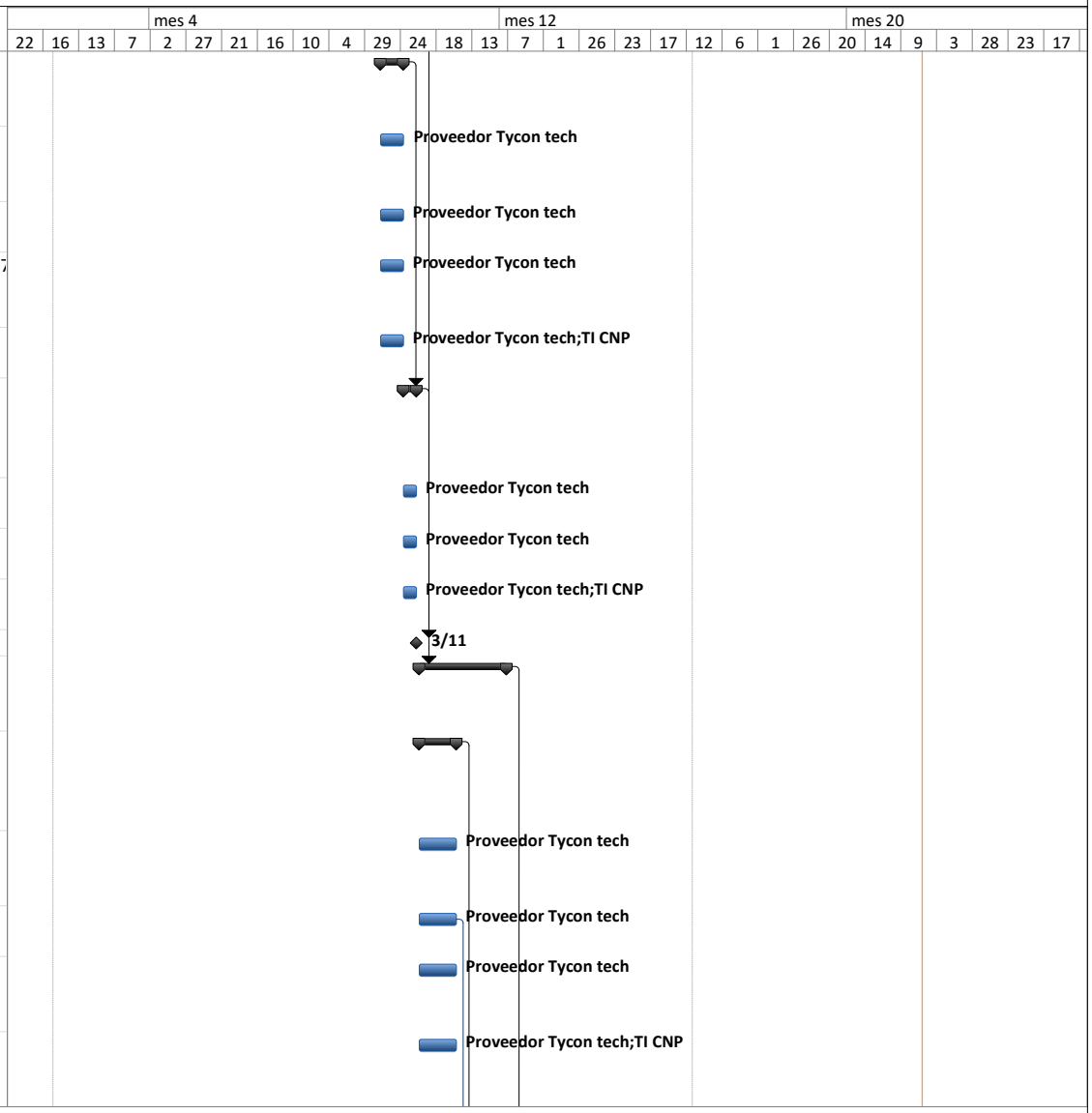


Proyecto: 201-2_ROIRCNP_Tiemp
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin
División	Hito externo	Sólo duración	Fecha límite
Hito	Tarea inactiva	Informe de resumen manual	Progreso
Resumen	Hito inactivo	Resumen manual	
Resumen del proyecto	Resumen inactivo	Sólo el comienzo	

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	Nombre de tarea	Duración	Comienzo	Fin
63	**Realizar las adecuaciones para que los servicios sean publicados desde un único equipo y en forma directa**	**12 días**	**mar 10/10/17**	**mié 25/10/17**
64	Verificar que servicios hacia internet están publicados desde el ISA Server y el TMG	12 días	mar 10/10/17	mié 25/10/17
65	Crear y validar las reglas de firewall en un entorno de prueba	12 días	mar 10/10/17	mié 25/10/17
66	Migrar las reglas al nuevo firewall	12 días	mar 10/10/1	mié 25/10/17
67	Realizar pruebas de funcionamiento de los servicios	12 días	mar 10/10/17	mié 25/10/17
68	**Realizar las adecuaciones para que todos los servicios publicados en internet cuenten con protección de IPS, AV y DOS**	**7 días**	**jue 26/10/17**	**vie 3/11/17**
69	Crear profiles de AV, IPS y Antivirus en el firewall	7 días	jue 26/10/17	vie 3/11/17
70	Asignar los profiles a los servicios publicados en internet	7 días	jue 26/10/17	vie 3/11/17
71	Realizar pruebas de los servicios publicados en internet	7 días	jue 26/10/17	vie 3/11/17
72	Finalizacion Etapa III	0 días	**vie 3/11/17**	vie 3/11/17
73	**Etapa IV - Switch de LAN**	**31 días**	**lun 6/11/17**	**vie 5/1/18**
74	**Implementar segmentación por VLANs para red de usuarios y red de servidores. Configurar ruteo por capa 3 (nivel de red)**	**19 días**	**lun 6/11/17**	**vie 1/12/17**
75	Definir rangos de red	19 días	lun 6/11/17	vie 1/12/17
76	Configuración en Switchs, Vlans, puertos de Trunk	19 días	lun 6/11/17	vie 1/12/17
77	Migración de equipos a nuevas redes, asignación de puertos de switch a nuevas Vlans	19 días	lun 6/11/17	vie 1/12/17
78	Pruebas de funcionamiento	19 días	lun 6/11/17	vie 1/12/17

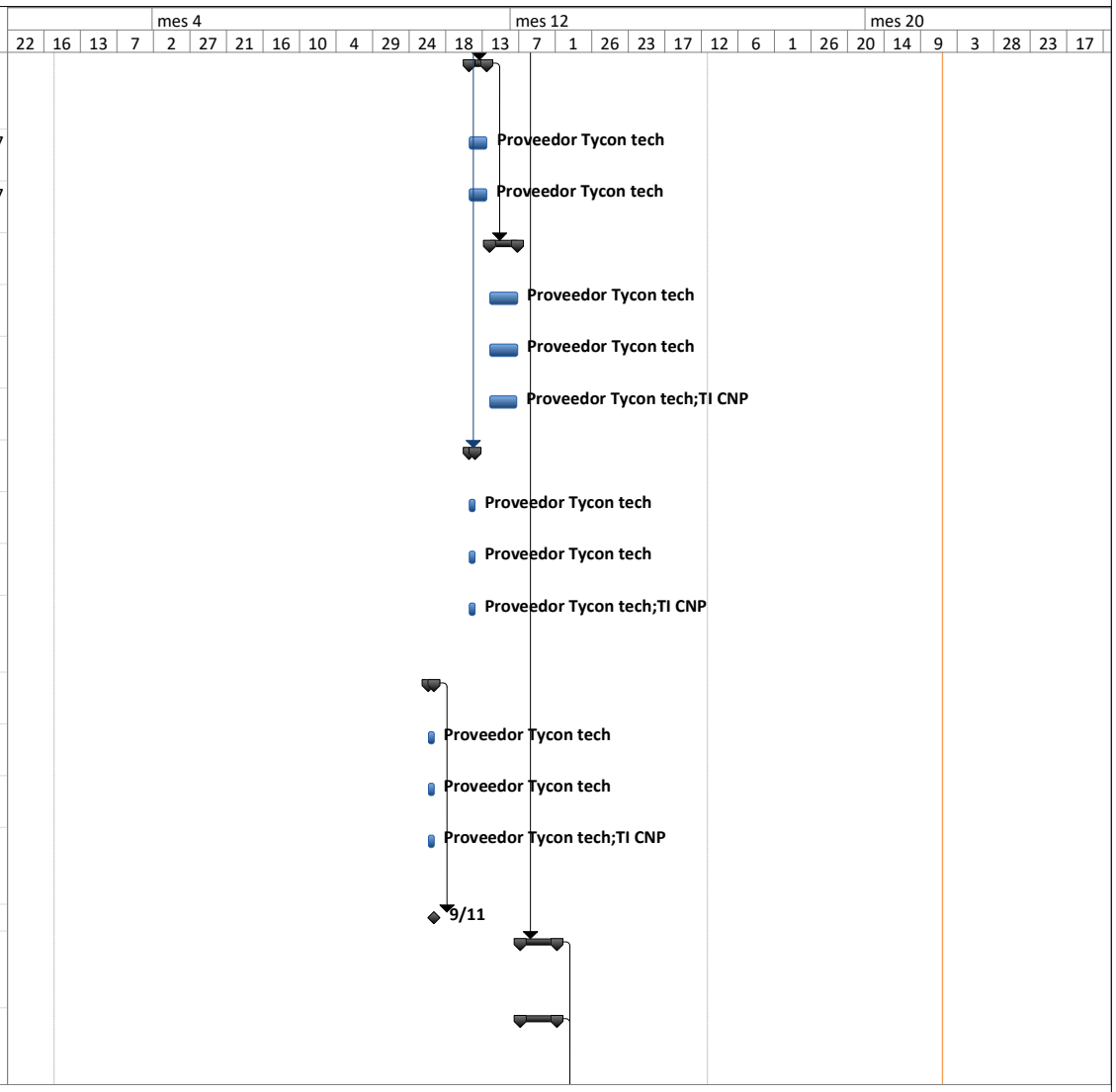


Proyecto: 201-2_ROIRCNP_Tiemp
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin				
División	Hito externo	Sólo duración	Fecha límite				
Hito	Tarea inactiva	Informe de resumen manual	Progreso				
Resumen	Hito inactivo	Resumen manual					
Resumen del proyecto	Resumen inactivo	Sólo el comienzo					

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	Nombre de tarea	Duración	Comienzo	Fin
79	**Realizar las adecuaciones para utilizar otro puerto de backup en caso de falta en el puerto que está en uso**	**8 días**	**lun 4/12/17**	**vie 15/12/17**
80	Configurar port channel en cada uno de los switch	8 días	lun 4/12/17	vie 15/12/17
81	Pruebas de puertos de backup y continuidad de servicio	8 días	lun 4/12/17	vie 15/12/17
82	**Realizar las adecuaciones para utilizar acceso SSH (secure shell) encriptado**	**4 días**	**lun 18/12/17**	**vie 5/1/18**
83	Configurar acceso por secure shell a los switchs	4 días	lun 18/12/17	vie 5/1/18
84	Cancelar la configuración para acceder por telnet	4 días	lun 18/12/17	vie 5/1/18
85	Pruebas de acceso por shh a los equipos	28 horas	lun 18/12/17	vie 5/1/18
86	**Realizar las adecuaciones para no utilizar la vlan nativa para tráfico de red**	**4 días**	**lun 4/12/17**	**jue 7/12/17**
87	Configurar VLAN para gestión de dispositivos de red	4 días	lun 4/12/17	jue 7/12/17
88	Configurar una dirección ip de la nueva vlan a los dispositivos	4 días	lun 4/12/17	jue 7/12/17
89	Pruebas de acceso	4 días	lun 4/12/17	jue 7/12/17
90	**Realizar las adecuaciones para asignar una red exclusiva para las impresoras**	**4 días**	**lun 6/11/17**	**jue 9/11/17**
91	Configurar VLAN para impresoras y asignar puertos	4 días	lun 6/11/17	jue 9/11/17
92	Configurar la nueva dirección IP en las impresoras	4 días	lun 6/11/17	jue 9/11/17
93	Pruebas de funcionamiento	4 días	lun 6/11/17	jue 9/11/17
94	Finalizacion Etapa IV	0 días	**jue 9/11/17**	jue 9/11/17
95	**Etapa V - Protección de Redes Internas**	**19 días**	**lun 8/1/18**	**jue 1/2/18**
96	**Realizar las adecuaciones para que todo el tráfico entre redes de la empresa pase a través del firewall**	**19 días**	**lun 8/1/18**	**jue 1/2/18**

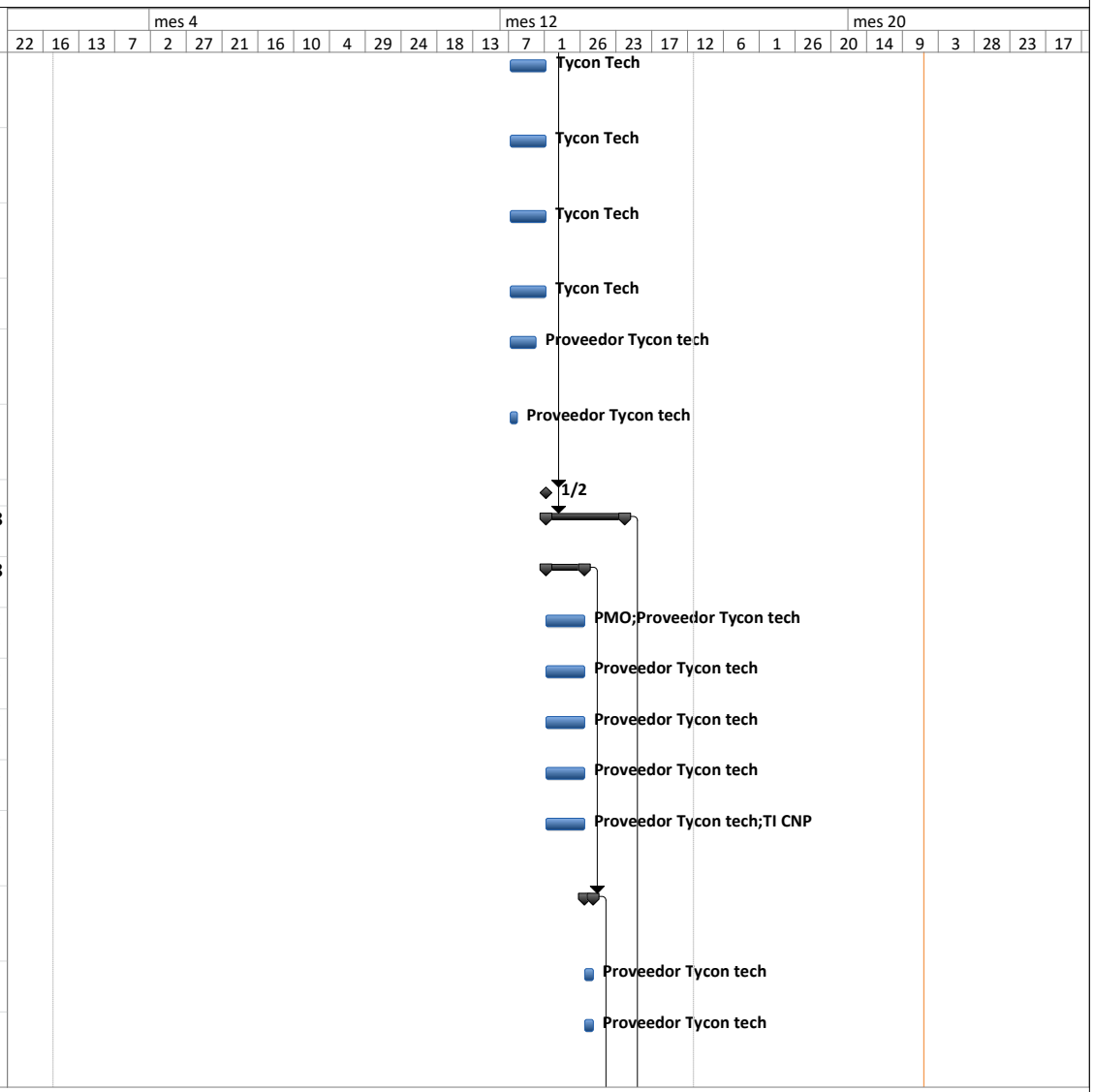


Proyecto: 201-2_ROIRCNP_Tiemp
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin				
División	Hito externo	Sólo duración	Fecha límite				
Hito	Tarea inactiva	Informe de resumen manual	Progreso				
Resumen	Hito inactivo	Resumen manual					
Resumen del proyecto	Resumen inactivo	Sólo el comienzo					

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	Nombre de tarea	Duración	Comienzo	Fin
97	Adquisición de firewall UTM	19 días	lun 8/1/18	jue 1/2/18
98	Ajustes de firewall UTM en la topología	19 días	lun 8/1/18	jue 1/2/18
99	Ajustes de configuración en reglas de a	19 días	lun 8/1/18	jue 1/2/18
100	Pruebas y testeos de conexión entre las distintas redes	19 días	lun 8/1/18	jue 1/2/18
101	Aplicar IPS, AV, restricciones de ancho de banda para el tráfico LAN to LAN y LAN to WAN	14 días	lun 8/1/18	jue 25/1/18
102	Permitir el acceso a la infraestructura tecnológica solo desde la red de informática.	5 días	lun 8/1/18	vie 12/1/18
103	Finalizacion Etapa V	0 días	**jue 1/2/18**	jue 1/2/18
104	**Etapa VI - Webfiltering, Antispam y Procedimientos**	**39 días**	**vie 2/2/18**	**mié 28/3/18**
105	**Implementar un esquema de WebFiltering en alta disponibilidad**	**19 días**	**vie 2/2/18**	**mié 28/2/18**
106	Adquisición de firewall UTM (con funcionalidad de WebFilter)	19 días	vie 2/2/18	mié 28/2/18
107	Configuración inicial del equipo y del servicio de webfiltering	19 días	vie 2/2/18	mié 28/2/18
108	Relevamiento de configuración del WebSense	19 días	vie 2/2/18	mié 28/2/18
109	Migración de configuración al nuevo equipo	19 días	vie 2/2/18	mié 28/2/18
110	Pruebas del servicio de Webfiltering	19 días	vie 2/2/18	mié 28/2/18
111	**Desarrollar las directrices de un procedimiento backup y control de cambios sobre el equipamiento de TI**	**4 días**	**jue 1/3/18**	**mar 6/3/18**
112	Indicar recomendaciones para generar un procedimiento de backup	4 días	jue 1/3/18	mar 6/3/18
113	Indicar recomendaciones para generar un procedimiento de control de cambios	4 días	jue 1/3/18	mar 6/3/18

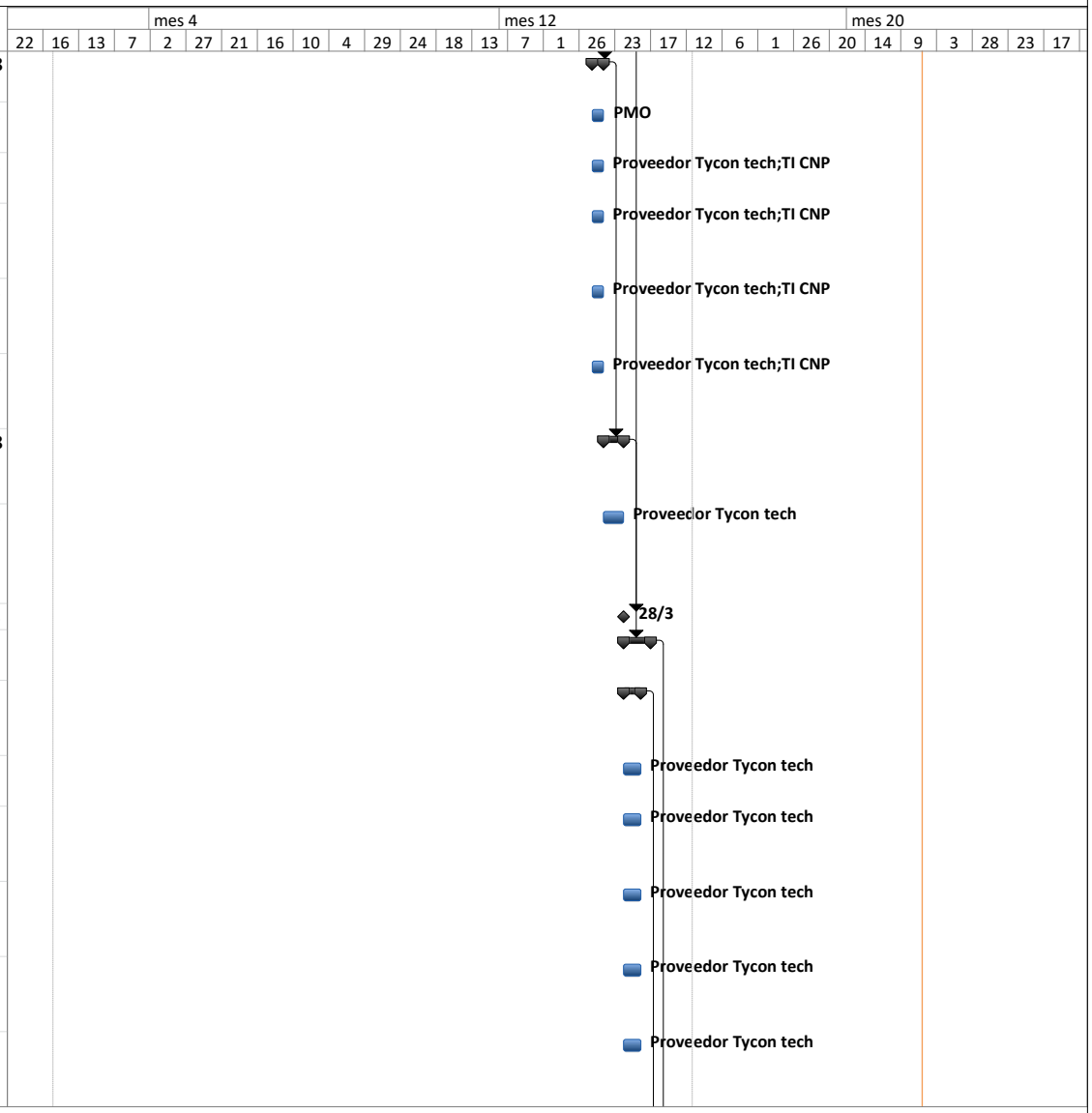


Proyecto: 201-2_ROIRCNP_Tiemp
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin
División	Hito externo	Sólo duración	Fecha límite
Hito	Tarea inactiva	Informe de resumen manual	Progreso
Resumen	Hito inactivo	Resumen manual	
Resumen del proyecto	Resumen inactivo	Sólo el comienzo	

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	Nombre de tarea	Duración	Comienzo	Fin
114	**Implementar un esquema de Antispam en alta disponibilidad**	**6 días**	**mié 7/3/18**	**mié 14/3/18**
115	Gestionar la adquisición del equipamiento	6 días	mié 7/3/18	mié 14/3/18
116	Configuración inicial del equipamiento	6 días	mié 7/3/18	mié 14/3/18
117	Relevamiento de configuración actual	6 días	mié 7/3/18	mié 14/3/18
118	Migración de configuración	6 días	mié 7/3/18	mié 14/3/18
119	Pruebas de servicio	6 días	mié 7/3/18	mié 14/3/18
120	**Desarrollar las directrices de un procedimiento diferencial para el ABM de cuentas de administrador de domino**	**10 días**	**jue 15/3/18**	**mié 28/3/18**
121	Indicar recomendaciones para generar un procedimiento para ABM de cuentas de administrador de dominio	10 días	jue 15/3/18	mié 28/3/18
122	Finalizacion Etapa VI	0 días	**mié 28/3/18**	mié 28/3/18
123	**Etapa VII - RED WiFi, MPLS y Backup Satélital**	**13 días**	**jue 29/3/18**	**lun 16/4/18**
124	**Implementar cifrado WPA2 o WPA2/Enterprise, SSID Corporativo y SSID Invitados, ajustes de seguridad**	**8 días**	**jue 29/3/18**	**lun 9/4/18**
125	Sincronizar wireless controller con usuarios active directory	8 días	jue 29/3/18	lun 9/4/18
126	Configurar cifrado WPA2/Enterprise con autenticación para SSID Corporativo	8 días	jue 29/3/18	lun 9/4/18
127	Configurar cifrado WPA2	8 días	jue 29/3/18	lun 9/4/18
128	Definir red vlan de red WiFi corporativa y vlan de red WiFi invitados	8 días	jue 29/3/18	lun 9/4/18
129	Ajustes en red LAN	8 días	jue 29/3/18	lun 9/4/18

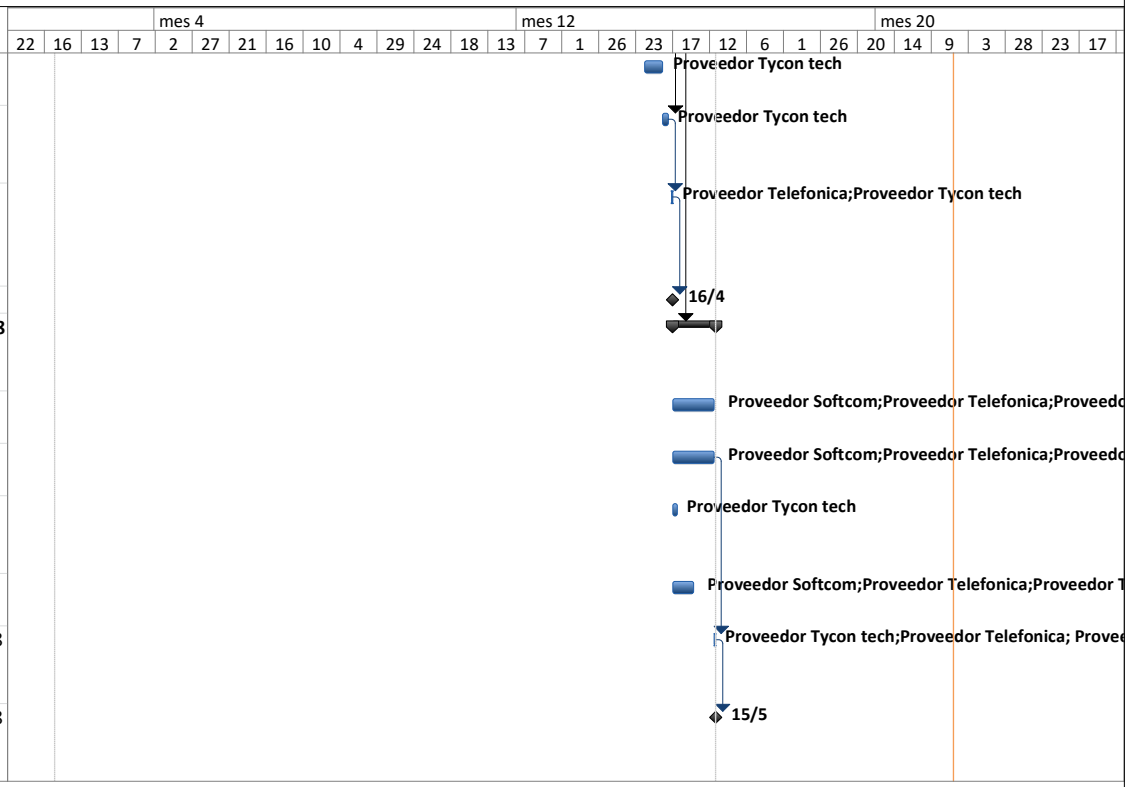


Proyecto: 201-2_ROIRCNP_Tiemp
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin		
División	Hito externo	Sólo duración	Fecha límite		
Hito	Tarea inactiva	Informe de resumen manual	Progreso		
Resumen	Hito inactivo	Resumen manual			
Resumen del proyecto	Resumen inactivo	Sólo el comienzo			

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	Nombre de tarea	Duración	Comienzo	Fin
130	Documentación, pruebas y test de conexión	8 días	jue 29/3/18	lun 9/4/18
131	Desarrollar un procedimiento para implementar conmutación de enlace MPLS y Backup Satelital	4 días	mar 10/4/18	vie 13/4/18
132	Interactuar con el proveedor y coordinar implementación de conmutación automática de enlace principal a enlace backup y viceversa	1 día	lun 16/4/18	lun 16/4/18
133	Finalizacion Etapa VII	0 días	**lun 16/4/18**	lun 16/4/18
134	**Cierre**	**21 días**	**mar 17/4/1**	**mar 15/5/18**
135	Informe final del proyecto	20 días	mar 17/4/18	lun 14/5/18
136	Entrega de ingenieria de detalle completa	20 días	mar 17/4/18	lun 14/5/18
137	Propuesta de soporte y mantenimiento	3 días	mar 17/4/1	jue 19/4/18
138	Lecciones aprendidas y recomendaciones	10 días	mar 17/4/18	lun 30/4/18
139	Reunion de entrega	1 día	mar 15/5/1	mar 15/5/18
140	Finalizacion del proyecto	0 días	mar 15/5/1	mar 15/5/18

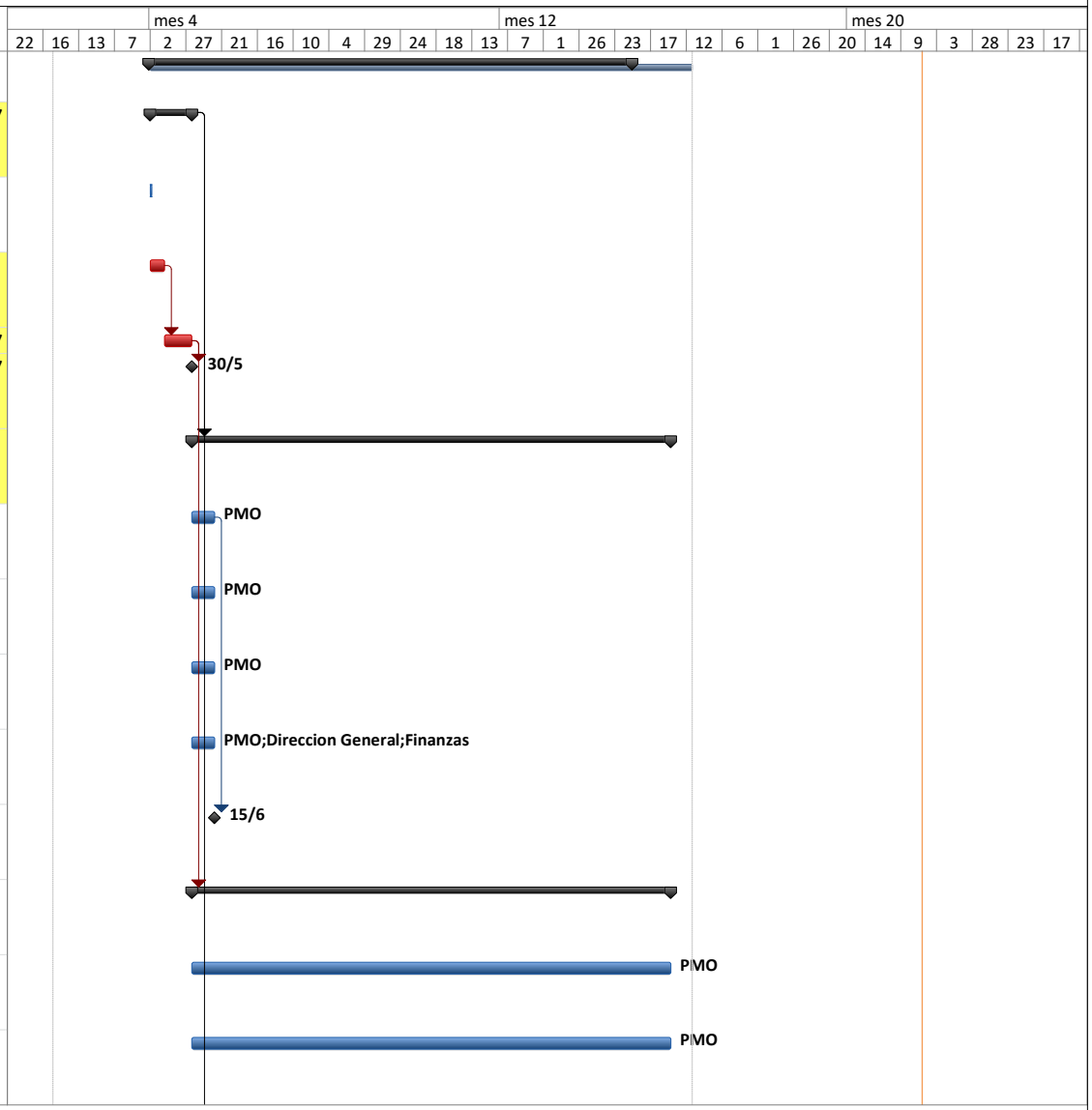


Proyecto: 201-2_ROIRCNP_Tiemp
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin
División	Hito externo	Sólo duración	Fecha límite
Hito	Tarea inactiva	Informe de resumen manual	Progreso
Resumen	Hito inactivo	Resumen manual	
Resumen del proyecto	Resumen inactivo	Sólo el comienzo	

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	Nombre de tarea	Duración	Comienzo	Fin
1	**Remediación Infraestructura y Seguridad Informática**	**223 días**	**lun 1/5/17**	**mar 3/4/18**
2	Inicio	20 días	mar 2/5/17	mar 30/5/17
3	Kick off de inicio del proyecto	1 día	mar 2/5/17	mar 2/5/17
4	Caso de negocio	8 días	mar 2/5/17	jue 11/5/17
5	Acta de proyecto	12 días	vie 12/5/17	mar 30/5/17
6	Aprobación Project charter	0 días	mar 30/5/17	mar 30/5/17
7	Gestion del proyecto	221 días	mié 31/5/17	lun 30/4/18
8	Plan de gestión de proyecto	12 días	mié 31/5/17	jue 15/6/17
9	Linea base de alcance	12 días	mié 31/5/17	jue 15/6/17
10	Linea base de tiempo	12 días	mié 31/5/17	jue 15/6/17
11	Linea base de costos	12 días	mié 31/5/17	jue 15/6/17
12	Aprobación Plan de gestion del proyetco	0 días	jue 15/6/17	jue 15/6/17
13	**Comunicaciones**	**221 días**	**mié 31/5/17**	**lun 30/4/18**
14	Reporte de hitos	221 días	mié 31/5/17	lun 30/4/18
15	minutas	221 días	mié 31/5/17	lun 30/4/18

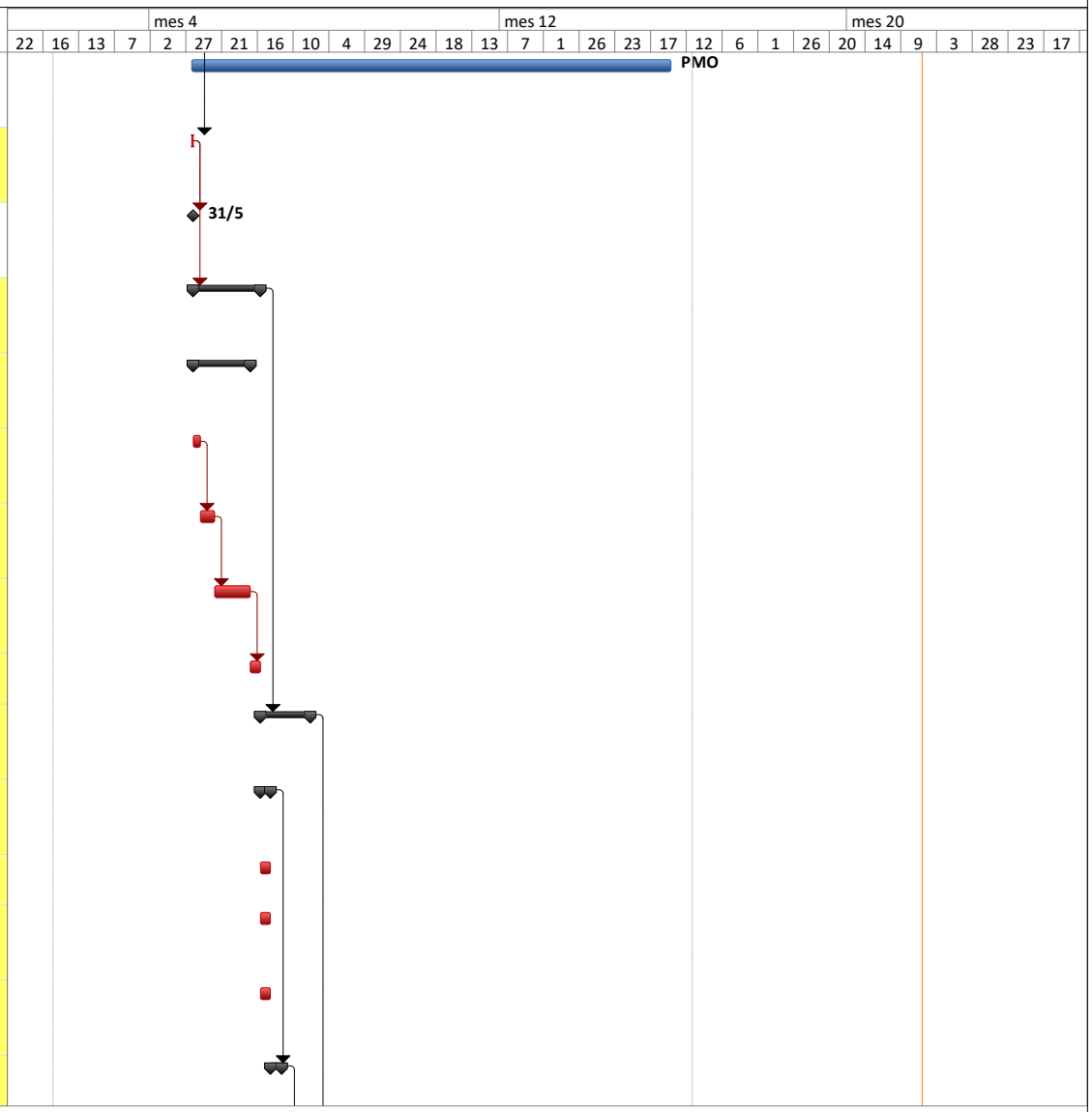


Proyecto: 201-4_ROIRCNP_Tiemp
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin	
División	Hito externo	Sólo duración	Fecha límite	
Hito	Tarea inactiva	Informe de resumen manual	Tareas críticas	
Resumen	Hito inactivo	Resumen manual	División crítica	
Resumen del proyecto	Resumen inactivo	Sólo el comienzo	Progreso	

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	Nombre de tarea	Duración	Comienzo	Fin
16	Reporte de status	221 días	mié 31/5/17	lun 30/4/18
17	Kick Off Puesta en marcha	1 día	mié 31/5/17	mié 31/5/17
18	Hito Cick off puesta en marcha	0 días	mié 31/5/17	mié 31/5/17
19	Gestion de Contratación	31 días	jue 1/6/17	lun 17/7/17
20	Búsqueda del proveedor	26 días	jue 1/6/17	lun 10/7/17
21	Invitacion a proveedores	3 días	jue 1/6/17	lun 5/6/17
22	RFP (Request for Proposal)	8 días	mar 6/6/17	jue 15/6/17
23	Análisis y Selección de proveedores	15 días	vie 16/6/17	lun 10/7/17
24	Contratación	5 días	mar 11/7/17	lun 17/7/17
25	Etapa I - Servicios DNS Externo y DHCP	24 días	mar 18/7/17	lun 21/8/17
26	Habilitar protección de IPS, AV y publicar solo puertos necesarios para el servicio de DNS Externo	5 días	mar 18/7/17	lun 24/7/17
27	Solicitar al proveedor habilitar solo el puerto 53, protocolos TCP y UDP	5 días	mar 18/7/17	lun 24/7/17
28	Solicitar al proveedor del firewall que habilite para protección de IPS y AV en la publicación	5 días	mar 18/7/17	lun 24/7/17
29	Realizar pruebas del servicio	5 días	mar 18/7/17	lun 24/7/17
30	Ajustar configuración de DNS Server Externo Segundario	6 días	mar 25/7/17	mar 1/8/17

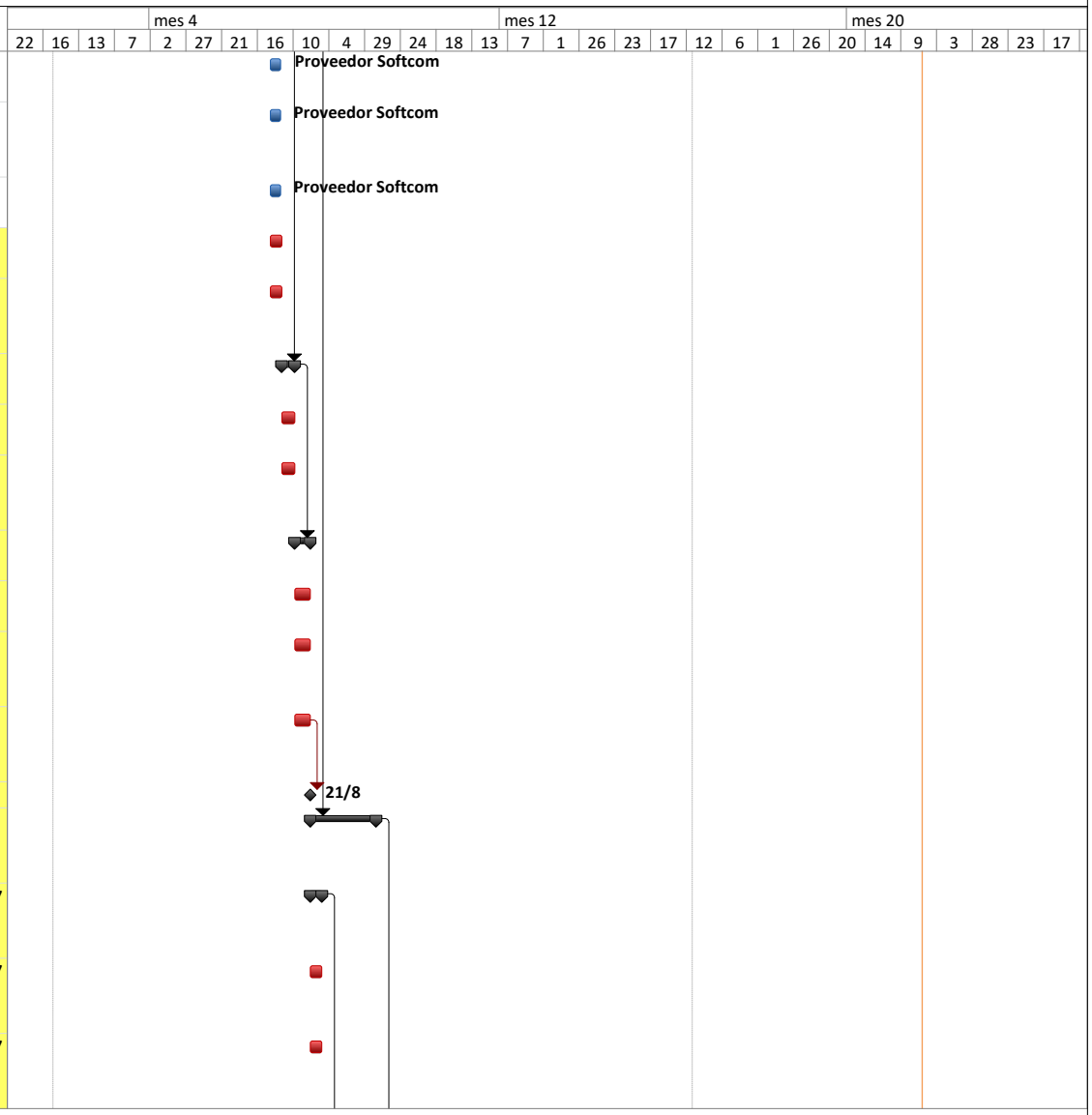


Proyecto: 201-4_ROIRCNP_Tiemp
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin		
División	Hito externo	Sólo duración	Fecha límite		
Hito	Tarea inactiva	Informe de resumen manual	Tareas críticas		
Resumen	Hito inactivo	Resumen manual	División crítica		
Resumen del proyecto	Resumen inactivo	Sólo el comienzo	Progreso		

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	Nombre de tarea	Duración	Comienzo	Fin
31	Instalación de un servidor con Windows Server 2012	5 días	mar 25/7/17	lun 31/7/17
32	Habilitar servicio de DNS	5 días	mar 25/7/17	lun 31/7/17
33	Transferir zonas desde DNS principal al segundario	5 días	mar 25/7/17	lun 31/7/17
34	Gestionar configuraciones para publicación en internet	6 días	mar 25/7/17	mar 1/8/17
35	Realizar pruebas de servicios	6 días	mar 25/7/17	mar 1/8/17
36	Configurar otro registro MX para un Mail Server Segundario	7 días	mié 2/8/17	jue 10/8/17
37	En el servidor de DNS, agregar un DNS record de tipo MX (Mail Exchanger)	7 días	mié 2/8/17	jue 10/8/17
38	Asignar una prioridad para que actue como backup (debe ser un número mayor que el del primario)	7 días	mié 2/8/17	jue 10/8/17
39	Implementar un esquema de HA para el servidor de DHCP	6 días	vie 11/8/17	lun 21/8/17
40	Instalación de dos servidores con Windows Server 2012	6 días	vie 11/8/17	lun 21/8/17
41	Configurar los servicios de DHCP y conmutación por error en modo load balance	6 días	vie 11/8/17	lun 21/8/17
42	Realizar pruebas del servicio	6 días	vie 11/8/17	lun 21/8/17
43	Finalizacion Etapa I	0 días	**lun 21/8/17**	lun 21/8/17
44	Etapa II - Protección de Borde I	34 días	mar 22/8/17	vie 6/10/17
45	Implementar un clúster de firewall para borde y VPN en clúster de alta disponibilidad	6 días	mar 22/8/17	mar 29/8/17
46	Adquisición de firewall UTM para HA	6 días	mar 22/8/17	mar 29/8/17
47	Instalación y configuración inicial	6 días	mar 22/8/17	mar 29/8/17

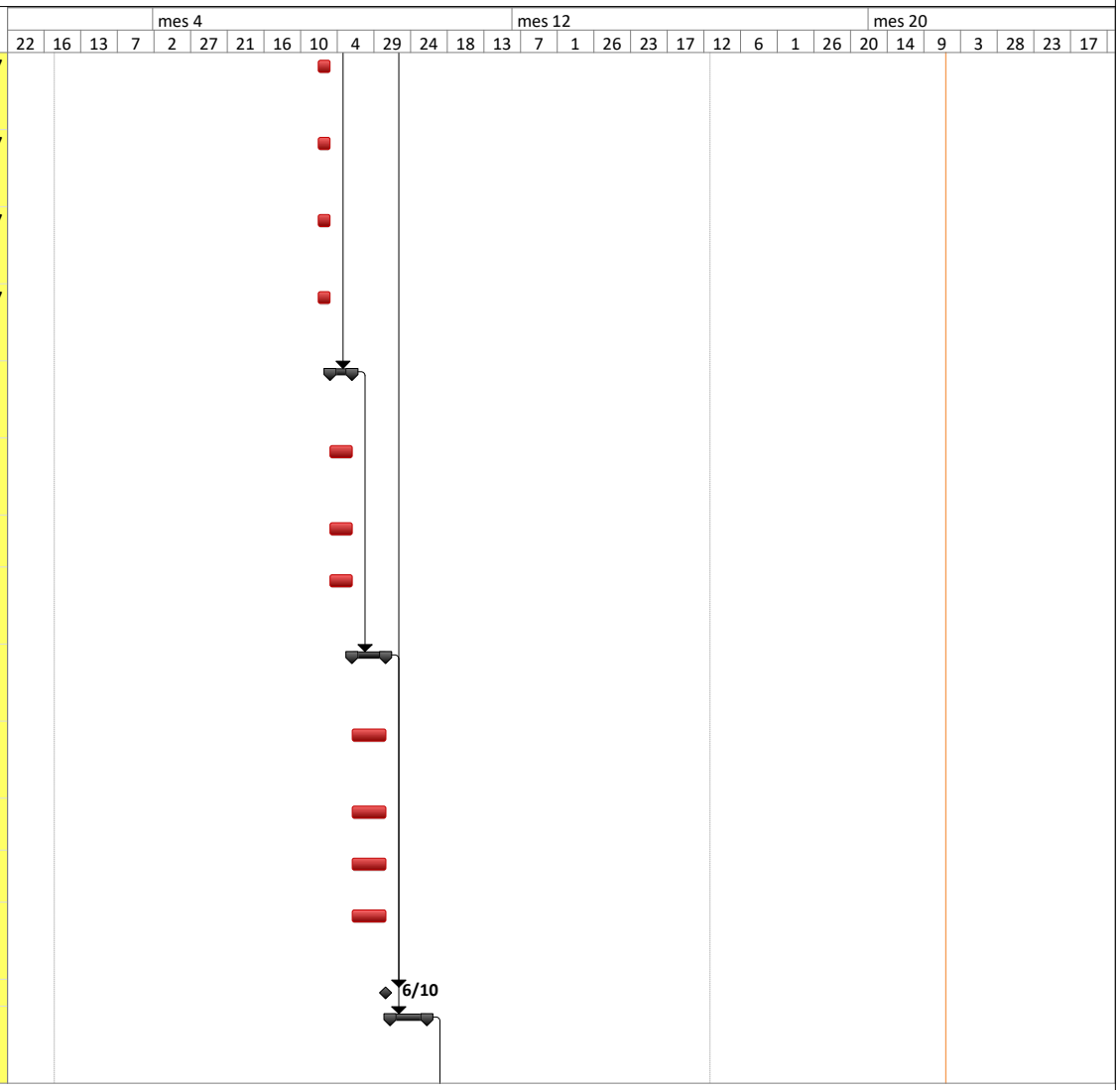


Proyecto: 201-4_ROIRCNP_Tiemp
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin				
División	Hito externo	Sólo duración	Fecha límite				
Hito	Tarea inactiva	Informe de resumen manual	Tareas críticas				
Resumen	Hito inactivo	Resumen manual	División crítica				
Resumen del proyecto	Resumen inactivo	Sólo el comienzo	Progreso				

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	Nombre de tarea	Duración	Comienzo	Fin
48	Importar configuraciones de borde	6 días	mar 22/8/17	mar 29/8/17
49	Pruebas de funcionamiento	6 días	mar 22/8/17	mar 29/8/17
50	Importar configuraciones de VPN	6 días	mar 22/8/17	mar 29/8/17
51	Pruebas de funcionamiento	6 días	mar 22/8/17	mar 29/8/17
52	Ajustar servicios publicados en internet y configurar aplicaciones publicadas en la red DMZ	11 días	mié 30/8/17	mié 13/9/17
53	Solicitar al proveedor del firewall habilitar solo los puertos necesarios de los servicio publicados en intenret	11 días	mié 30/8/17	mié 13/9/17
54	Verificar servicios que no están en la red DMZ y moverlos a esta red	11 días	mié 30/8/17	mié 13/9/17
55	Pruebas de funcionamiento	11 días	mié 30/8/17	mié 13/9/17
56	Implementar una alternativa tecnológica diferente al TMG, ya el servicio está discontinuado	17 días	jue 14/9/17	vie 6/10/17
57	Adquisición de firewall UTM	17 días	jue 14/9/17	vie 6/10/17
58	Relevar configuraciones de permisos de acceso en el TMG	17 días	jue 14/9/17	vie 6/10/17
59	Migrar configuraciones de permisos de acceso a los firewalls UTM	17 días	jue 14/9/17	vie 6/10/17
60	Pruebas de servicios	17 días	jue 14/9/17	vie 6/10/17
61	Finalizacion Etapa II	0 días	**vie 6/10/17**	vie 6/10/17
62	Etapa III - Protección de Borde II	19 días	mar 10/10/17	vie 3/11/17

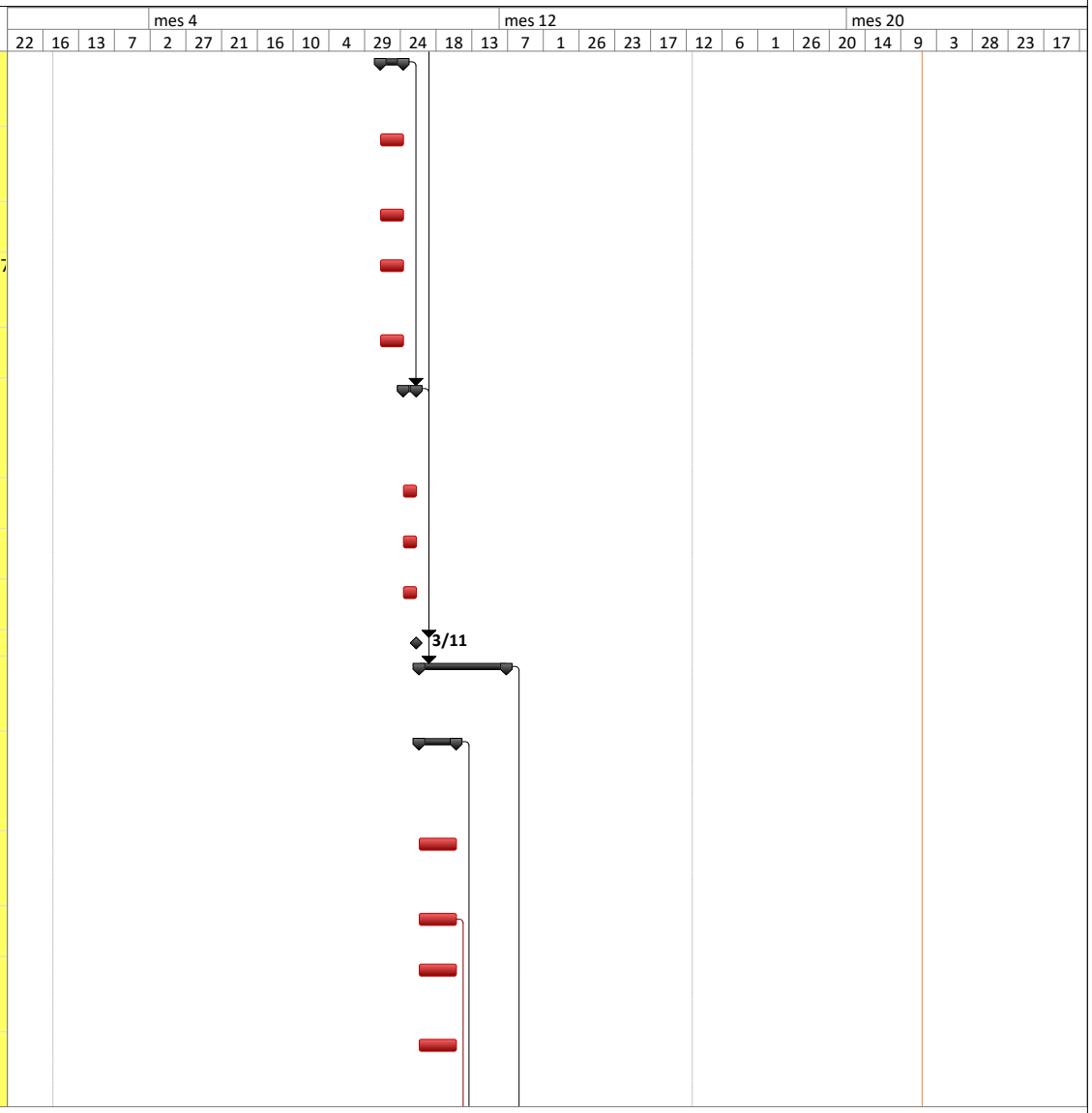


Proyecto: 201-4_ROIRCNP_Tiemp
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin
División	Hito externo	Sólo duración	Fecha límite
Hito	Tarea inactiva	Informe de resumen manual	Tareas críticas
Resumen	Hito inactivo	Resumen manual	División crítica
Resumen del proyecto	Resumen inactivo	Sólo el comienzo	Progreso

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	Nombre de tarea	Duración	Comienzo	Fin
63	Realizar las adecuaciones para que los servicios sean publicados desde un único equipo y en forma directa	12 días	mar 10/10/17	mié 25/10/17
64	Verificar que servicios hacia internet están publicados desde el ISA Server y el TMG	12 días	mar 10/10/17	mié 25/10/17
65	Crear y validar las reglas de firewall en un entorno de prueba	12 días	mar 10/10/17	mié 25/10/17
66	Migrar las reglas al nuevo firewall	12 días	mar 10/10/1	mié 25/10/17
67	Realizar pruebas de funcionamiento de los servicios	12 días	mar 10/10/17	mié 25/10/17
68	Realizar las adecuaciones para que todos los servicios publicados en internet cuenten con protección de IPS, AV y DOS	7 días	jue 26/10/17	vie 3/11/17
69	Crear profiles de AV, IPS y Antivirus en el firewall	7 días	jue 26/10/17	vie 3/11/17
70	Asignar los profiles a los servicios publicados en internet	7 días	jue 26/10/17	vie 3/11/17
71	Realizar pruebas de los servicios publicados en internet	7 días	jue 26/10/17	vie 3/11/17
72	Finalizacion Etapa III	0 días	**vie 3/11/17**	vie 3/11/17
73	Etapa IV - Switch de LAN	31 días	lun 6/11/17	vie 5/1/18
74	Implementar segmentación por VLANs para red de usuarios y red de servidores. Configurar ruteo por capa 3 (nivel de red)	19 días	lun 6/11/17	vie 1/12/17
75	Definir rangos de red	19 días	lun 6/11/17	vie 1/12/17
76	Configuración en Switchs, Vlans, puertos de Trunk	19 días	lun 6/11/17	vie 1/12/17
77	Migración de equipos a nuevas redes, asignación de puertos de switch a nuevas Vlans	19 días	lun 6/11/17	vie 1/12/17
78	Pruebas de funcionamiento	19 días	lun 6/11/17	vie 1/12/17

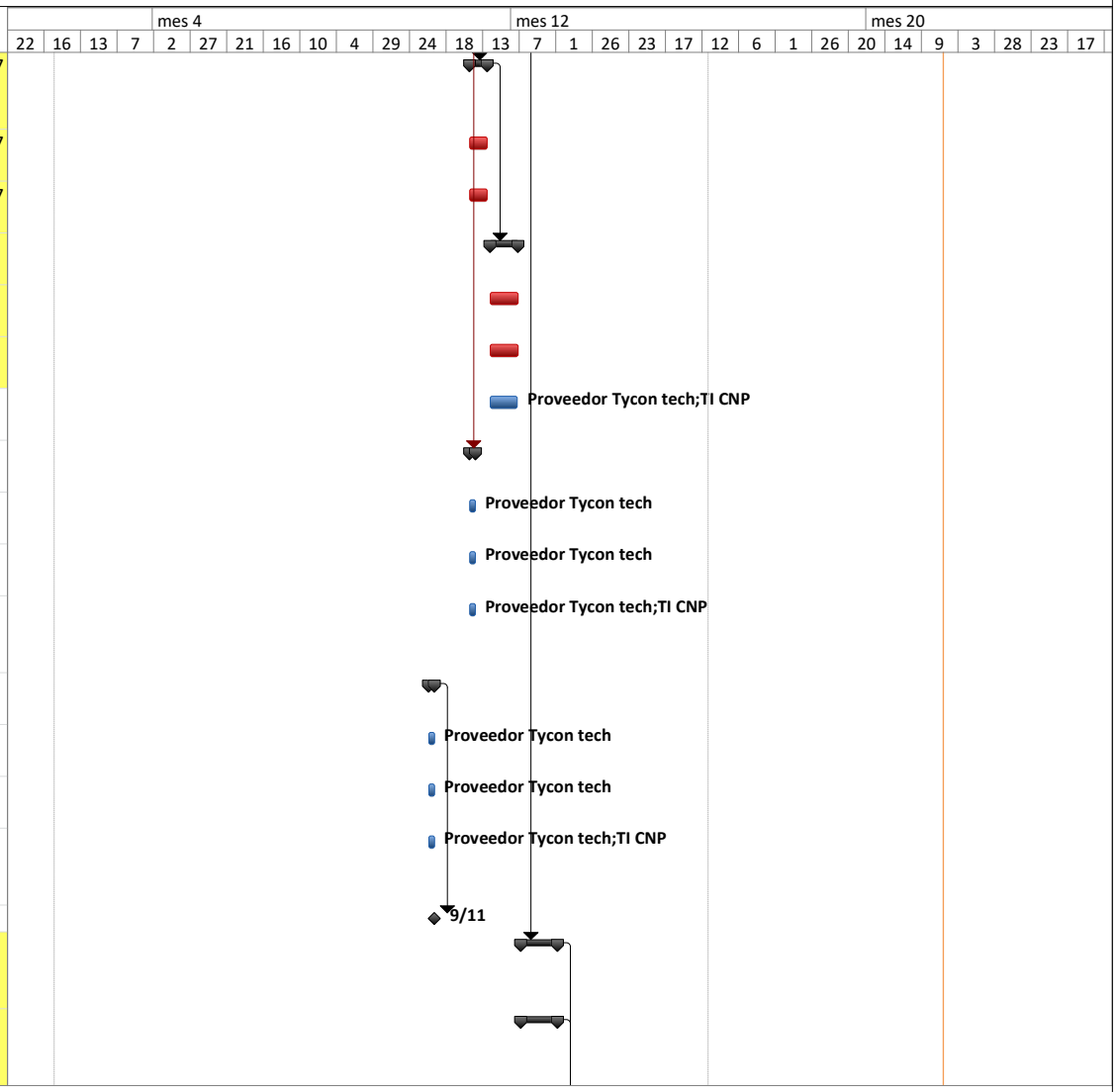


Proyecto: 201-4_ROIRCNP_Tiemp
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin		
División	Hito externo	Sólo duración	Fecha límite		
Hito	Tarea inactiva	Informe de resumen manual	Tareas críticas		
Resumen	Hito inactivo	Resumen manual	División crítica		
Resumen del proyecto	Resumen inactivo	Sólo el comienzo	Progreso		

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	Nombre de tarea	Duración	Comienzo	Fin
79	Realizar las adecuaciones para utilizar otro puerto de backup en caso de falta en el puerto que está en uso	8 días	lun 4/12/17	vie 15/12/17
80	Configurar port channel en cada uno de los switch	8 días	lun 4/12/17	vie 15/12/17
81	Pruebas de puertos de backup y continuidad de servicio	8 días	lun 4/12/17	vie 15/12/17
82	Realizar las adecuaciones para utilizar acceso SSH (secure shell) encriptado	4 días	lun 18/12/17	vie 5/1/18
83	Configurar acceso por secure shell a los switchs	4 días	lun 18/12/17	vie 5/1/18
84	Cancelar la configuración para acceder por telnet	4 días	lun 18/12/17	vie 5/1/18
85	Pruebas de acceso por shh a los equipos	28 horas	lun 18/12/17	vie 5/1/18
86	**Realizar las adecuaciones para no utilizar la vlan nativa para tráfico de red**	**4 días**	**lun 4/12/17**	**jue 7/12/17**
87	Configurar VLAN para gestión de dispositivos de red	4 días	lun 4/12/17	jue 7/12/17
88	Configurar una dirección ip de la nueva vlan a los dispositivos	4 días	lun 4/12/17	jue 7/12/17
89	Pruebas de acceso	4 días	lun 4/12/17	jue 7/12/17
90	**Realizar las adecuaciones para asignar una red exclusiva para las impresoras**	**4 días**	**lun 6/11/17**	**jue 9/11/17**
91	Configurar VLAN para impresoras y asignar puertos	4 días	lun 6/11/17	jue 9/11/17
92	Configurar la nueva dirección IP en las impresoras	4 días	lun 6/11/17	jue 9/11/17
93	Pruebas de funcionamiento	4 días	lun 6/11/17	jue 9/11/17
94	Finalizacion Etapa IV	0 días	**jue 9/11/17**	jue 9/11/17
95	Etapa V - Protección de Redes Internas	19 días	lun 8/1/18	jue 1/2/18
96	Realizar las adecuaciones para que todo el tráfico entre redes de la empresa pase a través del firewall	19 días	lun 8/1/18	jue 1/2/18

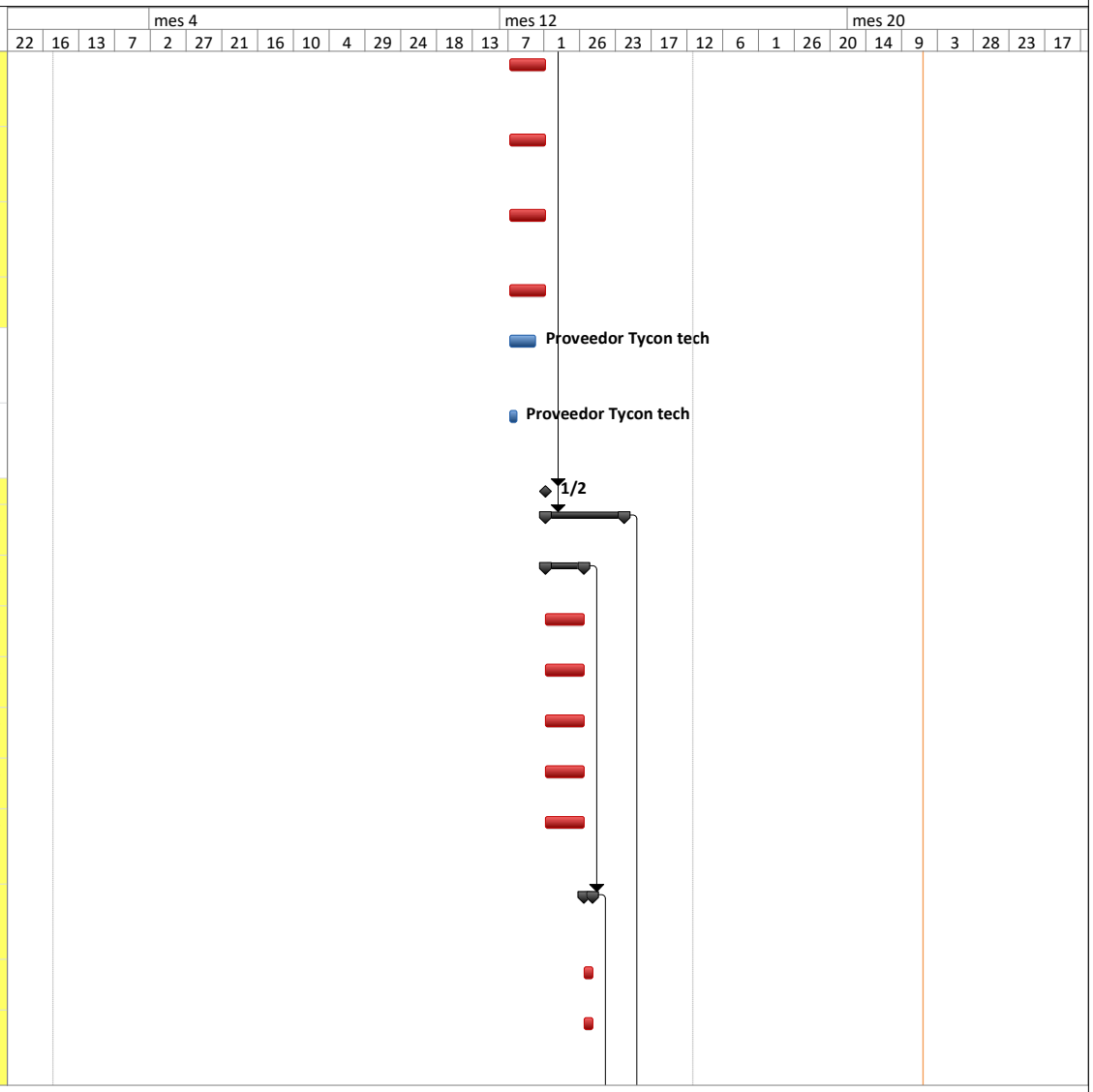


Proyecto: 201-4_ROIRCNP_Tiemp
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin
División	Hito externo	Sólo duración	Fecha límite
Hito	Tarea inactiva	Informe de resumen manual	Tareas críticas
Resumen	Hito inactivo	Resumen manual	División crítica
Resumen del proyecto	Resumen inactivo	Sólo el comienzo	Progreso

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	Nombre de tarea	Duración	Comienzo	Fin
97	Adquisición de firewall UTM	19 días	lun 8/1/18	jue 1/2/18
98	Ajustes de firewall UTM en la topología	19 días	lun 8/1/18	jue 1/2/18
99	Ajustes de configuración en reglas de a	19 días	lun 8/1/18	jue 1/2/18
100	Pruebas y testeos de conexión entre las distintas redes	19 días	lun 8/1/18	jue 1/2/18
101	Aplicar IPS, AV, restricciones de ancho de banda para el tráfico LAN to LAN y LAN to WAN	14 días	lun 8/1/18	jue 25/1/18
102	Permitir el acceso a la infraestructura tecnológica solo desde la red de informática.	5 días	lun 8/1/18	vie 12/1/18
103	Finalizacion Etapa V	0 días	**jue 1/2/18**	jue 1/2/18
104	Etapa VI - Webfiltering, Antispam y Procedimientos	39 días	vie 2/2/18	mié 28/3/18
105	Implementar un esquema de WebFiltering en alta disponibilidad	19 días	vie 2/2/18	mié 28/2/18
106	Adquisición de firewall UTM (con funcionalidad de WebFilter)	19 días	vie 2/2/18	mié 28/2/18
107	Configuración inicial del equipo y del servicio de webfiltering	19 días	vie 2/2/18	mié 28/2/18
108	Relevamiento de configuración del WebSense	19 días	vie 2/2/18	mié 28/2/18
109	Migración de configuración al nuevo equipo	19 días	vie 2/2/18	mié 28/2/18
110	Pruebas del servicio de Webfiltering	19 días	vie 2/2/18	mié 28/2/18
111	Desarrollar las directrices de un procedimiento backup y control de cambios sobre el equipamiento de TI	4 días	jue 1/3/18	mar 6/3/18
112	Indicar recomendaciones para generar un procedimiento de backup	4 días	jue 1/3/18	mar 6/3/18
113	Indicar recomendaciones para generar un procedimiento de control de cambios	4 días	jue 1/3/18	mar 6/3/18

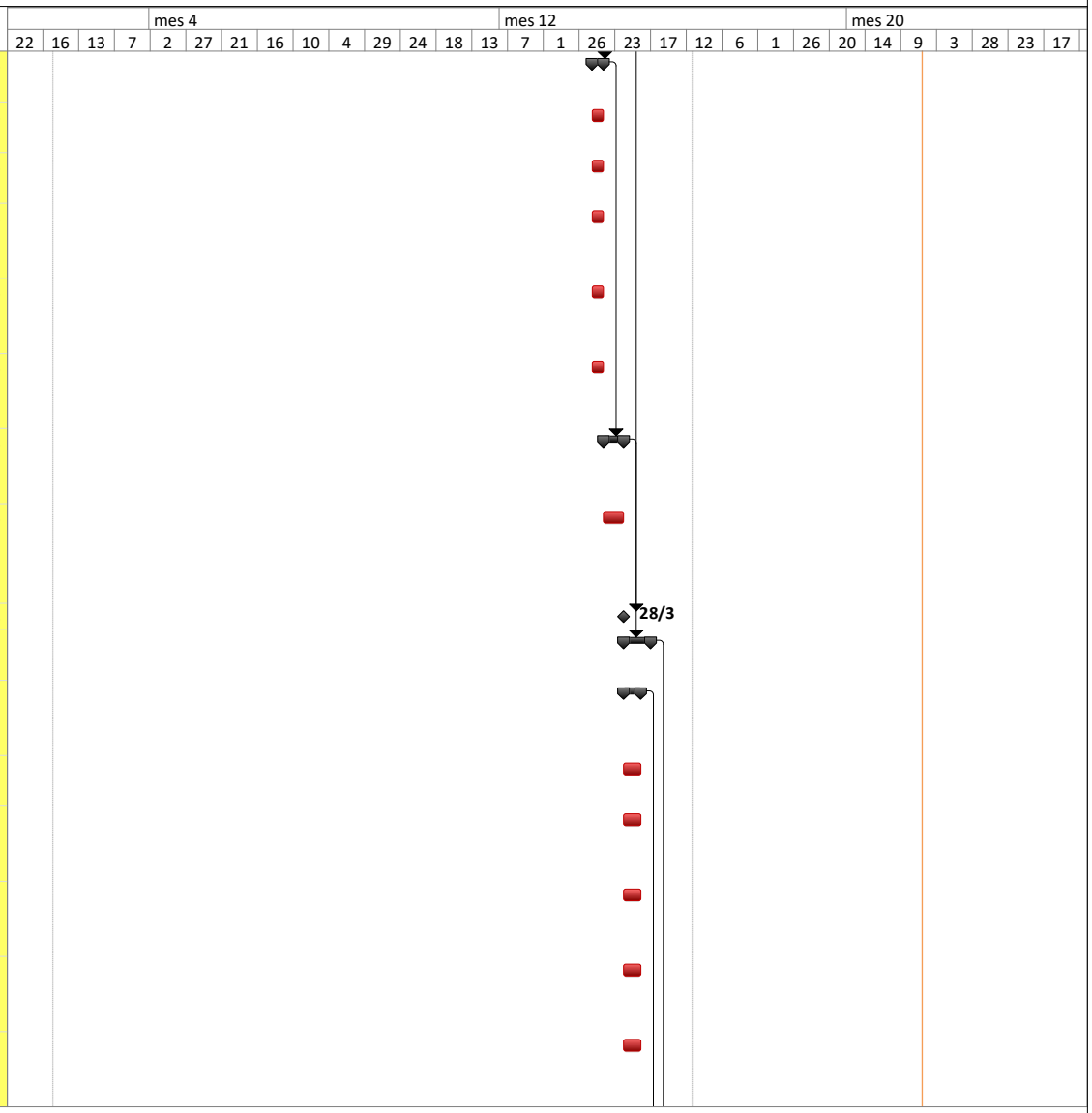


Proyecto: 201-4_ROIRCNP_Tiemp
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin		
División	Hito externo	Sólo duración	Fecha límite		
Hito	Tarea inactiva	Informe de resumen manual	Tareas críticas		
Resumen	Hito inactivo	Resumen manual	División crítica		
Resumen del proyecto	Resumen inactivo	Sólo el comienzo	Progreso		

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	Nombre de tarea	Duración	Comienzo	Fin
114	Implementar un esquema de Antispam en alta disponibilidad	6 días	mié 7/3/18	mié 14/3/18
115	Gestionar la adquisición del equipamiento	6 días	mié 7/3/18	mié 14/3/18
116	Configuración inicial del equipamiento	6 días	mié 7/3/18	mié 14/3/18
117	Relevamiento de configuración actual	6 días	mié 7/3/18	mié 14/3/18
118	Migración de configuración	6 días	mié 7/3/18	mié 14/3/18
119	Pruebas de servicio	6 días	mié 7/3/18	mié 14/3/18
120	Desarrollar las directrices de un procedimiento diferencial para el ABM de cuentas de administrador de domino	10 días	jue 15/3/18	mié 28/3/18
121	Indicar recomendaciones para generar un procedimiento para ABM de cuentas de administrador de dominio	10 días	jue 15/3/18	mié 28/3/18
122	Finalizacion Etapa VI	0 días	mié 28/3/18	mié 28/3/18
123	Etapa VII - RED WiFi, MPLS y Backup Satélital	13 días	jue 29/3/18	lun 16/4/18
124	Implementar cifrado WPA2 o WPA2/Enterprise, SSID Corporativo y SSID Invitados, ajustes de seguridad	8 días	jue 29/3/18	lun 9/4/18
125	Sincronizar wireless controller con usuarios active directory	8 días	jue 29/3/18	lun 9/4/18
126	Configurar cifrado WPA2/Enterprise con autenticación para SSID Corporativo	8 días	jue 29/3/18	lun 9/4/18
127	Configurar cifrado WPA2	8 días	jue 29/3/18	lun 9/4/18
128	Definir red vlan de red WiFi corporativa y vlan de red WiFi invitados	8 días	jue 29/3/18	lun 9/4/18
129	Ajustes en red LAN	8 días	jue 29/3/18	lun 9/4/18

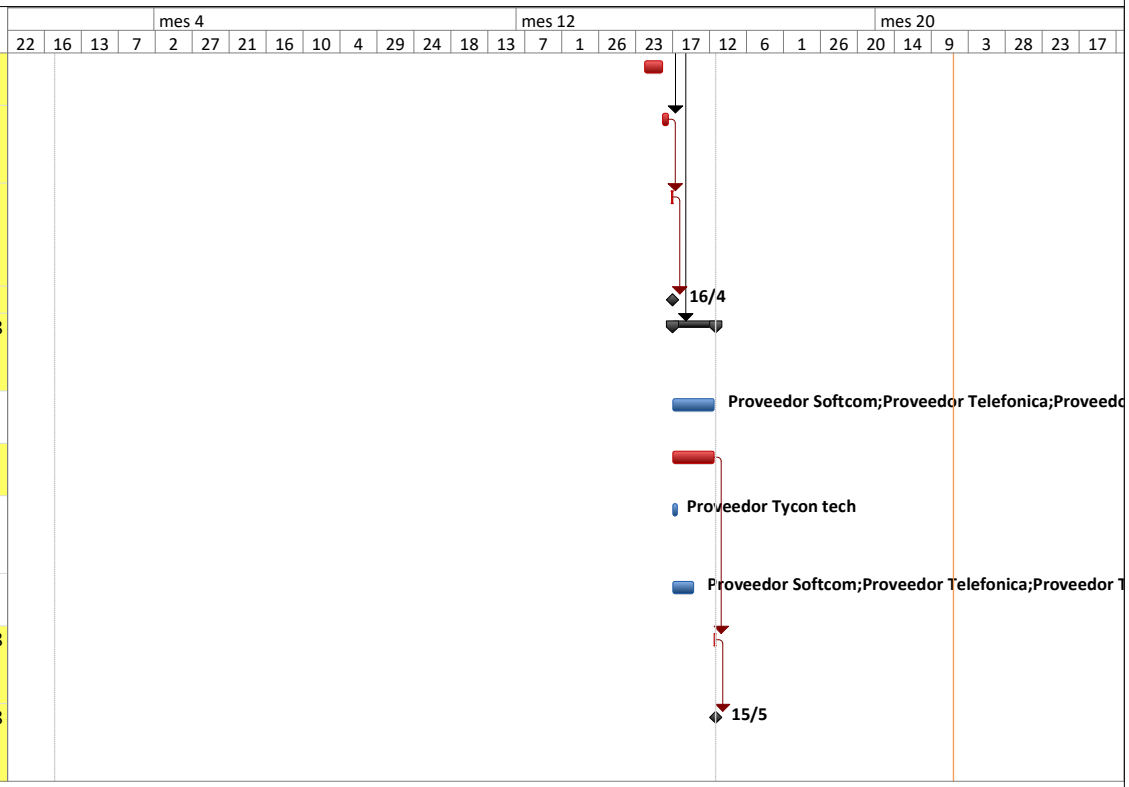


Proyecto: 201-4_ROIRCNP_Tiemp
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin		
División	Hito externo	Sólo duración	Fecha límite		
Hito	Tarea inactiva	Informe de resumen manual	Tareas críticas		
Resumen	Hito inactivo	Resumen manual	División crítica		
Resumen del proyecto	Resumen inactivo	Sólo el comienzo	Progreso		

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	Nombre de tarea	Duración	Comienzo	Fin
130	Documentación, pruebas y test de conexión	8 días	jue 29/3/18	lun 9/4/18
131	Desarrollar un procedimiento para implementar conmutación de enlace MPLS y Backup Satelital	4 días	mar 10/4/18	vie 13/4/18
132	Interactuar con el proveedor y coordinar implementación de conmutación automática de enlace principal a enlace backup y viceversa	1 día	lun 16/4/18	lun 16/4/18
133	Finalizacion Etapa VII	0 días	**lun 16/4/18**	lun 16/4/18
134	Cierre	21 días	mar 17/4/18	mar 15/5/18
135	Informe final del proyecto	20 días	mar 17/4/18	lun 14/5/18
136	Entrega de ingenieria de detalle completa	20 días	mar 17/4/18	lun 14/5/18
137	Propuesta de soporte y mantenimiento	3 días	mar 17/4/18	jue 19/4/18
138	Lecciones aprendidas y recomendaciones	10 días	mar 17/4/18	lun 30/4/18
139	Reunion de entrega	1 día	mar 15/5/18	mar 15/5/18
140	Finalizacion del proyecto	0 días	mar 15/5/18	mar 15/5/18

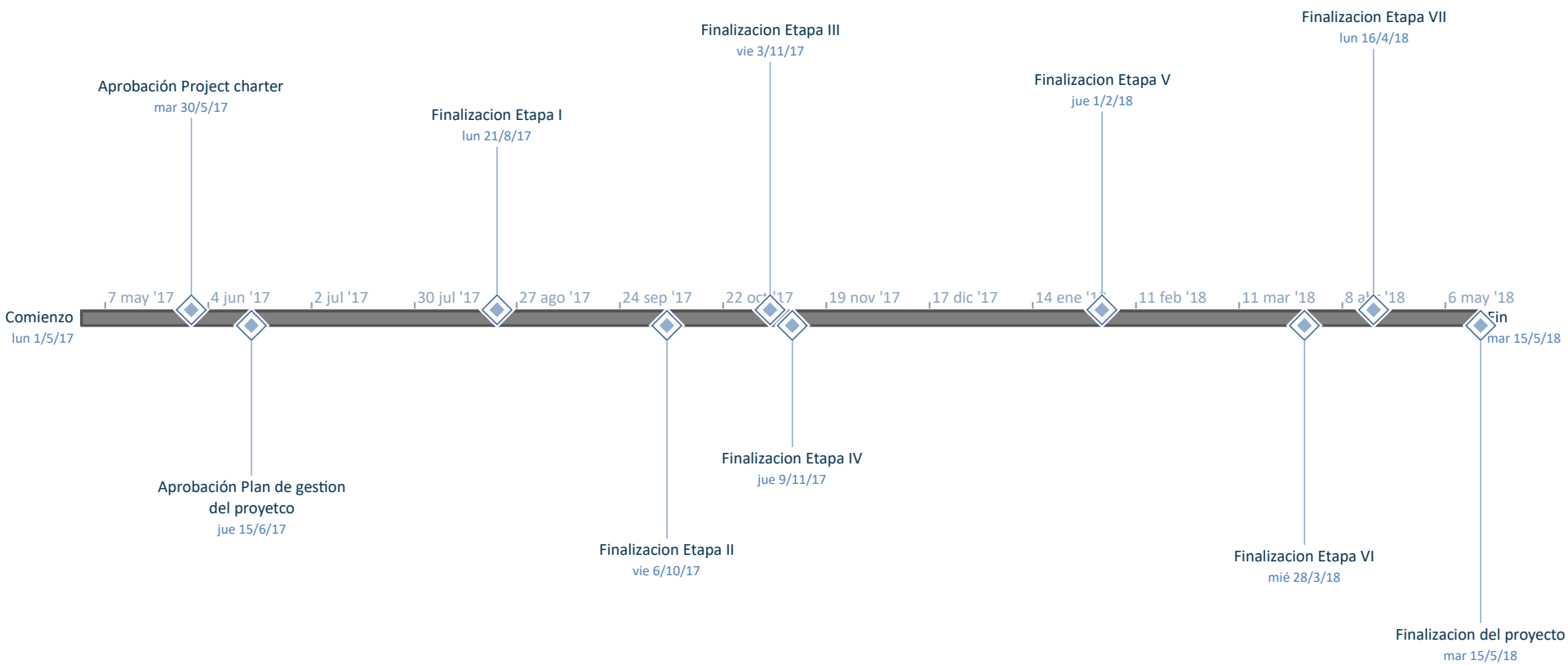


Proyecto: 201-4_ROIRCNP_Tiemp
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin				
División	Hito externo	Sólo duración	Fecha límite				
Hito	Tarea inactiva	Informe de resumen manual	Tareas críticas				
Resumen	Hito inactivo	Resumen manual	División crítica				
Resumen del proyecto	Resumen inactivo	Sólo el comienzo	Progreso				

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Hitos



Autor: James Vallejo PM

Compañía Nacional del Petróleo

Costo

Plan de gestión

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Autor: James Vallejo Mejia

Registro de cambios

Fecha	Versión	Descripción	Autor	Aprobación
23/3/2017	1	Plan de gestión	PM	
17/04/2017	2	Costo - Plan de gestión		

Contenido

Plan de gestión del costo

1 Introducción

En el siguiente plan de gestión de los Costos, Se establecen los procedimientos, políticas y la documentación necesaria para planificar, administrar, ejecutar el gasto y controlar los costos del proyecto. El beneficio de este proceso es que proporciona la dirección sobre cómo Se gestionarán los costos del proyecto a lo largo del mismo.

En el plan de gestión de costos se manejarán los siguientes parámetros:

Unidades de medida	Recurso	Tiempo	Moneda
	unidades	Horas	Pesos Argentinos ($)

2 Herramientas

Para la elaboración del Presupuesto final y análisis de Costos, se utilizará la herramienta informática Microsoft Excel versión 2013

3 Elaboración del presupuesto y estimación de costos

El costo total del proyecto se realiza mediante estimación ascendente, subiendo en detalle desde el costo de cada paquete de trabajo, realizando el análisis necesario hasta lograr el cálculo de los entregables de la EDT, se bajará hasta el nivel 3 de la EDT, detallando y precisando el costo de cada actividad.

Para el cálculo se tendrá en cuenta la cantidad de horas requeridas para cada paquete de trabajo, cantidad de recursos, Experiencia y nivel de especialización de los recursos, costo de equipamiento y gastos administrativos.

En la gráfica se muestra la plantilla a utilizar para el costo de cada paquete de trabajo, con su respectivo detalle y nivel de precisión:

Detalle de costos por cada paquete de trabajo									
Paquetes de trabajo	**Duración hrs**	**Analista de soporte junior**		**Ingeniero Senior**		**Personal Administrativo**		**Equipamiento**	**Costo total**
		Cantidad recursos	**Costo en Pesos ARG. $**	**Cantidad recursos**	**Costo en Pesos ARG. $**	**Cantidad**	**Costo en Pesos ARG. $**	**Costo en Pesos ARG. $**	**Costo en Pesos ARG. $**
Etapa I - Servicios DNS Externo y DHCP									**$ 1.132.475,00**
Habilitar protección de IPS, AV y publicar solo puertos necesarios para el	**105**		**$ 26.250,00**		**$ 36.750,00**		**$ 183.750,00**		**$ 246.750,00**
Solicitar al proveedor habilitar solo el puerto 53, protocolos TCP y UDP	35	2	$ 8.750,00	2	$ 12.250,00	3	$ 61.250,00		
Solicitar al proveedor del firewall que habilite para protección de IPS y AV en	35	2	$ 8.750,00	2	$ 12.250,00	3	$ 61.250,00		
Realizar pruebas del servicio	35	2	$ 8.750,00	2	$ 12.250,00	3	$ 61.250,00		

Se estimará una reserva de contingencia de acuerdo a juicio de expertos y siguiendo los lineamientos del negocio, ya que el foco de la compañía es llevar a cabo proyectos, la oficina informática, por lineamiento estratégico también debe usar el valor de referencia. Desde la PgMO, de TI, estiman un valor para la reserva de contingencia que corresponde al 15% del valor del proyecto, teniendo en cuenta el valor de contención de los riesgos en caso de que se llegase a presentar. Además se establece un 20% de reserva de gerencia del proyecto, teniendo un margen adecuado, en caso de generarse otros costos.

Los costos para la gestión del proyecto, se estimará por analogía, tomando como referencia los proyectos de los otros países dónde actualizaron su infraestructura previamente.

La estimación de costos de servicios públicos se realizará de manera paramétrica, teniendo en cuenta un valor de referencia de aumento del 3%, con relación a la facturación actual.

4 Plantilla de presupuesto total

Presupuesto	
Fase	**Costo**
Total del proyecto	
Reserva de contingencia (15%)	
Linea base de costos	
Reserva de gerencia (20%)	
Presupuesto Total	

5 Consideraciones globales

La estimación de costos incluye todos los impuestos vigentes: IVA, impuesto a las ganancias, impuesto 25413, IIBB.

Todos los costos se presentan en Pesos Argentinos, Se tiene en cuenta el valor de inflación actual, sin embargo Para los proveedores se maneja el siguiente esquema:

- Un valor fijo por la realización de todas actividades a cargo. El oferente debe identificar las etapas o hitos de certificación y el porcentaje de facturación asociado respecto del total correspondiente al proyecto.

- Un valor hora de técnico especialista para eventuales tareas adicionales que se requieran realizar por fuera de las enunciadas, con intervención directa de los recursos del oferente afectados al proyecto.

- Un valor mensual para brindar soporte con especialistas certificados.

6 Control y seguimiento

El control del presupuesto se realizará frecuentemente, cada vez que se realicé un pago o adquisición, se tomará como referencia la última línea base aprobada.

Las empresas contratistas deberán pasar un informe semanal con el avance del proyecto, al finalizar cada fase se realizará la revisión correspondiente y así se realizará el desembolso, por las labores realizadas.

El control del desempeño se hará cada mes y se estimará de acuerdo a la metodología Gestión de Valor Ganado (EVM). Evaluando así el desempeño y avance del proyecto.[1]

Se prevé que el informe de desempeño, con el respectivo control de costos será entregado a la dirección general, durante el los días viernes hábiles de cada semana, también incluirán los cambios necesarios y actualizaciones del plan de proyecto.

[1] (Project Manager Institute, s.f.)

Referencias

Project Manager Institute. (s.f.). *La gestión del valor ganado y su aplicación*. Obtenido de https://www.pmi.org/learning/library/earned-value-management-best-practices-7045

Proyecto remediación y optimización infraestructura de red y seguridad informática CNP

Presupuesto	
Etapa	**Costo**
Etapa I - Servicios DNS Externo y DHCP	$ 1.132.475,00
Etapa II - Protección de Borde I	$ 3.752.144,67
Etapa III - Protección de Borde II	$ 1.249.000,00
Etapa IV - Switch de LAN	$ 2.481.325,00
Etapa V - Protección de Redes Internas	$ 1.717.900,00
Etapa VI - Webfiltering, Antispam y Procedimientos	$ 2.453.427,00
Etapa VII - RED WiFi, MPLS y Backup Satelital	$ 1.090.825,00
Gestión del proyecto	$ 1.800.000,00
Gestion de Contratación	$ 400.000,00
Servicios Públicos	$ 95.600,00
Total del proyecto	$ 16.172.696,67
Reserva de contingencia (15%)	$ 2.425.904,50
Línea base de costos	$ 18.598.601,17
Reserva de gerencia (20%)	$ 3.719.720,23
Presupuesto	**$ 22.318.321,40**

Presupuesto

	Valor en Pesos ARG.
Gestión del proyecto	$ 1.800.000,00

	Valor en Pesos ARG.
Gestion de Contratación	$ 400.000,00

Servicios Públicos	Mensual	Diario	% Calculado de incremento
Se calcula un incremento del 3% en la facturación, se incluye el costo en el valor total del proyecto	$ 400.000,00	$ 13.333,33	3%

Tabla de Salarios Base recursos TI y personal administrativo			
Recurso	**Salario Mes (Pesos ARG.)**	**Salario día (Pesos ARG.)**	**Salario Hora (Pesos ARG.)**

Autor: James Vallejo PM

Analista de Comunicaciones Junior	$ 30.000,00	$ 1.000,00	$ 125,00
Analista de comunicaciones Senior	$ 42.000,00	$ 1.400,00	$ 175,00
Personal administrativo	$ 140.000,00	$ 4.666,67	$ 583,33

Se utiliza la tabla de salarios Tabla de Salarios Base recursos TI y personal administrativo, para realizar el calculo del costo por cada paquete de trabajo en la línea base de costo detallada

Detalle de costos por cada paquete de trabajo

Paquetes de trabajo	Duración hrs	Analista de soporte junior		Ingeniero Senior		Personal Administrativo		Equipamiento	Costo total
		Cantidad recursos	Costo en Pesos ARG. $	Cantidad recursos	Costo en Pesos ARG. $	Cantidad	Costo en Pesos ARG. $	Costo en Pesos ARG. $	Costo en Pesos ARG. $
Etapa I - Servicios DNS Externo y DHCP									**$ 1.132.475,00**
Habilitar protección de IPS, AV y publicar solo puertos necesarios para el servicio de	**105**		**$ 26.250,00**		**$ 36.750,00**		**$ 183.750,00**		**$ 246.750,00**
Solicitar al proveedor habilitar solo el puerto 53, protocolos TCP y UDP	35	2	$ 8.750,00	2	$ 12.250,00	3	$ 61.250,00		
Solicitar al proveedor del firewall que habilite para protección de IPS y AV en la	35	2	$ 8.750,00	2	$ 12.250,00	3	$ 61.250,00		
Realizar pruebas del servicio	35	2	$ 8.750,00	2	$ 12.250,00	3	$ 61.250,00		
Ajustar configuración de DNS Server Externo Segundario	**205**		**$ 61.500,00**		**$ 107.625,00**		**$ 358.750,00**		**$ 527.875,00**
Instalación de un servidor con Windows Server 2012	41	3	$ 15.375,00	3	$ 21.525,00	3	$ 71.750,00		
Habilitar servicio de DNS	41	2	$ 10.250,00	3	$ 21.525,00	3	$ 71.750,00		
Transferir zonas desde DNS principal al segundario	41	2	$ 10.250,00	3	$ 21.525,00	3	$ 71.750,00		
Gestionar configuraciones para publicación en internet	41	2	$ 10.250,00	3	$ 21.525,00	3	$ 71.750,00		
Realizar pruebas de servicios	41	3	$ 15.375,00	3	$ 21.525,00	3	$ 71.750,00		
Configurar otro registro MX para un Mail Server Segundario	**100**		**$ 25.000,00**		**$ 35.000,00**		**$ 175.000,00**		**$ 235.000,00**
En el servidor de DNS, agregar un DNS record de tipo MX (Mail Exchanger)	50	2	$ 12.500,00	2	$ 17.500,00	3	$ 87.500,00		
Asignar una prioridad para que actúe como backup (debe ser un número mayor que el del primario)	50	2	$ 12.500,00	2	$ 17.500,00	3	$ 87.500,00		
Implementar un esquema de HA para el servidor de DHCP	**144**		**$ 42.000,00**		**$ 75.600,00**		**$ 252.000,00**		**$ 369.600,00**

Instalación de dos servidores con Windows Server 2012	48	2	$ 12.000,00	3	$ 25.200,00	3	$ 84.000,00		
Configurar los servicios de DHCP y conmutación por error en modo load	48	2	$ 12.000,00	3	$ 25.200,00	3	$ 84.000,00		
Realizar pruebas del servicio	48	3	$ 18.000,00	3	$ 25.200,00	3	$ 84.000,00		
Etapa II - Protección de Borde I									**$ 3.752.144,67**
Implementar un clúster de firewall para borde y VPN en clúster de alta disponibilidad	**300**		**$ 75.000,00**		**$ 122.500,00**		**$ 495.833,33**	**$ 685.368,00**	**$ 1.378.701,33**
Adquisición de firewall UTM para HA	50	0	$ -	1	$ 8.750,00	2	$ 58.333,33	Cisco ASA 5545 (2)	
Instalación y configuración inicial	50	2	$ 12.500,00	2	$ 17.500,00	3	$ 87.500,00		
Importar configuraciones de borde	50	2	$ 12.500,00	2	$ 17.500,00	3	$ 87.500,00		
Pruebas de funcionamiento	50	3	$ 18.750,00	3	$ 26.250,00	3	$ 87.500,00		
Importar configuraciones de VPN	50	2	$ 12.500,00	3	$ 26.250,00	3	$ 87.500,00		
Pruebas de funcionamiento	50	3	$ 18.750,00	3	$ 26.250,00	3	$ 87.500,00		
Ajustar servicios publicados en internet y configurar aplicaciones publicadas en la red	**270**		**$ 78.750,00**		**$ 110.250,00**		**$ 472.500,00**		**$ 661.500,00**
Solicitar al proveedor del firewall habilitar solo los puertos necesarios de los servicio publicados en internet	90	2	$ 22.500,00	2	$ 31.500,00	3	$ 157.500,00		
Verificar servicios que no están en la red DMZ y moverlos a esta red	90	2	$ 22.500,00	2	$ 31.500,00	3	$ 157.500,00		
Pruebas de funcionamiento	90	3	$ 33.750,00	3	$ 47.250,00	3	$ 157.500,00		
Implementar una alternativa tecnológica diferente al TMG, ya el servicio está	**548**		**$ 68.500,00**		**$ 383.600,00**		**$ 879.083,33**	**$ 380.760,00**	**$ 1.711.943,33**
Adquisición de firewall UTM	137	0	$ -	1	$ -	2	$ 159.833,33	Fortigate 200 D (2) + Licencias	
Relevar configuraciones de permisos de acceso en el TMG	137	2	$ 34.250,00	3	$ 71.925,00	3	$ 239.750,00		
Migrar configuraciones de permisos de acceso a los firewalls UTM	137	2	$ 34.250,00	3	$ 71.925,00	3	$ 239.750,00		
Pruebas de servicios	137	3	$ -	3	$ 239.750,00	3	$ 239.750,00		
Etapa III - Protección de Borde II									**$ 1.249.000,00**
Realizar las adecuaciones para que los servicios sean publicados desde un único equipo y en forma directa	**208**		**$ 65.000,00**		**$ 100.100,00**		**$ 364.000,00**		**$ 529.100,00**
Verificar que servicios hacia internet están publicados desde el ISA Server y el TMG	52	2	$ 13.000,00	2	$ 18.200,00	3	$ 91.000,00		
Crear y validar las reglas de firewall en un entorno de prueba	52	2	$ 13.000,00	3	$ 27.300,00	3	$ 91.000,00		
Migrar las reglas al nuevo firewall	52	3	$ 19.500,00	3	$ 27.300,00	3	$ 91.000,00		

Realizar pruebas de funcionamiento de los servicios	52	3	$ 19.500,00	3	$ 27.300,00	3	$ 91.000,00		
Realizar las adecuaciones para que todos los servicios publicados en internet cuenten con protección de IPS, AV y DOS	**276**		**$ 92.000,00**		**$ 144.900,00**		**$ 483.000,00**		**$ 719.900,00**
Crear profiles de AV, IPS y Antivirus en el firewall	92	2	$ 23.000,00	3	$ 48.300,00	3	$ 161.000,00		
Asignar los profiles a los servicios publicados en internet	92	3	$ 34.500,00	3	$ 48.300,00	3	$ 161.000,00		
Realizar pruebas de los servicios publicados en internet	92	3	$ 34.500,00	3	$ 48.300,00	3	$ 161.000,00		
Etapa IV - Switch de LAN									**$ 2.841.325,00**
Implementar segmentación por VLANs para red de usuarios y red de servidores. Configurar ruteo por capa 3 (nivel de red)	**600**		**$ 281.250,00**		**$ 183.750,00**		**$ 1.050.000,00**	**$ 400.000,00**	**$ 1.915.000,00**
Definir rangos de red	150	1	$ 18.750,00	2	$ 52.500,00	3	$ 262.500,00		
Configuración en Switchs, Vlans, puertos de Trunk	150	4	$ 75.000,00	2	$ 52.500,00	3	$ 262.500,00	Cisco 3850 (8) + cables de red UTP (400)	
Migración de equipos a nuevas redes, asignación de puertos de switch a nuevas Vlans	150	5	$ 93.750,00	3	$ 78.750,00	3	$ 262.500,00		
Pruebas de funcionamiento	150	5	$ 93.750,00	3	$ -	3	$ 262.500,00		
Realizar las adecuaciones para utilizar otro puerto de backup en caso de falta en el puerto que está en uso	**118**		**$ 36.875,00**		**$ 61.950,00**		**$ 206.500,00**		**$ 305.325,00**
Configurar port channel en cada uno de los switch	59	2	$ 14.750,00	3	$ 30.975,00	3	$ 103.250,00		
Pruebas de puertos de backup y continuidad de servicio	59	3	$ 22.125,00	3	$ 30.975,00	3	$ 103.250,00		
Realizar las adecuaciones para utilizar acceso SSH (secure shell) encriptado	**84**		**$ 31.500,00**		**$ 29.400,00**		**$ 147.000,00**		**$ 207.900,00**
Configurar acceso por secure shell a los switchs	28	3	$ 10.500,00	2	$ 9.800,00	3	$ 49.000,00		
Cancelar la configuración para acceder por telnet	28	3	$ 10.500,00	2	$ 9.800,00	3	$ 49.000,00		
Pruebas de acceso por shh a los equipos	28	3	$ 10.500,00	2	$ 9.800,00	3	$ 49.000,00		
Realizar las adecuaciones para no utilizar la vlan nativa para tráfico de red	**81**		**$ 30.375,00**		**$ 37.800,00**		**$ 141.750,00**		**$ 209.925,00**

Configurar VLAN para gestión de dispositivos de red	27	2	$ 6.750,00	2	$ 9.450,00	3	$ 47.250,00		
Configurar una dirección ip de la nueva vlan a los dispositivos	27	3	$ 10.125,00	3	$ 14.175,00	3	$ 47.250,00		
Pruebas de acceso	27	4	$ 13.500,00	3	$ 14.175,00	3	$ 47.250,00		
Realizar las adecuaciones para asignar una red exclusiva para las impresoras	**81**		**$ 23.625,00**		**$ 37.800,00**		**$ 141.750,00**		**$ 203.175,00**
Configurar VLAN para impresoras y asignar puertos	27	2	$ 6.750,00	3	$ 14.175,00	3	$ 47.250,00		
Configurar la nueva dirección IP en las impresoras	27	2	$ 6.750,00	3	$ 14.175,00	3	$ 47.250,00		
Pruebas de funcionamiento	27	3	$ 10.125,00	2	$ 9.450,00	3	$ 47.250,00		
Etapa V - Protección de Redes Internas									**$ 1.717.900,00**
Realizar las adecuaciones para que todo el tráfico entre redes de la empresa pase a través del firewall	**739**		**$ 131.250,00**		**$ 210.000,00**		**$ 1.050.000,00**		**$ 1.391.250,00**
Adquisición de firewall UTM	150	0	$ -	1	$ 26.250,00	3	$ 262.500,00	Cisco ASA 5545 (2)	
Ajustes de firewall UTM en la topología de red	150	2	$ 37.500,00	2	$ 52.500,00	3	$ 262.500,00		
Ajustes de configuración en reglas de acceso	150	2	$ 37.500,00	2	$ 52.500,00	3	$ 262.500,00		
Pruebas y testeos de conexión entre las distintas redes	150	3	$ 56.250,00	3	$ 78.750,00	3	$ 262.500,00		
Aplicar IPS, AV, restricciones de ancho de banda para el tráfico LAN to LAN y LAN to WAN	**105**	**2**	**$ 26.250,00**	**2**	**$ 36.750,00**	**3**	**$ 183.750,00**		**$ 246.750,00**
Permitir el acceso a la infraestructura tecnológica solo desde la red de informática.	**34**	**2**	**$ 8.500,00**	**2**	**$ 11.900,00**	**3**	**$ 59.500,00**		**$ 79.900,00**
Etapa VI - Webfiltering, Antispam y Procedimientos									**$ 2.453.427,00**
Implementar un esquema de WebFiltering en alta disponibilidad	**735**	**11**	**$ 202.125,00**	**12**	**$ 308.700,00**	**15**	**$ 1.286.250,00**		**$ 1.797.102,00**
Adquisición de firewall UTM (con funcionalidad de WebFilter)	147	0	$ -	1	$ 25.725,00	3	$ 257.250,00	Fortigate 200 D (2) + Licencia	
Configuración inicial del equipo y del servicio de webfiltering	147	2	$ 36.750,00	3	$ 77.175,00	3	$ 257.250,00		
Relevamiento de configuración del WebSense	147	2	$ 36.750,00	2	$ 51.450,00	3	$ 257.250,00		
Migración de configuración al nuevo equipo	147	3	$ 55.125,00	3	$ 77.175,00	3	$ 257.250,00		
Pruebas del servicio de Webfiltering	147	4	$ 73.500,00	3	$ 77.175,00	3	$ 257.250,00		

Desarrollar las directrices de un procedimiento backup y control de cambios sobre el equipamiento de TI	**50**	**0**	**$ -**		**$ 17.500,00**		**$ 58.333,33**		**$ 75.833,33**
Indicar recomendaciones para generar un procedimiento de backup	25	0	$ -	2	$ 8.750,00	2	$ 29.166,67		
Indicar recomendaciones para generar un procedimiento de control de cambios	25	0	$ -	2	$ 8.750,00	2	$ 29.166,67		
Implementar un esquema de Antispam en alta disponibilidad	**235**		**$ 52.875,00**		**$ 98.700,00**		**$ 411.250,00**		**$ 562.825,00**
Gestionar la adquisición del equipamiento	47	0	$ -	1	$ 8.225,00	3	$ 82.250,00	Licencia Fortigate 200D antispam	
Configuración inicial del equipamiento	47	1	$ 5.875,00	2	$ 16.450,00	3	$ 82.250,00		
Relevamiento de configuración actual	47	2	$ 11.750,00	3	$ 24.675,00	3	$ 82.250,00		
Migración de configuración	47	2	$ 11.750,00	3	$ 24.675,00	3	$ 82.250,00		
Pruebas de servicio	47	4	$ 23.500,00	3	$ 24.675,00	3	$ 82.250,00		
Desarrollar las directrices de un procedimiento diferencial para el ABM de cuentas de administrador de domino	**10**		**$ 2.500,00**		**$ 3.500,00**		**$ 11.666,67**		**$ 17.666,67**
Indicar recomendaciones para generar un procedimiento para ABM de cuentas de administrador de dominio	10	2	$ 2.500,00	2	$ 3.500,00	2	$ 11.666,67		
Etapa VII - RED WiFi, MPLS y Backup Satelital									**$ 1.090.825,00**
Implementar cifrado WPA2 o WPA2/Enterprise, SSID Corporativo y SSID Invitados, ajustes de seguridad	**360**		**$ 127.500,00**		**$ 199.500,00**		**$ 630.000,00**		**$ 957.000,00**
Sincronizar wireless controller con usuarios active directory	60	3	$ 22.500,00	4	$ 42.000,00	3	$ 105.000,00		
Configurar cifrado WPA2/Enterprise con autenticación para SSID Corporativo	60	3	$ 22.500,00	3	$ 31.500,00	3	$ 105.000,00		
Configurar cifrado WPA2	60	3	$ 22.500,00	3	$ 31.500,00	3	$ 105.000,00		
Definir red vlan de red WiFi corporativa y vlan de red WiFi invitados	60	2	$ 15.000,00	4	$ 42.000,00	3	$ 105.000,00		
Ajustes en red LAN	60	4	$ 30.000,00	3	$ 31.500,00	3	$ 105.000,00		
Documentación, pruebas y test de conexión	60	2	$ 15.000,00	2	$ 21.000,00	3	$ 105.000,00		

Desarrollar un procedimiento para implementar conmutación de enlace MPLS y Backup Satelital	**29**	**2**	**$ 7.250,00**	**3**	**$ 15.225,00**	**3**	**$ 50.750,00**		**$ 73.225,00**
Interactuar con el proveedor y coordinar implementación de conmutación automática de enlace principal a enlace backup y viceversa	**24**	**2**	**$ 6.000,00**	**3**	**$ 12.600,00**	**3**	**$ 42.000,00**		**$ 60.600,00**

Compañía Nacional del Petróleo

Costo

Distribución del presupuesto

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Autor: James Vallejo Mejia

Registro de cambios

Fecha	Versión	Descripción	Autor	Aprobación
23/3/2017	1	Distribución	PM	
17/04/2017	2	Distribución		

Contenido

Distribución del presupuesto

A continuación se muestra la distribución del presupuesto, para su estimación se tiene en cuenta el valor de cada fase entregable del proyecto, a ese valor se le suma el costo de gestión de proyecto y servicios públicos durante cada etapa.

E: Entregable
PM: Project managment
SP: Servicios Públicos

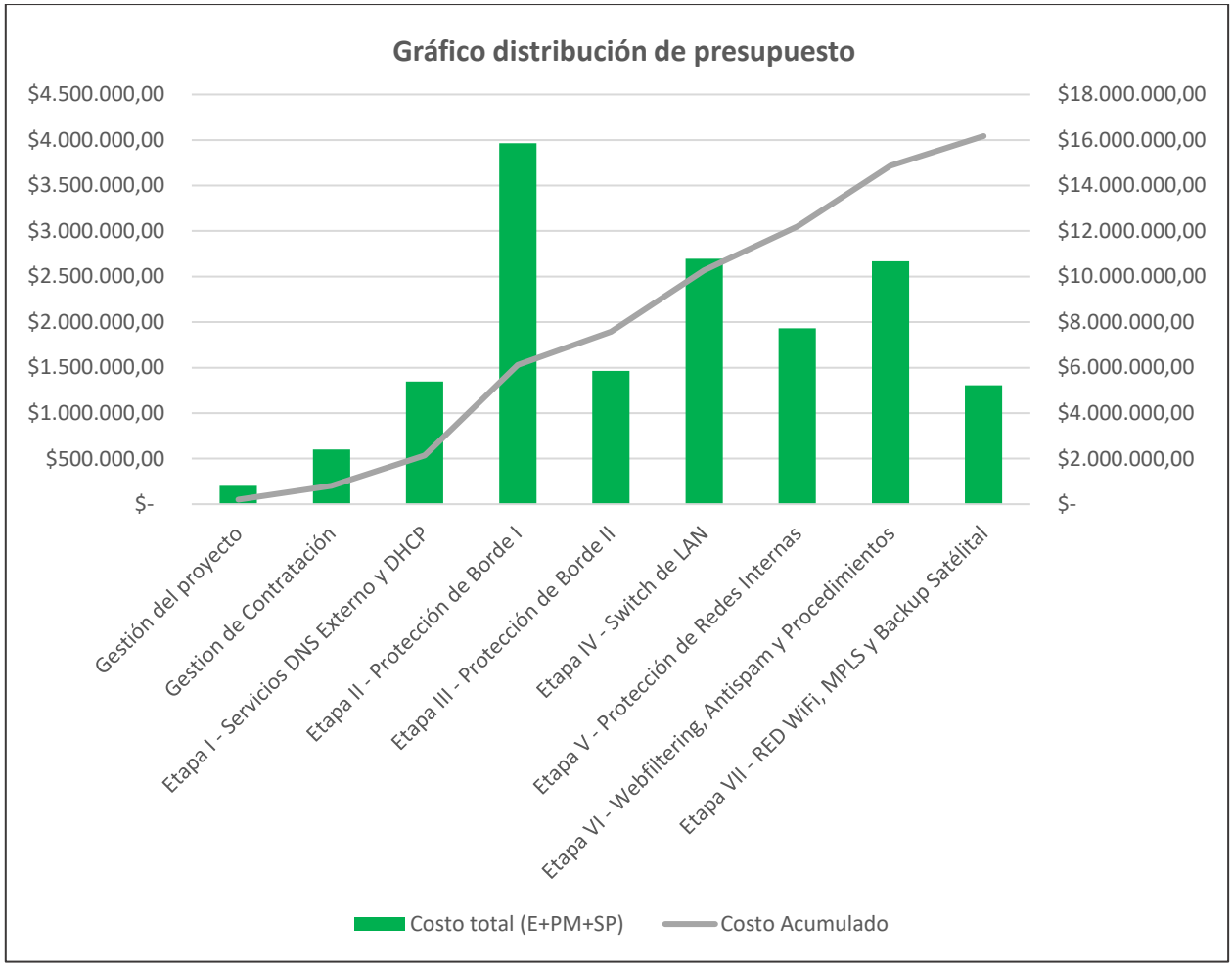
Costo de PM por Etapa	$ 200.000,00
Costo de Servicios Públicos por etapa (Ejecución)	$ 13.657,14

E+PM+SP=Costo total Etapa del proyecto

Tabla distribución del presupuesto

Distribución del presupuesto			
Etapa	**Costo Entregable**	**Costo total (E+PM+SP)**	**Costo Acumulado**
Gestión del proyecto	$ 1.800.000,00	$ 200.000,00	$ 200.000,00
Gestion de Contratación	$ 400.000,00	$ 600.000,00	$ 800.000,00
Etapa I - Servicios DNS Externo y DHCP	$ 1.132.475,00	$ 1.346.132,14	$ 2.146.132,14
Etapa II - Protección de Borde I	$ 3.752.144,67	$ 3.965.801,81	$ 6.111.933,96
Etapa III - Protección de Borde II	$ 1.249.000,00	$ 1.462.657,14	$ 7.574.591,10
Etapa IV - Switch de LAN	$ 2.481.325,00	$ 2.694.982,14	$ 10.269.573,24
Etapa V - Protección de Redes Internas	$ 1.717.900,00	$ 1.931.557,14	$ 12.201.130,38
Etapa VI - Webfiltering, Antispam y Procedimien	$ 2.453.427,00	$ 2.667.084,14	$ 14.868.214,53
Etapa VII - RED WiFi, MPLS y Backup Satélital	$ 1.090.825,00	$ 1.304.482,14	**$ 16.172.696,67**
Servicios Públicos	$ 95.600,00		
Total del proyecto	**$ 16.172.696,67**		
Reserva de contingencia (15%)	$ 2.425.904,50		
Linea base de costos	$ 18.598.601,17		
Reserva de gerencia (20%)	$ 3.719.720,23		
Presupuesto	**$ 22.318.321,40**	$ 16.172.696,67	

Gráfico distribución del presupuesto



Compañía Nacional del Petróleo

Riesgos

Plan de gestión

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Autor: James Vallejo Mejia

Registro de cambios

Fecha	Versión	Descripción	Autor	Aprobación
23/3/2017	1	Plan de gestión	PM	
17/04/2018	2	Riesgos		

Contenido

Plan de gestión de Riesgos

1 Introducción

La Gestión de los Riesgos del Proyecto incluye los procesos relacionados con llevar a cabo la planificación de la gestión, la identificación, el análisis, la planificación de respuesta a los riesgos, así como su monitoreo y control. Los objetivos de la Gestión de los Riesgos del Proyecto son aumentar la probabilidad y el impacto de eventos positivos, y disminuir la probabilidad y el impacto de eventos negativos para el proyecto.[1]

Para este proyecto se realiza el plan de riesgos conocidos para así mitigarlos proactivamente, de igual forma se dispondrá de una reserva de contingencia para aquellos riesgos que puedan acontecer y generar impacto negativo.

2 Metodología

Se realizarán jornadas de asesoramiento, donde participarán todos los involucrados (clientes, proveedores, empleados, auditores.), en estas reuniones se debe realizar la identificación y el análisis de los posibles riesgos, además de sus acciones de mitigación, contención, impacto en caso de ocurrencia.

El equipo de proyectos estará a cargo de estas reuniones y se podrá solicitar estimación de los desvíos en tiempo, costos y alcance. Con esto se buscará estimar las reservas de contingencia. Finalmente se desarrollará una matriz con los riesgos identificados, la cual se llevará a cabo durante la primera línea base, y será actualizada con cada cambio ocurrido en las líneas base, con su respectiva solicitud de Cambio RFC.

El Project manager estará a cargo de liderar los criterios necesarios para realizar una línea base nueva de acuerdo a los riesgos que se planteen; de igual forma toda la información relacionada como planes de mitigación, costos posibles y demás estarán plasmados en los informes de estado semanal y mensual.

[1] (CASTAÑO, s.f.)

3 Registro de riesgos

En este formato se registrarán los riesgos inicialmente:

ID	Riesgo	Categoría de riesgo	Causa	Tipo de Riesgo (Op/Amenaza)

4 Matriz de probabilidad e impacto

Con la experiencia en otros proyectos y alineados al cumplimiento de objetivos estratégicos de la compañía, se definen los siguientes niveles de probabilidad:

Clasificación de riesgos						
Magnitud de impacto	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Probabilidad de amenaza				

Alto Riesgo (15-25)
Medio Riesgo (6-12)
Bajo Riesgo (1-5)

Valores	
1	Muy bajo
2	Bajo
3	Moderado
4	Alto
5	Muy alto

5 Análisis cualitativo

Una vez que se tienen identificados y registrados los riesgos, se procede con el análisis cuantitativo, de la siguiente manera:

Se establece la valoración del riesgo, multiplicando el valor de impacto y el valor de Probabilidad

(PxI), según el resultado y de acuerdo a la matriz descrita anteriormente se procede con la clasificación del riesgo

En la tabla se muestra un ejemplo:

Riesgo	Impacto	Probabilidad	P x I	Categoría
1	5	3	15	Alto
2	3	3	9	Moderado
3	4	3	12	Moderado
4	2	2	4	Bajo
5	4	3	12	Moderado

6 Análisis cuantitativo

Después de haber realizado el análisis cualitativo, por cada paquete de trabajo afectado, se asignará un valor del 5%, sobre la línea base de costo, y se establecerá dentro de la reserva de contingencia.

7 Estrategia y respuestas potenciales

Estrategia	Respuesta potencial
Mitigar/ Transferir/ Aceptar/	Respuesta potencial, después de definir la estrategia

8 Valoración de riesgo

Valoración del riesgo		Respuesta
Menor a 5	Bajo	No se generan planes de mitigación o planes de respuesta, si el riesgo se transforma en problema
Entre 6 a 12	Medio	Se generan planes de respuesta para mitigar la ocurrencia del riesgo o el impacto si el riesgo se transforma en problema.
Mayor a 12	Alto	Cuando se identifica un riesgo de esta categoría se procede a cuantificar cual es el desvío que se produciría en las líneas bases correspondientes y cuál es el costo de evitarlo o mitigarlo. Luego se generan planes de respuesta. Y se ejecutan para eliminar o disminuir el riesgo a “Riesgo medio”.

9 Cambios en Líneas Base

Riesgo	Modificación
1	Se define la modificación realizada sobre la línea base

Referencias

Project Manager Institute. (s.f.). *La gestión del valor ganado y su aplicación*. Obtenido de https://www.pmi.org/learning/library/earned-value-management-best-practices-7045

Compañía Nacional del Petróleo

Calidad

Plan de gestión

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Autor: James Vallejo Mejia

Registro de cambios

Fecha	Versión	Descripción	Autor	Aprobación
23/3/2017	1	Plan de gestión	PM	
17/04/2017	2	Calidad	PM	

Contenido

Plan de gestión de Calidad

1 Introducción

En la Gestión de la Calidad del Proyecto se incluyen los procesos y actividades de la organización que establecen las políticas de calidad, los objetivos y las responsabilidades de calidad, necesarios para cumplir con los altos estándares dentro del mundo TI; brindando así experiencia de servicios Eficientes, conectividad de alta velocidad a los usuarios, seguridad informática, integridad y confidencialidad

2 Documentación de referencia

- PMBOOK – Project Management Body of Knowledge
- Acta Constitutiva del Proyecto
- Planes de Gestión del proyecto
- Líneas Bases del Proyecto
- Normas ISO/IEC 27000, 27001, 27002, 27007 (Seguridad de la información)[1]
- Marco de referencia ITIL – Administración de servicios TI[2]
- ISO 9001 Gestion de calidad
- Normas para cableado estructurado ANSI/EIA/TIA
- Marco de referencia COBIT - framework, dirigida al control y supervisión de tecnología de la información TI [3]

3 Planificación de la gestión de la Calidad

Durante la planificación de la gestión de la calidad se identificarán los requisitos y estándares de calidad del proyecto y sus entregables, así como la documentación con las consignas del cumplimiento de los mismos.

La gestión de la calidad está enfocada en controlar y cumplir los siguientes requisitos:

Objetivo de la revisión de la calidad	Medida de calidad	Método de evaluación de calidad
Procesos del proyecto	Estándares de calidad de los procesos	Actividades de aseguramiento de la calidad
Entregables del proyecto	Estándares de calidad de los entregables	Actividades de control de la calidad

[1] (ISO)
[2] (Axelos, s.f.)
[3] (ISACA, s.f.)

4 Línea base de calidad

Línea base de calidad					
Factor de calidad	Objetivo de calidad	Métricas a usar	Frecuencia de revisión	Responsable	Aprobador
Performance del proyecto	CPI>=0,95	CPI: Cost Performance Índex Acumulado	Frecuencia quincenal	PM	Dirección TI
	SPI>=0,95	SPI: Schedule Performance Index Acumulado	Frecuencia quincenal	PM	Dirección TI

Línea base de calidad					
Entregable	**Objetivo de calidad**	**Control**	**Revisiones**	**Responsable**	**Aprobador**
	Se deberá supervisar, controlar y Verificar, el correcto hacer de todos los entregables de acuerdo a los requisitos de calidad de cada Entregable.	semanal	Se revisará inicio y fin de cada entregable		

5 Procesos de gestión de la calidad

Procesos de gestión de calidad	
Aseguramiento de calidad	El aseguramiento de la calidad se hará monitoreando la performance del trabajo, los resultados del control de calidad y las métricas.
Control de calidad	• Revisión de los entregables para ver si están Conformes o no a lo requerido. • Los resultados de estas mediciones se enviarán al proceso de aseguramiento de la calidad. • Se hará la medición de las métricas y se informaran al proceso de aseguramiento de la calidad. • Para los errores encontrados se buscara el detectar las causas raíces para eliminar la fuente de error. • Se formularán como solicitudes de cambio.
Mejora de procesos	Para mejorar el proceso se deberá seguir los siguientes pasos: 1. Delimitar el proceso. 2. Determinar la oportunidad de mejora. 3. Analizar la información sobre el proceso. 4. Definir y aplicar las acciones correctivas. 5. Verificar si las acciones correctivas han sido efectivas. 6. Estandarizar las mejoras logradas e incorporarlas al proyecto.

Referencias

Axelos. (s.f.). *ITIL*. Obtenido de https://www.axelos.com/best-practice-solutions/itil?utm_source=itil.co.uk&utm_medium=redirect&utm_campaign=redirects

ISACA. (s.f.). *Cobit*. Obtenido de http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx

ISO. (s.f.). *ISO 27701.* https://www.iso.org/standard/54534.html.

Compañía Nacional del Petróleo

RRHH

OBS y Estructura Organizacional

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Autor: James Vallejo Mejia

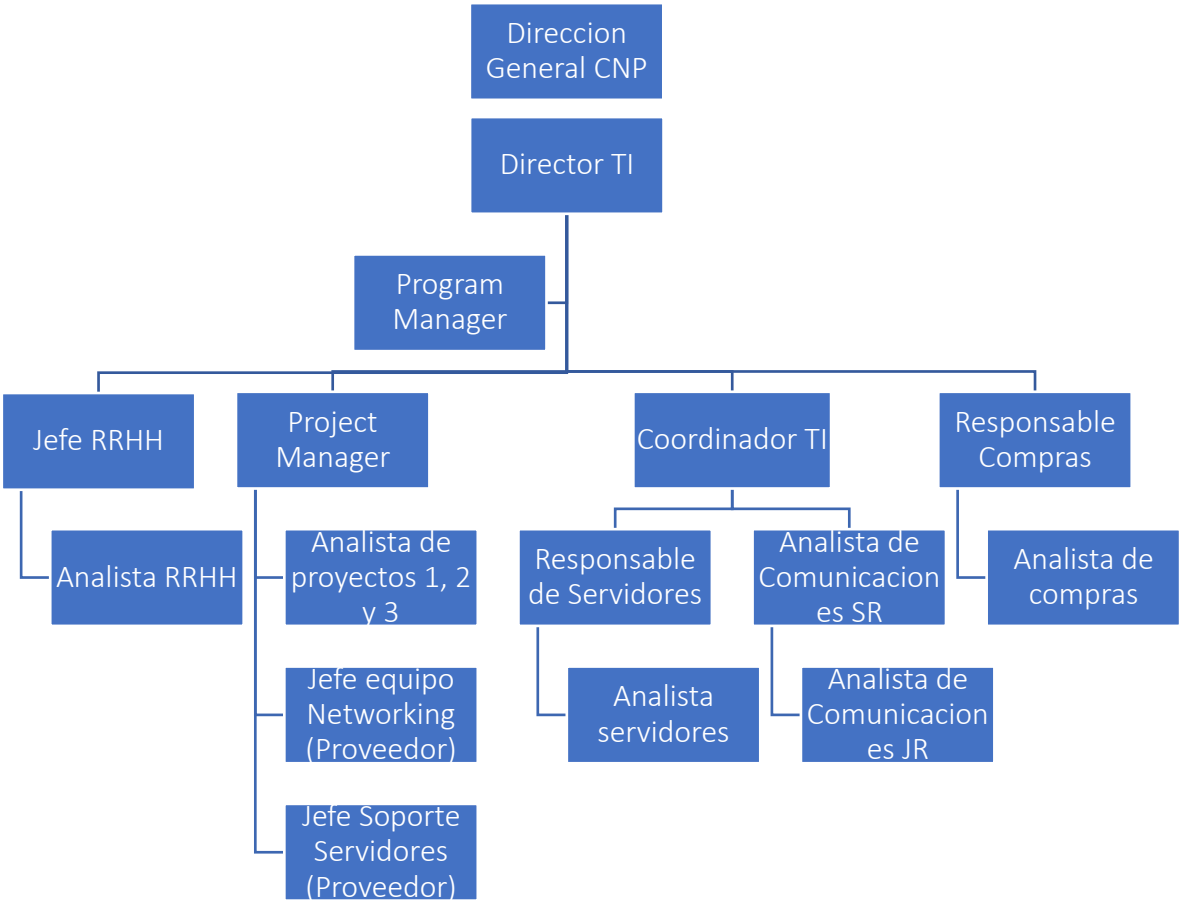
Registro de cambios

Fecha	Versión	Descripción	Autor	Aprobación
23/3/2017	1	Plan de gestión	PM	
17/10/2018	2	OBS	PM	

Contenido

Organización

1 OBS



2 Estructura de la organización

3 Tipo de organización

La organización es del estilo funcional clásica, que consiste en una jerarquía donde cada Empleado tiene un superior claramente definido. Los miembros de la plantilla se agrupan por especialidades, tales como: Planeamiento estratégico y gestión, Legal, RRHH, TI.

Compañía Nacional del Petróleo

Proyecto Remediación y optimización infraestructura de red y seguridad informática

	Misión / Objetivo	Principales Responsabilidades y Tareas	Ubicación del Puesto		Relaciones de Trabajo		Requerimientos de educación	Conocimientos y Competencias Requeridos
			Reporta a	Recibe reportes de	Internos con	Externos con		
Project Manager	Lograr los objetivos del proyecto	Gerenciar el proyecto para lograr los objetivos de costo, plazo y alcance Anticiparse a los problemas y ejecutar planes correctivos Seguimiento y control	Direccion TI	Proveedores, analistas TI, Analistas de proyectos	Direccion TI, RRHH, Finanzas, equipos de proyectos	Proveedores	Profesional de Ingeniería o Administración con conocimientos comprobables en gerenciamiento de Proyectos	Negociación Liderazgo Proactividad
Coordinador TI	Coordinacion del área TI	Gestionar los equipos tecnicos a su cargo Dar resolución a los problemas técnicos de las áreas bajo su supervisión	Direccion TI	PMO, Analistas TI, Proveedores	PM RRHH Analistas TI Direccion TI Finanzas equipo de proyectos	Proveedores	Profesional de Ingeniería con conocimientos comprobables en coordinación técnica	Negociación Liderazgo Proactividad
Analista TI	Mantener los servicios TI funcionando correctamente	Administracion de la infraesrtructura de red, monitoreo y soporte	Coordinador TI	Proveedores, equipos de proyectos	PMO, Coordinacion TI, RRHH	Proveedores	Profesional en ingenieria o Terciario en TI, conocimientos en seguridad informatica y telecomunicaciones	Proactividad, trabajo en equipo
Analista de proyectos	Apoyar tareas de la PMO	Planificacion, ejecucion, control de proyectos	PMO	Analistas TI, Proveedores	Analistas TI, Project manager, RRHH	proveedores	Profesional de Ingeniería o Administración con conocimientos comprobables en gestión de Proyectos	Negociación Liderazgo Proactividad
Oficial de seguridad informática	Velar por el cumplimiento de procesos de seguridad informatica	implementar, verificar, mantener la seguridad informatica de la oficina TI	Direccion TI	Proveedores, analistas TI, Analistas de proyectos, direccion TI	PM RRHH Analistas TI Direccion TI Finanzas equipo de proyectos	proveedores	Profesional de Ingeniería con conocimientos en ISO 27000	Liderazgo, trabajo en equipo, investigación

PM Proveedor de redes	Apoyo a proyectos TI	implementacion de la infraesrtructura de red, monitoreo y soporte	PMO	PMO, coordinador TI, analistas TI	Equipo del proveedor	proveedores	Profesional de Ingeniería o Administración con conocimientos comprobables en gerenciamiento de Proyectos	Negociación Liderazgo Proactividad
Asistente administrativo	Apoyar labores administradores en la oficina TI	Documentación, gestion de compras, contrataciones	Coordinador TI	Analistas TI, proveedores	RRHH, Proveedores, coordinacion TI, Finanzas	proveedores	profesional en administracion	Conocimiento de tecnología, presupuestos, facturación, control de inventarios

Recursos, roles y responsabilidades

Compañía Nacional del Petróleo

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Análisis de interesados

Interesado	Interno I Externo E	Expectativas del interesado en el proyecto	Nivel de Participación: D: Desinteresado / R: Reticente / N: Neutral / P: Partidario / L: Líder — Actual	Nivel de Participación — Deseado	Evaluación del Impacto	Estrategias Potenciales para obtener apoyo o Reducir Obstáculos	Interrelaciones
Dirección general	I	Verificar beneficios del proyecto, cumplimiento de metas, muestra de resultados.	P	L	Constituyen el Sponsor del Proyecto; tienen la potestad de continuar o cancelar el proyecto, financiar el proyecto asignar partidas adicionales, , etc.	Mantener alto su involucramiento Monitorear su adhesión al proyecto Evacuar rápidamente sus dudas y temores	Equipo de Proyecto
Empleados (Equipo de Proyecto)	I	Lograr un proyecto exitoso Mantener su fuente de trabajo Participar en la operación del emprendimiento una vez finalizado el proyecto	P	P	Constituyen la fuerza de trabajo: son generadores de paquetes de trabajo, por lo que impactan directamente en el éxito del proyecto	Mantener alto su compromiso y motivación Detectar rápidamente conflictos internos Detectar rápidamente aquellos recursos que no estén alineados con el proyecto Incentivar al equipo con las proyecciones de futuro dentro de la organización	Administrativos
Empleados (Administrativos	I	Son los usuarios finales y quienes usarán los servicios tecnológicos	P	P	Verificación de la calidad de los servicios instalados, reconocer los avances tecnológicos y sus beneficios	Se debe establecer comunicación constante, durante y después del proyecto, informar oportunamente de los cambios a realizar.	Equipo de Proyecto
Empleados TI	I	Personal de apoyo en el área de tecnología, brindar soporte, recibir los servicios implementados en el proyecto	P	P	estarán involucrados durante todo el proyecto, están alineados con los objetivos de la organización, brindarán soporte ante cualquier eventualidad.	Establecer un canal constante de comunicación, brindar la capacitación necesaria por parte de los proveedores que ejecutan los entregables.	Equipo de Proyecto
Competidores	E	Expectantes de la tecnología de la compañía, como valor agregado a los servicios.	R	N	no tienen impacto directo en el proyecto, Se espera tener tecnología de vanguardia, para estar a la altura de las grandes compañías	Ejecutar el proyecto, mostrar los beneficios de los servicios TI de la compañía	Clientes de la compañía
Clientes de la compañía	E	Percibir seguridad, integridad, confianza y eficiencia en los servicios TI y conectividad a la red.	N	P	Por tratarse de clientes de la compañía, su impacto es muy importante, deben lograr conectividad a las redes de la compañía correctamente.	Informar los servicios TI prestados, demostrar la seguridad en la conexión de la nueva red	Administrativos
Contratistas	E	Ejecutarán las tareas de los entregables, brindar servicios de calidad, apoyar el equipo de proyecto	P	P	Son los actores principales en la ejecución del proyecto, de ellos dependen lo resultados y éxito.	Brindar apoyo, información requerida, acceso, herramientas e involucramiento	Equipo de Proyecto
Sindicatos	E	Defender a los trabajadores involucrados Obtener beneficios para su gremio	N	P	Pueden obstaculizar el desarrollo de los trabajos y demandar compensaciones extraordinarias	Contar con asesoramiento legal Mantener reuniones periódicas con los delegados gremiales para prevenir conflictos	Dirección general
Fabricantes equipos TI	E	Encargados de proveer los equipos y dar soporte por garantía	N	P	Podrían retrasar la entrega de algún equipo o demorar algún tema de garantía o activación de licencias	Establecer contratos de soporte que cubran contingencia, en caso de fallas, realizar las adquisiciones con el tiempo planificado	Equipo de Proyecto
Público en general	E	Acceder a la página web y demás recursos públicos, de una manera rápida, segura y confiable.	N	P	Mostrarán su nivel de satisfacción con los servicios públicos de la compañía	Culminar cada etapa del proyecto, cumplir los estándares de calidad.	Clientes de la compañía

Compañía Nacional del Petróleo

Plan de comunicaciones

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Autor: James Vallejo Mejia

Registro de cambios

Fecha	Versión	Descripción	Autor	Aprobación
23/9/2018	1	Comunicaciones	PM	

Contenido

Plan de comunicaciones

Matriz de comunicaciones

Tipo	Periodicidad	Descripción	Asistentes	Entregable
Kick Off	abril de 2017	Se presenta el proyecto a los Stakeholders, objetivos, presupuesto, riesgos principales, roles y cronogramas.	Principales Staleholders (Sponsor, Proveedores, Gobierno, Representantes de la comunidad, Equipo PM)	Project Charter, línea base del proyecto
Reporte de avance	Semanal Todos los Miércoles	Se hará una consolidación de toda la información que cada integrante del proyecto deba comunicar, se incluirá el avance en porcentaje (%) de cumplimiento de tareas, entregables, sugerencias pedidos de cambios, reportes. Se enviará por E-mail, se da el visto bueno después de las observaciones	Responsables de cada área dentro del Proyecto, Proveedores	Reporte de avance en formato PDF, para proveedores deberán envía además una versión del MS-Project, con el avance de tareas.
Reuniones puntuales	Se programará si se requiere	Abordar temas puntuales del proyecto, desvíos de linea base del proyecto, problemas con proveedores, Nuevos riesgos, cambio de personal	Personal Necesario	Minuta de la reunión
Reunión ejecutiva	Mensual	Se realizará reunión informativa entre socios y PM, análisis de costos, riesgos y decisiones importantes	PM, Sponsor	Informe ejecutivo

Disponibilidad de la informacion

Medios tecnológicos	Frecuente	Se mantendrán las diferentes redes sociales para la comunicación Interna entre integrantes del proyecto y equipos de trabajo.	Equipo de proyecto.	Comunicaciones por redes sociales
Almacenamiento de información	Semanal	Se creará una carpeta en un servidor con acceso limitado a equipo de proyecto y proveedores mediante acceso seguro por VPN (Virtual private Network) allí se cargarán todos los documentos con avances del proyecto.	Responsables de cada área dentro del Proyecto, Proveedores	Documentos Digitales

Compañía Nacional del Petróleo

Matriz de riesgos

ID	Categoria	Tipo	Riesgo	Causa	Entregable afectado	Análisis cualitativio				Acción	Plan de respuesta	Análisis cualitativio				Responsable
						Prob.	Imp.	Riesgo	Prioridad			Prob.	Imp.	Riesgo	Prioridad	
R1	Técnico	Amenaza	Indisponibilidad en los servicios de la red interna durante la ejecución de tareas	Puede ser causado por Falla en alguno de los equipos, configuracion incorrecta	Etapa IV switch de LAN	3	5	15	Alto	Transferir	Se establece la ejecucion de tareas disruptivas, fuera del horario laboral, se planifica alta disponibilidad para mantener el servicio	1	3	3	Baja	Proveedor
R2	Organizacional	Amenaza	Retraso en la ejecucion de tareas de Seguridad	Demora en adquisicion de equipos, no por compras si no por autorizaciones de filiales	Etapa II proteccion de borde	2	5	10	Medio	Transferir	Se informa de este riesgo a la direccion, y a las filiales para que agilicen los procedimientos necesarios	1	3	3	Baja	Direccion TI
R3	Externo	Amenaza	Restricción de las importaciones	Cambio en las politicas de estado	Etapa II proteccion de borde, Etapa IV switch LAN, Etapa V y etapa VI Webfiltering	3	5	15	Alto	Aceptar	Se establece reserva de contingencia para comprar mas costoso Nacional	2	3	6	Media	PM
R4	Técnico	Oportunidad	Actualizacion y mejoras en software de dispositivos	Actualizacion los, Nuevo Firmware, parches	Todos	1	3	3	Bajo	Explotar	Ir a comité de cambios para autorizar la actualizacion o instalacion de feature nuevo	2	2	4	Baja	PM
R5	Organizacional	Amenaza	Intervención de sindicatos	Resistencia a cambios de tecnologia y accesos	Todos	2	3	6	Medio	Mitigar	Brindar capacitacion y acompañamiento a los usuarios finales	1	3	3	Baja	PM
R6	Gestion del PM	Amenaza	incumplimiento de contratos	La posibilidad de que ocurra existe, teniendo ne cuenta el previo análisis para escoger proveedores	todos	1	3	3	Bajo	Mitigar	Imponer claúsulas de protección	1	2	2	Baja	PM

Compañía Nacional del Petróleo

Informe de avance N° 3

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Autor: James Vallejo Mejia

RESUMEN DE ESTADO DEL PROYECTO

RESUMEN DE ESTADO DEL PROYECTO	
Porcentaje completado:	**34%**

-2%	+/-2%	+/-5%
OK	GARANTIZARÁ UN COLOR DE ADVERTENCIA AMARILLO	GARANTIZARÁ UN COLOR DE ADVERTENCIA ROJO

Alcance	Tiempo	Costo	Riesgos	Calidad

El cronograma del proyecto tiene un retraso del 3% con respecto a la línea base. A la fecha 03 de noviembre de 2017, se debería tener completado el 37% del proyecto, Se retrasa la actividad Migrar reglas al nuevo firewall en la etapa III, ya que al realizar las pruebas con los servidores ISA y TMG, se presenta un problema con los certificados, que se encuentran vencidos. Para no afectar el tiempo del proyecto, se realizarán estas actividades en paralelo con las de la siguiente fase, además se pacta con los proveedores y equipo TI, realizar el esfuerzo necesario, extendiendo una hora diaria la jornada.

Los costos se mantienen según lo planificado, se incurre en gastos para solucionar issues utilizando los fondos de la reserva de contingencia.

Durante la etapa II se materializó el riesgo Retraso en la ejecución de tareas de Seguridad, pero como se tenía planificado su plan de respuesta y la responsabilidad, por ello este riesgo se transfirió a la dirección TI, Después del análisis se presentaron cambios en el cronograma, alcance y presupuesto; se adiciona una nueva Etapa, Etapa VIII: Implementar un clúster de firewall para borde y VPN en clúster de alta disponibilidad

TRABAJOS PLANIFICADOS PARA EL ÚLTIMO MES

Nombre de tarea	% completado	Duración	Comienzo	Fin
Etapa III - Protección de Borde II	**41%**	**19 días**	**vie 29/9/17**	**jue 26/10/17**
Realizar las adecuaciones para que los servicios sean publicados desde un único equipo y en forma directa	**45%**	**12 días**	**vie 29/9/17**	**mar 17/10/17**
Verificar que servicios hacia internet están publicados desde el ISA Server y el TMG	100%	12 días	vie 29/9/17	mar 17/10/17
Crear y validar las reglas de firewall en un entorno de prueba	80%	12 días	vie 29/9/17	mar 17/10/17
Migrar las reglas al nuevo firewall	0%	12 días	vie 29/9/17	mar 17/10/17
Realizar pruebas de funcionamiento de los servicios	0%	12 días	vie 29/9/17	mar 17/10/17
Realizar las adecuaciones para que todos los servicios publicados en internet cuenten con protección de IPS, AV y DOS	**33%**	**7 días**	**mié 18/10/17**	**jue 26/10/17**
Crear profiles de AV, IPS y Antivirus en el firewall	0%	7 días	mié 18/10/17	jue 26/10/17
Asignar los profiles a los servicios publicados en internet	0%	7 días	mié 18/10/17	jue 26/10/17
Realizar pruebas de los servicios publicados en internet	0%	7 días	mié 18/10/17	jue 26/10/17
Finalización Etapa III	0%	0 días	jue 26/10/17	jue 26/10/17

TRABAJO COMPLETADO EL ÚLTIMO MES

Nombre de tarea	% completado	Duración	Comienzo	Fin
Etapa III - Protección de Borde II	**31%**	**19 días**	**vie 29/9/17**	**jue 26/10/17**
Realizar las adecuaciones para que los servicios sean publicados desde un único equipo y en forma directa	**45%**	**12 días**	**vie 29/9/17**	**mar 17/10/17**
Verificar que servicios hacia internet están publicados desde el ISA Server y el TMG	100%	12 días	vie 29/9/17	mar 17/10/17

TRABAJO PLANIFICADO PARA EL PROXIMO MES

Migrar las reglas al nuevo firewall	0%	12 días	vie 29/9/17	mar 17/10/17
Realizar pruebas de funcionamiento de los servicios	0%	12 días	vie 29/9/17	mar 17/10/17
Realizar las adecuaciones para que todos los servicios publicados en internet cuenten con protección de IPS, AV y DOS	**33%**	**7 días**	**mié 18/10/17**	**jue 26/10/17**
Crear profiles de AV, IPS y Antivirus en el firewall	0%	7 días	mié 18/10/17	jue 26/10/17
Asignar los profiles a los servicios publicados en internet	0%	7 días	mié 18/10/17	jue 26/10/17
Realizar pruebas de los servicios publicados en internet	0%	7 días	mié 18/10/17	jue 26/10/17
Finalización Etapa III	0%	0 días	jue 26/10/17	jue 26/10/17
Nombre de tarea	% completado	Duración	Comienzo	Fin
Etapa IV - Switch de LAN	0%	31 días	vie 27/10/17	mar 12/12/17
Implementar segmentación por VLANs para red de usuarios y red de servidores. Configurar ruteo por capa 3 (nivel de red)	0%	19 días	vie 27/10/17	mié 22/11/17
Definir rangos de red	0%	19 días	vie 27/10/17	mié 22/11/17
Configuración en Switchs, Vlans, puertos de Trunk	0%	19 días	vie 27/10/17	mié 22/11/17
Migración de equipos a nuevas redes, asignación de puertos de switch a nuevas Vlans	0%	19 días	vie 27/10/17	mié 22/11/17
Pruebas de funcionamiento	0%	19 días	vie 27/10/17	mié 22/11/17
Realizar las adecuaciones para utilizar otro puerto de backup en caso de falta en el puerto que está en uso	0%	8 días	jue 23/11/17	mar 5/12/17
Configurar port channel en cada uno de los switch	0%	8 días	jue 23/11/17	mar 5/12/17
Pruebas de puertos de backup y continuidad de servicio	0%	8 días	jue 23/11/17	mar 5/12/17
Realizar las adecuaciones para utilizar acceso SSH (secure shell) encriptado	0%	4 días	mié 6/12/17	mar 12/12/17
Configurar acceso por secure shell a los switchs	0%	4 días	mié 6/12/17	mar 12/12/17
Cancelar la configuración para acceder por telnet	0%	4 días	mié 6/12/17	mar 12/12/17
Pruebas de acceso por shh a los equipos	0%	4 días	mié 6/12/17	mar 12/12/17

Realizar las adecuaciones para no utilizar la vlan nativa para tráfico de red	0%	4 días	jue 23/11/17	mié 29/11/17
Configurar VLAN para gestión de dispositivos de red	0%	4 días	jue 23/11/17	mié 29/11/17
Configurar una dirección ip de la nueva vlan a los dispositivos	0%	4 días	jue 23/11/17	mié 29/11/17
Pruebas de acceso	0%	4 días	jue 23/11/17	mié 29/11/17
Realizar las adecuaciones para asignar una red exclusiva para las impresoras	0%	4 días	vie 27/10/17	mié 1/11/17
Configurar VLAN para impresoras y asignar puertos	0%	4 días	vie 27/10/17	mié 1/11/17
Configurar la nueva dirección IP en las impresoras	0%	4 días	vie 27/10/17	mié 1/11/17
Pruebas de funcionamiento	0%	4 días	vie 27/10/17	mié 1/11/17
Finalización Etapa IV	0%	0 días	mié 1/11/17	mié 1/11/17

ISSUES ABIERTOS

I-002	Se retrasa la actividad Migrar reglas al nuevo firewall en la etapa III, ya que al realizar las pruebas con los servidores ISA y TMG, se presenta un problema con los certificados, que se encuentran vencidos.

RIESGOS ABIERTOS

No hay riesgos abiertos

ENTREGABLES E HITOS

Hito	WBS	Planificado	Pronosticado	Actual	Estado
Finalización Etapa I	1.4.5	21/8/17	21/8/17	21/8/17	Completado
Finalización Etapa II	1.5.3	28/9/17	28/9/17	28/9/17	Completado
Finalización Etapa III	1.6.3	26/10/17	16/11/17	16/11/17	Retrasado
Finalización Etapa IV	1.7.6	1/11/17	1/11/17	1/11/117	A tiempo
Entregable	WBS	Planificado	Pronosticado	Actual	Estado
Etapa I - Servicios DNS Externo y DHCP	1.4	21/8/17	21/8/17	21/8/17	Completado
Etapa II - Protección de Borde I	1.5	28/9/17	28/9/17	28/9/17	Completado
Etapa III - Protección de Borde II	1.6	26/10/17	16/11/17	16/11/17	Retrasado
Etapa IV - Switch de LAN	1.7	1/11/17	1/11/17	1/11/117	A tiempo

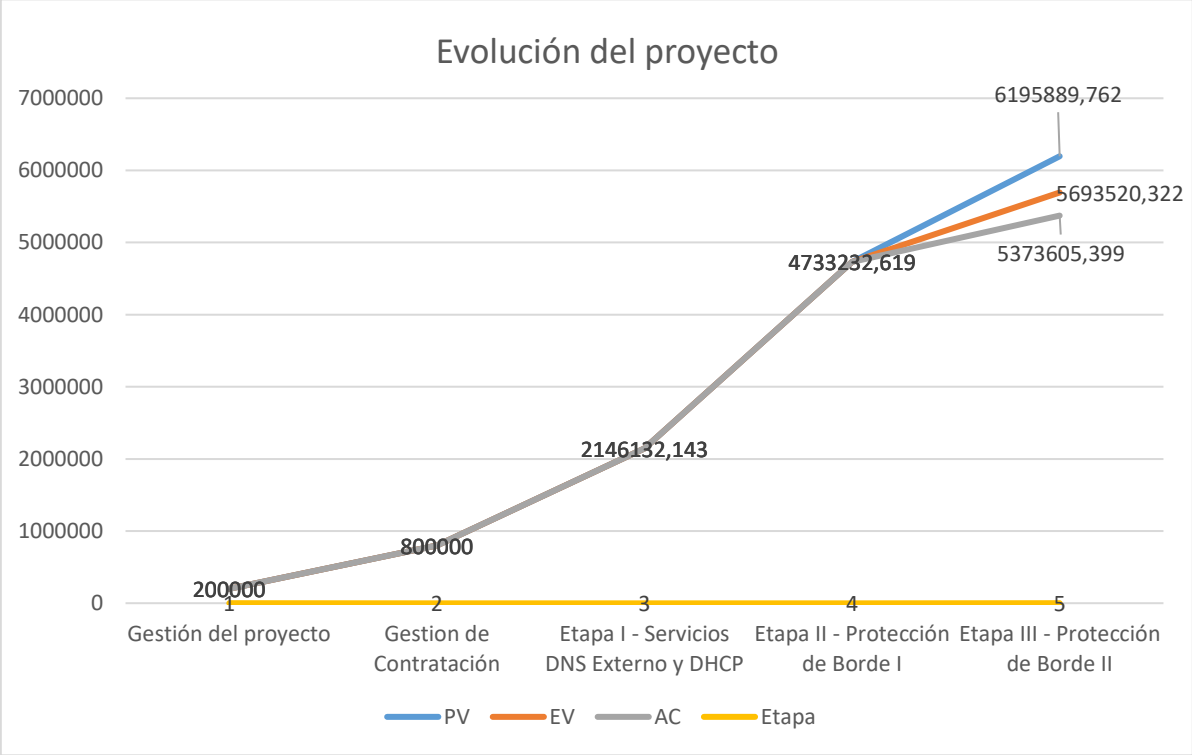
SOLICITUD DE CAMBIO ABIERTA

Nombre de solicitud de cambio	**Numero de solicitud de cambio**	**Fecha de la solicitud**	**Estado actual**
Incluir nueva actividad, tendido de Cableado estructurado	RFC_PM_002	06/10/2017	En revisión por el comité de cambios

Evolución del proyecto EVM

Indicadores

PV	AC	EV
6195889,8	5693520,322	5373605,399



Variaciones e Índices de desempeño

Schedule – El proyecto está retrasado/adelantado según el cronograma	
Schedule Variance (SV)	-502369,4402
Schedule Performance Index (SPI):	0,91
En este caso, el SPI nos indica que solo hemos realizado el 91% de lo que estaba planificado en el cronograma.	

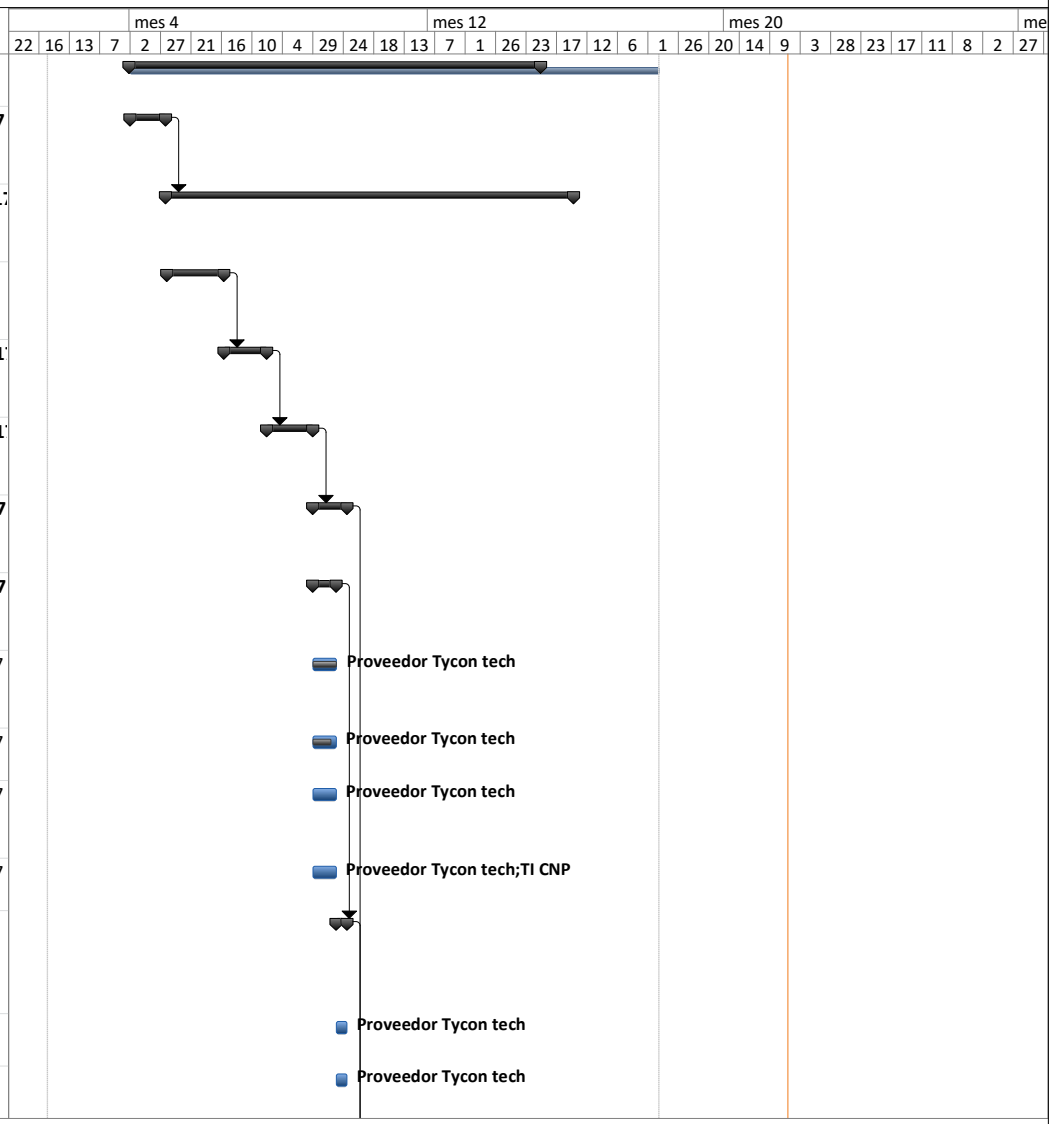
Cost - Project Esta sobre/ Bajo Presupuesto	
Cost Variance (CV):	319914,9227
Cost Performance Index (CPI):	1,059
Pero sin embargo, nuestro Índice de Desempeño de Costo (CPI) es mayor de 1. Vamos retrasado según el cronograma pero no hemos gastado más de lo que teníamos que haber gastado tras la tercera etapa	

CSI	0,9736263
OK, altas posibilidades de cumplir y recuperar el tiempo retrasado	

.

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	EDT	Nombre de tarea	% completado	Duración	Comienzo
1	1	**Remediación Infraestructura y Seguridad Informática**	**34%**	**223 días**	**lun 1/5/17**
2	**1.1**	**Inicio**	**100%**	**20 días**	**mar 2/5/17**
7	**1.2**	**Gestion del proyecto**	**39%**	**221 días**	**mié 31/5/17**
19	**1.3**	**Gestion de Contratación**	**100%**	**31 días**	**jue 1/6/17**
25	**1.4**	**Etapa I - Servicios DNS Externo y DHCP**	**100%**	**24 días**	**mar 18/7/17**
44	**1.5**	**Etapa II - Protección de Borde I**	**99%**	**28 días**	**mar 22/8/17**
55	**1.6**	**Etapa III - Protección de Borde II**	**31%**	**19 días**	**vie 29/9/17**
56	**1.6.1**	**Realizar las adecuaciones para que los servicios sean publicados desde un único equipo y en forma directa**	**45%**	**12 días**	**vie 29/9/17**
57	1.6.1.1	Verificar que servicios hacia internet están publicados desde el ISA Server y el TMG	100%	12 días	vie 29/9/17
58	1.6.1.2	Crear y validar las reglas de firewall en un entorno de prueba	80%	12 días	vie 29/9/17
59	1.6.1.3	Migrar las reglas al nuevo firewall	0%	12 días	vie 29/9/17
60	1.6.1.4	Realizar pruebas de funcionamiento de los servicios	0%	12 días	vie 29/9/17
61	**1.6.2**	**Realizar las adecuaciones para que todos los servicios publicados en internet cuenten con protección de IPS, AV y DOS**	**0%**	**7 días**	**mié 18/10/17**
62	1.6.2.1	Crear profiles de AV, IPS y Antivirus en el firewall	0%	7 días	mié 18/10/17
63	1.6.2.2	Asignar los profiles a los servicios publicados en internet	0%	7 días	mié 18/10/17

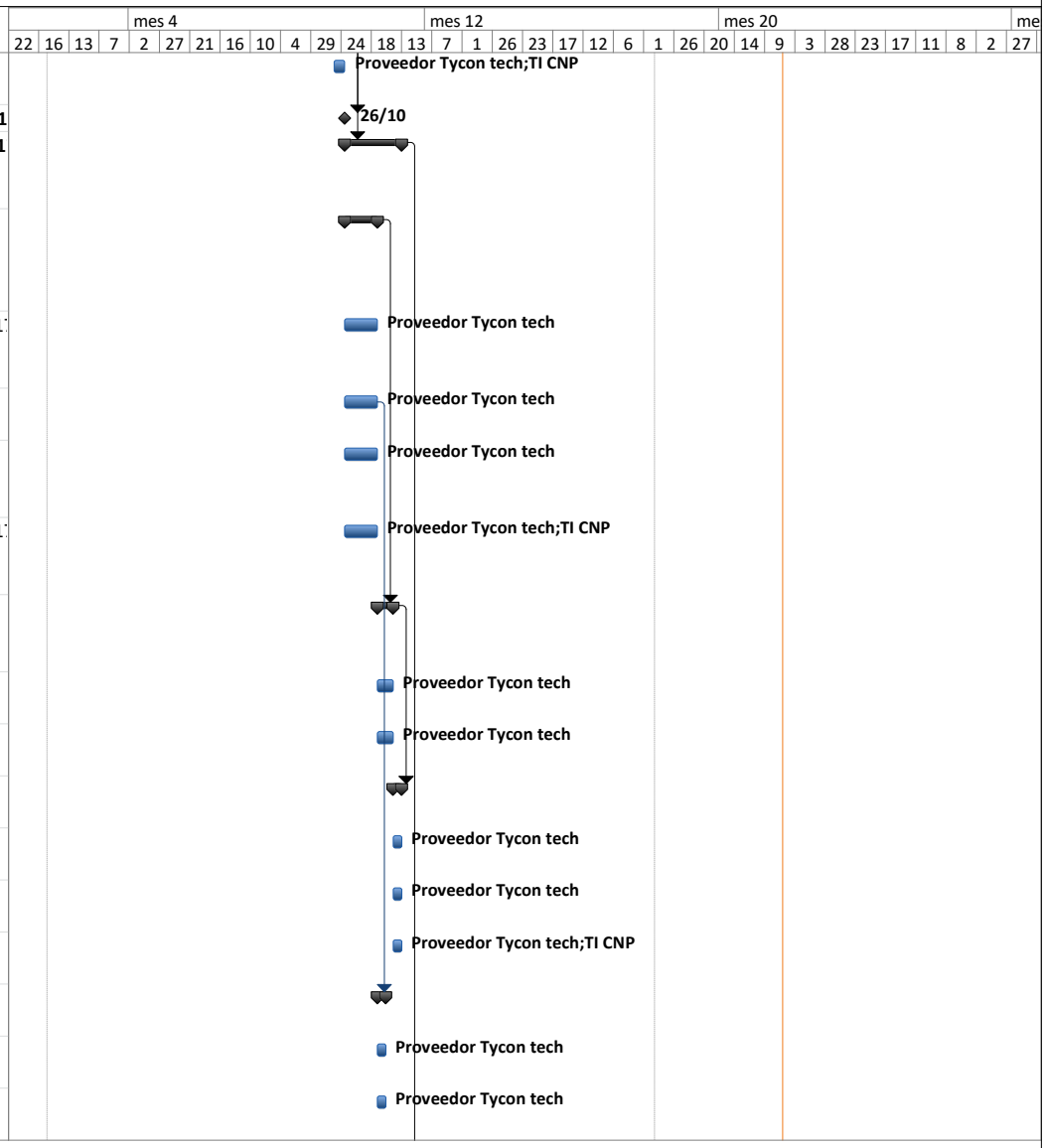


Proyecto: 304-0_ROIRCNP_Evento
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin
División	Hito externo	Sólo duración	Fecha límite
Hito	Tarea inactiva	Informe de resumen manual	Progreso
Resumen	Hito inactivo	Resumen manual	
Resumen del proyecto	Resumen inactivo	Sólo el comienzo	

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	EDT	Nombre de tarea	% completado	Duración	Comienzo
64	1.6.2.3	Realizar pruebas de los servicios publicados en internet	0%	7 días	mié 18/10/17
65	1.6.3	Finalizacion Etapa III	0%	0 días	**jue 26/10/1**
66	**1.7**	**Etapa IV - Switch de LAN**	**0%**	**31 días**	**vie 27/10/1**
67	**1.7.1**	**Implementar segmentación por VLANs para red de usuarios y red de servidores. Configurar ruteo por capa 3 (nivel de red)**	**0%**	**19 días**	**vie 27/10/17**
68	1.7.1.1	Definir rangos de red	0%	19 días	vie 27/10/1
69	1.7.1.2	Configuración en Switchs, Vlans, puertos de Trunk	0%	19 días	vie 27/10/17
70	1.7.1.3	Migración de equipos a nuevas redes, asignación de puertos de switch a nuevas Vlans	0%	19 días	vie 27/10/17
71	1.7.1.4	Pruebas de funcionamiento	0%	19 días	vie 27/10/1
72	**1.7.2**	**Realizar las adecuaciones para utilizar otro puerto de backup en caso de falta en el puerto que está en uso**	**0%**	**8 días**	**jue 23/11/17**
73	1.7.2.1	Configurar port channel en cada uno de los switch	0%	8 días	jue 23/11/17
74	1.7.2.2	Pruebas de puertos de backup y continuidad de servicio	0%	8 días	jue 23/11/17
75	**1.7.3**	**Realizar las adecuaciones para utilizar acceso SSH (secure shell) encriptado**	**0%**	**4 días**	**mié 6/12/17**
76	1.7.3.1	Configurar acceso por secure shell a los switchs	0%	4 días	mié 6/12/17
77	1.7.3.2	Cancelar la configuración para acceder por telnet	0%	4 días	mié 6/12/17
78	1.7.3.3	Pruebas de acceso por shh a los equipos	0%	4 días	mié 6/12/17
79	**1.7.4**	**Realizar las adecuaciones para no utilizar la vlan nativa para tráfico de red**	**0%**	**4 días**	**jue 23/11/17**
80	1.7.4.1	Configurar VLAN para gestión de dispositivos de red	0%	4 días	jue 23/11/17
81	1.7.4.2	Configurar una dirección ip de la nueva vlan a los dispositivos	0%	4 días	jue 23/11/17

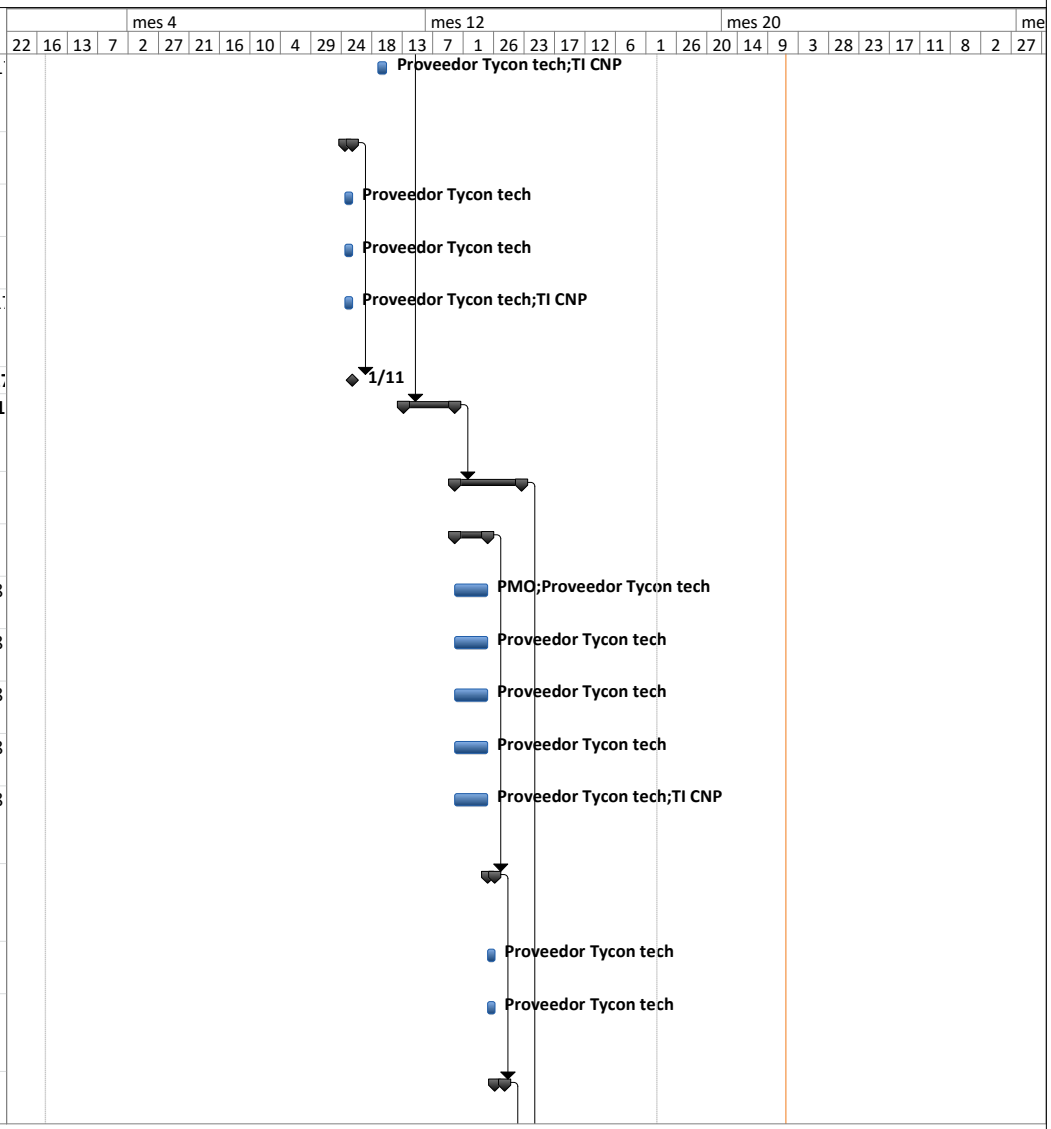


Proyecto: 304-0_ROIRCNP_Evento
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin				
División	Hito externo	Sólo duración	Fecha límite				
Hito	Tarea inactiva	Informe de resumen manual	Progreso				
Resumen	Hito inactivo	Resumen manual					
Resumen del proyecto	Resumen inactivo	Sólo el comienzo					

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	EDT	Nombre de tarea	% completado	Duración	Comienzo
82	1.7.4.3	Pruebas de acceso	0%	4 días	jue 23/11/1
83	**1.7.5**	**Realizar las adecuaciones para asignar una red exclusiva para las impresoras**	**0%**	**4 días**	**vie 27/10/17**
84	1.7.5.1	Configurar VLAN para impresoras y asignar puertos	0%	4 días	vie 27/10/17
85	1.7.5.2	Configurar la nueva dirección IP en las impresoras	0%	4 días	vie 27/10/17
86	1.7.5.3	Pruebas de funcionamiento	0%	4 días	vie 27/10/1
87	1.7.6	Finalizacion Etapa IV	0%	0 días	**mié 1/11/1**
88	**1.8**	**Etapa V - Protección de Redes Internas**	**0%**	**19 días**	**jue 14/12/1**
97	**1.9**	**Etapa VI - Webfiltering, Antispam y Procedimientos**	**0%**	**39 días**	**jue 25/1/18**
98	**1.9.1**	**Implementar un esquema de WebFiltering en alta disponibilidad**	**0%**	**19 días**	**jue 25/1/18**
99	1.9.1.1	Adquisición de firewall UTM (con funcionalidad de WebFilter)	0%	19 días	jue 25/1/18
100	1.9.1.2	Configuración inicial del equipo y del servicio de webfiltering	0%	19 días	jue 25/1/18
101	1.9.1.3	Relevamiento de configuración del WebSense	0%	19 días	jue 25/1/18
102	1.9.1.4	Migración de configuración al nuevo equipo	0%	19 días	jue 25/1/18
103	1.9.1.5	Pruebas del servicio de Webfiltering	0%	19 días	jue 25/1/18
104	**1.9.2**	**Desarrollar las directrices de un procedimiento backup y control de cambios sobre el equipamiento de TI**	**0%**	**4 días**	**mié 21/2/18**
105	1.9.2.1	Indicar recomendaciones para generar un procedimiento de backup	0%	4 días	mié 21/2/18
106	1.9.2.2	Indicar recomendaciones para generar un procedimiento de control de cambios	0%	4 días	mié 21/2/18
107	**1.9.3**	**Implementar un esquema de Antispam en alta disponibilidad**	**0%**	**6 días**	**mar 27/2/18**

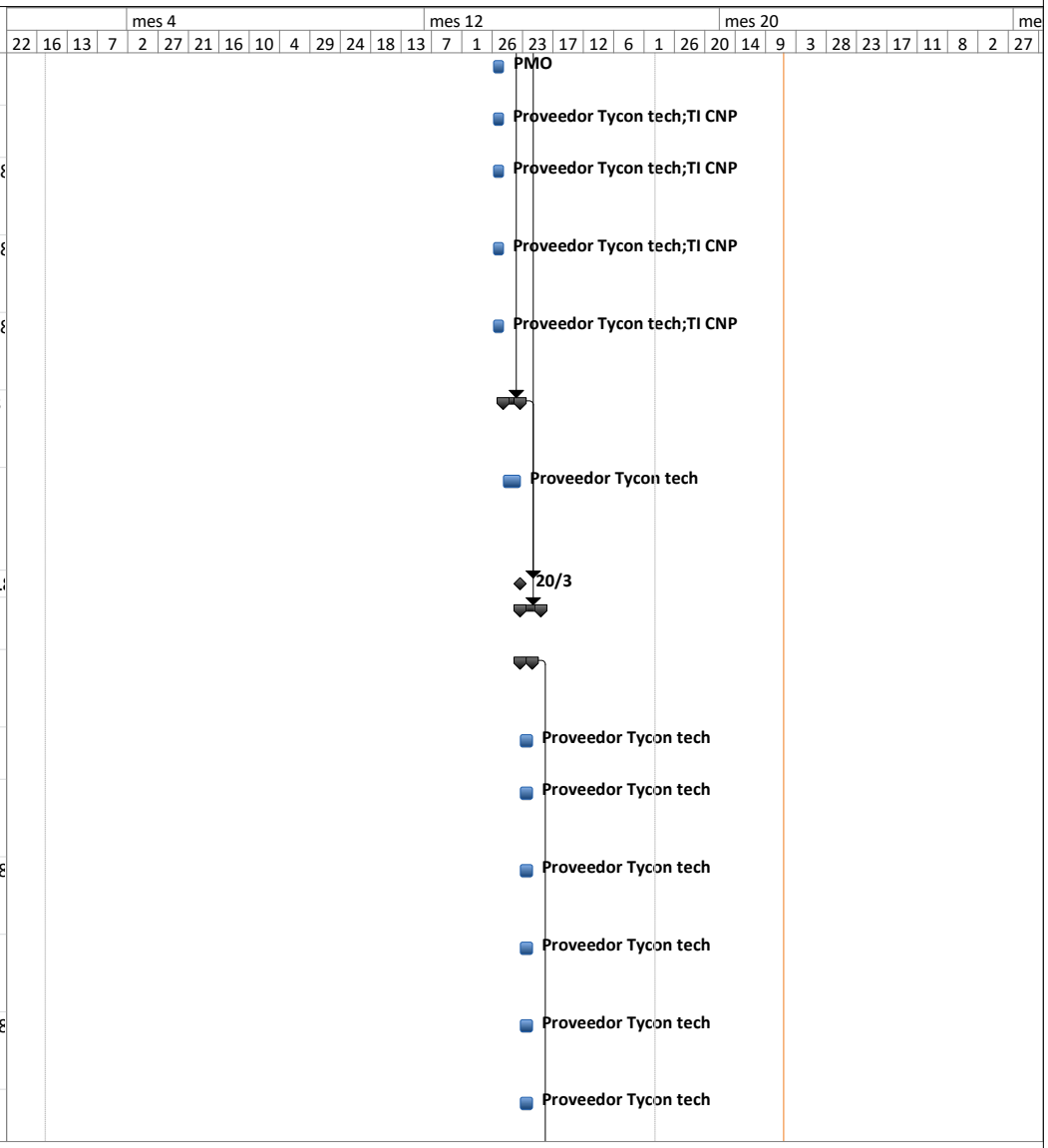


Proyecto: 304-0_ROIRCNP_Evento
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin		
División	Hito externo	Sólo duración	Fecha límite		
Hito	Tarea inactiva	Informe de resumen manual	Progreso		
Resumen	Hito inactivo	Resumen manual			
Resumen del proyecto	Resumen inactivo	Sólo el comienzo			

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	EDT	Nombre de tarea	% completado	Duración	Comienzo
108	1.9.3.1	Gestionar la adquisición del equipamiento	0%	6 días	mar 27/2/18
109	1.9.3.2	Configuración inicial del equipamiento	0%	6 días	mar 27/2/18
110	1.9.3.3	Relevamiento de configuración actual	0%	6 días	mar 27/2/18
111	1.9.3.4	Migración de configuración	0%	6 días	mar 27/2/18
112	1.9.3.5	Pruebas de servicio	0%	6 días	mar 27/2/18
113	**1.9.4**	**Desarrollar las directrices de un procedimiento diferencial para el ABM de cuentas de administrador de domino**	**0%**	**10 días**	**mié 7/3/18**
114	1.9.4.1	Indicar recomendaciones para generar un procedimiento para ABM de cuentas de administrador de dominio	0%	10 días	mié 7/3/18
115	1.9.5	Finalizacion Etapa VI	0%	0 días	**mar 20/3/1**
116	**1.10**	**Etapa VII - RED WiFi, MPLS y Backup Satélital**	**0%**	**13 días**	**mié 21/3/18**
117	**1.10.1**	**Implementar cifrado WPA2 o WPA2/Enterprise, SSID Corporativo y SSID Invitados, ajustes de seguridad**	**0%**	**8 días**	**mié 21/3/18**
118	1.10.1.1	Sincronizar wireless controller con usuarios active directory	0%	8 días	mié 21/3/18
119	1.10.1.2	Configurar cifrado WPA2/Enterprise con autenticación para SSID Corporativo	0%	8 días	mié 21/3/18
120	1.10.1.3	Configurar cifrado WPA2	0%	8 días	mié 21/3/18
121	1.10.1.4	Definir red vlan de red WiFi corporativa y vlan de red WiFi invitados	0%	8 días	mié 21/3/18
122	1.10.1.5	Ajustes en red LAN	0%	8 días	mié 21/3/18
123	1.10.1.6	Documentación, pruebas y test de conexión	0%	8 días	mié 21/3/18

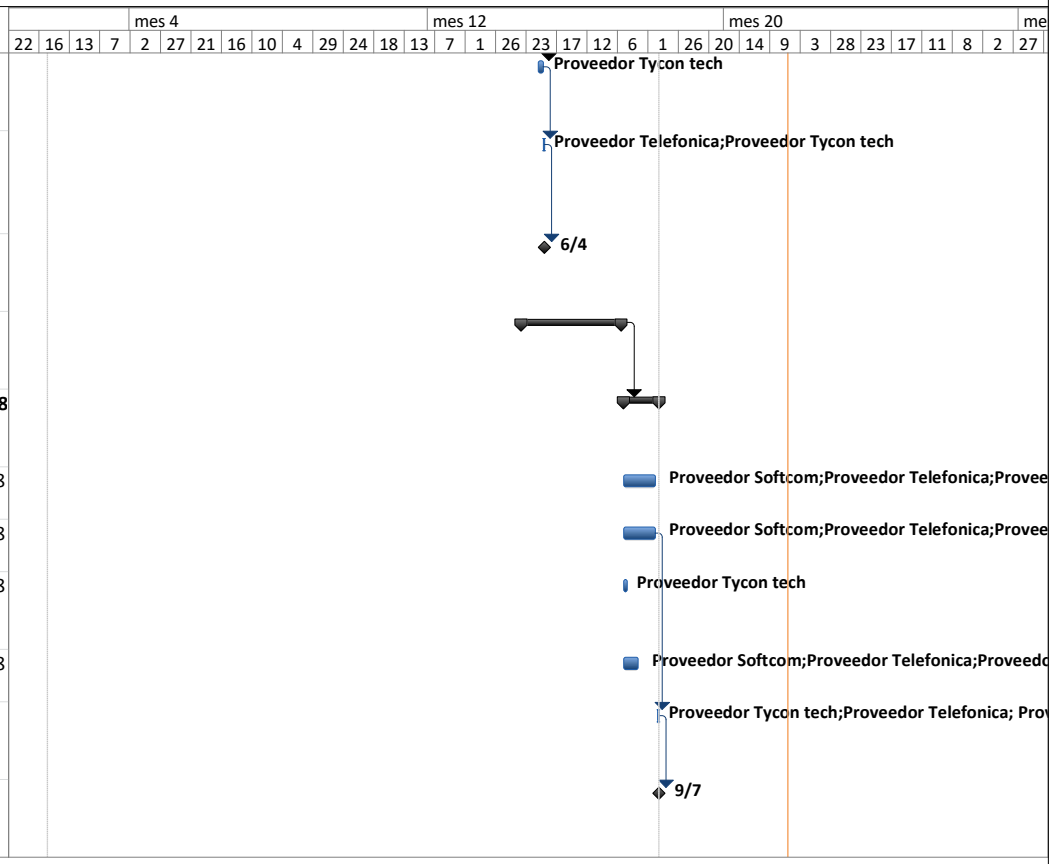


Proyecto: 304-0_ROIRCNP_Evento
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin		
División	Hito externo	Sólo duración	Fecha límite		
Hito	Tarea inactiva	Informe de resumen manual	Progreso		
Resumen	Hito inactivo	Resumen manual			
Resumen del proyecto	Resumen inactivo	Sólo el comienzo			

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	EDT	Nombre de tarea	% completado	Duración	Comienzo
124	1.10.2	Desarrollar un procedimiento para implementar conmutación de enlace MPLS y Backup Satelital	0%	4 días	lun 2/4/18
125	1.10.3	Interactuar con el proveedor y coordinar implementación de conmutación automática de enlace principal a enlace backup y viceversa	0%	1 día	vie 6/4/18
126	1.10.4	Finalizacion Etapa VII	0%	0 días	vie 6/4/18
127	**1.11**	**Etapa VIII: Implementar un clúster de firewall para borde y VPN en clúster de alta disponibilidad**	**0%**	**60 días**	**lun 19/3/18**
137	**1.12**	**Cierre**	**0%**	**21 días**	**lun 11/6/18**
138	1.12.1	Informe final del proyecto	0%	20 días	lun 11/6/18
139	1.12.2	Entrega de ingenieria de detalle completa	0%	20 días	lun 11/6/18
140	1.12.3	Propuesta de soporte y mantenimiento	0%	3 días	lun 11/6/18
141	1.12.4	Lecciones aprendidas y recomendaciones	0%	10 días	lun 11/6/18
142	1.12.5	Reunion de entrega	0%	1 día	lun 9/7/18
143	1.12.6	Finalizacion del proyecto	0%	0 días	lun 9/7/18



Proyecto: 304-0_ROIRCNP_Evento
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin		
División	Hito externo	Sólo duración	Fecha límite		
Hito	Tarea inactiva	Informe de resumen manual	Progreso		
Resumen	Hito inactivo	Resumen manual			
Resumen del proyecto	Resumen inactivo	Sólo el comienzo			

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Log de issues								
Proyecto: Proyecto Remediación y optimización infraestructura de red y seguridad informática							**Date:** 12/11/2017	
Issue	**Descripción**	**Prioridad (H, M, L)**	**Categoría**	**Reportado por**	**Asignado a**	**Estado**	**Fecha de resolu**	**Resolución/ Comentarios**
I-001	Cambio en entregable Implementar un clúster de firewall para borde y VPN en clúster de alta disponibilidad de la Etapa II, la dirección recorta presupuesto, para esta actividad se usarán equipos en stock que tienen en casa matriz, pero estarán en sitio en marzo de 2019	H	Project Mangment	Marcelo cueto Director de tecnología Sponsor	Project Manager	Cerrado	30/6/2017	Se propone Crear una nueva etapa del proyecto con este entregable, se registra en el control de cambios, se modifica cronograma y presupuesto
I-002	Falta de cableado estructurado para ejecutar la actividad Migración de equipos a nuevas redes, asignación de puertos de switch a nuevas Vlans de la etapa IV *Implementar segmentación por VLANs para red de usuarios y red de servidores. Configurar ruteo por capa 3 (nivel de red)*	H	Técnica	Proveedor Tycon Tech	Project Manager	Cerrado		Se utiliza la reserva de gestión, para cubrir esta actividad y cumplir con el entregable. Se realiza en paralelo con los demás paquetes de trabajo edl entregable, logrando cumplir en tiempo
I-003	Para este paquete de trabajo Configurar VLAN para impresoras y asignar puertos, por parte de adinistradores de aplicaciones en TI, no es posible realizar el cambio a otra red, pues se requiere un cambio en los servidores de impresión.	M	Técnica	Proveedor Tycon Tech	Project Manager	Cerrado		Se incluye una nueva tarea, de configuración de servidores de impresión para no afectar el tiempo del entregable, se reduce el tiempo del paquete de trabajo Pruebas de funcionamiento del entregable Realizar las adecuaciones para asignar una red exclusiva para las impresoras, se reduce de 7 a 3 dias. Los otros 4 dias se asignan a la actividad nueva
I-004	El enlace de Back up, de la sede BRM Cabo Virgenes no funciona, afectando el entregable Etapa VII - RED WiFi, MPLS y Backup Satélital	M	Técnico	Proveedor Tycon Tech	Project Manager	Cerrado		Se escala con proveedor TASA, para solucionar el inconveniente, por temas contractuales, no es posible utilizar el procedimiento de conmutación, Este paquete de trabajo, no se ejecutará. Se informa al Sponsor e interesados.
I-005	Alto procesamiento del Equipo Fortigate 200D, por sobrecarga, entra en modo de protección, con lo cual, deja de operar afectando a los usuarios, esto sucede al incluir Antispam en un nuevo Vdom del equipo	H	Técnico	Servicedesk CNP	Tycon Tech	Cerrado		Se deshabilitan features innecesarios para evitar generar alto procesamiento en el dispotitivo.

GESTION DE PROYECTOS **FORMATO DE GESTIÓN DE RFC A PROYECTO**		
Nombre del proyecto: Proyecto Remediación y optimización infraestructura de red y seguridad informática	**Fecha**: 01/08/2017	**Proponente:** Dirección TI
Tipo de cambio a proponer: Agregar nueva etapa al proyecto: Implementar un clúster de firewall para borde y VPN en clúster de alta disponibilidad, eliminación de entregable de la etapa 2	**No. De Cambio: 01**	**No. Del proyecto: 02**
Puede anexar todos los documentos que considere necesarios como soporte del cambio y referenciarlos en cada casilla		
Descripción del cambio		
Desde la dirección TI, se propone suprimir la tarea de la Etapa II Implementar un clúster de firewall para borde y VPN en clúster de alta disponibilidad y crear una nueva etapa Al final llamada Etapa VIII, con el mismo nombre, esta propuesta viene desde casa matriz ya que informan que tienen disponibilidad de los equipos requeridos, y se ahorraría el costo de los mismos, se propone al final del proyecto, dada la disponibilidad de los equipos, ya que estarán libres y los enviarían desde Chile a Argentina en enero de 2018.		
Condiciones actuales del proyecto (en términos del plan global del proyecto) Aún está por finalizar la etapa I, se registraría el cambio, si se aprueba por el sponsor, se procede con la documentación e información necesaria a todo el equipo		
Cambio propuesto (precisar actividades que cambian, recursos adicionales, cambios en presupuesto, entre otros) En la **Etapa II - Protección de Borde I** , se suprimen las actividades del entregable: **Implementar un clúster de firewall para borde y VPN en clúster de alta disponibilidad**		

Nombre de tarea	Duración	Comienzo	Fin
Implementar un clúster de firewall para borde y VPN en clúster de alta disponibilidad	**6 días**	**mar 22/8/17**	**mar 29/8/17**
Adquisición de firewall UTM para HA	6 días	mar 22/8/17	mar 29/8/17
Instalación y configuración inicial	6 días	mar 22/8/17	mar 29/8/17
Importar configuraciones de borde	6 días	mar 22/8/17	mar 29/8/17
Pruebas de funcionamiento	6 días	mar 22/8/17	mar 29/8/17
Importar configuraciones de VPN	6 días	mar 22/8/17	mar 29/8/17
Pruebas de funcionamiento	6 días	mar 22/8/17	mar 29/8/17

Por tanto Cambian las fechas, para el inicio de las fases posteriores, cambiando el cronograma del resto del proyecto.

El entregable **Ajustar servicios publicados en internet y configurar aplicaciones publicadas en la red DMZ, se adelanta los 6 días que duraba el entregable suprimido.**

Nueva fecha:

Nombre de tarea	Duración	Comienzo	Fin
Ajustar servicios publicados en internet y configurar aplicaciones publicadas en la red DMZ	**11 días**	**mar 22/8/17**	**mar 5/9/17**

Se corre todo el cronograma del resto del proyecto 6 días.

En cuanto a la nueva Etapa queda de la siguiente manera:

Nombre de tarea	Duración	Comienzo	Fin
Etapa VIII: Implementar un clúster de firewall para borde y VPN en clúster de alta disponibilidad	**60 días**	**lun 19/3/18**	**vie 8/6/18**
Adquisición de firewall UTM para HA	7 días	lun 19/3/18	mar 27/3/18
Provisión de los equipos ASA	20 días	lun 19/3/18	vie 13/4/18
Instalación y configuración inicial	7 días	lun 16/4/18	mar 24/4/18
Importar configuraciones de borde	7 días	mié 25/4/18	jue 3/5/18
Pruebas de funcionamiento	7 días	vie 4/5/18	lun 14/5/18
Importar configuraciones de VPN	7 días	mar 15/5/18	mié 23/5/18
Permitir el acceso a la infraestructura tecnológica solo desde la red de informática.	5 días	jue 24/5/18	mié 30/5/18
Pruebas de funcionamiento	7 días	jue 31/5/18	vie 8/6/18
Finalización Etapa VIII	0 días	**vie 8/6/18**	vie 8/6/18

Para el detalle del nuevo cronograma ver documento 304-2_ROIRCNP_Evento de Cambio 1_Diagrama de Gantt

Presupuesto:

El nuevo presupuesto cambia, disminuye, teniendo en cuenta que ya no se pagará por dispositivos nuevos, el costo de recursos se calcula en base al esfuerzo realizado en horas.

$ 21.279.938,56

Posibles consecuencias del cambio (en resultados del proyecto, económicos, en procesos, en la organización, entre otros) El proyecto Pasará de un costo inicial de **$ 22.318.321,40** A un costo después del cambio: **$ 21.279.938,56** **Diferencia:** **$ 1.038.382,84** **En relación al tiempo, Se extiende el proyecto 39 días más.** Ya que la orden viene directamente desde la dirección de TI, se informa a todos los involucrados.
Justificación del cambio Por Minimizar costos, y aprovechando la infraestructura en stock disponible ofrecida por la casa matriz
Acciones a desarrollar si se acepta la propuesta de cambio Modificar cronograma, presupuesto y documentos necesarios, subirlos a la carpeta de proyecto, informar a proveedores y demás involucrados, Validar cláusulas con proveedores.

Nombre y firma del gerente del proyecto (Solicitante): James Vallejo Mejia	Fecha: 01/08/2017
Nombre y firma del Coordinador de TI: Pablo Barbieri	Fecha: 01/08/2017
Aprobada (X) Rechazada ( )	No. Acta: RFC_PM_001
Nombre y firma del Director TI: Marcelo Cueto	Fecha: 01/08/2017

Decisiones tomadas frente a la propuesta
Se Aprueba el cambio.

Elaboró: James Vallejo	Fecha:01/08/2017	Código: RFC_PM_001
Revisó: Marcelo Cueto	Fecha:01/08/2017	Pagina:
Aprobó: Marcelo cueto	Fecha:01/08/2017	Versión:1

Compañía Nacional del Petróleo

Evento de cambio 1

Reporte especial

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Autor: James Vallejo Mejia

Registro de cambios

Fecha	Versión	Descripción	Autor	Aprobación
23/3/2018	1		PM	

Contenido

Evento de Cambio 1 – Reporte especial

1 Eventos generados y sus impactos

En el siguiente apartado, se comunica el evento realizado y la gestión después del cambio solicitado y aprobado por la dirección TI, sponsor del proyecto Remediación y optimización infraestructura de red y seguridad informática.

La dirección TI Argentina con el apoyo del equipo de TI Chile, lograron sellar un acuerdo en el cuál, la casa matriz (Chile), pone a su disposición los equipos de Tecnología en stock, para las implementaciones necesarias en el proyecto remediación y optimización infraestructura de red y seguridad informática las sucursales de Argentina.

Los cambios reflejados en los entregables son los siguientes: En color rojo, las actividades que se suprimen de la etapa II:

Nombre de tarea	Duración	Comienzo	Fin
Etapa II - Protección de Borde I	**34 días**	**mar 22/8/17**	**vie 6/10/17**
Implementar un clúster de firewall para borde y VPN en clúster de alta disponibilidad	**6 días**	**mar 22/8/17**	**mar 29/8/17**
Adquisición de firewall UTM para HA	6 días	mar 22/8/17	mar 29/8/17
Instalación y configuración inicial	6 días	mar 22/8/17	mar 29/8/17
Importar configuraciones de borde	6 días	mar 22/8/17	mar 29/8/17
Pruebas de funcionamiento	6 días	mar 22/8/17	mar 29/8/17
Importar configuraciones de VPN	6 días	mar 22/8/17	mar 29/8/17
Pruebas de funcionamiento	6 días	mar 22/8/17	mar 29/8/17
Ajustar servicios publicados en internet y configurar aplicaciones publicadas en la red DMZ	**11 días**	**mié 30/8/17**	**mié 13/9/17**
Implementar una alternativa tecnológica diferente al TMG, ya el servicio está discontinuado	**17 días**	**jue 14/9/17**	**vie 6/10/17**

El siguiente entregable ahora se adelanta durante 6 días, que es el tiempo que se suprime

Nueva Etapa a implementar:

Nombre de tarea	Duración	Comienzo	Fin
Etapa VIII: Implementar un clúster de firewall para borde y VPN en clúster de alta disponibilidad	**60 días**	**lun 19/3/18**	**vie 8/6/18**
Adquisición de firewall UTM para HA	7 días	lun 19/3/18	mar 27/3/18
Provisión de los equipos ASA	20 días	lun 19/3/18	vie 13/4/18
Instalación y configuración inicial	7 días	lun 16/4/18	mar 24/4/18
Importar configuraciones de borde	7 días	mié 25/4/18	jue 3/5/18
Pruebas de funcionamiento	7 días	vie 4/5/18	lun 14/5/18
Importar configuraciones de VPN	7 días	mar 15/5/18	mié 23/5/18
Permitir el acceso a la infraestructura tecnológica solo desde la red de informática.	5 días	jue 24/5/18	mié 30/5/18
Pruebas de funcionamiento	7 días	jue 31/5/18	vie 8/6/18
Finalización Etapa VIII	0 días	**vie 8/6/18**	vie 8/6/18

Cambios en presupuesto

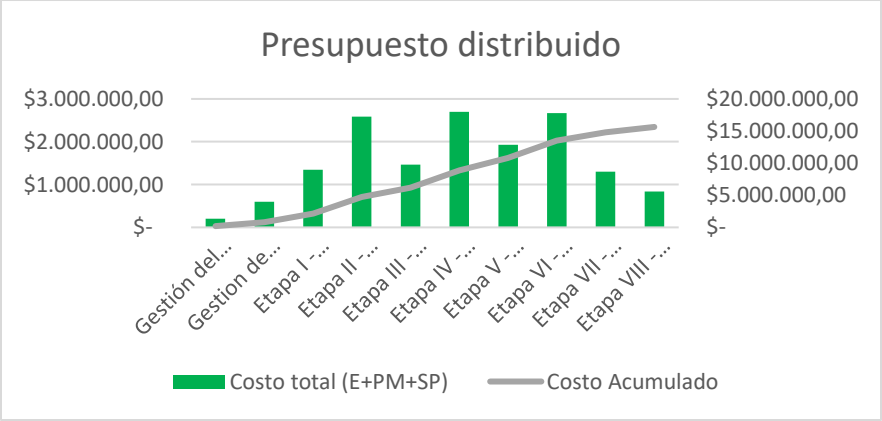
La implicación de esta propuesta, reduce significativamente el costo del proyecto de la siguiente manera:

Presupuesto inicial: $ 22.318.321,40

Presupuesto después del cambio: $ 21.279.938,56

Diferencia: $ 1.038.382,84

Presupuesto	
Etapa	**Costo**
Etapa I - Servicios DNS Externo y DHCP	$ 1.132.475,00
Etapa II - Protección de Borde I	$ 2.373.443,33
Etapa III - Protección de Borde II	$ 1.249.000,00
Etapa IV - Switch de LAN	$ 2.481.325,00
Etapa V - Protección de Redes Internas	$ 1.717.900,00
Etapa VI - Webfiltering, Antispam y Procedimientos	$ 2.453.427,00
Etapa VII - RED WiFi, MPLS y Backup Satélital	$ 1.090.825,00
Etapa VIII - Implementar un clúster de firewall para borde y VPN en clúster de alta disponibilidad	$ 626.250,00
Gestión del proyecto	$ 1.800.000,00
Gestion de Contratación	$ 400.000,00
Servicios Públicos	$ 95.600,00
Total del proyecto	$ 15.420.245,33
Reserva de contingencia (15%)	$ 2.313.036,80
Linea base de costos	$ 17.733.282,13
Reserva de gerencia (20%)	$ 3.546.656,43
Presupuesto	**$ 21.279.938,56**



Ver detalle del presupuesto: 304-3_ROIRCNP_Evento de Cambio 1_Presupuesto

Cambio en tiempo

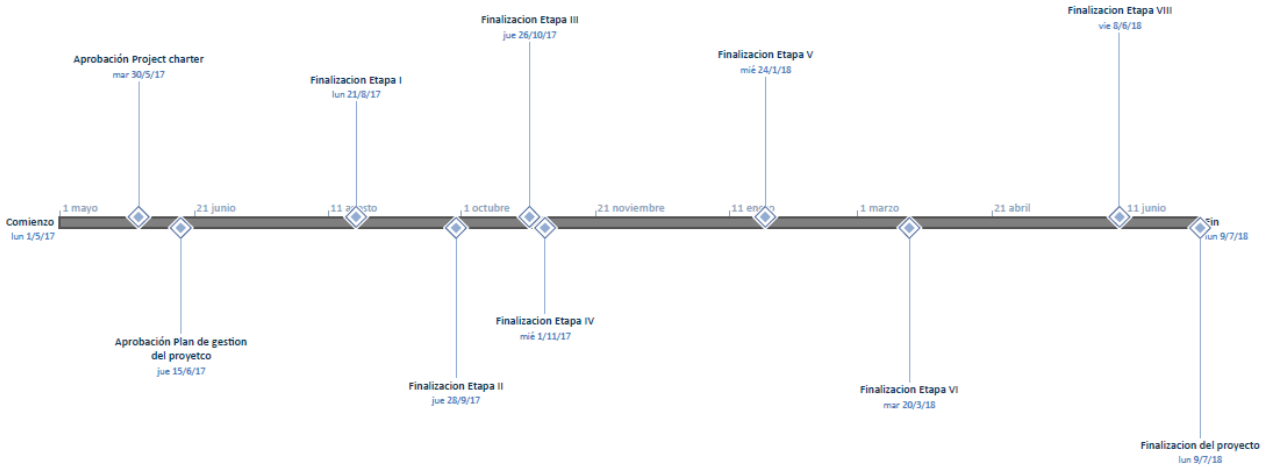
En cuanto al tiempo el proyecto Finaliza 39 días después, debido a que es necesario esperar que envíen el Equipo desde Chile a Argentina.

A continuación se observan las nuevas fechas de hitos, para mayor detalle:

Ver

304-2_ROIRCNP_Evento de Cambio 1_Diagrama de Gantt

304-4_ROIRCNP_Evento de Cambio 1_Hitos

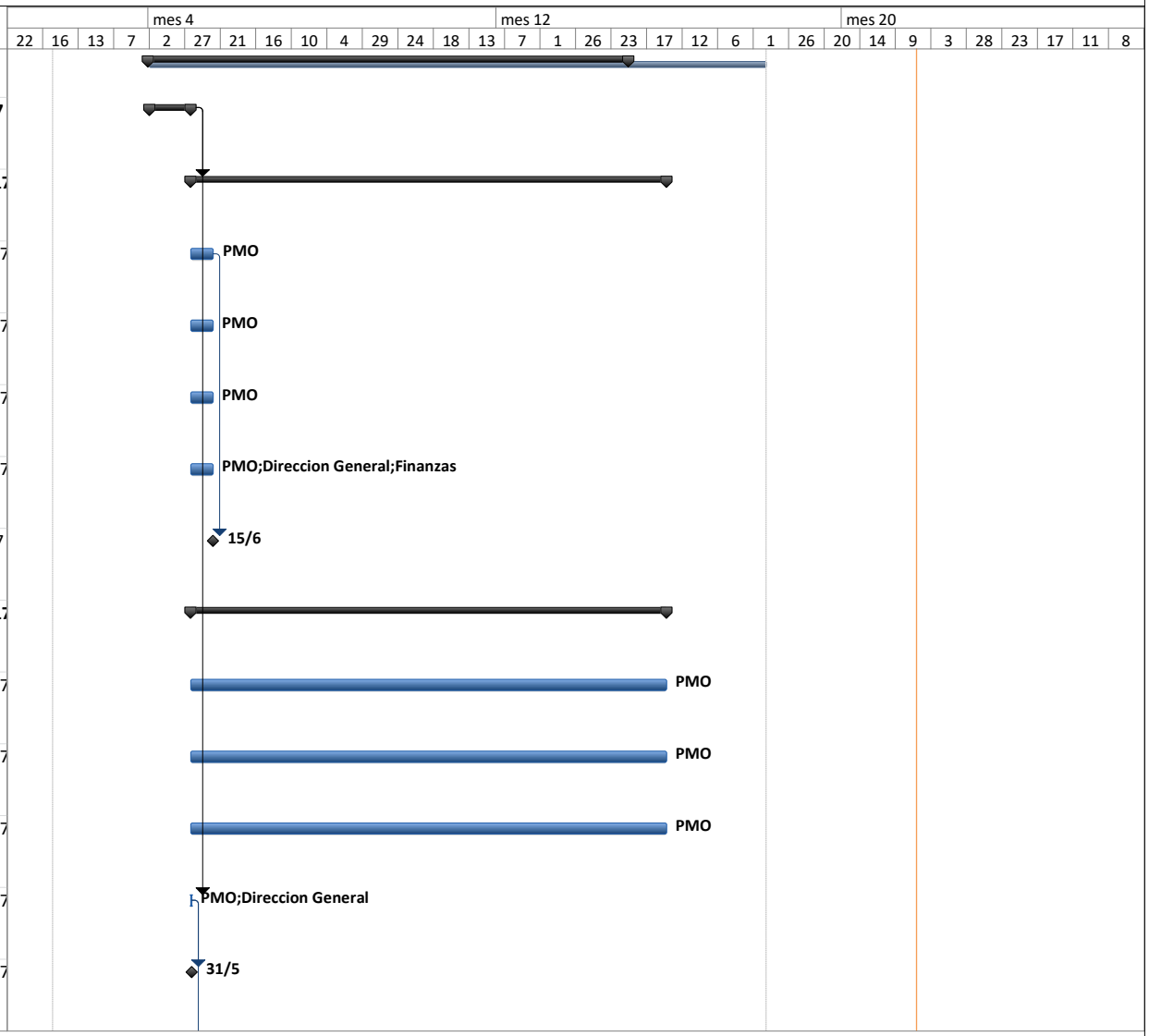


Cambio con proveedores

Con respecto a las actividades que corresponden a proveedores, se informa y se acepta el cambio, de igual forma se pagarán los recursos durante el tiempo de las actividades según lo estimado.

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	Nombre de tarea	Duración	Comienzo
1	**Remediación Infraestructura y Seguridad Informática**	**223 días**	**lun 1/5/17**
2	**Inicio**	**20 días**	**mar 2/5/17**
7	**Gestion del proyecto**	**221 días**	**mié 31/5/17**
8	Plan de gestión de proyecto	12 días	mié 31/5/17
9	Linea base de alcance	12 días	mié 31/5/17
10	Linea base de tiempo	12 días	mié 31/5/17
11	Linea base de costos	12 días	mié 31/5/17
12	Aprobación Plan de gestion del proyetco	0 días	jue 15/6/17
13	**Comunicaciones**	**221 días**	**mié 31/5/17**
14	Reporte de hitos	221 días	mié 31/5/17
15	minutas	221 días	mié 31/5/17
16	Reporte de status	221 días	mié 31/5/17
17	Kick Off Puesta en marcha	1 día	mié 31/5/17
18	Hito Cick off puesta en marcha	0 días	mié 31/5/17

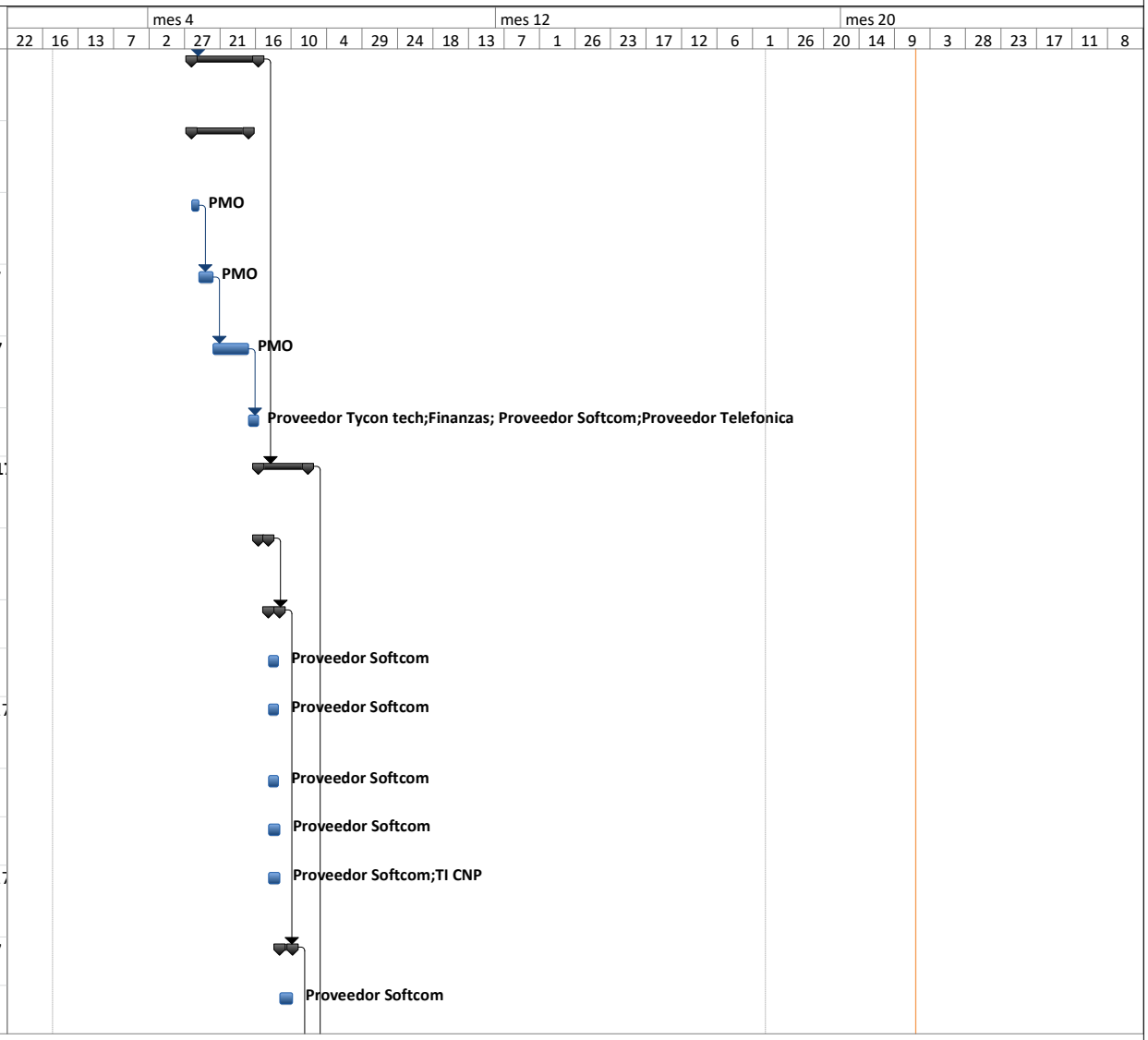


Proyecto: 304-0_ROIRCNP_Evento
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin		
División	Hito externo	Sólo duración	Fecha límite		
Hito	Tarea inactiva	Informe de resumen manual	Progreso		
Resumen	Hito inactivo	Resumen manual			
Resumen del proyecto	Resumen inactivo	Sólo el comienzo			

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	Nombre de tarea	Duración	Comienzo
19	**Gestion de Contratación**	**31 días**	**jue 1/6/17**
20	**Búsqueda del proveedor**	**26 días**	**jue 1/6/17**
21	Invitacion a proveedores	3 días	jue 1/6/17
22	RFP (Request for Proposal)	8 días	mar 6/6/17
23	Análisis y Selección de proveedores	15 días	vie 16/6/17
24	Contratación	5 días	mar 11/7/17
25	**Etapa I - Servicios DNS Externo y DHCP**	**24 días**	**mar 18/7/1**
26	**Habilitar protección de IPS, AV y publicar solo puertos necesarios para el servicio de DNS Externo**	**5 días**	**mar 18/7/17**
30	**Ajustar configuración de DNS Server Externo Segundario**	**6 días**	**mar 25/7/17**
31	Instalación de un servidor con Windows Server 2012	5 días	mar 25/7/17
32	Habilitar servicio de DNS	5 días	mar 25/7/17
33	Transferir zonas desde DNS principal al segundario	5 días	mar 25/7/17
34	Gestionar configuraciones para publicación en internet	6 días	mar 25/7/17
35	Realizar pruebas de servicios	6 días	mar 25/7/17
36	**Configurar otro registro MX para un Mail Server Segundario**	**7 días**	**mié 2/8/17**
37	En el servidor de DNS, agregar un DNS record de tipo MX (Mail Exchanger)	7 días	mié 2/8/17

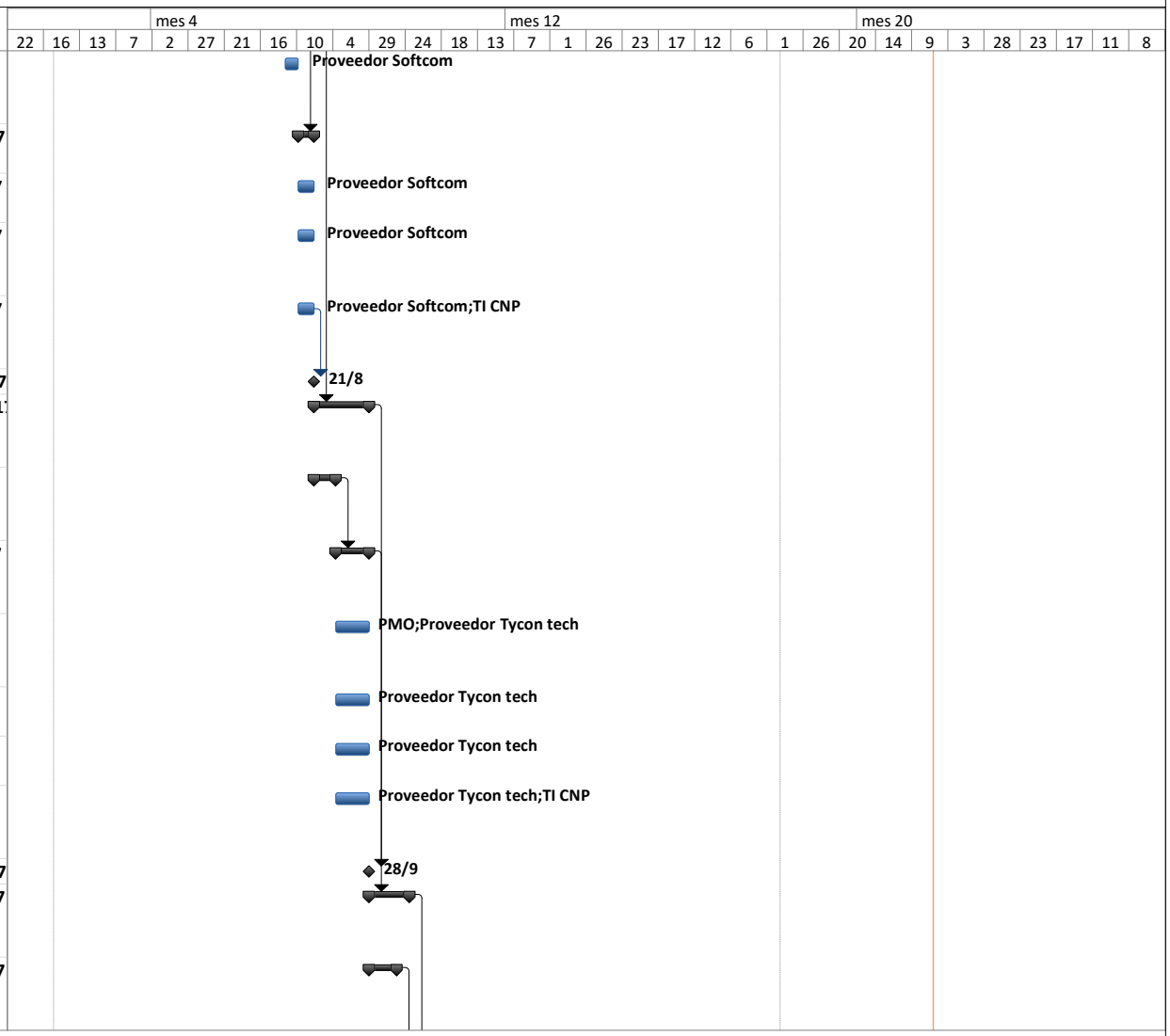


Proyecto: 304-0_ROIRCNP_Evento
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin				
División	Hito externo	Sólo duración	Fecha límite				
Hito	Tarea inactiva	Informe de resumen manual	Progreso				
Resumen	Hito inactivo	Resumen manual					
Resumen del proyecto	Resumen inactivo	Sólo el comienzo					

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	Nombre de tarea	Duración	Comienzo
38	Asignar una prioridad para que actue como backup (debe ser un número mayor que el del primario)	7 días	mié 2/8/17
39	**Implementar un esquema de HA para el servidor de DHCP**	**6 días**	**vie 11/8/17**
40	Instalación de dos servidores con Windows Server 2012	6 días	vie 11/8/17
41	Configurar los servicios de DHCP y conmutación por error en modo load balance	6 días	vie 11/8/17
42	Realizar pruebas del servicio	6 días	vie 11/8/17
43	Finalizacion Etapa I	0 días	**lun 21/8/17**
44	**Etapa II - Protección de Borde I**	**28 días**	**mar 22/8/1**
45	**Ajustar servicios publicados en internet y configurar aplicaciones publicadas en la red DMZ**	**11 días**	**mar 22/8/17**
49	**Implementar una alternativa tecnológica diferente al TMG, ya el servicio está discontinuado**	**17 días**	**mié 6/9/17**
50	Adquisición de firewall UTM	17 días	mié 6/9/17
51	Relevar configuraciones de permisos de acceso en el TMG	17 días	mié 6/9/17
52	Migrar configuraciones de permisos de acceso a los firewalls UTM	17 días	mié 6/9/17
53	Pruebas de servicios	17 días	mié 6/9/17
54	Finalizacion Etapa II	0 días	**jue 28/9/17**
55	**Etapa III - Protección de Borde II**	**19 días**	**vie 29/9/17**
56	**Realizar las adecuaciones para que los servicios sean publicados desde un único equipo y en forma directa**	**12 días**	**vie 29/9/17**

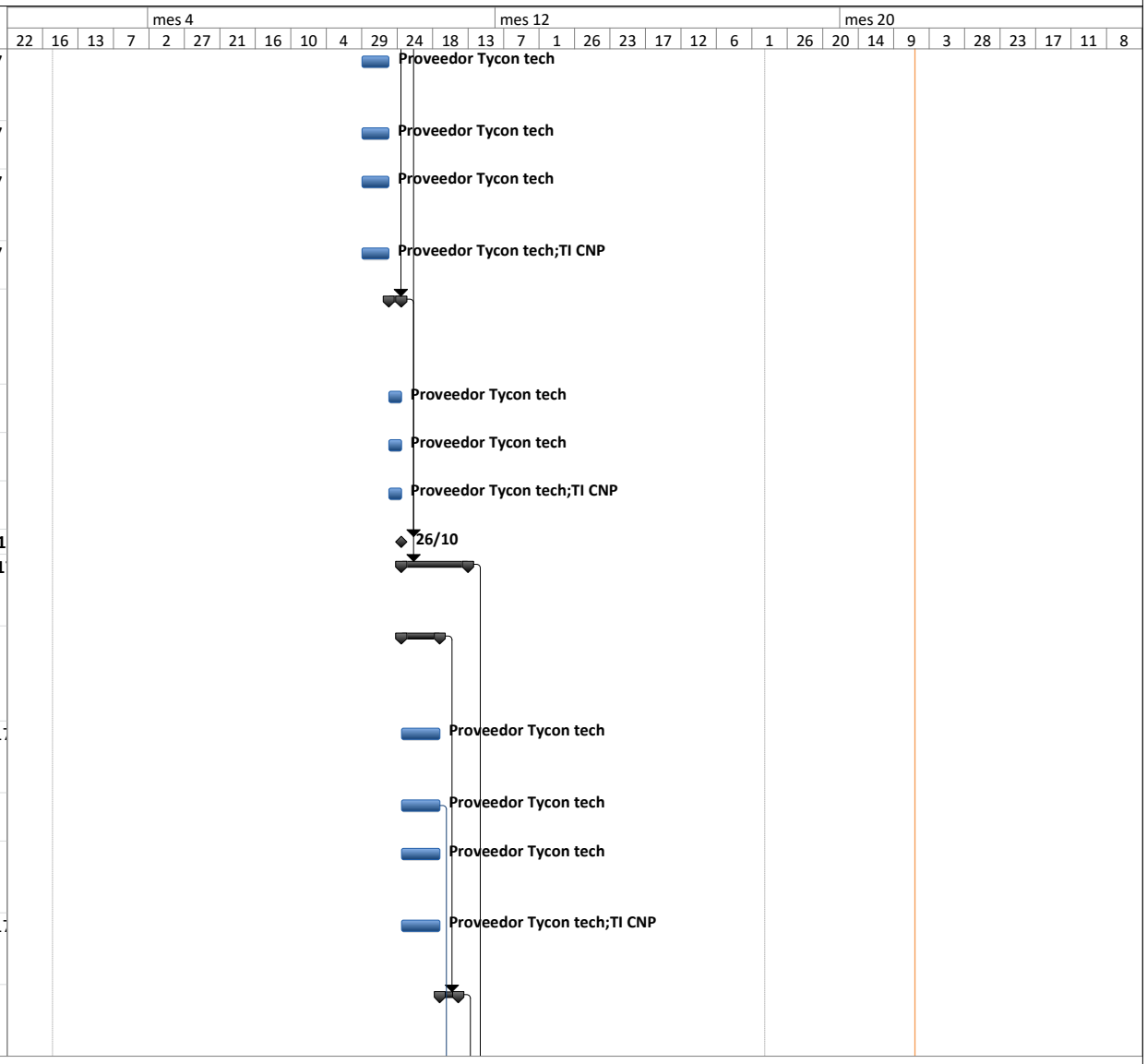


Proyecto: 304-0_ROIRCNP_Evento
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin
División	Hito externo	Sólo duración	Fecha límite
Hito	Tarea inactiva	Informe de resumen manual	Progreso
Resumen	Hito inactivo	Resumen manual	
Resumen del proyecto	Resumen inactivo	Sólo el comienzo	

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	Nombre de tarea	Duración	Comienzo
57	Verificar que servicios hacia internet están publicados desde el ISA Server y el TMG	12 días	vie 29/9/17
58	Crear y validar las reglas de firewall en un entorno de prueba	12 días	vie 29/9/17
59	Migrar las reglas al nuevo firewall	12 días	vie 29/9/17
60	Realizar pruebas de funcionamiento de los servicios	12 días	vie 29/9/17
61	**Realizar las adecuaciones para que todos los servicios publicados en internet cuenten con protección de IPS, AV y DOS**	**7 días**	**mié 18/10/17**
62	Crear profiles de AV, IPS y Antivirus en el firewall	7 días	mié 18/10/17
63	Asignar los profiles a los servicios publicados en internet	7 días	mié 18/10/17
64	Realizar pruebas de los servicios publicados en internet	7 días	mié 18/10/17
65	Finalizacion Etapa III	0 días	**jue 26/10/1**
66	**Etapa IV - Switch de LAN**	**31 días**	**vie 27/10/1**
67	**Implementar segmentación por VLANs para red de usuarios y red de servidores. Configurar ruteo por capa 3 (nivel de red)**	**19 días**	**vie 27/10/17**
68	Definir rangos de red	19 días	vie 27/10/1
69	Configuración en Switchs, Vlans, puertos de Trunk	19 días	vie 27/10/17
70	Migración de equipos a nuevas redes, asignación de puertos de switch a nuevas Vlans	19 días	vie 27/10/17
71	Pruebas de funcionamiento	19 días	vie 27/10/1
72	**Realizar las adecuaciones para utilizar otro puerto de backup en caso de falta en el puerto que está en uso**	**8 días**	**jue 23/11/17**

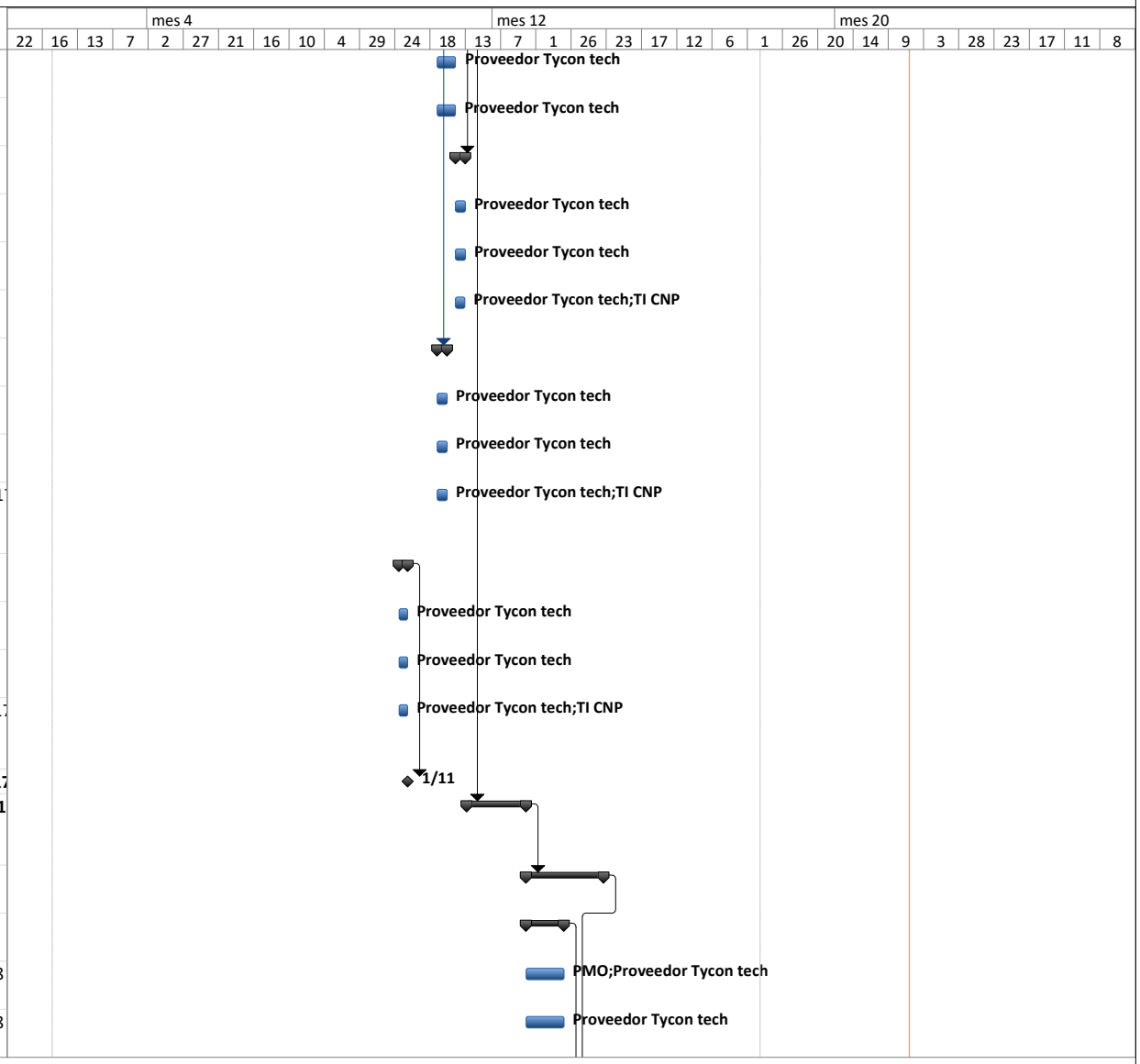


Proyecto: 304-0_ROIRCNP_Evento
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin				
División	Hito externo	Sólo duración	Fecha límite				
Hito	Tarea inactiva	Informe de resumen manual	Progreso				
Resumen	Hito inactivo	Resumen manual					
Resumen del proyecto	Resumen inactivo	Sólo el comienzo					

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	Nombre de tarea	Duración	Comienzo
73	Configurar port channel en cada uno de los switch	8 días	jue 23/11/17
74	Pruebas de puertos de backup y continuidad de servicio	8 días	jue 23/11/17
75	**Realizar las adecuaciones para utilizar acceso SSH (secure shell) encriptado**	**4 días**	**mié 6/12/17**
76	Configurar acceso por secure shell a los switchs	4 días	mié 6/12/17
77	Cancelar la configuración para acceder por telnet	4 días	mié 6/12/17
78	Pruebas de acceso por shh a los equipos	28 horas	mié 6/12/17
79	**Realizar las adecuaciones para no utilizar la vlan nativa para tráfico de red**	**4 días**	**jue 23/11/17**
80	Configurar VLAN para gestión de dispositivos de red	4 días	jue 23/11/17
81	Configurar una dirección ip de la nueva vlan a los dispositivos	4 días	jue 23/11/17
82	Pruebas de acceso	4 días	jue 23/11/1
83	**Realizar las adecuaciones para asignar una red exclusiva para las impresoras**	**4 días**	**vie 27/10/17**
84	Configurar VLAN para impresoras y asignar puertos	4 días	vie 27/10/17
85	Configurar la nueva dirección IP en las impresoras	4 días	vie 27/10/17
86	Pruebas de funcionamiento	4 días	vie 27/10/1
87	Finalizacion Etapa IV	0 días	**mié 1/11/1**
88	**Etapa V - Protección de Redes Internas**	**19 días**	**jue 14/12/1**
97	**Etapa VI - Webfiltering, Antispam y Procedimientos**	**39 días**	**jue 25/1/18**
98	**Implementar un esquema de WebFiltering en alta disponibilidad**	**19 días**	**jue 25/1/18**
99	Adquisición de firewall UTM (con funcionalidad de WebFilter)	19 días	jue 25/1/18
100	Configuración inicial del equipo y del servicio de webfiltering	19 días	jue 25/1/18

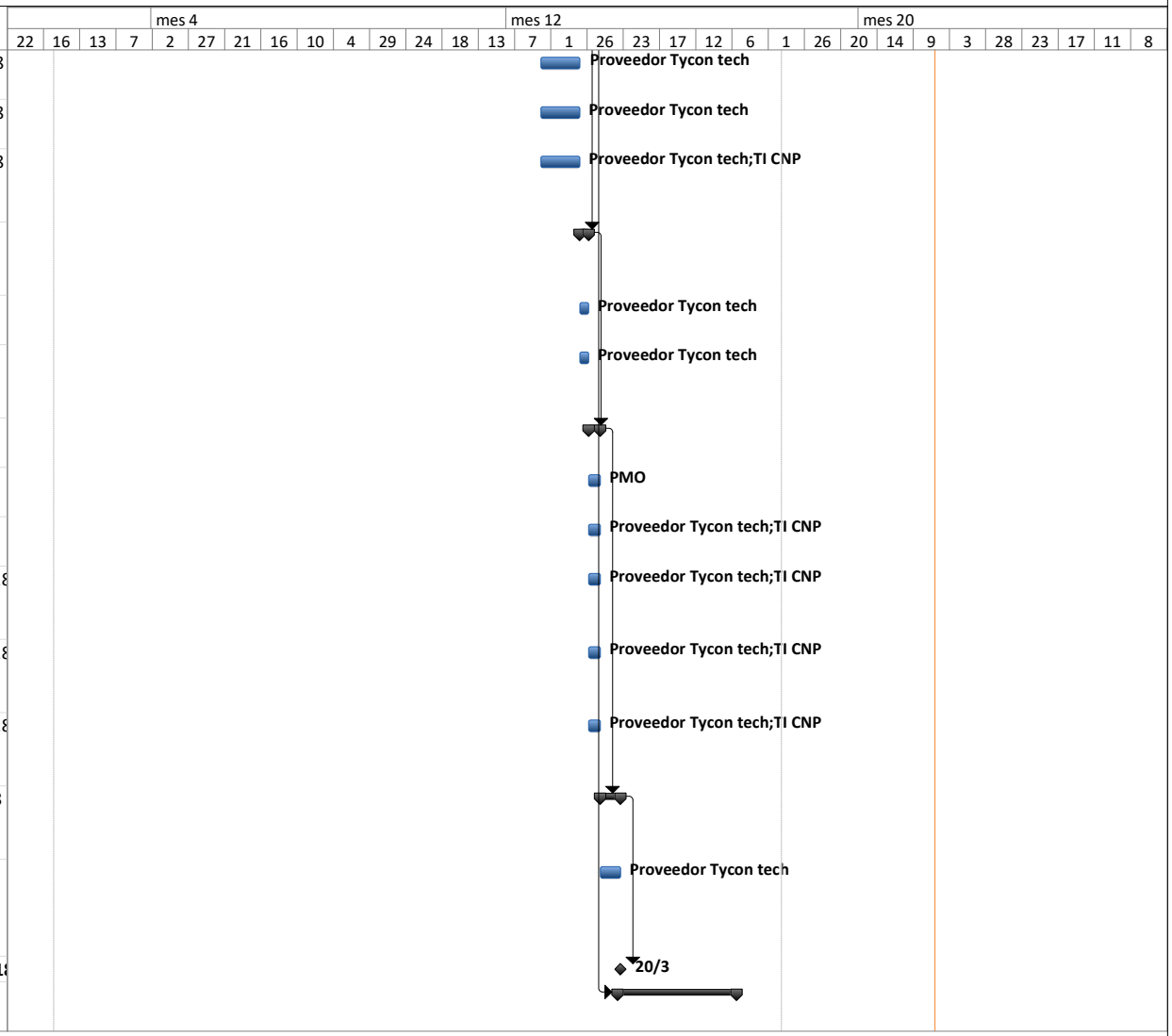


Proyecto: 304-0_ROIRCNP_Evento
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin		
División	Hito externo	Sólo duración	Fecha límite		
Hito	Tarea inactiva	Informe de resumen manual	Progreso		
Resumen	Hito inactivo	Resumen manual			
Resumen del proyecto	Resumen inactivo	Sólo el comienzo			

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	Nombre de tarea	Duración	Comienzo
101	Relevamiento de configuración del WebSense	19 días	jue 25/1/18
102	Migración de configuración al nuevo equipo	19 días	jue 25/1/18
103	Pruebas del servicio de Webfiltering	19 días	jue 25/1/18
104	**Desarrollar las directrices de un procedimiento backup y control de cambios sobre el equipamiento de TI**	**4 días**	**mié 21/2/18**
105	Indicar recomendaciones para generar un procedimiento de backup	4 días	mié 21/2/18
106	Indicar recomendaciones para generar un procedimiento de control de cambios	4 días	mié 21/2/18
107	**Implementar un esquema de Antispam en alta disponibilidad**	**6 días**	**mar 27/2/18**
108	Gestionar la adquisición del equipamiento	6 días	mar 27/2/18
109	Configuración inicial del equipamiento	6 días	mar 27/2/18
110	Relevamiento de configuración actual	6 días	mar 27/2/18
111	Migración de configuración	6 días	mar 27/2/18
112	Pruebas de servicio	6 días	mar 27/2/18
113	**Desarrollar las directrices de un procedimiento diferencial para el ABM de cuentas de administrador de domino**	**10 días**	**mié 7/3/18**
114	Indicar recomendaciones para generar un procedimiento para ABM de cuentas de administrador de dominio	10 días	mié 7/3/18
115	Finalizacion Etapa VI	0 días	**mar 20/3/18**
116	**Etapa VII - RED WiFi, MPLS y Backup Satélital**	**60 días**	**lun 19/3/18**

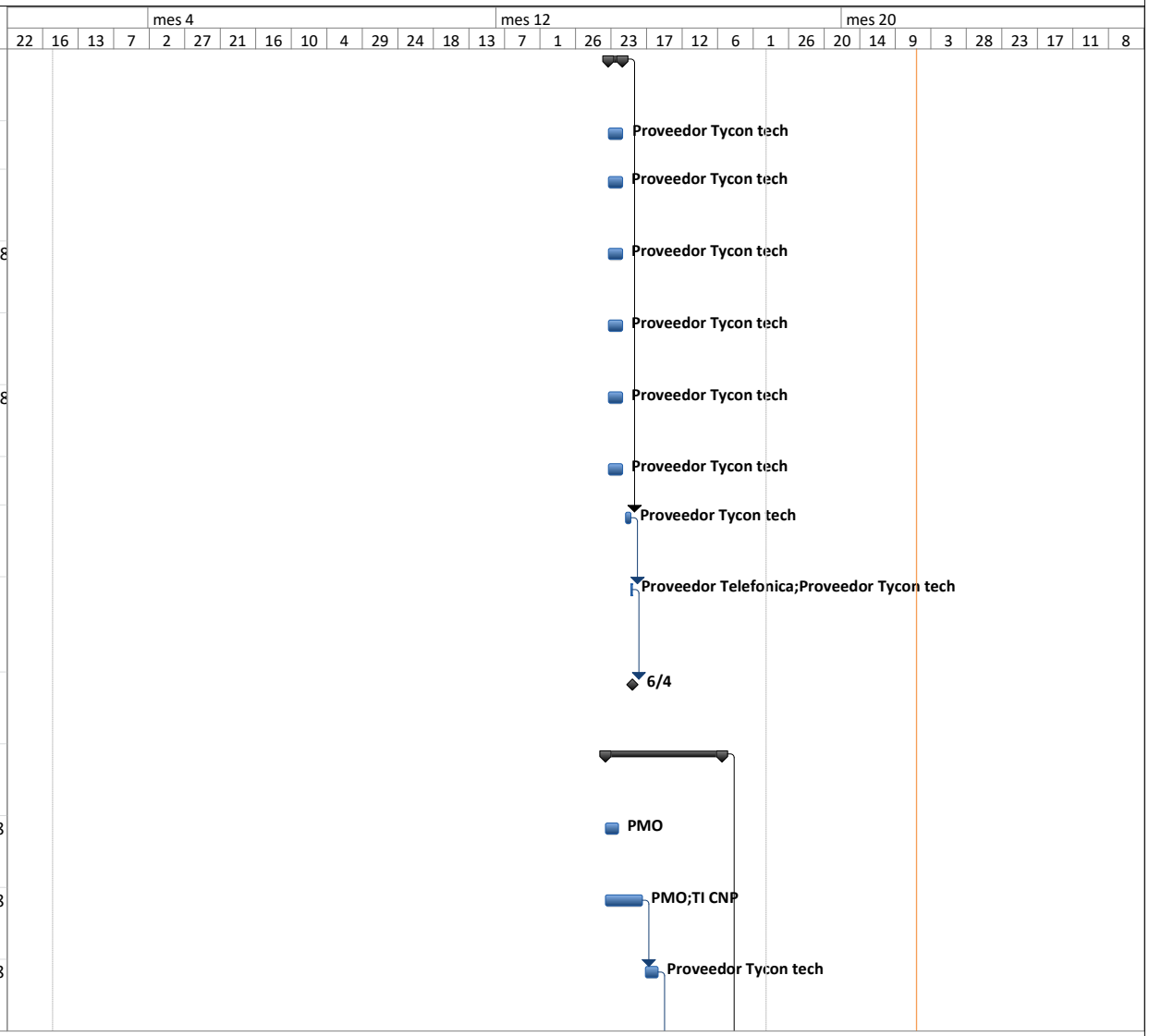


Proyecto: 304-0_ROIRCNP_Evento
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin
División	Hito externo	Sólo duración	Fecha límite
Hito	Tarea inactiva	Informe de resumen manual	Progreso
Resumen	Hito inactivo	Resumen manual	
Resumen del proyecto	Resumen inactivo	Sólo el comienzo	

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	Nombre de tarea	Duración	Comienzo
117	**Implementar cifrado WPA2 o WPA2/Enterprise, SSID Corporativo y SSID Invitados, ajustes de seguridad**	**8 días**	**mié 21/3/18**
118	Sincronizar wireless controller con usuarios active directory	8 días	mié 21/3/18
119	Configurar cifrado WPA2/Enterprise con autenticación para SSID Corporativo	8 días	mié 21/3/18
120	Configurar cifrado WPA2	8 días	mié 21/3/18
121	Definir red vlan de red WiFi corporativa y vlan de red WiFi invitados	8 días	mié 21/3/18
122	Ajustes en red LAN	8 días	mié 21/3/18
123	Documentación, pruebas y test de conexión	8 días	mié 21/3/18
124	Desarrollar un procedimiento para implementar conmutación de enlace MPLS y Backup Satelital	4 días	lun 2/4/18
125	Interactuar con el proveedor y coordinar implementación de conmutación automática de enlace principal a enlace backup y viceversa	1 día	vie 6/4/18
126	Finalizacion Etapa VII	0 días	vie 6/4/18
127	**Etapa VIII: Implementar un clúster de firewall para borde y VPN en clúster de alta disponibilidad**	**60 días**	**lun 19/3/18**
128	Adquisición de firewall UTM para HA	7 días	lun 19/3/18
129	Provision de los equipos ASA	20 días	lun 19/3/18
130	Instalación y configuración inicial	7 días	lun 16/4/18

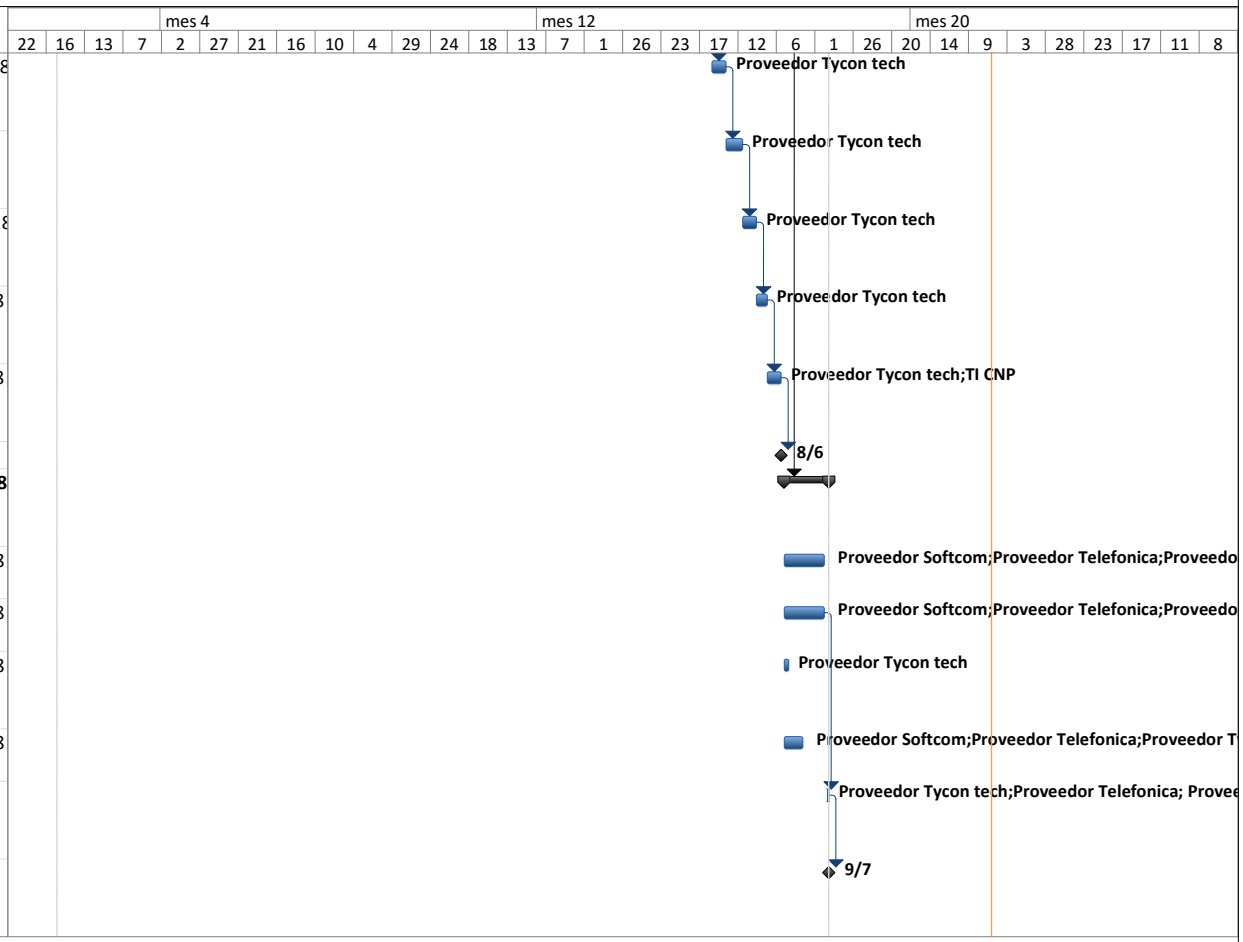


Proyecto: 304-0_ROIRCNP_Evento
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin
División	Hito externo	Sólo duración	Fecha límite
Hito	Tarea inactiva	Informe de resumen manual	Progreso
Resumen	Hito inactivo	Resumen manual	
Resumen del proyecto	Resumen inactivo	Sólo el comienzo	

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	Nombre de tarea	Duración	Comienzo
131	Importar configuraciones de borde	7 días	mié 25/4/18
132	Pruebas de funcionamiento	7 días	vie 4/5/18
133	Importar configuraciones de VPN	7 días	mar 15/5/18
134	Permitir el acceso a la infraestructura t	5 días	jue 24/5/18
135	Pruebas de funcionamiento	7 días	jue 31/5/18
136	Finalizacion Etapa VIII	0 días	**vie 8/6/18**
137	**Cierre**	**21 días**	**lun 11/6/18**
138	Informe final del proyecto	20 días	lun 11/6/18
139	Entrega de ingenieria de detalle completa	20 días	lun 11/6/18
140	Propuesta de soporte y mantenimiento	3 días	lun 11/6/18
141	Lecciones aprendidas y recomendaciones	10 días	lun 11/6/18
142	Reunion de entrega	1 día	lun 9/7/18
143	Finalizacion del proyecto	0 días	lun 9/7/18

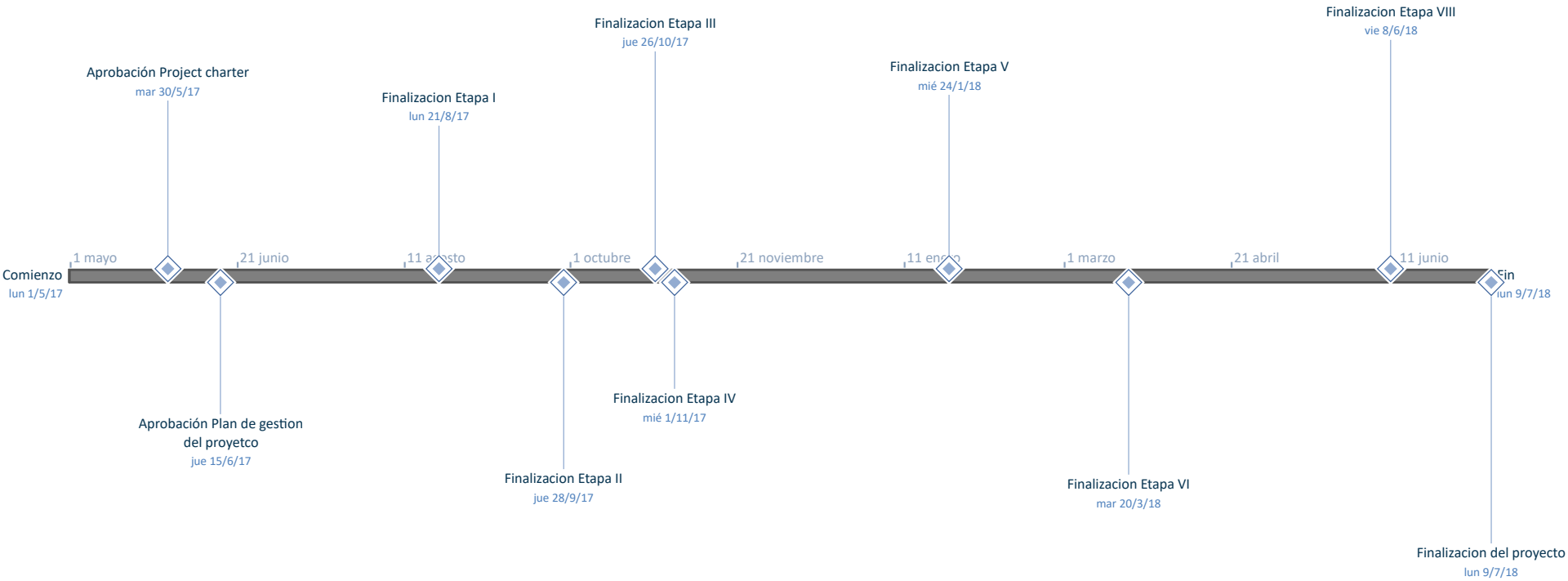


Proyecto: 304-0_ROIRCNP_Evento
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin
División	Hito externo	Sólo duración	Fecha límite
Hito	Tarea inactiva	Informe de resumen manual	Progreso
Resumen	Hito inactivo	Resumen manual	
Resumen del proyecto	Resumen inactivo	Sólo el comienzo	

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Hitos



Autor: James Vallejo PM

Proyecto remediación y optimización infraestructura de red y seguridad informática CNP

Presupuesto	
Etapa	**Costo**
Etapa I - Servicios DNS Externo y DHCP	$ 1.132.475,00
Etapa II - Protección de Borde I	$ 2.373.443,33
Etapa III - Protección de Borde II	$ 1.249.000,00
Etapa IV - Switch de LAN	$ 2.481.325,00
Etapa V - Protección de Redes Internas	$ 1.717.900,00
Etapa VI - Webfiltering, Antispam y Procedimientos	$ 2.453.427,00
Etapa VII - RED WiFi, MPLS y Backup Satélital	$ 1.090.825,00
Etapa VIII - Implementar un clúster de firewall para borde y VPN en clúster de alta disponibilidad	$ 626.250,00
Gestión del proyecto	$ 1.800.000,00
Gestion de Contratación	$ 400.000,00
Servicios Públicos	$ 95.600,00
Total del proyecto	$ 15.420.245,33
Reserva de contingencia (15%)	$ 2.313.036,80
Linea base de costos	$ 17.733.282,13
Reserva de gerencia (20%)	$ 3.546.656,43
Presupuesto	**$ 21.279.938,56**

Presupuesto

	Valor en Pesos ARG.
Gestión del proyecto	$ 1.800.000,00

	Valor en Pesos ARG.
Gestion de Contratación	$ 400.000,00

Servicios Públicos	Mensual	Diario	% Calculado de incremento
Se calcula un incremento del 3% en la facturación, se incluye el costo en el valor total del proyecto	$ 400.000,00	$ 13.333,33	3%

Tabla de Salarios Base recursos TI y personal administrativo

Autor: James Vallejo PM

Recurso	Salario Mes (Pesos ARG.)	Salario dia (Pesos ARG.)	Salario Hora (Pesos ARG.)
Analista de Comunicaciones Junior	$ 30.000,00	$ 1.000,00	$ 125,00
Analista de comunicaciones Senior	$ 42.000,00	$ 1.400,00	$ 175,00
Personal administrativo	$ 140.000,00	$ 4.666,67	$ 583,33

Se utiliza la tabla de salarios Tabla de Salarios Base recursos TI y personal administrativo, para realizar el calculo del costo por cada paquete de trabajo en la linea base de costo detallada

Detalle de costos por cada paquete de trabajo

Paquetes de trabajo	Duración hrs	Analista de soporte junior		Ingeniero Senior		Personal Administrativo		Equipamiento	Costo total
		Cantidad recursos	Costo en Pesos ARG. $	Cantidad recursos	Costo en Pesos ARG. $	Cantidad	Costo en Pesos ARG. $	Costo en Pesos ARG. $	Costo en Pesos ARG. $
Etapa I - Servicios DNS Externo y DHCP									**$ 1.132.475,00**
Habilitar protección de IPS, AV y publicar solo puertos necesarios para el servicio de	**105**		**$ 26.250,00**		**$ 36.750,00**		**$ 183.750,00**		**$ 246.750,00**
Solicitar al proveedor habilitar solo el puerto 53, protocolos TCP y UDP	35	2	$ 8.750,00	2	$ 12.250,00	3	$ 61.250,00		
Solicitar al proveedor del firewall que habilite para protección de IPS y AV en la	35	2	$ 8.750,00	2	$ 12.250,00	3	$ 61.250,00		
Realizar pruebas del servicio	35	2	$ 8.750,00	2	$ 12.250,00	3	$ 61.250,00		
Ajustar configuración de DNS Server Externo Segundario	**205**		**$ 61.500,00**		**$ 107.625,00**		**$ 358.750,00**		**$ 527.875,00**
Instalación de un servidor con Windows Server 2012	41	3	$ 15.375,00	3	$ 21.525,00	3	$ 71.750,00		
Habilitar servicio de DNS	41	2	$ 10.250,00	3	$ 21.525,00	3	$ 71.750,00		
Transferir zonas desde DNS principal al segundario	41	2	$ 10.250,00	3	$ 21.525,00	3	$ 71.750,00		
Gestionar configuraciones para publicación en internet	41	2	$ 10.250,00	3	$ 21.525,00	3	$ 71.750,00		
Realizar pruebas de servicios	41	3	$ 15.375,00	3	$ 21.525,00	3	$ 71.750,00		
Configurar otro registro MX para un Mail Server Segundario	**100**		**$ 25.000,00**		**$ 35.000,00**		**$ 175.000,00**		**$ 235.000,00**
En el servidor de DNS, agregar un DNS record de tipo MX (Mail Exchanger)	50	2	$ 12.500,00	2	$ 17.500,00	3	$ 87.500,00		

Autor: James Vallejo PM

Asignar una prioridad para que actue como backup (debe ser un número mayor que el del primario)	50	2	$ 12.500,00	2	$ 17.500,00	3	$ 87.500,00		
Implementar un esquema de HA para el servidor de DHCP	**144**		**$ 42.000,00**		**$ 75.600,00**		**$ 252.000,00**		**$ 369.600,00**
Instalación de dos servidores con Windows Server 2012	48	2	$ 12.000,00	3	$ 25.200,00	3	$ 84.000,00		
Configurar los servicios de DHCP y conmutación por error en modo load	48	2	$ 12.000,00	3	$ 25.200,00	3	$ 84.000,00		
Realizar pruebas del servicio	48	3	$ 18.000,00	3	$ 25.200,00	3	$ 84.000,00		
Etapa II - Protección de Borde I									**$ 2.373.443,33**
Ajustar servicios publicados en internet y configurar aplicaciones publicadas en la red	**270**		**$ 78.750,00**		**$ 110.250,00**		**$ 472.500,00**		**$ 661.500,00**
Solicitar al proveedor del firewall habilitar solo los puertos necesarios de los servicio publicados en intenret	90	2	$ 22.500,00	2	$ 31.500,00	3	$ 157.500,00		
Verificar servicios que no están en la red DMZ y moverlos a esta red	90	2	$ 22.500,00	2	$ 31.500,00	3	$ 157.500,00		
Pruebas de funcionamiento	90	3	$ 33.750,00	3	$ 47.250,00	3	$ 157.500,00		
Implementar una alternativa tecnológica diferente al TMG, ya el servicio está	**548**		**$ 68.500,00**		**$ 383.600,00**		**$ 879.083,33**	**$ 380.760,00**	**$ 1.711.943,33**
Adquisición de firewall UTM	137	0	$ -	1	$ -	2	$ 159.833,33	Fortigate 200 D (2) + Licencias	
Relevar configuraciones de permisos de acceso en el TMG	137	2	$ 34.250,00	3	$ 71.925,00	3	$ 239.750,00		
Migrar configuraciones de permisos de acceso a los firewalls UTM	137	2	$ 34.250,00	3	$ 71.925,00	3	$ 239.750,00		
Pruebas de servicios	137	3	$ -	3	$ 239.750,00	3	$ 239.750,00		
Etapa III - Protección de Borde II									**$ 1.249.000,00**
Realizar las adecuaciones para que los servicios sean publicados desde un único equipo y en forma directa	**208**		**$ 65.000,00**		**$ 100.100,00**		**$ 364.000,00**		**$ 529.100,00**
Verificar que servicios hacia internet están publicados desde el ISA Server y el TMG	52	2	$ 13.000,00	2	$ 18.200,00	3	$ 91.000,00		
Crear y validar las reglas de firewall en un entorno de prueba	52	2	$ 13.000,00	3	$ 27.300,00	3	$ 91.000,00		
Migrar las reglas al nuevo firewall	52	3	$ 19.500,00	3	$ 27.300,00	3	$ 91.000,00		
Realizar pruebas de funcionamiento de los servicios	52	3	$ 19.500,00	3	$ 27.300,00	3	$ 91.000,00		

Realizar las adecuaciones para que todos los servicios publicados en internet cuenten con protección de IPS, AV y DOS	**276**		**$ 92.000,00**		**$ 144.900,00**		**$ 483.000,00**		**$ 719.900,00**
Crear profiles de AV, IPS y Antivirus en el firewall	92	2	$ 23.000,00	3	$ 48.300,00	3	$ 161.000,00		
Asignar los profiles a los servicios publicados en internet	92	3	$ 34.500,00	3	$ 48.300,00	3	$ 161.000,00		
Realizar pruebas de los servicios publicados en internet	92	3	$ 34.500,00	3	$ 48.300,00	3	$ 161.000,00		
Etapa IV - Switch de LAN									**$ 2.841.325,00**
Implementar segmentación por VLANs para red de usuarios y red de servidores. Configurar ruteo por capa 3 (nivel de red)	**600**		**$ 281.250,00**		**$ 183.750,00**		**$ 1.050.000,00**	**$ 400.000,00**	**$ 1.915.000,00**
Definir rangos de red	150	1	$ 18.750,00	2	$ 52.500,00	3	$ 262.500,00		
Configuración en Switchs, Vlans, puertos de Trunk	150	4	$ 75.000,00	2	$ 52.500,00	3	$ 262.500,00	Cisco 3850 (8) + cables de red UTP (400)	
Migración de equipos a nuevas redes, asignación de puertos de switch a nuevas Vlans	150	5	$ 93.750,00	3	$ 78.750,00	3	$ 262.500,00		
Pruebas de funcionamiento	150	5	$ 93.750,00	3	$ -	3	$ 262.500,00		
Realizar las adecuaciones para utilizar otro puerto de backup en caso de falta en el puerto que está en uso	**118**		**$ 36.875,00**		**$ 61.950,00**		**$ 206.500,00**		**$ 305.325,00**
Configurar port channel en cada uno de los switch	59	2	$ 14.750,00	3	$ 30.975,00	3	$ 103.250,00		
Pruebas de puertos de backup y continuidad de servicio	59	3	$ 22.125,00	3	$ 30.975,00	3	$ 103.250,00		
Realizar las adecuaciones para utilizar acceso SSH (secure shell) encriptado	**84**		**$ 31.500,00**		**$ 29.400,00**		**$ 147.000,00**		**$ 207.900,00**
Configurar acceso por secure shell a los switchs	28	3	$ 10.500,00	2	$ 9.800,00	3	$ 49.000,00		
Cancelar la configuración para acceder por telnet	28	3	$ 10.500,00	2	$ 9.800,00	3	$ 49.000,00		
Pruebas de acceso por shh a los equipos	28	3	$ 10.500,00	2	$ 9.800,00	3	$ 49.000,00		
Realizar las adecuaciones para no utilizar la vlan nativa para tráfico de red	**81**		**$ 30.375,00**		**$ 37.800,00**		**$ 141.750,00**		**$ 209.925,00**
Configurar VLAN para gestión de dispositivos de red	27	2	$ 6.750,00	2	$ 9.450,00	3	$ 47.250,00		

Autor: James Vallejo PM

Configurar una dirección ip de la nueva vlan a los dispositivos	27	3	$ 10.125,00	3	$ 14.175,00	3	$ 47.250,00		
Pruebas de acceso	27	4	$ 13.500,00	3	$ 14.175,00	3	$ 47.250,00		
Realizar las adecuaciones para asignar una red exclusiva para las impresoras	**81**		**$ 23.625,00**		**$ 37.800,00**		**$ 141.750,00**		**$ 203.175,00**
Configurar VLAN para impresoras y asignar puertos	27	2	$ 6.750,00	3	$ 14.175,00	3	$ 47.250,00		
Configurar la nueva dirección IP en las impresoras	27	2	$ 6.750,00	3	$ 14.175,00	3	$ 47.250,00		
Pruebas de funcionamiento	27	3	$ 10.125,00	2	$ 9.450,00	3	$ 47.250,00		
Etapa V - Protección de Redes Internas									**$ 1.717.900,00**
Realizar las adecuaciones para que todo el tráfico entre redes de la empresa pase a través del firewall	**739**		**$ 131.250,00**		**$ 210.000,00**		**$ 1.050.000,00**		**$ 1.391.250,00**
Adquisición de firewall UTM	150	0	$ -	1	$ 26.250,00	3	$ 262.500,00	Cisco ASA 5545 (2)	
Ajustes de firewall UTM en la topología de red	150	2	$ 37.500,00	2	$ 52.500,00	3	$ 262.500,00		
Ajustes de configuración en reglas de acceso	150	2	$ 37.500,00	2	$ 52.500,00	3	$ 262.500,00		
Pruebas y testeos de conexión entre las distintas redes	150	3	$ 56.250,00	3	$ 78.750,00	3	$ 262.500,00		
Aplicar IPS, AV, restricciones de ancho de banda para el tráfico LAN to LAN y LAN to WAN	**105**	**2**	**$ 26.250,00**	**2**	**$ 36.750,00**	**3**	**$ 183.750,00**		**$ 246.750,00**
Permitir el acceso a la infraestructura tecnológica solo desde la red de informática.	**34**	**2**	**$ 8.500,00**	**2**	**$ 11.900,00**	**3**	**$ 59.500,00**		**$ 79.900,00**
Etapa VI - Webfiltering, Antispam y Procedimientos									**$ 2.453.427,00**
Implementar un esquema de WebFiltering en alta disponibilidad	**735**	**11**	**$ 202.125,00**	**12**	**$ 308.700,00**	**15**	**$ 1.286.250,00**		**$ 1.797.102,00**
Adquisición de firewall UTM (con funcionalidad de WebFilter)	147	0	$ -	1	$ 25.725,00	3	$ 257.250,00	Fortigate 200 D (2) + Licencia	
Configuración inicial del equipo y del servicio de webfiltering	147	2	$ 36.750,00	3	$ 77.175,00	3	$ 257.250,00		
Relevamiento de configuración del WebSense	147	2	$ 36.750,00	2	$ 51.450,00	3	$ 257.250,00		
Migración de configuración al nuevo equipo	147	3	$ 55.125,00	3	$ 77.175,00	3	$ 257.250,00		
Pruebas del servicio de Webfiltering	147	4	$ 73.500,00	3	$ 77.175,00	3	$ 257.250,00		

Autor: James Vallejo PM

Desarrollar las directrices de un procedimiento backup y control de cambios sobre el equipamiento de TI	**50**	**0**	**$ -**		**$ 17.500,00**		**$ 58.333,33**		**$ 75.833,33**
Indicar recomendaciones para generar un procedimiento de backup	25	0	$ -	2	$ 8.750,00	2	$ 29.166,67		
Indicar recomendaciones para generar un procedimiento de control de cambios	25	0	$ -	2	$ 8.750,00	2	$ 29.166,67		
Implementar un esquema de Antispam en alta disponibilidad	**235**		**$ 52.875,00**		**$ 98.700,00**		**$ 411.250,00**		**$ 562.825,00**
Gestionar la adquisición del equipamiento	47	0	$ -	1	$ 8.225,00	3	$ 82.250,00	Licencia Fortigate 200D antispam	
Configuración inicial del equipamiento	47	1	$ 5.875,00	2	$ 16.450,00	3	$ 82.250,00		
Relevamiento de configuración actual	47	2	$ 11.750,00	3	$ 24.675,00	3	$ 82.250,00		
Migración de configuración	47	2	$ 11.750,00	3	$ 24.675,00	3	$ 82.250,00		
Pruebas de servicio	47	4	$ 23.500,00	3	$ 24.675,00	3	$ 82.250,00		
Desarrollar las directrices de un procedimiento diferencial para el ABM de cuentas de administrador de domino	**10**		**$ 2.500,00**		**$ 3.500,00**		**$ 11.666,67**		**$ 17.666,67**
Indicar recomendaciones para generar un procedimiento para ABM de cuentas de administrador de dominio	10	2	$ 2.500,00	2	$ 3.500,00	2	$ 11.666,67		
Etapa VII - RED WiFi, MPLS y Backup Satélital									**$ 1.090.825,00**
Implementar cifrado WPA2 o WPA2/Enterprise, SSID Corporativo y SSID Invitados, ajustes de seguridad	**360**		**$ 127.500,00**		**$ 199.500,00**		**$ 630.000,00**		**$ 957.000,00**
Sincronizar wireless controller con usuarios active directory	60	3	$ 22.500,00	4	$ 42.000,00	3	$ 105.000,00		
Configurar cifrado WPA2/Enterprise con autenticación para SSID Corporativo	60	3	$ 22.500,00	3	$ 31.500,00	3	$ 105.000,00		
Configurar cifrado WPA2	60	3	$ 22.500,00	3	$ 31.500,00	3	$ 105.000,00		
Definir red vlan de red WiFi corporativa y vlan de red WiFi invitados	60	2	$ 15.000,00	4	$ 42.000,00	3	$ 105.000,00		
Ajustes en red LAN	60	4	$ 30.000,00	3	$ 31.500,00	3	$ 105.000,00		
Documentación, pruebas y test de conexión	60	2	$ 15.000,00	2	$ 21.000,00	3	$ 105.000,00		

Desarrollar un procedimiento para implementar conmutación de enlace MPLS y Backup Satelital	**29**	**2**	**$ 7.250,00**	**3**	**$ 15.225,00**	**3**	**$ 50.750,00**		**$ 73.225,00**
Interactuar con el proveedor y coordinar implementación de conmutación automática de enlace principal a enlace backup y viceversa	**24**	**2**	**$ 6.000,00**	**3**	**$ 12.600,00**	**3**	**$ 42.000,00**		**$ 60.600,00**
Etapa VIII - Implementar un clúster de firewall para borde y VPN en clúster de alta disponibilidad	**384**		**$ 75.000,00**		**$ 113.750,00**		**$ 437.500,00**		**$ 626.250,00**
Adquisición de firewall UTM para HA	50	2	$ 12.500,00	2	$ 17.500,00	3	$ 87.500,00		
Provision de los equipos ASA	50	2	$ 12.500,00	2	$ 17.500,00	3	$ 87.500,00		
Instalación y configuración inicial	50	3	$ 18.750,00	3	$ 26.250,00	3	$ 87.500,00		
Importar configuraciones de borde	50	2	$ 12.500,00	3	$ 26.250,00	3	$ 87.500,00		
Pruebas de funcionamiento	50	3	$ 18.750,00	3	$ 26.250,00	3	$ 87.500,00		
Importar configuraciones de VPN	50	2	$ 12.500,00	3	$ 26.250,00	3	$ 87.500,00		
Permitir el acceso a la infraestructura tecnológica solo desde la red de informática.	34	3	$ 12.750,00	3	$ 17.850,00	3	$ 59.500,00		
Pruebas de funcionamiento	50	4	$ 25.000,00	3	$ 26.250,00	3	$ 87.500,00		

GESTION DE PROYECTOS **FORMATO DE GESTIÓN DE RFC A PROYECTO**		
Nombre del proyecto: Proyecto Remediación y optimización infraestructura de red y seguridad informática	**Fecha**: 06/10/2017	**Proponente:** Dirección TI
Tipo de cambio a proponer: incluir nueva actividad, tendido de Cableado estructurado	**No. De Cambio: 02**	**No. Del proyecto: 02**
Puede anexar todos los documentos que considere necesarios como soporte del cambio y referenciarlos en cada casilla		
Descripción del cambio		
Falta de cableado estructurado para ejecutar la actividad Migración de equipos a nuevas redes, asignación de puertos de switch a nuevas Vlans de la ***etapa IV Implementar segmentación por VLANs para red de usuarios y red de servidores. Configurar ruteo por capa 3 (nivel de red)***		
Condiciones actuales del proyecto (en términos del plan global del proyecto) Es necesario tener el cableado estructurado para continuar con los entregables del proyecto, se tenía como un supuesto, ya que esto estaba dentro de contratación de TI CNP y hacia parte de otro proyecto del programa		
Cambio propuesto (precisar actividades que cambian, recursos adicionales, cambios en presupuesto, entre otros)		
Posibles consecuencias del cambio (en resultados del proyecto, económicos, en procesos, en la organización, entre otros) Aumentan los costos en el proyecto, para ello se utilizará la reserva de gerencia.		
Justificación del cambio Se requiere tener el cableado estructurado del datacenter para continuar con la migración de usuarios en tiempo previsto		
Acciones a desarrollar si se acepta la propuesta de cambio Calcular costos, informar a la dirección, incluí nueva actividad, solicitar cotizaciones a proveedores, contratar proveedores para el cableado requerido.		
Nombre y firma del gerente del proyecto (Solicitante): James Vallejo Mejia		Fecha: 06/10/2017

Nombre y firma del Coordinador de TI: Pablo Barbieri	Fecha: 06/10/2017
Aprobada (X) Rechazada ( )	No. Acta: RFC_PM_002
Nombre y firma del Director TI: Marcelo Cueto	Fecha: 06/10/2017
Decisiones tomadas frente a la propuesta	
Se Aprueba el cambio.	

Elaboró: James Vallejo	Fecha:06/10/2017	Código: RFC_PM_002
Revisó: Marcelo Cueto	Fecha:06/10/2017	Pagina:
Aprobó: Marcelo cueto	Fecha:06/10/2017	Versión:1

Compañía Nacional del Petróleo

Evento de cambio 2

Reporte especial

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Autor: James Vallejo Mejia

Registro de cambios

Fecha	Versión	Descripción	Autor	Aprobación
23/7/2018	1	Cambio	PM	

Contenido

Evento de Cambio 2 – Reporte especial

1 Eventos generados y sus impactos

En el siguiente apartado, se comunica el evento realizado y la gestión después del cambio solicitado y aprobado por la dirección TI, sponsor del proyecto remediación y optimización infraestructura de red y seguridad informática.

Para la continuación del proyecto es necesario contar con el cableado estructurado certificado para la conexión de los equipos de red de usuarios hacia los equipos de red (switches) ubicados en el datacenter de la sede administrativa en Tucumán 1, CABA

Los cambios reflejados en los entregables son los siguientes: En color verde, las actividades que se agregan en la etapa IV

Nombre de tarea	Duración	Comienzo	Fin
Etapa IV - Switch de LAN	**31 días**	**lun 6/11/17**	**vie 5/1/18**
Implementar segmentación por VLANs para red de usuarios y red de servidores. Configurar ruteo por capa 3 (nivel de red)	**19 días**	**lun 6/11/17**	**vie 1/12/17**
Búsqueda de Proveedores Cableado estructurado	3 días	lun 6/11/17	mié 8/11/17
Contratación de proveedor cableado estructurado	2 días	lun 6/11/17	mar 7/11/17
Implementación cableado estructurado	10 días	lun 6/11/17	vie 17/11/17
Definir rangos de red	19 días	lun 6/11/17	vie 1/12/17
Configuración en Switchs, Vlans, puertos de Trunk	19 días	lun 6/11/17	vie 1/12/17
Migración de equipos a nuevas redes, asignación de puertos de switch a nuevas Vlans	19 días	lun 6/11/17	vie 1/12/17
Pruebas de funcionamiento	19 días	lun 6/11/17	vie 1/12/17

Se realiza Fast Tracking para no afectar el tiempo de finalización del entregable y no retrasar el proyecto, se cumplirá con el tiempo planeado.

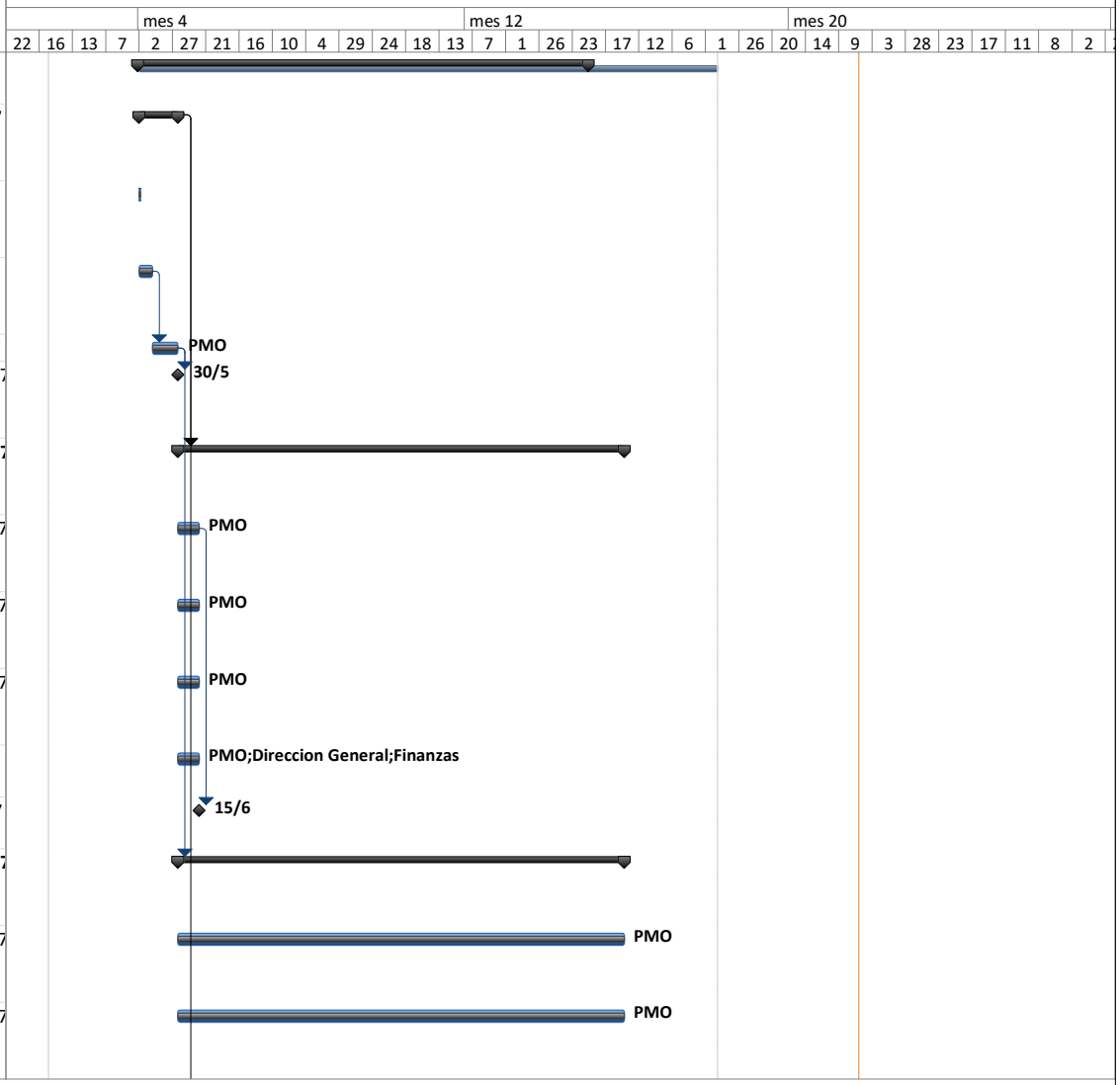
Cambios en presupuesto

Para la ejecución de estas nuevas actividades se utiliza dinero de la reserva de gerencia con la autorización de la dirección TI.

Estimación Fondo de Contingencia	$ 3.546.656,43
Costo por Evento 2 RFC_PM_002	$ 750.000
Consumo Reserva de gerencia	-$ 750.000
Saldo Reserva de gerencia	$ 2.796.656,43

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	EDT	Nombre de tarea	% completa	Duración	Comienzo
1	**1**	**Remediación Infraestructura y Seguridad Informática**	**65%**	**223 días**	**lun 1/5/17**
2	**1.1**	**Inicio**	**100%**	**20 días**	**mar 2/5/17**
3	1.1.1	Kick off de inicio del proyecto	100%	1 día	mar 2/5/17
4	1.1.2	Caso de negocio	100%	8 días	mar 2/5/17
5	1.1.3	Acta de proyecto	100%	12 días	vie 12/5/17
6	1.1.4	Aprobación Project charter	100%	0 días	mar 30/5/17
7	**1.2**	**Gestion del proyecto**	**100%**	**221 días**	**mié 31/5/17**
8	1.2.1	Plan de gestión de proyecto	100%	12 días	mié 31/5/17
9	1.2.2	Linea base de alcance	100%	12 días	mié 31/5/17
10	1.2.3	Linea base de tiempo	100%	12 días	mié 31/5/17
11	1.2.4	Linea base de costos	100%	12 días	mié 31/5/17
12	1.2.5	Aprobación Plan de gestion del proyetco	100%	0 días	jue 15/6/17
13	**1.2.6**	**Comunicaciones**	**100%**	**221 días**	**mié 31/5/17**
14	1.2.6.1	Reporte de hitos	100%	221 días	mié 31/5/17
15	1.2.6.2	minutas	100%	221 días	mié 31/5/17

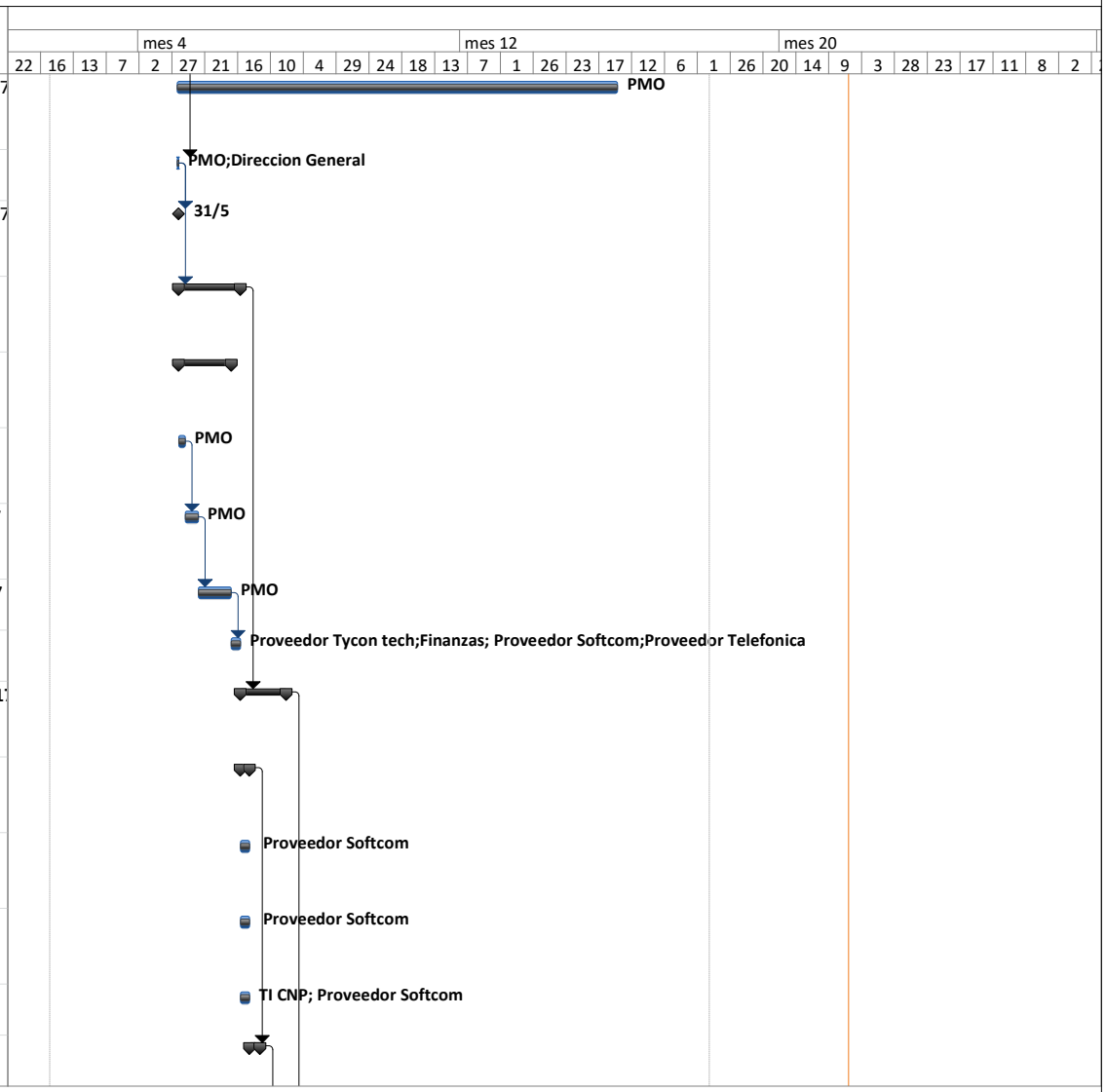


Proyecto: 304-0_ROIRCNP_Evento
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin		
División	Hito externo	Sólo duración	Fecha límite		
Hito	Tarea inactiva	Informe de resumen manual	Progreso		
Resumen	Hito inactivo	Resumen manual			
Resumen del proyecto	Resumen inactivo	Sólo el comienzo			

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	EDT	Nombre de tarea	% completa	Duración	Comienzo
16	1.2.6.3	Reporte de status	100%	221 días	mié 31/5/17
17	1.2.7	Kick Off Puesta en marcha	100%	1 día	mié 31/5/17
18	1.2.8	Hito Cick off puesta en marcha	100%	0 días	mié 31/5/17
19	**1.3**	**Gestion de Contratación**	**100%**	**31 días**	**jue 1/6/17**
20	**1.3.1**	**Búsqueda del proveedor**	**100%**	**26 días**	**jue 1/6/17**
21	1.3.1.1	Invitacion a proveedores	100%	3 días	jue 1/6/17
22	1.3.1.2	RFP (Request for Proposal)	100%	8 días	mar 6/6/17
23	1.3.1.3	Análisis y Selección de proveedores	100%	15 días	vie 16/6/17
24	1.3.2	Contratación	100%	5 días	mar 11/7/17
25	**1.4**	**Etapa I - Servicios DNS Externo y DHCP**	**100%**	**24 días**	**mar 18/7/17**
26	**1.4.1**	**Habilitar protección de IPS, AV y publicar solo puertos necesarios para el servicio de DNS Externo**	**100%**	**5 días**	**mar 18/7/17**
27	1.4.1.1	Solicitar al proveedor habilitar solo el puerto 53, protocolos TCP y UDP	100%	5 días	mar 18/7/17
28	1.4.1.2	Solicitar al proveedor del firewall que habilite para protección de IPS y AV en la publicación	100%	5 días	mar 18/7/17
29	1.4.1.3	Realizar pruebas del servicio	100%	5 días	mar 18/7/17
30	**1.4.2**	**Ajustar configuración de DNS Server Externo Segundario**	**100%**	**6 días**	**mar 25/7/17**

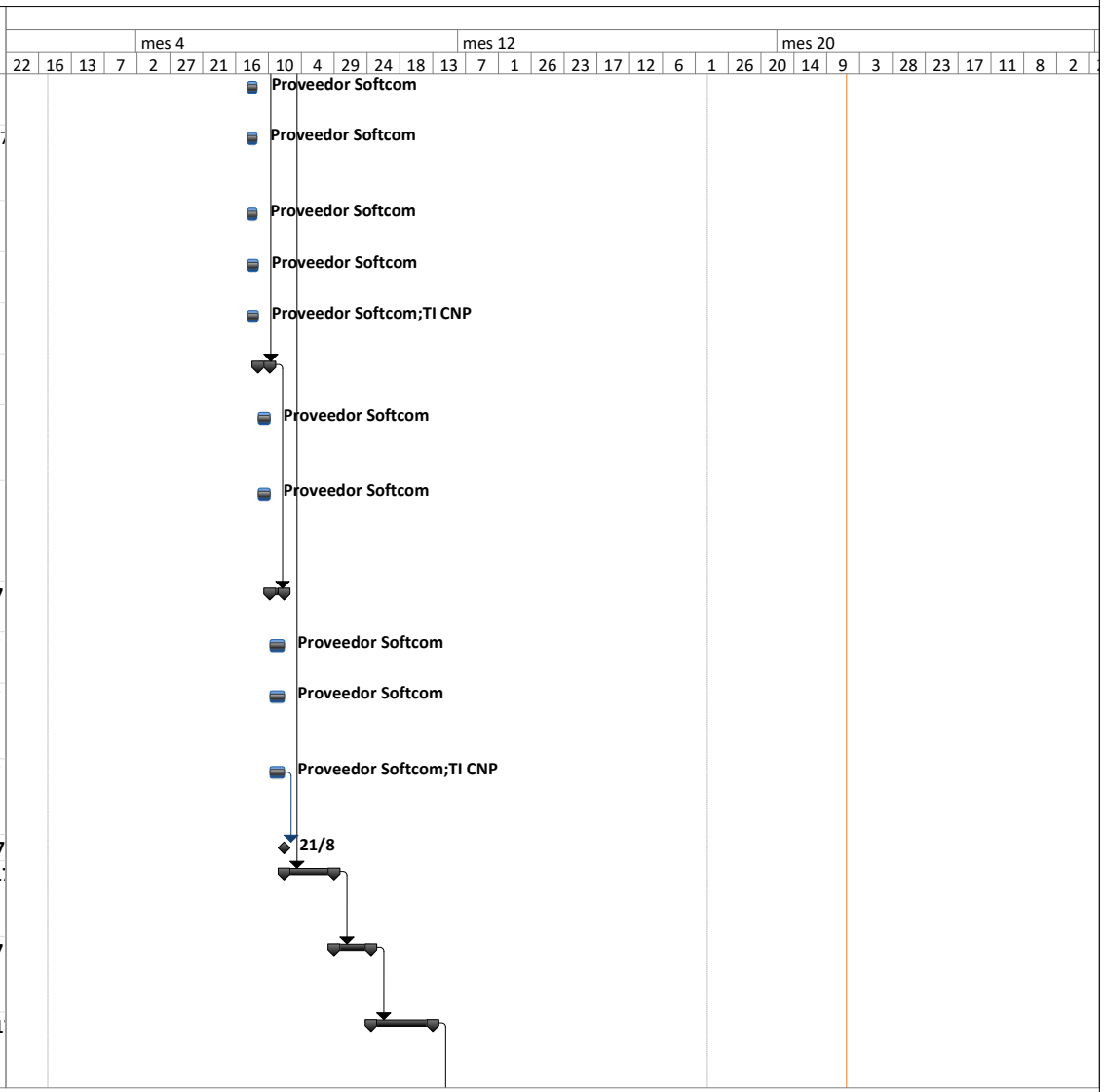


Proyecto: 304-0_ROIRCNP_Evento
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin				
División	Hito externo	Sólo duración	Fecha límite				
Hito	Tarea inactiva	Informe de resumen manual	Progreso				
Resumen	Hito inactivo	Resumen manual					
Resumen del proyecto	Resumen inactivo	Sólo el comienzo					

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	EDT	Nombre de tarea	% completa	Duración	Comienzo
31	1.4.2.1	Instalación de un servidor con Windows Server 2012	100%	5 días	mar 25/7/17
32	1.4.2.2	Habilitar servicio de DNS	100%	5 días	mar 25/7/17
33	1.4.2.3	Transferir zonas desde DNS principal al segundario	100%	5 días	mar 25/7/17
34	1.4.2.4	Gestionar configuraciones para publicación en internet	100%	6 días	mar 25/7/17
35	1.4.2.5	Realizar pruebas de servicios	100%	6 días	mar 25/7/17
36	**1.4.3**	**Configurar otro registro MX para un Mail Server Segundario**	**100%**	**7 días**	**mié 2/8/17**
37	1.4.3.1	En el servidor de DNS, agregar un DNS record de tipo MX (Mail Exchanger)	100%	7 días	mié 2/8/17
38	1.4.3.2	Asignar una prioridad para que actue como backup (debe ser un número mayor que el del primario)	100%	7 días	mié 2/8/17
39	**1.4.4**	**Implementar un esquema de HA para el servidor de DHCP**	**100%**	**6 días**	**vie 11/8/17**
40	1.4.4.1	Instalación de dos servidores con Windows Server 2012	100%	6 días	vie 11/8/17
41	1.4.4.2	Configurar los servicios de DHCP y conmutación por error en modo load balance	100%	6 días	vie 11/8/17
42	1.4.4.3	Realizar pruebas del servicio	100%	6 días	vie 11/8/17
43	1.4.5	Finalizacion Etapa I	100%	0 días	**lun 21/8/17**
44	**1.5**	**Etapa II - Protección de Borde I**	**100%**	**28 días**	**mar 22/8/17**
55	**1.6**	**Etapa III - Protección de Borde II**	**100%**	**19 días**	**vie 29/9/17**
66	**1.7**	**Etapa IV - Switch de LAN**	**0%**	**31 días**	**vie 27/10/17**

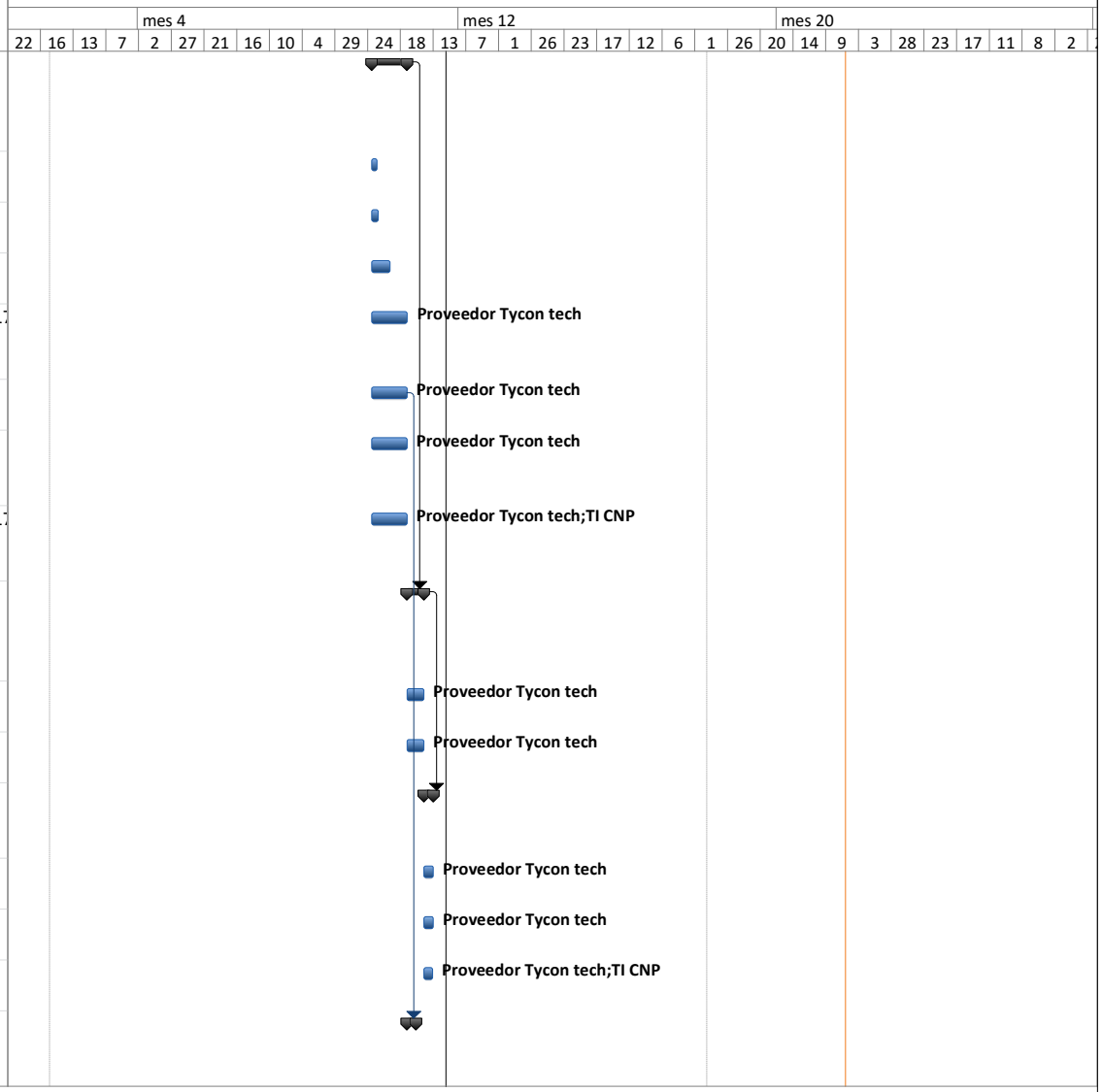


Proyecto: 304-0_ROIRCNP_Evento
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin
División	Hito externo	Sólo duración	Fecha límite
Hito	Tarea inactiva	Informe de resumen manual	Progreso
Resumen	Hito inactivo	Resumen manual	
Resumen del proyecto	Resumen inactivo	Sólo el comienzo	

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	EDT	Nombre de tarea	% completa	Duración	Comienzo
67	**1.7.1**	**Implementar segmentación por VLANs para red de usuarios y red de servidores. Configurar ruteo por capa 3 (nivel de red)**	**0%**	**19 días**	**vie 27/10/17**
68	1.7.1.1	Busqueda de Proveedores Cableado estructurado	0%	2 días	vie 27/10/17
69	1.7.1.2	Contratacion de proveedor cableado estructurado	0%	3 días	vie 27/10/17
70	1.7.1.3	Implementacion cableado estructurado	0%	10 días	vie 27/10/17
71	1.7.1.4	Definir rangos de red	0%	19 días	vie 27/10/17
72	1.7.1.5	Configuración en Switchs, Vlans, puertos de Trunk	0%	19 días	vie 27/10/17
73	1.7.1.6	Migración de equipos a nuevas redes, asignación de puertos de switch a nuevas Vlans	0%	19 días	vie 27/10/17
74	1.7.1.7	Pruebas de funcionamiento	0%	19 días	vie 27/10/17
75	**1.7.2**	**Realizar las adecuaciones para utilizar otro puerto de backup en caso de falta en el puerto que está en uso**	**0%**	**8 días**	**jue 23/11/17**
76	1.7.2.1	Configurar port channel en cada uno de los switch	0%	8 días	jue 23/11/17
77	1.7.2.2	Pruebas de puertos de backup y continuidad de servicio	0%	8 días	jue 23/11/17
78	**1.7.3**	**Realizar las adecuaciones para utilizar acceso SSH (secure shell) encriptado**	**0%**	**4 días**	**mié 6/12/17**
79	1.7.3.1	Configurar acceso por secure shell a los switchs	0%	4 días	mié 6/12/17
80	1.7.3.2	Cancelar la configuración para acceder por telnet	0%	4 días	mié 6/12/17
81	1.7.3.3	Pruebas de acceso por shh a los equipos	0%	28 horas	mié 6/12/17
82	**1.7.4**	**Realizar las adecuaciones para no utilizar la vlan nativa para tráfico de red**	**0%**	**4 días**	**jue 23/11/17**

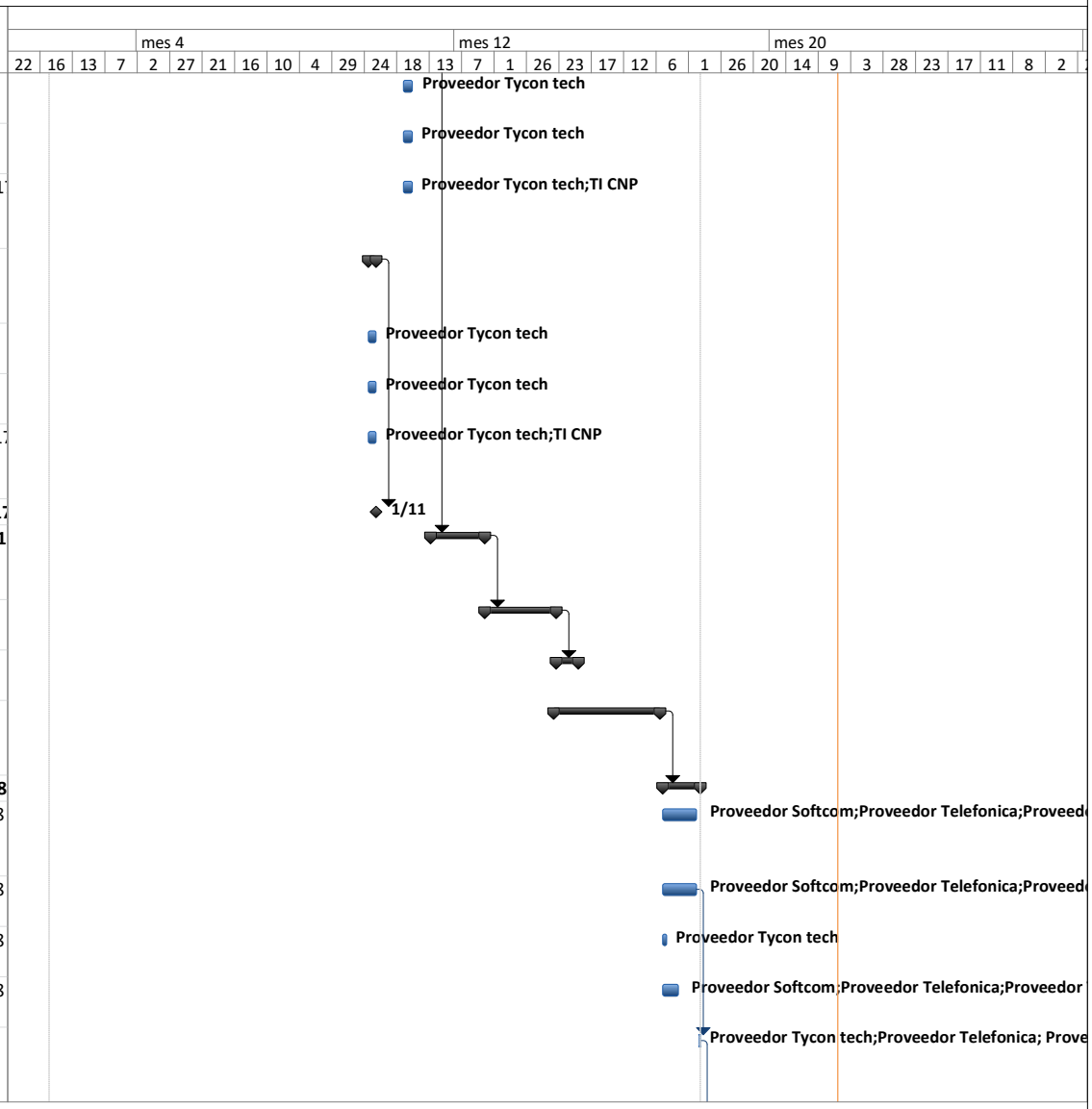


Proyecto: 304-0_ROIRCNP_Evento
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin				
División	Hito externo	Sólo duración	Fecha límite				
Hito	Tarea inactiva	Informe de resumen manual	Progreso				
Resumen	Hito inactivo	Resumen manual					
Resumen del proyecto	Resumen inactivo	Sólo el comienzo					

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	EDT	Nombre de tarea	% completa	Duración	Comienzo
83	1.7.4.1	Configurar VLAN para gestión de dispositivos de red	0%	4 días	jue 23/11/17
84	1.7.4.2	Configurar una dirección ip de la nueva vlan a los dispositivos	0%	4 días	jue 23/11/17
85	1.7.4.3	Pruebas de acceso	0%	4 días	jue 23/11/1
86	**1.7.5**	**Realizar las adecuaciones para asignar una red exclusiva para las impresoras**	**0%**	**4 días**	**vie 27/10/17**
87	1.7.5.1	Configurar VLAN para impresoras y asignar puertos	0%	4 días	vie 27/10/17
88	1.7.5.2	Configurar la nueva dirección IP en las impresoras	0%	4 días	vie 27/10/17
89	1.7.5.3	Pruebas de funcionamiento	0%	4 días	vie 27/10/1
90	1.7.6	Finalizacion Etapa IV	0%	0 días	**mié 1/11/1**
91	**1.8**	**Etapa V - Protección de Redes Internas**	**0%**	**19 días**	**jue 14/12/1**
100	**1.9**	**Etapa VI - Webfiltering, Antispam y Procedimientos**	**0%**	**39 días**	**jue 25/1/18**
119	**1.10**	**Etapa VII - RED WiFi, MPLS y Backup Satélital**	**0%**	**13 días**	**mié 21/3/18**
130	**1.11**	**Etapa VIII: Implementar un clúster de firewall para borde y VPN en clúster de alta disponibilidad**	**0%**	**60 días**	**lun 19/3/18**
140	**1.12**	**Cierre**	0%	**21 días**	**lun 11/6/18**
141	1.12.1	Informe final del proyecto	0%	20 días	lun 11/6/18
142	1.12.2	Entrega de ingenieria de detalle completa	0%	20 días	lun 11/6/18
143	1.12.3	Propuesta de soporte y mantenimiento	0%	3 días	lun 11/6/18
144	1.12.4	Lecciones aprendidas y recomendaciones	0%	10 días	lun 11/6/18
145	1.12.5	Reunion de entrega	0%	1 día	lun 9/7/18

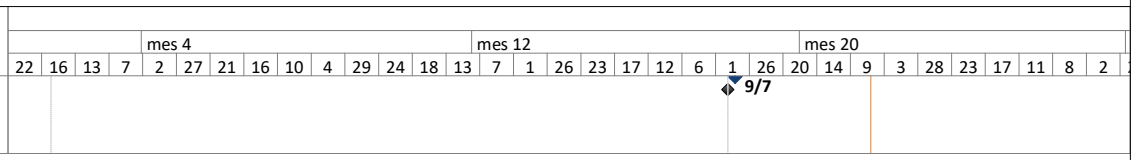


Proyecto: 304-0_ROIRCNP_Evento
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin		
División	Hito externo	Sólo duración	Fecha límite		
Hito	Tarea inactiva	Informe de resumen manual	Progreso		
Resumen	Hito inactivo	Resumen manual			
Resumen del proyecto	Resumen inactivo	Sólo el comienzo			

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Id	EDT	Nombre de tarea	% completa	Duración	Comienzo
146	1.12.6	Finalizacion del proyecto	0%	0 días	lun 9/7/18



Proyecto: 304-0_ROIRCNP_Evento
Fecha: mié 24/10/18

Tarea	Tareas externas	Tarea manual	Sólo fin
División	Hito externo	Sólo duración	Fecha límite
Hito	Tarea inactiva	Informe de resumen manual	Progreso
Resumen	Hito inactivo	Resumen manual	
Resumen del proyecto	Resumen inactivo	Sólo el comienzo	

Compañía Nacional del Petróleo

Reporte de cierre

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Autor: James Vallejo Mejia

RESUMEN DE ESTADO DEL PROYECTO

RESUMEN DE ESTADO DEL PROYECTO	
Porcentaje completado:	**100%**

-2%	+/-2%	+/-5%
OK	GARANTIZARÁ UN COLOR DE ADVERTENCIA AMARILLO	GARANTIZARÁ UN COLOR DE ADVERTENCIA ROJO

Alcance	Tiempo	Costo	Riesgos	Calidad

ENTREGABLES

Entregable	WBS	Estado
Gestion de contratación	1.3	Completado
Servicios DNS externo y DHCP	1.4	Completado
Protección de borde I	1.5	Completado
Protección de borde II	1.6	Completado
Switch LAN	1.7	Completado
Protección de redes internas	1.8	Completado
Filtrado web, anti spam y procedimientos	1.9	Completado
Red WiFi, MPLS y Backup Satelital	1.10	Completado
Implementar un clúster de firewall para borde y VPN en clúster de alta disponibilidad	1.11	Completado

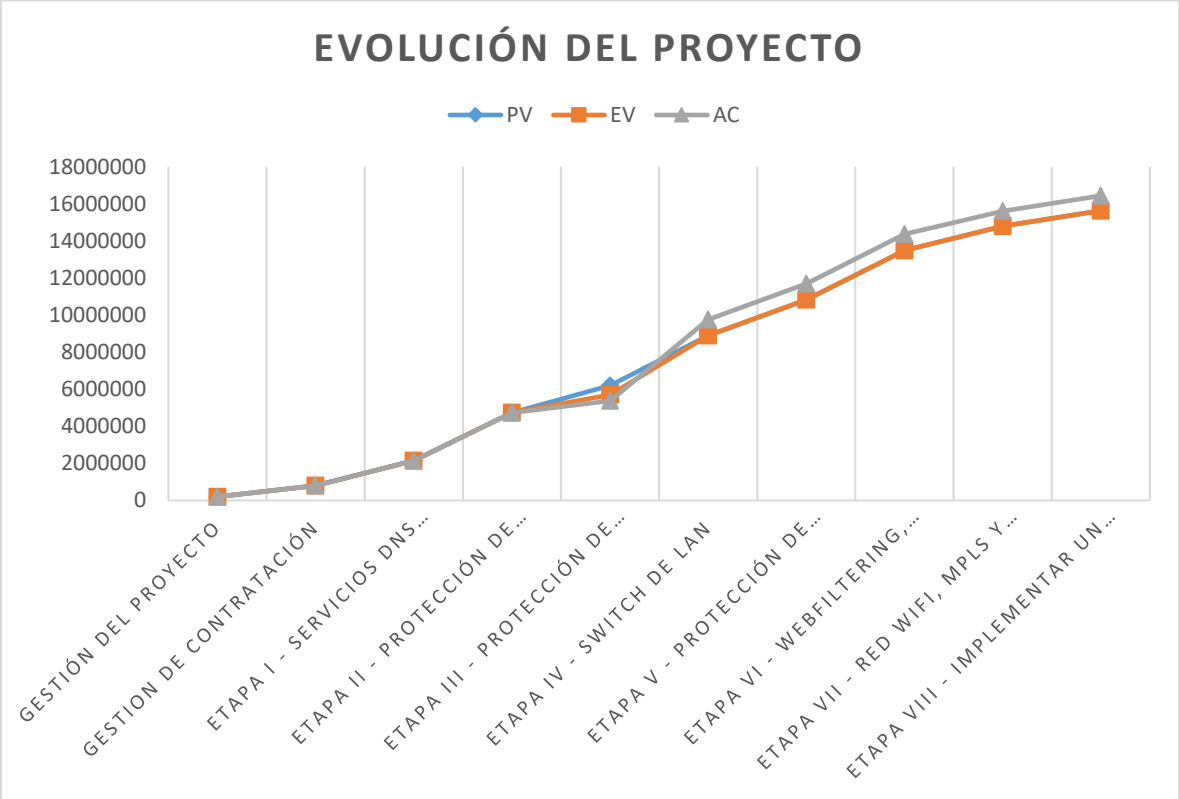
SOLICITUDES DE CAMBIO REALIZADAS

Nombre de solicitud de cambio	Numero de solicitud de cambio	Fecha de la solicitud	Estado actual
Agregar nueva etapa al proyecto: Implementar un clúster de firewall para borde y VPN en clúster de alta disponibilidad, eliminación de entregable de la etapa 2	RFC_PM_001	01/08/2017	Aprobado y aplicado en la línea base
Incluir nueva actividad, tendido de Cableado estructurado	RFC_PM_002	06/10/2017	Aprobado y aplicado en la línea base

Evolución del proyecto EVM

Indicadores

PV	AC	EV
15633902,4761905	16443302,48	15633902,48



Variaciones e Índices de desempeño

Schedule – El proyecto está retrasado/adelantado según el cronograma	
Schedule Variance (SV)	1
Schedule Performance Index (SPI):	1
En este caso, el SPI nos indica que el proyecto termino en el tiempo programado	

Cost - Project Esta sobre/ Bajo Presupuesto	
Cost Variance (CV):	-890400
Cost Performance Index (CPI):	0,95
El proyecto, tuvo un costo mayor al previsto, sin embargo se contaba con las reservas de contingencia y gestión adecuadas, para cubrir el sobre costo	

CSI	0,95
Dentro del margen de aceptación	

.

Compañia Nacional del Petróleo

Cierre

Registro de aceptación

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Autor: James Vallejo Mejia

Registro de cambios

Fecha	Versión	Descripción	Autor	Aprobación
09/7/2017	1	Project charter	PM	

Registro de aceptación

Este documento establece la aceptación formal de todos los entregables para el **Proyecto Remediación y optimización infraestructura de red y seguridad informática.** El **Proyecto Remediación y optimización infraestructura de red y seguridad informática** ha cumplido con todos los criterios de aceptación definidos en el documento de requisitos y la declaración del alcance del proyecto. Se realizó una auditoría de proyecto para verificar que todos los entregables cumplan con los requisitos de calidad y adaptación de mejores prácticas TI. Además, se realizó una evaluación del La infraestructura incluyendo un análisis de vulnerabilidades después de ejecutar el proyecto y se determinó la implementación cumple con los requisitos de calidad y funcionales definidos en este proyecto.

La transición a la operación se ha completado. La administración de la infraestructura se entregó a Operaciones (Equipo de informática CNP) y también se completó la transferencia de conocimientos del Equipo del Proyecto a Operaciones (Equipo de informática CNP). Toda la capacitación ha concluido y los manuales de administración, mantenimiento y plantillas de configuración se han entregado y almacenado en la Carpeta **Proyecto Remediación y optimización infraestructura de red y seguridad informática**

El Project Manager está autorizado para continuar con el cierre formal de este proyecto. El proceso de cierre incluirá una revisión posterior al proyecto, la documentación de las lecciones aprendidas, la liberación del Equipo del Proyecto, el cierre de todas las adquisiciones y el archivo de todos los documentos relevantes del proyecto. Una vez que se complete el proceso de cierre, se notificará al Sponsor del Proyecto y el Gerente del Proyecto se liberará del proyecto.

Aprobado por el Sponsor:

_____ Fecha: _____

Marcelo Cueto
Director de Tecnología CNP

Compañía Nacional del Petróleo

Acta de cierre

Proyecto Remediación y optimización infraestructura de red y seguridad informática

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Autor: James Vallejo Mejia

Fecha	09/07/2017
Proyecto	**Proyecto Remediación y optimización infraestructura de red y seguridad informática**
Dirección Responsable	Tecnologías de la información TI
Líder del Proyecto	James Vallejo Mejia
Patrocinador Ejecutivo	Marcelo Cueto, Director TI

CRONOGRAMA			
Fecha Inicio Programada	*1/4/17*	**Fecha Fin Programada**	*21/2/18*
Fecha Inicio Real	*1/5/17*	**Fecha Fin Real**	*9/7/18*

LECCIONES APRENDIDAS
En próximos proyectos, se pueden programar mayor número de actividades en paralelo, y así disminuir el tiempo de ejecución siempre y cuando se cuente con los recursos y presupuesto.
La comunicación debe ser el pilar para avanzar y cumplir con los objetivos del proyecto, en este proyecto en general se tuvo una comunicación constante con proveedores e interesados, logrando cumplir la meta
Generar un presupuesto más conservador, para así destinar el dinero en otros proyectos, y no retenerlo hasta que finalice, impidiendo adquisiciones importantes

Entregables	Descripción
Servicios DNS externo y DHCP	Configuraciones y recomendaciones para el funcionamiento de este servicio en alta disponibilidad
Protección de borde I	implementaciones y ajustes sobre servicios publicados hacia internet, VPN, DMZ, protección
Protección de borde II	Protección IPS (sistema de prevención de intrusos), DDOS (ataque de denegación de servicio distribuido)
Red LAN	Ajustes, configuración e implementación nueva red LAN
Protección de redes internas	Filtrado de tráfico, ancho de banda y permisos de acceso
Filtrado web, anti spam y procedimientos	Filtrado de contenidos web, implementación de procedimientos para la buena gestión de la oficina informática
Red WiFi, MPLS y Backup Satelital	Implementación red Wifi, revisión de enlaces de respaldo con proveedores

RECOMENDACIONES
Mantener el alcance inicial, e incluir lo necesarios para evitar sobrecostos, o retrasos.

BENEFICIOS ALCANZADOS
Red moderna, con equipamiento de última tecnología, red De datos cableada y Wifi segura, acceso a la red de todos los sites, de manera rápida, protección contra ataques externos, filtrado web, Alta disponibilidad de todos los equipos, administración centralizada de todos los dispositivos, manuales y personal capacitado para administrar, configurar y brindar soporte.

CIERRE DE ADQUISICIONES					
Adquisiciones Programadas	**Cantidad**	**Presupuesto**	**¿Se realizó la adquisición?**	**Monto Devengado**	**¿Se encuentra cerrada la adquisición?**
Firewall Fortigate 200 D + Licencias	2	$ 380760	Si	380760	Cerrada
Firewall Cisco ASA 5545	2	$ 685.368,00	Si	Se adquirió por filial Chile, no hubo pago de equipos de parte del presupuesto del proyecto	Cerrada
Switch Cisco 3850	8	$ 400.000,00	Si	$ 400.000,00	Cerrada
	Presupuesto Total	1466128	**Ejecutado Total**	780760	

Presupuesto (Pesos ARG.)		
Costo Final del proyecto	$ 16443302,48	
Costo planificado del proyecto	$ 15633902,4761905	
Presupuesto con reservas	$ 21.574.785,42	
Valor ganado	$ 15633902,4761905	
Uso de reservas	$ 809400,0038095	
Saldo al Final del proyecto	$ 5.131.482,94	

1. DOCUMENTACIÓN GENERADA EN EL PROYECTO		
Documento	**Ubicación**	
	Física	**Digital**
Documento de configuración: enumeración del ajuste o configuración realizada, mapa conceptual de la configuración resultante, esquema gráfico, detalle de la versión del software, identificación de las actualizaciones incluidas y/o parches que quedaron instalados al momento de la finalización de la labor.	**X**	X
Archivo en formato Microsoft Visio 2010 (o posterior) con el esquema y el detalle de configuración, incluyendo identificaciones de los componentes, identificación lógica, detalle de conexiones, rutas lógicas configuradas, interfaces, puertos utilizados, etc.		X
Documentos con las directrices para el posterior desarrollo del procedimiento de configuración, control, backup y actuaciones operativas necesarias para el correcto mantenimiento y actualización del estándar.		X
Propuesta de soporte por parte del proveedor		x

OBSERVACIONES DEL PROYECTO
Un proyecto Finalizado cumpliendo el alcance, tiempo y gastando menos del presupuesto planificado, un servicio de calidad y una red moderna

FIRMAS				
Nombre	**Cargo o Rol en el Proyecto**	**Elaborado / Revisado / Aprobado**	**Fecha**	**Firma**
James Vallejo Mejia	Project Manager	Elaborado	9/7/2018	
Marcelo Cueto	Director TI	Revisado	9/7/2018	
Marcelo Tocman Ramos	Director General	Aprobado	9/7/018	

cnp
Compañía Nacional del Petróleo

Informe Final hallazgo de vulnerabilidades y desvíos infraestructura de red CNP

Compañía Nacional del Petróleo

CNP CIPETROL Argentina S.A.

Febrero 2017

ST-GT-2016-242

Compañía Nacional del Petróleo

1 Hallazgos

1.1 Dominio: Infraestructura

1.1.1 Servicios DNS Externo

Hallazgo	Descripción	Criticidad
1.1.1.1 Existe un solo server de DNS externo	El servicio de DNS está publicado en internet por lo cual está expuesto a más ataques, es necesario una alta disponibilidad en el servicio.	Alta
1.1.1.2 Servidor de DNS principal expuesto a Internet con todos los ports abiertos, sin sistema de protección de intrusos (IPS) y antivirus (AV)	Un atacante desde internet puede intentar explotar vulnerabilidades de Windows 2003 Server (en este caso) y afectar el funcionamiento del servicio. No solo de este servicio, sino la posibilidad de ejecutar código remoto desde este server y afectar otros servicios de la empresa.	Alta
1.1.1.3 Un solo registro MX, no hay Mail Server secundario	El servicio de correo está publicado en internet por lo cual está expuesto a más ataques, es necesario una alta disponibilidad en el servicio.	Alta
1.1.1.4 Existe registro DNS server, pero no está asociado a un server	Se identificó en registro SOA de “Cnpcipetrol.com.ar” una referencia a un DNS server que no responde.	Media

1.1.2 Servicios DNS Interno

Hallazgo	Descripción	Criticidad

Hallazgo		Descripción	Criticidad
1.1.2.1	En el DHCP interno se apunta a una zona Cnp.cl que está en el server público.	Los clientes pueden realizar consultas a este server y obtener erronamente Ips Públicas cuando deben acceder a Ips privadas	Media

1.1.3 Servicios DHCP

Hallazgo		Descripción	Criticidad
1.1.3.1	No se cuenta con servicios DHCP en HA	El servicio DCHP se brinda desde un solo server	Alta

1.1.4 Dispositivos Móviles

Hallazgo		Descripción	Criticidad
1.1.4.1	No se identifica herramienta para gestión de dispositivos móviles	No se identifica una herramienta para dispositivos móviles corporativos	Media

1.1.5 Sistema de Inventario de Dispositivos

Hallazgo		Descripción	Criticidad
1.1.5.1	Se identifica un sistema de inventario de activos de IT, pero desactualizado y con alcance incompleto.	Se identifica un sistema de inventario de activos de IT, pero desactualizado y con alcance incompleto.	Media


cnp
Compañía Nacional del Petróleo

1.2 Dominio: Seguridad

1.2.1 Protección de Borde

Hallazgo	Descripción	Criticidad

Compañía Nacional del Petróleo

Hallazgo	Descripción	Criticidad
1.2.1.1 Firewall de borde y VPN sin HA	El firewall de borde no está en alta disponibilidad	Alta
1.2.1.2 No se cuenta con balanceo de Tráfico Saliente a Internet	No se identifica un adecuado uso de los enlaces a Internet a nivel de balanceo de ancho de banda	Media
1.2.1.3 FW Fortigate 200B EoS	Equipo EoS y End of Support 01-Apr-2020	Media
1.2.1.4 FW Fortigate 110C EoS	Equipo EoS y End of Support 20-Aug-2018	Media
1.2.1.5 ACLs entrantes	Existen ACLs a servicios con NAT a nivel IP y a servidores no en DMZ	Alta
1.2.1.6 Servicio Microsoft TNG esta discontinuado desde el 31/12/2015	Este servicio esta discontinuado por Microsoft	Alta
1.2.1.7 Servicio TNG no está en HA	Este servicio no está en HA	Alta
1.2.1.8 Se identifican publicaciones de servicios a Internet en cadena desde el FW Fortigate 200B y el TNG	Se identifican publicaciones de servicios a servidores internos encadenados desde el Fortifate y el TNG. Esto implica doble punto de falla.	Alta
1.2.1.9 Red DMZ para publicaciones externas	No existe una red con características de red DMZ para publicas servicios en internet de forma segura.	Alta
1.2.1.10 Falta Monitoreo de Servicios	No se identifica un monitoreo de los Fws	Media
1.2.1.11 Auditoria de cambios, accesos y backups periódicos	Es recomendable realizar backups periódicos de la configuración del firewall, para que, ante cualquier error humano en la configuración del mismo, se pueda regresar a una versión anterior de la configuración. También para el caso de tener que reemplazar el equipo por presentar alguna falta, tener la configuración más actualizada disponible.	Media

Hallazgo	Descripción	Criticidad
1.2.1.12 Servicios publicados en internet sin sistema de protección de intrusos (IPS), ni antivirus (AV) habilitados en el firewall.	Un atacante mal intencionado puede afectar servicios que estén publicados en los servidores ya que no cuentan con protección de IPS, ni antivirus habilitados en el firewall.	Alta
1.2.1.13 Almacenamiento de historial de Logs	Para poder realizar troubleshooting de problemas es necesario un historial de logs del firewall.	Media
1.2.1.14 Análisis de Vulnerabilidades Externo, no se identifica procedimiento de ejecución periódico.	No se identifica un procedimiento periódico de ejecución de Análisis de Vulnerabilidades Externo	Media

1.2.2 Protección de redes interna

Hallazgo	Descripción	Criticidad

Hallazgo	Descripción	Criticidad
1.2.2.1 El tráfico entre redes interna no pasa a través del firewall, por lo cual no se pueden aplicar políticas de seguridad sobre la mismas.	Es recomendable permitir, prohibir o permitir solo algunos servicios entre las distintas redes de la empresa, tanto del sitio central, como de los sitios remotos.	Alta
1.2.2.2 El tráfico entre redes LAN-LAN y LAN-WAN no tiene aplicado IPS, AV o restricciones de ancho de banda.	Al tráfico entre distintas redes es recomendable aplicarle sistema de protección de intrusos, antivirus, o restricción o reserva de ancho de banda para determinados servicios a nivel de firewall de red.	Alta
1.2.2.3 No se cuenta con Protección de acceso a servidores y equipos de infraestructura/networking.	El acceso a tareas de administración de servidores, equipos de infraestructura y networking no está protegido por un FW	Alta

1.2.3 WebFilter

Hallazgo	Descripción	Criticidad

Hallazgo	Descripción	Criticidad
1.2.3.1 Servicio de WebFiltering no está en HA	Este servicio no está en HA. La indisponibilidad afecta la navegación de usuarios	Alta
1.2.3.2 No se identifican procedimiento de backup de configuración	Es recomendable permitir, prohibir o permitir solo algunos servicios entre las distintas redes de la empresa, tanto del sitio central, como de los sitios remotos.	Media
1.2.3.3 No hay procedimientos de reportes, desvíos, consumos	No se identifican procedimientos de reportes, desvíos, consumos	Media
1.2.3.4 No se identifican políticas aplicadas por grupos de usuarios	No se identifican políticas por grupos de usuarios y sincronizadas con Active Directory	Media

1.2.4 Antivirus

Hallazgo	Descripción	Criticidad
1.2.4.1 La consola de AV no está en HA	La consola de AV no está en HA	Media
1.2.4.2 No se identifican procedimientos de backup de configuración ni control de cambios	No se identifican procedimientos de backup de configuración ni control de cambios	Media
1.2.4.3 No hay procedimientos de reportes, desvíos, consumos	No se identifican procedimientos de reportes, desvíos, consumos	Media

1.2.5 Antispam

Hallazgo	Descripción	Criticidad

Hallazgo	Descripción	Criticidad
1.2.5.1 La consola de Antispam no está en HA	La consola de Antispam no está en HA. La indisponibilidad afecta el servicio de mails entrante y saliente.	Alta
1.2.5.2 No se identifican procedimientos de backup de configuración ni control de cambios	No se identifican procedimientos de backup de configuración ni control de cambios	Media
1.2.5.3 No hay procedimientos de reportes, desvíos, consumos	No se identifican procedimientos de reportes, desvíos, consumos	Media

1.2.6 NAC

Hallazgo	Descripción	Criticidad
1.2.6.1 No se identifica un servicio de NAC	No se identifica la implementación de servicio de NAC (Network Access Control). Esto permite el acceso irrestricto a la red de equipos no corporativos por cable o WiFi	Alta

1.2.7 Procedimientos de Seguridad

Hallazgo	Descripción	Criticidad
1.2.7.1 ABM cuentas de administrador		Alta
1.2.7.2 Gestión de credenciales de administrador		Alta
1.2.7.3 ABM de usuarios		Media

Compañía Nacional del Petróleo

1.2.8 Seguridad de acceso física

Hallazgo	Descripción	Criticidad
1.2.8.1 Los equipos de acceso biométrico no tienen password de administración	Equipos biométricos de BA 192.168.1.193 y .194 sin password de administración y accesibles desde cualquier red de la empresa, cualquier usuario puede habilitar, bloquear tarjetas de acceso.	Alta

1.3 Dominio: Monitoreo, Auditoría / Correlación de Logs

1.3.1 Monitoreo

Hallazgo	Descripción	Criticidad
1.3.1.1 No se cuenta con herramientas de monitoreo a nivel de detalle de servidores	No se cuenta con una herramienta de monitoreo a nivel de detalle de parámetros de salud por servidor (Memoria, cpu, uso de disco, etc)	Alta
1.3.1.2 No se cuenta con herramientas de monitoreo a nivel de servicios/ Aplicaciones	No se cuenta con una herramienta de monitoreo a nivel de servicios/aplicaciones parámetros de consumo, utilización	Alta
1.3.1.3 No se cuenta con herramientas de monitoreo a nivel de detalle de dispositivos de comunicaciones (Dispositivo / Interface)	No se cuenta con una herramienta a nivel de detalle de parámetros de salud por dispositivo, ni parámetros de consumo, utilización	Alta
1.3.1.4 No se cuenta con herramienta de monitoreo a nivel de utilización / disponibilidad de vínculos/enlaces. (MPLS, Internet, Satélite, radioenlaces)	No se cuenta con una herramienta de monitoreo para enlaces a nivel de disponibilidad, consumo	Alta

1.3.2 Auditoría / Correlación de logs

Hallazgo	Descripción	Criticidad

Compañía Nacional del Petróleo

Hallazgo	Descripción	Criticidad
1.3.2.1 No se cuenta con sistema de auditoría de acceso, modificaciones en servidores, equipos de infraestructura, networking	No se identifica un sistema centralizado de almacenamiento de logs	Alta
1.3.2.2 No se cuenta con sistema de correlación de logs / reporting de auditoría	No se cuenta con un sistema de correlación de logs de seguridad/auditoría. Ni reportes por tecnologías, tipos de dispositivos o usuarios/grupos	Alta
1.3.2.3 No se cuenta con procedimiento de reportes de consumo / accesos de usuarios.	No se cuenta con reportes de consumos por servicios, aplicaciones, enlaces o usuarios/grupos.	Alta

1.4 Dominio: Telecomunicaciones / Networking

1.4.1 Switch de red LAN

Hallazgo	Descripción	Criticidad

Compañía Nacional del Petróleo

Hallazgo	Descripción	Criticidad
1.4.1.1 No hay segmentación de vlans de para separar y controlar el tráfico entre servidores, servicios y usuarios	No se identifica una adecuada separación de tráfico entre usuarios y servidores	Alta
1.4.1.2 Si bien se cuenta con equipos Layer3, no se están aplicando Vlans ni ruteo interno	No se utilizan los equipos a nivel L3	Alta
1.4.1.3 Se cuenta con Switches L3 en stack, los switches en cascada están conectados solo a un port ethernet.	Se cuenta con Switches L3 en stack, los switches en cascada están conectados solo a un port ethernet. No están en etherchannel distribuido.	Alta
1.4.1.4 Acceso telnet habilitado, passwords no encriptadas en la configuración, acceso directo al "enable" en algunos casos.	Telnet, protocolo obsoleto, no cifrado, se pueden obtener las credenciales de acceso sniffeando el tráfico de red.	Alta
1.4.1.5 Acceso a los equipos habilitado desde todas las redes, red de usuarios compartida con red de gestión de los equipos, IP de administración en la VLan 1 Nativa.	Debe existir una vlan exclusiva de gestión de equipos de IT que, por buenas prácticas no sea a vlan 1, nativa, y solo puedan acceder a los dispositivos los administradores de red.	Alta
1.4.1.6 Falta Auditoria de cambios, accesos y backups periódicos	No se identifican procedimientos de auditoría, control de cambios, ni backups de configuraciones.	Media
1.4.1.7 Falta Monitoreo de disponibilidad y desempeño	No se identifica monitoreo adecuado de disponibilidad y desempeño a nivel de equipo y ports	Media
1.4.1.8 Falta Almacenamiento de historial de logs	No se identifica un almacenamiento y correlación de logs.	Media

Hallazgo	Descripción	Criticidad
1.4.1.9 Consultas SNMP de lectura configuradas como “public”	Las consultas por SNMP no tienen autenticación.	Media
1.4.1.10 Deficiente Orden de patcheras, identificación de cables	Se identifica un defiende orden e identificación de patch cords en las patcheras	Media
1.4.1.11 Password de acceso débiles	Deben contener mayúsculas, minúsculas, caracteres especiales y mínimo 8 caracteres de longitud.	Media
1.4.1.12 Deficiente documentación de arquitectura de conexiones	Se identifica una deficiente documentación de información de topología, configuraciones, credenciales de administración	Media

1.4.2 Red WiFi

Hallazgo	Descripción	Criticidad

Hallazgo		Descripción	Criticidad
1.4.2.1	La controladora WiFi no está en HA	La controladora de servicio WiFi no está en HA	Alta
1.4.2.2	Seguridad WiFi con cifrado WEP vulnerable y obsoleto.	Cifrado WEP obsoleto se puede obtener la clave wifi en pocos minutos y así tener acceso a toda la red.	Alta
1.4.2.3	La red WiFi no está segmentada en red corporativa y red de invitados	Debería existir una red WiFi exclusiva para uso corporativo, y otra red WiFi exclusiva para uso de "invitados" y dispositivos como tablets y celulares.	Alta
1.4.2.4	Desde la red WiFi se puede tener acceso a toda la infraestructura IT (firewalls, switch, servidores, videoconferencia, etc.)	No es recomendable tener acceso desde una red WiFi a toda la infraestructura de IT de la empresa, solo una red definida para el sector de sistemas debería acceder a switch, routers, servidores, etc.	Alta
1.4.2.5	Auditoria de cambios, accesos y backups periódicos	No se identifica procedimientos para auditar configuración (control de cambios) ni backups de configuración periódicos	Media
1.4.2.6	Falta de Monitoreo de disponibilidad y desempeño	No se identifica Monitoreo de la disponibilidad de los distintos Access point. Tampoco análisis de logs. Seguridad a nivel de accesos no autorizados.	Media
1.4.2.7	Falta Almacenamiento de historial de logs	No se identifica una herramienta de almacenamiento y correlación de logs	Media
1.4.2.8	No hay control de accesos por dispositivos	Prohibir la conexión de celulares en el WiFi corporativo (especialmente los que tienen Android rooteado), solo deben acceder desde el WiFi de invitados.	Media
1.4.2.9	Red Wifi corporativa con restricciones y habilitaciones a repasar	Se pueden bajar de internet torrents saliendo por el proxy. Si se desactiva el proxy funciona el Skype, si se tiene proxy no funciona. Desactivando el proxy, en algunas oportunidades funciona el acceso a internet.	Media

1.4.3 Enlaces MPLS / Backup Satelite

Hallazgo	Descripción	Criticidad

Hallazgo	Descripción	Criticidad
1.4.3.1 No se identifica claramente procedimiento de activación/Rollback de backup enlaces MPLS satelital		Alta
1.4.3.2 No se cuenta con notificación de activación / rollback de uso de enlaces MPLS satelital		Alta
1.4.3.3 No se identifica claramente que tipo de tráfico está habilitado en los enlaces MPLS satelital		Media
1.4.3.4 No se identifican ACLs no shappers para controlar tráfico indebido en enlaces MPLS		Alta
1.4.3.5 No se identifica las políticas de clasificación/marcado de paquetes QoS en los enlaces MPLS (no está documentado)		Alta
1.4.3.6 No se identifica monitoreo granular por colas QoS de los enlaces MPLS		Media
1.4.3.7 No se identifica monitoreo granular por servicio en los enlaces MPLS		Media

1.4.4 Video Conferencia/Telefonía IP

Hallazgo	Descripción	Criticidad

Hallazgo	Descripción	Criticidad
1.4.4.1 No se identifican procedimientos de backup de configuración.	No se identifican procedimientos de backup de configuración ni control de cambios	Media
1.4.4.2 La PBX IP no está en HA	La PBX no está en alta disponibilidad	Alta
1.4.4.3 Equipos sin password de acceso	Desde un browser se podían observar las cámaras de los equipos de videoconferencia situados en las oficinas de los gerentes. (ya solucionado)	Alta
1.4.4.4 Se puede tener acceso a los equipos desde cualquier red, inclusive las redes de los sitios remotos y la red WiFi.	Los equipos deben estar en una vlan exclusiva de video conferencia.	Media
1.4.4.5 Monitoreo de disponibilidad y desempeño	No se identifican procedimientos para monitoreo de disponibilidad, desempeño	Media

1.4.5 Impresoras / Plotters

Hallazgo	Descripción	Criticidad

Hallazgo	Descripción	Criticidad
1.4.5.1 Acceso a administración de los equipos sin password.	Cualquier usuario puede, por ejemplo, cambiar la dirección ip de una impresora y por ende, dejar sin servicio a la misma, o bien duplicar una ip y afectar el servicio de red.	Alta
1.4.5.2 Las impresoras están en la misma red que los usuarios y que los equipos de la infraestructura IT.	Las impresoras deben estar en una vlan separada, de acuerdo con las buenas practicas.	Alta
1.4.5.3 Impresoras con conexión Wifi tienen cifrado WEP	El cifrado WEP es vulnerable, se recomienda cifrado WPA2.	Media

1.4.6 Antenas Canopy de Plataformas BRM

Hallazgo	Descripción	Criticidad
1.4.6.1 Equipos sin password de acceso y se puede acceder desde cualquier red.	Cualquier usuario desde un browser puede cambiar la configuración de una antena (ejemplos: http://172.18.3.175/ y .181) y dejar sin servicio de red una plataforma. Inclusive el concentrador de antenas (http://192.168.3.173) está sin password de administración por lo que puede ser afectado todo el servicio de red de las plataformas. Es importante tener en cuenta que desde cualquier red hay visibilidad con las antenas.	Alta
1.4.6.2 Las antenas locales y remotas de todas las plataformas comparten la misma red.	Un problema en ese segmento de la red y se afecta el servicio de todas las plataformas, se recomienda una vlan diferente por plataforma.	Alta
1.4.6.3 Monitoreo de disponibilidad y desempeño	La disponibilidad y el rendimiento de las antenas no está monitoreado.	Media

1.5 Dominio: Tecnologías Microsoft

1.5.1 Controladores de Domínio (Active Directory)

Hallazgo	Descripción	Criticidad

Compañía Nacional del Petróleo

Hallazgo	Descripción	Criticidad
1.5.1.1 Existen 30 cuentas dentro del grupo Domain Admins	Cualquier usuario que pertenezca al grupo “Domain Admins” tiene control total sobre todos los objetos del Directorio para dicho dominio.	Alta
1.5.1.2 Actualizaciones críticas de seguridad no implementadas	Una actualización crítica de seguridad que no se implementa representa una vulnerabilidad mediante la cual se podría afectar al sistema.	Alta
1.5.1.3 Gestión de cuentas de usuarios	Existen usuarios que no han actualizado sus contraseñas de acuerdo a las políticas vigentes. Se observa un porcentaje de usuarios para los cuales sus contraseñas no caducan.	Alta
1.5.1.4 Gestión de cuentas de máquinas.	Existe un porcentaje de equipos que no se contacta con los controladores de dominio para renovar credenciales, objetos deshabilitados y cuentas en el contenedor por defecto que no aplican directivas de grupo.	Media
1.5.1.5 Nivel Funcional del Bosque	El bosque se encuentra en nivel Funcional Windows 2003, esto impide el aprovechamiento de las nuevas mejoras implementadas tanto en 2008 como en 2012	Media
1.5.1.6 Dominio sin redundancia	Existe dentro del bosque un dominio PETROFARO.AR con un solo controlador de dominio. Ante una falla del equipo PETROARBUE03.petrofaro.ar deja sin servicio a sus usuarios	Alta
1.5.1.7 Sitios sin redundancia	Existen 3 sitios de AD (Río Gallegos, PCA, BRM) para los cuales hay 1 solo controlador de dominio. En caso de falla de algunos de los controladores de dominio (SIPARRGL11.cipetrol.ar, siparpca11.cipetrol.ar, siparbrm11.cipetrol.ar) el rendimiento de ese sitio se vería afectado.	Media
1.5.1.8 DHCP sin redundancia	Si bien existen 5 Servidores configurados como DHCP, ninguno de los rangos configurados posee alta disponibilidad. Tampoco en el sitio Buenos Aires a pesar de	Alta

Hallazgo	Descripción	Criticidad
	contar con 2 Controladores de Dominio para CIPETROL.AR. Una falla en el servicio de DHCP puede afectar a todos los clientes de ese segmento.	
1.5.1.9 Existen OUs sin protección contra borrado accidental	Se observan que no todas las OUs se encuentran protegidas contra borrado accidental, esto implica que un simple error puede eliminar a todas las cuentas dentro de un contenedor específico.	Alta

1.5.2 Microsoft Exchange Server (Servidores de correo)

Hallazgo	Descripción	Criticidad

Hallazgo	Descripción	Criticidad
1.5.2.1 No existe redundancia en la solución de correo	Existen 3 servidores de correo (SIPARBUE30.cipetrol.ar, SIPARBRM30.cipetrol.ar, SIPARPCA30.cipetrol.ar) uno para cada sitio, cada uno con su base de datos y usuarios. No existe configuración que brinde redundancia a la base de datos, entrada y/o salida de correos hacia internet.	Alta
1.5.2.2 Actualizaciones críticas de seguridad no implementadas	Una actualización crítica de seguridad que no se implementa representa una vulnerabilidad mediante la cual se podría afectar al sistema.	Alta
1.5.2.3 No existen registros SPF/DMARC	No existen publicaciones de registros TXT para SPF/DMARC que faciliten la entrega de correos en otras organizaciones. Este tipo de registro ayuda a identificar el origen y prevenir que correos no autorizados utilicen el dominio de la empresa.	Media
1.5.2.4 Configuración del banner SMTP	En una sesión de SMTP el servidor se identifica con un nombre diferente al publicado (imsva.Cnpcipetrol.com.ar). Esto podría afectar la reputación del dominio Cnpcipetrol.com.ar	Media
1.5.2.5 Rendimiento de Servidores de correo	Se han observado que existen problemas de rendimiento (escasa memoria RAM disponible, escaso espacio libre en disco, etc.)	Media
1.5.2.6 Tamaño de las bases y tareas de mantenimiento	Se ha observado que una base cuenta con más de cien GB y no hay suficiente espacio libre para realizar las tareas de mantenimiento. Posiblemente nunca se hallan realizado mantenimiento de las bases (defrag off-line) y puedan existir corrupciones lógicas.	Alta
1.5.2.7 Higiene de mensajes	Las tareas de higiene de correo se realizan en el mismo equipo que posee las bases y al cual se conectan los usuarios, es decir que un mensaje malicioso llega directamente al servidor de correo destino sin pasar por una instancia previa para su control y detección.	Media
1.5.2.8 Resguardo de bases de mensajería	Se ha observado que el Servidor de correo de Buenos Aires ha estado sin resguardo durante más de 15 días. Esto hace que los archivos de tipo logs no se borren y ante	Alta

Hallazgo	Descripción	Criticidad
	alguna falla de disco podría perderse información.	

1.5.3 Microsoft Lync (Servidores de Mensajería instantánea)

Hallazgo	Descripción	Criticidad
1.5.3.1 Configuración de HW Componente Edge	El EDGE server no sigue la recomendación mínima de HW, tanto en memoria como en procesadores.	Media
1.5.3.2 Configuración de HW Componente Front End	El Front End server no sigue la recomendación mínima de HW.	Media
1.5.3.3 Eventos de errores de replicación en Front End server	Los eventos de errores de los servidores deberán ser analizados, investigados y remediados. Un evento de error en un equipo podría representar una disrupción en el servicio si no es resuelto.	Media
1.5.3.4 El site de Lync no tiene asignada una cuenta de servicio Kerberos	Se debe crear una cuenta de AD y asignarla para la autenticación Kerberos de los servicios de Lync.	Media
1.5.3.5 Base de datos de Lync sin último service pack	El servidor SQL donde se encuentra la base de datos de configuración del Lync no tiene el ultimo Service Pack instalado.	Media
1.5.3.6 Servidores Lync con actualizaciones de seguridad y 2 rollup pendientes de instalación.	Se recomiendo actualizar la base de datos y el Lync con la última versión de Rollup o Service Pack. Así como también las actualizaciones de seguridad.	Media

1.5.4 Microsoft SQL (Servidores de Bases de datos)

Hallazgo	Descripción	Criticidad

Compañía Nacional del Petróleo

Hallazgo	Descripción	Criticidad
1.5.4.1 Servidores SQLExpress instalados	Se observan que existen servidores con versiones Express, las cuales al ser gratuitas tienen reducidas capacidades y funcionalidades. En case que la aplicación sea critica o maneje un volumen importante de datos debería evitarse utilizar este tipo de versiones	Media
1.5.4.2 Versiones fuera del ciclo de vida del soporte	Se han observado instancias de SQL 2000 que ya no se encuentra soportado por el fabricante. En caso de aplicaciones de negocio debería utilizarse versiones soportadas.	Alto
1.5.4.3 Configuraciones de utilización de memoria del Servidor	Se ha observado que en algunos casos se ha especificado el tamaño máximo a utilizar por el motor de base de datos. No obstante, también hay casos en los que esto no se encuentra configurado y representa un riesgo dado que el motor podría hacer un uso excesivo de la memoria en perjuicio del Sistema Operativo que ejecuta el Servidor.	Media
1.5.4.4 Ubicación de bases y logs en el mismo disco/misma partición.	Este tipo de configuraciones atenta con el rendimiento y las posibilidades de recuperación de la base en caso de fallas de disco, es decir que podrían perderse días de transacciones desde el ultimo resguardo en caso de fallas. En el caso de aplicaciones del negocio esto debería resolverse rápidamente.	Media
1.5.4.5 Actualizaciones criticas de seguridad no instaladas	Existen servidores SQL donde se encuentra pendiente la instalación de parches críticos de seguridad. Esto representa un riesgo/vulnerabilidad dado que el equipo podría ser afectado ante un ataque.	Alto
1.5.4.6 Service Pack para SQL no instalados.	El fabricante distribuye correcciones a problemas/falencias que se descubren en el producto. No tener instalada este tipo de actualizaciones hace que el equipo tengo un grado mayor de vulnerabilidad ante fallas y/o ataques.	Alto
1.5.4.7 Se encontraron 28 instancias de SQL	Se infiere que es un numero alto de motores de bases de datos en relación a la cantidad de usuarios y equipos que se encuentran en la empresa. Esta cantidad agrega complejidad en la administración y mantenimiento. Cuatro de esas instancias corren en equipos que son	Alto

Hallazgo	Descripción	Criticidad
	estaciones de trabajo (Windows 7 / Windows 10)	
1.5.4.8 Gestión de monitoreo y alertas	Al no haber en la empresa una solución de motor de base de datos del tipo Clúster con Alta disponibilidad se infiere que las aplicaciones no son críticas para el negocio. No se cuenta con evidencia para constatar una correcta gestión de las alertas y del monitoreo de la salud de los servidores.	Media
1.5.4.9 Tareas de mantenimiento	No se cuenta con evidencia para constatar una correcta gestión de las tareas de mantenimiento y gestión de la salud de los bases existentes.	Media
1.5.4.10 Hardware fuera del ciclo de vida	Existen Servidores de SQL que se encuentran en un Hardware fuera de su ciclo de vida de soporte. Esto representa un riesgo en caso de falla de poder conseguir el reemplazo de la parte (siparbue01.cipetrol.ar es un ProLiant ML350 G3 con Microsoft SQL Server 2000). También se ha observado que un Servidor corre en un Hardware de estación de trabajo (HP Compaq Pro 6300 SFF), lo cual representa un riesgo dado que no posee las características adecuadas para cubrir la función que está brindando	Alto

1.6 Dominio: Infraestructura Virtual

1.6.1 VMware Vsphere

Hallazgo	Descripción	Criticidad

Compañía Nacional del Petróleo

Hallazgo	Descripción	Criticidad
1.6.1.1 Sistemas operativos fuera de Soporte para Vcenters	Todos los Vcenters de la empresa son Windows 2008 Standard R2 sistema operativo ya no soportado por vmware ante algún caso de soporte ni tampoco soportado por microsoft	Media
1.6.1.2 Servers agregados por IP	Todos los servers de ESXI están agregados por ip en lugar de FQDN como lo marcan las mejoras prácticas de vmware. Tanto para el correcto funcionamiento de HA como de DRS vmware recomienda manejarse siempre por FQDN.	Media
1.6.1.3 Servers con un solo path de SAN (192.168.1.180 / 192.168.1.181)	La mayoría de los servers de ESXI cuentan con 2 paths y en algunos casos como en los casos de los servers 192.168.1.180 / 192.168.1.181 cuentan con 1 solo path de SAN esto significa que antes la caída de una placa de FC o la caída de algunos de los paths estos hosts se quedan sin redundancia dejando las máquinas virtuales sin funcionamiento alguno.	Alta
1.6.1.4 No hay VLANS implementas en ningún host ESXI en ninguno de los vcenter	No se encontraron configuradas VLANS de ningún tipo para poder separar el tráfico de management, el tráfico de VMOTION y el tráfico de máquinas virtuales como marcan las mejoras prácticas de VMware.	Alta
1.6.1.5 Todos los esxi y vcenters tienen versiones Completamente distintas dentro de los Clusters y Vcenters.	Se relevaron en todos los Vcenters de la empresa versiones de ESXI diferentes y en algunos casos dentro del mismo clúster versiones diferentes de ESXI. Se recomiendan siempre según las mejores prácticas de vmware mantener la misma versión de ESXI en todos los clusters acordes con la matriz de vmware para cada vcenter.	Alta
1.6.1.6 Ausencia de servidor secundario de NTP	En varios hosts se detectó 1 solo server de NTP dejando sin redundancia de este servicio a varios hosts.	Media
1.6.1.7 Ausencia de servidor de archiving de logs	Se detectó la ausencia de un repositorio y servidor de logs configurados para todos los servers de ESXI y los Vcenters. Ante un inconveniente en la infraestructura virtual no se podrá analizar el incidente por falta de logs. Se recomienda configurar un server de logs y	Media

Hallazgo	Descripción	Criticidad
	un archiving de logs por host	
1.6.1.8 Ausencia de paths de iscsi	En algunos hosts se detectó la falta de HA en paths para iscsi	Alta
1.6.1.9 Todos los hosts se encuentran sin Red de Vmotion	Ninguno de los servidores de la empresa tiene configurada red de VMOTION, ante la caída de un host las máquinas virtuales se quedarán apagadas sin pasar a otro host	Alta

Hallazgo	Descripción	Criticidad

Compañía Nacional del Petróleo

Hallazgo	Descripción	Criticidad
1.6.1.10 Clusters sin HA y DRS	Se detectaron clusters sin configuración de HA y DRS por lo tanto ante la caída de una host de ESXI las máquinas virtuales se apagarán con el host sin pasar a otro host en el clúster y además al no contar con DRS configurado no hay balanceo de carga entre los hosts del clúster	Alta
1.6.1.11 Ausencia de servidor de patching de hosts y máquinas virtuales	No se detectó ningún servidor de patching de hosts y máquinas virtuales. Se recomienda la implementación de update manager para patching de hosts, vcenters y máquinas virtuales	Media
1.6.1.12 Versiones de VMtools desactualizadas en todos los hosts y máquinas virtuales	Se detectaron versiones de VMtools desactualizadas en todos los hosts como además distintas versiones de VMtools en todos los clusters.	Media
1.6.1.13 Servidores virtuales con placa de red virtuales E1000 o PCNet23 completamente fuera de standardes virtuales	Se relevaron en el ambiente virtual placas de red virtual E1000 y PCNet23, placas de red virtual que bajan la performance de los servidores virtuales provocando lentitud en la red y en los sistemas de la empresa.	Media
1.6.1.14 Alertas y alarmas sin configuración	No se detectaron alarmas y alertas configuradas para el ambiente virtual y en algunos casos se modificaron alarmas de espacio en disco en DATASTORES para que los Vcenters no disparen alarmas de espacio en disco. Se detectó un DATASTORES con el 3% libre esto hace imposible él HA de máquinas virtuales y el vmotion de las mismas.	Alta
1.6.1.15 Vcenters sin HA de DATASTORES	Se detectaron Vcenters sin espacio en disco dificultando la migración de máquinas virtuales ante un evento en los datastores y dejan sin HA de DATASTORES al vcenter	Alta
1.6.1.16 Falta de bocas de SAN en switchs de fibra para multipathing.	Se relevó la falta de ports de SAN en la red y por esta ausencia se configuro en varios casos ports por iscsi dando más lentitud a la red de máquinas virtuales.	Alta


cnp
Compañía Nacional del Petróleo

1.7 Dominio: Tecnología de Almacenamiento Netapp y Switches de Fibra Óptica Brocade 300

1.7.1 Equipos de almacenamiento Masivo Netapp

Hallazgo	Descripción	Criticidad

Hallazgo	Descripción	Criticidad
1.7.1.1 Contrato de Mantenimiento	Ningún equipo NetApp, salvo SIPARBUE17, tiene contrato de mantenimiento activo con el fabricante (NetApp) pero si lo tienen con el canal. Los contratos con el canal son de 3 años mientras que con el fabricante son de 1 año.	Alto
1.7.1.2 Versión de código de Sistema Operativo	Los equipos relevados están en versiones de código dispares lo que hace difícil una administración homogénea. El hardware aun esta soportado por lo que es posible actualizarlos.	Alto
1.7.1.3 Licencias	Hay equipos licenciados con funciones que no se están usando. No está claro si se licencio de más o no se han usado estas funciones (como backup a disco, restauración desde disco y demás) o no se las utilizo por desconocimiento de las mismas.	Media
1.7.1.4 Puertos de fibra onboard Netapp	Los equipos Netapp están en licenciados para usar puertos de fibra canal, pero la mayoría no se utiliza lo que implica una muy alta latencia en el tiempo de respuesta a pedidos de lectura y escritura.	Alto
1.7.1.5 Red de producción y mantenimiento	La red de producción de carpetas compartidas (shares CIFS), así como la red ISCSI y la red de administración de los equipos locales y remotos es la misma. Por lo tanto, cualquier persona puede acceder potencialmente a los equipos y apagarlos o cambiar su configuración.	Alto
1.7.1.6 Volúmenes de producción y volúmenes de sistema operativo	Los volúmenes de producción de los equipos Netapp están creados en el mismo contenedor lógico (aggregate) que tiene el volumen de sistema operativo de Netapp. Si algún volumen se llena o se corrompe, también afectará el sistema operativo y el equipo entero estará inutilizable. Esto es común a todos los equipos.	Alto
1.7.1.7 Volumen raíz del sistema operativo exportado a	Los volúmenes de raíz del sistema operativo de todos los equipos Netapp (\vol0\C$) así	Alto

Hallazgo	Descripción	Criticidad
la red de producción.	como los directorios de usuarios (\home$) y de archivos de configuración (\etc$) están exportados a la intranet de la empresa y por ende montables y modificables por cualquier usuario. Esto conlleva una grave falla de seguridad ya que cualquier persona podría potencialmente desconfigurar los equipos.	
1.7.1.8 Tasa de transferencia ISCSI-Fibra Óptica	Nodos VMWARE y de geología están accediendo a sus datos por medio de la red ISCSI o por carpetas compartidas en la red de cobre convencional de 1Gb/s (en una red compartida en común con ISCSI e intranet de la empresa) mientras que los Equipos NetApp están licenciados para usar sus puertos de fibra a 4Gb/s pero no se utilizan por falta de puertos libres y acceso a los switches de fibra Óptica Brocade.	Media
1.7.1.9 Tasa de utilización de espacio	Se observa variedad de equipos con baja capacidad de disco y altamente utilizados (caso SIPARBUE06, SIPARBUE08 y SIPARBRM24) mientras que otros tienen espacio en disco disponible para alocar más espacio y proveer más servicio por red de fibra a más velocidad (caso SIPARBUE23-24)	Media
1.7.1.10 Equipos alertados	Los equipos SIPARBUE75 y SIPARBUE08 están alertados. El primero tiene perdida de visibilidad de discos (seguramente un error de hardware) y el segundo tiene luz ámbar por problemas en su puerto de fibra a pesar de no estar sirviendo discos por fibra óptica.	Alto
1.7.1.11 Equipos con alta latencia por capacidad mal distribuida	El Equipo SIPARBUE23 Tiene una latencia de 0,7 segundos, el equipo SIPARBUE24 de 0,5 segundos y el SIPARBUE08 de 11 segundos (para solo un pedido de lectura/escritura), todo por exportar datos productivos por red de cobre y no balancear carga entre equipos y fibra óptica.	Media

1.7.2 Switches de fibra Óptica Brocade 300 y red de fibra Óptica

Hallazgo	Descripción	Criticidad

Compañía Nacional del Petróleo

Hallazgo	Descripción	Criticidad
1.7.2.1 Contrato de Mantenimiento	No hay datos del contrato de mantenimiento del fabricante (Brocade) aunque el canal aún tiene soporte sobre los equipos.	Alto
1.7.2.2 Credenciales de acceso	Los accesos a los switches no son válidos por lo que es imposible saber si los puertos tienen errores de transporte, como están configuradas las zonas	Alto
1.7.2.3 Licencias	Solo hay 8 puertos licenciados por switch cuando la necesidad de puertos es al menos de 16 puertos licenciados. Sumado al problema de las credenciales todo esto resulta en el no aprovechamiento pleno de esta tecnología y la ralentización del servicio de datos.	Alto
1.7.2.4 Cableado de fibra Óptica	El cableado de fibra óptica no es simétrico ni está etiquetado. Pocos servidores tienen un paso por ambos switches de fibra óptica Brocade 300. Los cables son muy largos y están mal colocados ya algunos están ahorcados resultando en perdida de paquetes de datos.	Alto
1.7.2.5 Red de producción y mantenimiento	Los puertos de mantenimiento de los switches Brocade 300 están en la intranet productiva de la empresa por lo que son accesibles para todo el personal y potencialmente cualquiera, con las credenciales correctas, podría apagarlos o reconfigurarlos.	Alto
1.7.2.6 Equipos conectados a la red de fibra óptica	Se observan equipos conectados a la red de fibra óptica que no están haciendo uso de la misma (caso Servidores DELL R720 SIPARBUE180 y SIPARBUE181), así como equipos Netapp que podrían estar sirviendo datos por red de fibra óptica (caso NetApp SIPARBUE08) que solo trabajan por ISCSI. Esta situación se prolonga hace al menos un año por lo que es evidente que hace mucho tiempo que no se tiene acceso a los switches de fibra óptica.	Me

Hallazgo	Descripción	Criticidad
1.7.2.7 SFP quemados en puerto 3 de ambos switches	Los puertos 3 de ambos switches tienen errores de voltaje por lo que es de suponer que estén quemados y deban ser reemplazados.	Alto

CNP ARGENTINA S.A.

RFP – Remediación y Optimización Servicios Básicos de Red y Seguridad Informática

Especificaciones técnicas / comerciales

Índice

Objetivo

El objetivo del presente documento es solicitar servicios profesionales de consultoría especializada a fin de realizar un proyecto que ejecute remediaciones y optimizaciones a la infraestructura de Tecnología Informática (TI) de CNP CIPETROL Argentina S.A. para resolver las configuraciones de los servicios básicos de TI, las vulnerabilidades existentes asociadas a la seguridad informática y alinear las instalaciones a las mejores prácticas recomendadas.
Asimismo se requiere una propuesta para brindar soporte especializado de la instalación, a ejecutarse con posterioridad de haber finalizado el proyecto mencionado en primer término.

Alcance

El alcance de la solicitud comprende la realización de todas las tareas según se describe a continuación en este documento.

En los casos donde la actividad requiera de la adquisición de elementos de hardware o software será responsabilidad del oferente brindar las especificaciones técnicas y requerimientos para los mismos y ES será el responsable de concretar las adquisiciones. No es objeto de esta contratación la obtención de precios por parte de los oferentes para la adquisición de hardware o software.

En los casos donde ES deba realizar compra de materiales para continuar con la ejecución del proyecto, los plazos que sean requeridos para realizar la gestión de compra hasta la recepción de los mismos no serán contabilizados dentro del cronograma de actividades exigido al oferente para la concreción de sus actividades.

Las actividades específicas de remediación abarcarán a las siguientes instalaciones de la empresa:

- Central Administrativa – Tucumán 10, CABA (BA)
- Oficina regional en Rio Gallegos - San Juan 620, Rio Gallegos, Santa Cruz (RGL)
- Base Recepción Magallanes – RN1 Km 1, Cabo Vírgenes, Santa Cruz (BRM)

Proyecto de Remediación y Optimización de la Plataforma

Las tareas abarcadas en el proyecto son las que se detallan a continuación:

Servicios DNS Externo

- **Servidor de DNS principal expuesto a Internet con todos los ports abiertos, sin sistema de protección de intrusos (IPS) y antivirus (AV)**
  En la regla de publicación del servicio configurada en el firewall, habilitar la protección de IPS, el AV y también publicar solo los puertos necesarios para los servicios que brinda el servidor. En el caso del servicio de DNS, puertos tcp/53 y udp/53.

- **Ajustar configuración de DNS secundario**
  Ajustar la configuración del segundo DNS server para homogeneizar el servicio, según los ajustes que se realicen sobre el DNS primario.
- **Un solo registro MX, no hay Mail Server secundario**
  Implementar un Mail Server segundario, para que actué en caso de fallar el principal.

Servicios DHCP

- **No se cuenta con servicios DHCP en HA**
  Implementar un DHCP Server secundario, para que actúe en caso de fallar el principal.

Protección de Borde

- **Firewall de borde y VPN sin HA**
  Implementar un clúster de firewall para borde y VPN en clúster de alta disponibilidad.
- **ACLs entrantes y red DMZ**
  Publicar en internet solo los puertos de los servicios que son necesarios y que se utilizan.
  Todas las aplicaciones y servicios publicados en internet deben estar en la red DMZ.
- **Servicio Microsoft TNG esta discontinuado desde el 31/12/2015**
  Implementar una alternativa tecnológica diferente al TNG, como por ejemplo un firewall UTM, como lo puede ser FortiGate o Cisco ASA.
- **Se identifican publicaciones de servicios a Internet en cadena desde el FW Fortigate 200B y el TNG**
  Realizar las adecuaciones para que los servicios sean publicados desde un único equipo y en forma directa.
- **Servicios publicados en internet sin sistema de protección de intrusos (IPS), ni antivirus (AV) habilitados en el firewall.**
  Realizar las adecuaciones para que todos los servicios publicados en internet cuenten con protección de IPS, AV y Denegación de Servicio.

Protección de redes interna

- **El tráfico entre redes interna no pasa a través del firewall, por lo cual no se pueden aplicar políticas de seguridad sobre las mismas.**
  Realizar las adecuaciones para que todo el tráfico entre redes de la empresa pase a través del firewall para tener control y poder aplicar políticas de seguridad sobre el mismo.
- **El tráfico entre redes LAN-LAN y LAN-WAN no tiene aplicado IPS, AV o restricciones de ancho de banda.**
  Aplicar IPS, AV, restricciones de ancho de banda, etc.
- **No se cuenta con Protección de acceso a servidores y equipos de infraestructura/networking.**
  Realizar las adecuaciones para prohibir el acceso a la infraestructura tecnológica a todas las redes excepto la red de informática. Crear una red exclusiva para los administradores del equipamiento de TI.

WebFilter

- **Servicio de WebFiltering no está en HA**
  Implementar un esquema de WebFiltering en alta disponibilidad.
- **No se identifican procedimiento de backup de configuración**
  Desarrollar las directrices de un procedimiento para que se realicen backup y controles periódicos sobre el equipamiento que comprende la infraestructura de TI.

Antivirus

- **No se identifican procedimientos de backup de configuración ni control de cambios**
  Desarrollar las directrices de un procedimiento para el control de cambios, para que se realicen copias de seguridad y controles periódicos sobre el equipamiento que comprende la infraestructura de TI.

Antispam

- **La consola de Antispam no está en HA**
  Implementar un esquema de Antispam en alta disponibilidad.
- **No se identifican procedimientos de backup de configuración ni control de cambios**
  Desarrollar las directrices de un procedimiento para el control de cambios, para que se realicen copias de seguridad y controles periódicos sobre el equipamiento que comprende la infraestructura de TI.

Procedimientos de Seguridad

- **ABM cuentas de administrador**
  Desarrollar las directrices de un procedimiento diferencial para el ABM de cuentas de administrador de domino.

Switch de red LAN

- **No hay segmentación de vlans de para separar y controlar el tráfico entre servidores, servicios y usuarios**
  Implementar segmentación por VLANs para red de usuarios y red de servidores. Realizar las adecuaciones para solo la red de administradores pueda ingresar a los servidores.
- **Si bien se cuenta con equipos Layer3, no se están aplicando Vlans ni ruteo interno**
  Configurar ruteo por capa 3 (nivel de red).
- **Se cuenta con Switches L3 en stack, los switches en cascada están conectados solo a un port ethernet.**
  Realizar las adecuaciones para utilizar otro puerto de backup en caso de falta en el puerto que está en uso, para evitar cortes de servicios de red.
- **Acceso telnet habilitado, passwords no encriptadas en la configuración, acceso directo al "enable" en algunos casos.**
  Realizar las adecuaciones para utilizar acceso SSH (secure shell) encriptado.
- **Acceso a los equipos habilitado desde todas las redes, red de usuarios compartida con red de gestión de los equipos, IP de administración en la VLan 1 Nativa.**
  Realizar las adecuaciones para no utilizar la vlan nativa para tráfico de red.
- **Las impresoras están en la misma red que los usuarios y que los equipos de la infraestructura IT.**
  Realizar las adecuaciones para asignar una red exclusiva para las impresoras.
- **Falta Auditoria de cambios, accesos y backups periódicos**
  Desarrollar las directrices de un procedimiento para el control de cambios, para que se realicen copias de seguridad y controles periódicos sobre el equipamiento que comprende la infraestructura de TI.

Red WiFi

- **Seguridad WiFi con cifrado WEP vulnerable y obsoleto.**
  Implementar cifrado WPA2 o WPA2/Enterprise.
- **La red WiFi no está segmentada en red corporativa y red de invitados**
  Implementar un SSID WiFi exclusivo para tareas corporativas y un SSID WiFi exclusivo para invitados.
- **Desde la red WiFi se puede tener acceso a toda la infraestructura IT (firewalls, switch, servidores, videoconferencia, etc.)**
  Implementar una VLAN de sistemas y permitirle solo a ella el acceso a switch, routers, servidores, etc.

Enlaces MPLS / Backup Satélite

- **No se identifica claramente un procedimiento de activación/rollback de backup enlaces MPLS/Satelital**
  Desarrollar un procedimiento implementar conmutación automática de enlace principal a enlace backup y viceversa.
- **No se cuenta con notificación de activación/rollback de uso de enlaces MPLS/Satelital**
  Interactuar con el proveedor de telecomunicaciones y coordinar la implementación de una conmutación automática de enlace principal a enlace backup y viceversa.

Entregables

Se detalla a continuación una lista mínima de entregables deseados por cada punto de adecuación contenido en este documento:

- Documento de configuración: enumeración del ajuste o configuración realizada, mapa conceptual de la configuración resultante, esquema gráfico, detalle de la versión del software, identificación de las actualizaciones incluidas y/o parches que quedaron instalados al momento de la finalización de la labor.
- Archivo en formato Microsoft Visio 2010 (o posterior) con el esquema y el detalle de configuración, incluyendo identificaciones de los componentes, identificación lógica, detalle de conexiones, rutas lógicas configuradas, interfaces, puertos utilizados, etc.
- Documentos con las directrices para el posterior desarrollo del procedimiento de configuración, control, backup y actuaciones operativas necesarias para el correcto mantenimiento y actualización del estándar.

Plazo de Ejecución / Requisitos

Se solicita que el oferente presente un plan de alto nivel con la organización de las tareas, los plazos estimados para su realización, etapas, hitos relevantes, etc.

El oferente debe disponer de su equipo de trabajo a los 10 días hábiles de haber recibido por vía formal la confirmación de la contratación de los servicios, de tal forma que al cumplimiento del plazo mencionado se inicie la ejecución del proyecto. Asimismo en esa misma ventana de tiempo

el oferente deberá desarrollar y presentar a ES el plan detallado del proyecto que contiene todo el detalle de las tareas a desarrollar con sus tiempos asociados, dependencias, identificación de actividades que requieren disrupción de los servicios y el nivel de participación que será requerido por parte del personal del Área de TI de ES.

Las tareas se podrán realizar en días hábiles y en horarios de oficina, salvo aquellas actividades que puedan ocasionar alguna disrupción de los servicios de TI. En los casos donde exista riesgo de disrupción de los servicios ES definirá la mejor oportunidad para realizar las actividades fuera de los horarios habituales y el oferente las concretará sin costo adicional.

Para determinar el avance del proyecto, por cada etapa o hito que se identifique dentro del plan el oferente debe presentar la documentación asociada, según se especifica dentro del punto "Entregables". ES se reserva un plazo de 5 (cinco) días hábiles para analizar la información y prestar conformidad para dar por finalizada la etapa o hito y sus tareas asociadas y realizar el documento de certificación correspondiente (HES) para el posterior pago de los servicios, en los casos en que corresponda.

El oferente debe garantizar la calidad de las tareas realizadas, no solo en lo concerniente a las mejores prácticas de la especialidad -según recomendación del fabricante-, sino también a la compatibilidad de la plataforma con el entorno de los sistemas de ES. Todas las tareas realizadas por el oferente contarán con una garantía de 60 días, dentro de los cuales cualquier ajuste o retrabajo que el oferente deba realizar a fin de cumplir el requisito de calidad mencionado precedentemente, estarán comprendidos dentro del precio ofertado por la realización del proyecto y no serán objeto de facturación adicional o cambio del alcance de la propuesta.

Ante la situación que el oferente requiera la instalación de herramientas específicas sobre la red de ES para realizar sus labores, con antelación suficiente debe presentar un listado de las mismas indicando nombre, versión, objetivo para el cual se desea instalar, riesgos que supone su instalación, un plan para la mitigación de tales riesgos y la posterior desinstalación. En estos casos el oferente debe presentar alternativas para el relevamiento previendo la eventual circunstancia que ES no apruebe la instalación de tales herramientas.

En los casos sobre los cuales el oferente requiera la participación de personal de ES para la concreción de alguna actividad, el oferente debe presentar con antelación suficiente una alternativa de acción previendo la eventual circunstancia que ES no apruebe la participación de personal propio en la actividad.

En los casos que deban realizarse tareas directamente por parte del oferente en algunas de las oficinas en el interior del país, ES realizará la coordinación y se hará cargo de los gastos de traslado, alojamiento y viáticos.

Soporte de incidentes, mantenimiento preventivo y capacitación

Se requiere que el oferente presente una propuesta para brindar soporte, mantenimiento preventivo a la instalación y capacitación a los recursos de ES a partir del período de post-implementación del proyecto “Remediación y Optimización de la Plataforma”.

El alcance de este servicio será por 12 (doce) meses con opción de ser extendido por un período de idéntica duración.

La base de cálculo para el servicio será de 20 horas mensuales, que en el caso de no ser utilizadas se acumularán por 3 (tres) períodos consecutivos.

Las horas incluidas en este servicio podrán ser utilizadas a criterio de ES para obtener soporte de incidentes, realizar mejoras o actualizaciones sobre el sistema de almacenamiento y obtener capacitación de sus recursos.

Se espera que el oferente brinde capacitación a los recursos de ES para la resolución del nivel 1 de los incidentes que se presenten y demás actividades básicas para la correcta operación de los componentes de la plataforma. Consecuentemente, se reserva para el oferente el servicio de soporte y la resolución de los incidentes que superen el nivel básico y la gestión de solución con el fabricante en los casos que corresponda.

Cualquiera de las partes podrá rescindir anticipadamente la prestación de este servicio, realizando una comunicación fehaciente con una antelación no menor a 60 días.

Confidencialidad / Tratamiento de la información

Toda la información sobre ES proporcionada durante el proceso de solicitud de propuestas, quedará supeditado a la no divulgación y no puede ser divulgada sin el permiso expreso de ES.

Las especificaciones, datos, documentaciones o cualquier otra información técnica o comercial suministradas a los oferentes durante este proceso, deben ser entendidas como propiedad de ES.

Se prohíbe la reproducción total o parcial de este documento y cualquiera de sus documentos adjuntos sin la autorización expresa previa por parte de ES. Cualquier intercambio de información y documentos entre ES y los oferentes serán considerados confidenciales.

ES es consciente de que la información contenida en las propuestas indica las operaciones actuales del oferente. Por lo tanto, el uso de esta información se limitará a esta solicitud, y será tratada como confidencial.

Actualización del alcance

Ninguna modificación podrá efectuarse al presente, salvo que fuera hecha por escrito y con el mutuo acuerdo de las partes.

Forma de Cotización

El oferente deberá cotizar según el siguiente esquema:

- ➔ Un valor fijo por la realización de todas actividades mencionadas en el punto “Proyecto de Remediación y Optimización de la Plataforma” de este documento. El oferente debe identificar las etapas o hitos de certificación y el porcentaje de facturación asociado respecto del total correspondiente al proyecto.

- ➔ Un valor hora de técnico especialista para eventuales tareas adicionales que se requieran realizar por fuera de las enunciadas en el punto “Proyecto de Remediación y Optimización de la Plataforma”, con intervención directa de los recursos del oferente afectados al proyecto.

- ➔ Un valor mensual para brindar soporte con especialistas certificados según se detalla en el punto “Soporte de incidentes, mantenimiento preventivo y capacitación”.

Certificación y Pago

Es requisito indispensable para la presentación de facturas y posterior cobro que el oferente previamente obtenga por parte de ES el documento de certificación correspondiente (HES), según se indica en el punto “Plazo de Ejecución / Requisitos”.

FIN DEL DOCUMENTO

MATRIZ DE COMPARACION DE PROVEEDORES

Compañía Nacional del Petróleo

Guía

IDENTIFICACION DE LA COMPARATIVA	
Autor:	PMO CNP James Vallejo Mejia
Proyecto	Proyecto Remediación y optimización infraestructura de red y seguridad informática
Fecha:	16-jun.-17

1. PONDERACION DE LOS CRITERIOS A TENER EN CUENTA EN LA VALORACION

Se asignan los porcentajes de ponderacion en la planilla utilizada por la compañía para seleccionas proveedores

Total Ponderaciones: **100,0%** **PONDERACION COMPLETA**

Aspectos Técnicos	
Calidad del producto/servicio	15,0%
Capacidad técnica del proveedor	15,0%
Calidad certificada (ISO o similar)	5,0%
Capacidad de adaptación	5,0%
Plazos de entrega	15,0%
Total aspectos técnicos	**55,0%**

Aspectos comerciales y económicos	
Precios	10,0%
Formas y plazos de pago	5,0%
Servicio postventa	5,0%
Garantías	5,0%
Total asp. comerc. y econ.	**25,0%**

Aspectos empresariales	
Estabilidad del proveedor	5,0%
Proximidad	3,0%
Facilidad de entendimiento	4,0%
Importancia como cliente	5,0%
Referencias de terceros	3,0%
Total aspectos empresariales	**20,0%**

2. IDENTIFICACION DE LOS PROVEEDORES A COMPARAR

Se seleccionasn los 4 proveedores mas acordes y que habian implementado proyectos previamente con la compañia

	Proveedores
A.	Network FLA
B.	Tycon Tech
C.	Softcom
D.	Intelligence TI

3. VALORACION DE LOS PROVEEDORES

Valoracion de 1 (mínimo) a 5 (máximo) las ofertas y características de cada proveedor.

PAUTAS DE VALORACION

Aspectos Técnicos	Network FLA	Tycon Tech	Softcom	Intelligence TI
Calidad del producto/servicio	5	5	5	5
Capacidad técnica	4	5	4	4
Calidad certificada (ISO o similar)	3	4	3	2
Capacidad de adaptación	4	4	2	3
Plazos de entrega	5	5	3	3

	1	2	3	4	5
Calidad del producto/servicio	Muy baja	Baja	Media	Alta	Muy Alta
Capacidad técnica	Muy baja	Baja	Media	Alta	Muy Alta
Calidad certificada (ISO o similar)	Muy baja	Baja	media	Alta	Muy alta
Capacidad de adaptación	Muy baja	Baja	media	Alta	Muy alta
Plazos de entrega	Muy altos	Altos	Medios	Bajos	Muy Bajos

Aspectos comerciales y econ.	Network FLA	Tycon Tech	Softcom	Intelligence TI
Precios	3	4	5	4
Formas y plazos de pago	3	4	3	2
Servicio postventa	4	5	4	4
Garantías	3	5	5	2

	1	2	3	4	5
Precios	Muy altos	Altos	Medios	Bajos	Muy Bajos
Formas y plazos de pago	Muy malas	Malas	Medias	Buenas	Muy buenas
Servicio postventa	Muy malo	Malo	Medio	Bueno	Muy bueno
Garantías	Muy mala	Mala	Media	Buena	Muy buena

Aspectos empresariales	Network FLA	Tycon Tech	Softcom	Intelligence TI
Estabilidad del proveedor	4	4	5	4
Proximidad	3	4	5	3
Facilidad de entendimiento	3	5	4	2
Importancia como cliente	3	4	3	3
Referencias de terceros	2	4	4	2

	1	2	3	4	5
Estabilidad del proveedor	Muy baja	Baja	Media	Alta	Muy Alta
Proximidad	Muy baja	Baja	Media	Alta	Muy Alta
Facilidad de entendimiento	Muy baja	Baja	Media	Alta	Muy Alta
Importancia como cliente	Muy baja	Baja	Media	Alta	Muy Alta
Referencias de terceros	Ninguna	Malas	Regulares	Buenas	Muy buenas

4. RESULTADOS DE LA COMPARACION

RESULTADOS	Aspectos Técnicos	Aspectos comerciales y econ.	Aspectos empresariales	TOTAL	POSICION
Network FLA	2,45	0,80	0,62	3,87	3
Tycon Tech	2,65	1,10	0,84	4,59	1
Softcom	2,05	1,10	0,83	3,98	2
Intelligence TI	2,05	0,80	0,58	3,43	4

Compañía Nacional del Petróleo

Informe Técnico
Proyecto Remediación

CNP Argentina S.A.

mayo 2018

Compañía Nacional del Petróleo

Contenido

Compañía Nacional del Petróleo

Compañía Nacional del Petróleo

1 Etapa I - Servicios DNS Externo y DHCP

1.1 Habilitar protección de IPS, AV y publicar solo puertos necesarios para el servicio de DNS Externo

1.1.1 Acciones:

- Habilitar solo el puerto 53, protocolos TCP y UDP
- Habilitar protección de IPS y AV en la publicación
- Realizar pruebas del servicio

1.1.2 Evidencia:

```
config firewall policy
    edit 59
        set srcintf "port15"
        set dstintf "port10"
        set srcaddr "all"
        set dstaddr "bld_dns2_externo_200.5.0.0"
        set action accept
        set schedule "always"
        set service "DNS"
        set utm-status enable
        set logtraffic all
        set comments "NAT DNS SECUNDARIO"
        set av-profile "AV-flow"
        set ips-sensor "default"
        set profile-protocol-options "default"
    next
    edit 66
        set srcintf "port15"
        set dstintf "port10"
        set srcaddr "all"
        set dstaddr "bld_dns1_externo_200.5.0.0"
        set action accept
        set schedule "always"
```

```
        set service "DNS"
        set utm-status enable
        set logtraffic all
        set comments "NAT DNS SECUNDARIO"
        set av-profile "AV-flow"
        set ips-sensor "default"
        set profile-protocol-options "default"
    next
end
```

1.1.3 Recomendaciones:

Cada vez que un servicio es publicado en internet se debe habilitar

1.2 Ajustar configuración de DNS Server Externo Segundario

1.2.1 Acciones:

- Instalación de un servidor con Windows Server 2012
- Habilitación de servicio de DNS en nuevo Server
- Transferencia de zonas desde DNS principal al segundario
- Configuraciones de Alta Disponibilidad
- Gestión de configuraciones para publicación en internet (Load Balance)
- Realización de pruebas de servicios

1.2.2 Datos y evidencias: La documentación respectiva para la implementación final se puede ver en el siguiente anexo:

1.2.3 Recomendaciones:

La documentación para DNS se encuentra en el siguiente Anexo:

\\192.168.1.17\privado$\TI

1.2.4 Monitoreo:

Se recomienda instrumentar al menos los siguientes parametros de Monitoreo

- Estado de los servidores UP/DOWN

- Estado del servicio de DNS UP/DOWN

Compañía Nacional del Petróleo

1.3 Implementar un esquema de HA para el servidor de DHCP

1.3.1 Acciones:

- Instalación de dos servidores con Windows Server 2012
- Configuración de los servicios de DHCP
- Importación de configuraciones de DHCP actual
- Configuración de conmutación por error en modo Load Balance
- Realización de pruebas del servicio

1.3.2 Datos y evidencias:

Servidores DHCP:

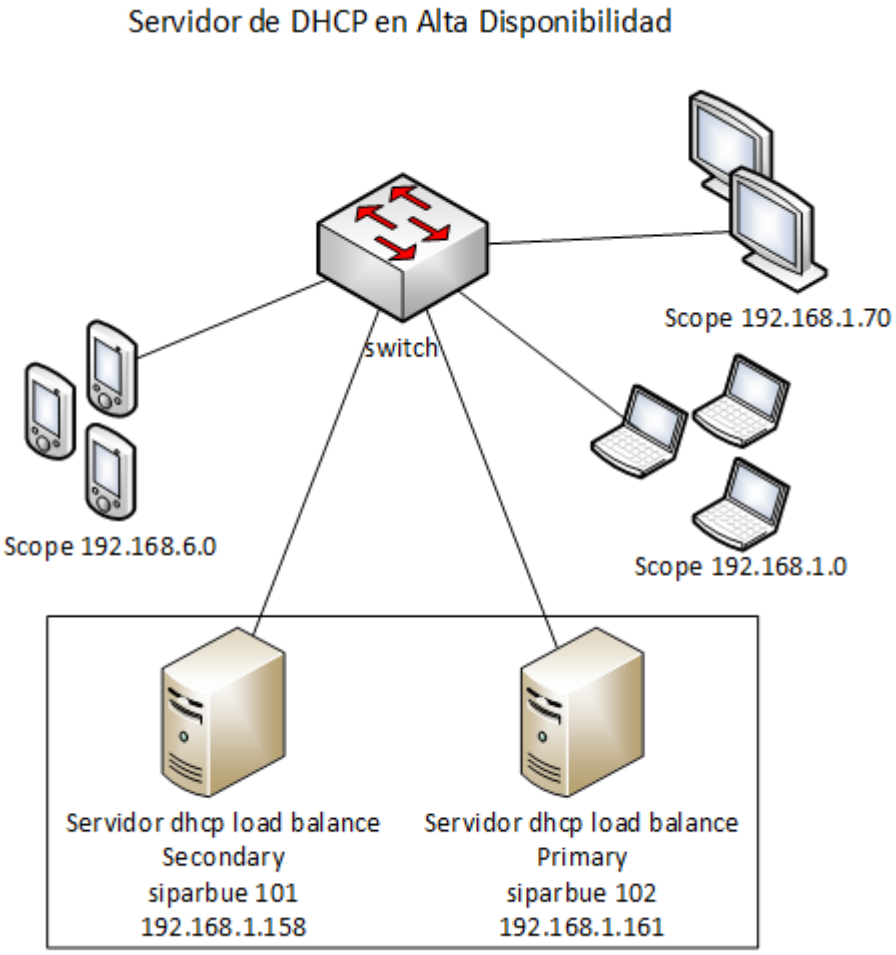
Siparbue102, IP: 192.168.1.161 (Primary)

Siparbue101, IP: 192.168.1.158 (Secondary)

Datos scope:

Vlan ID	Nombre	
240	Geologia	10.3.240.50 - 10.3.240.210
242	Cableada	10.3.242.10 - 10.3.242.210
244	WiFi_Corporativo	10.3.244.10 - 10.3.244.210
100	Telefonia VOIP	172.30.111.50 - 172.30.111.200
1	CIPETROL	192.168.1.47 - 192.168.1.200
6	Buenos Aires	192.168.6.40 - 192.168.1.170
70	Carteleras	192.168.70.11 - 192.168.70.254

Compañía Nacional del Petróleo



Configuraciones solicitadas a TASA: Anteriormente se tenían subinterfaces como default Gateway en el router, se dan de baja y se configuran en el CORE, el router de TASA queda con las siguientes Interfaces:

Router PPAL TASA Bs. As:

Router_3925#show ip int br
Interface IP-Address OK? Method Status Protocol
Embedded-Service-Engine unassigned YES NVRAM administratively down down
GigabitEthernet 10.3.0.0 YES NVRAM up up

Compañía Nacional del Petróleo

GigabitEthernet 10.255.255.0 YES NVRAM up up
GigabitEthernet unassigned YES unset up up
GigabitEthernet unassigned YES NVRAM administratively down down
Loopback0 192.168.144.0 YES NVRAM up up
Loopback1 10.3.252.0 YES NVRAM up up
Router_3925#show int desc
Interface Status Protocol Description
Em admin down down
Gi up up
Gi up up Contra Core
Gi up up
Gi admin down down
Lo0 up up Ip Gestion
Lo1 up up TOIP – SIP

Router BKP TASA Bs. As:

Router_BKP#show ip int br
Interface IP-Address OK? Method Status Protocol
GigabitEthernet 10.3.252.0 YES NVRAM up up
GigabitEthernet 10.3.255.0 YES NVRAM up up
GigabitEthernet 10.255.255.0 YES NVRAM up up
GigabitEthernet unassigned YES unset up up
GigabitEthernet 209.13.0.0 YES NVRAM up up
GigabitEthernet 209.13.0.0 YES NVRAM up up
FastEthernet unassigned YES unset up up
FastEthernet unassigned YES unset administratively down down
FastEthernet unassigned YES unset up down
FastEthernet unassigned YES unset up down
Vlan1 unassigned YES NVRAM up down
Vlan2 200.5.0.0 YES NVRAM up up
NVI0 10.3.252.0 YES unset up up
Loopback0 192.168.144.33 YES NVRAM up up
Router_BKP #show int desc
Interface Status Protocol Description
Gi up up
Gi up up TRAFICO SEGURO
Gi up up - CORE-
Gi up up
Gi up up INTERNET
Gi up up WIFI GUEST CORE
Fa up up
Fa admin down down
Fa up down

Fa0/2/3	*up*	*down*	
Vl1	*up*	*down*	
Vl2	*up*	*up*	
NV0	*up*	*up*	
Lo0	*up*	*up*	*Ip Gestion.*

Configuraciones en CORE Cisco 3850:

CORE-STACK-3850#show ip int br

Interface	*IP-Address*	*OK? Method Status*	*Protocol*
Vlan1	*192.168.1.251*	*YES manual up*	*up*
Vlan6	*192.168.6.251*	*YES NVRAM up*	*up*
Vlan70	*192.168.70.1*	*YES manual up*	*up*
Vlan100	*172.30.111.1*	*YES manual up*	*up*
Vlan240	*10.3.240.1*	*YES manual up*	*up*
Vlan242	*10.3.242.1*	*YES manual up*	*up*
Vlan999	*unassigned*	*YES unset up*	*up*
Vlan1228	*10.3.252.129*	*YES manual up*	*up*
Vlan1234	*10.3.234.1*	*YES manual down*	*down*
Vlan1238	*10.3.238.1*	*YES manual up*	*up*
Vlan1245	*10.3.238.129*	*YES manual down*	*down*
Vlan1296	*unassigned*	*YES unset administratively down down*	

CORE-STACK-3850#show int desc

Interface	*Status*	*Protocol*	*Description*
Vl1	*up*	*up*	
Vl6	*up*	*up*	*Vlan WiFi*
Vl70	*up*	*up*	*Cartelera Electr.*
Vl100	*up*	*up*	*TOIP*
Vl240	*up*	*up*	*Usuarios Geologia*
Vl242	*up*	*up*	*Usuarios Cableado*
Vl999	*up*	*up*	
Vl1228	*up*	*up*	*Core to Vdom Root*
Vl1234	*down*	*down*	*Red_Impresoras*
Vl1238	*up*	*up*	*videoconferencia*
Vl1245	*down*	*down*	*Vmware_Vmotion*

Compañía Nacional del Petróleo

1.3.3 Recomendaciones:

Los cambios de configuración se pueden realizar en cualquiera de los dos servidores, pero por una cuestión de orden se recomienda realizarlos en siparbue102.

1.3.4 Monitoreo:

Se recomienda instrumentar en la herramienta de monitoreo los siguientes parámetros:

- Estado de los servers UP/DOWN
- Estado de los servicios DHCP UP/DOWN
- Estado de los Pools de DHCP Enable/Disable
- Porcentaje de uso de cada Pools (Warning=80%, Critical=90%)
- Cantidad de IP asiganadas por cada Pool

Compañía Nacional del Petróleo

2 Etapa II - Protección de Borde I

2.1 Implementar un clúster de firewall para borde y VPN en clúster de alta disponibilidad

2.1.1 Acciones:

- Adquisición de firewall UTM para HA
- Instalación y configuración inicial
- Importar configuraciones de borde
- Pruebas de funcionamiento
- Importar configuraciones de VPN
- Pruebas de funcionamiento

2.1.2 Datos y Evidencias:

2.1.3 Recomendaciones:

2.2 Ajustar servicios publicados en internet y configurar aplicaciones publicadas en la red DMZ

2.2.1 Acciones:

- Habilitar solo los puertos necesarios de los servicio publicados en internet
- Verificar servicios que no están en la red DMZ y moverlos a esta red
- Pruebas de funcionamiento

2.2.2 Datos y Evidencias:

Se Define direccionamiento 10.3.248.0/24 para los equipos pertenecientes a la DMZ, el segmento anterior no se encontraba dentro de la MPLS. (10.0.1.0/24)

Se migran todos los equipos que estaban en la red 10.0.1.0/24:

Compañía Nacional del Petróleo

Name	External IP Address/Range	External Service Port	Mapped IP Address/Range	Map to Port
NAT_AM3_Arg	port15/200.5.104.17	0-65535/tcp	192.168.103.253	0-65535/tcp
NAT_IMSS_Argentina	port15/200.5.91.109	0-65535/tcp	192.168.1.22	0-65535/tcp
Webmail_Arg2	port15/200.5.91.108	0-65535/tcp	192.168.1.38	0-65535/tcp
NAT_192.168.1.4	port15/200.5.104.21	0-65535/tcp	192.168.1.4	0-65535/tcp
NAT_MVW2_ARG_10.3.248.18	port15/200.5.104.18	0-65535/tcp	10.3.248.18	0-65535/tcp
NAT_MVW2_ARG_10.3.248.19:443	port15/200.5.104.19	443/tcp	10.3.248.19	443/tcp
NAT_MVW2_ARG_10.3.248.20	port15/200.5.104.20	0-65535/tcp	10.3.248.20	0-65535/tcp
NAT_ARG_10.3.248.22:80	port15/200.5.104.19	80/tcp	10.3.248.22	80/tcp
NAT_AM2_Arg	port15/200.5.104.22	0-65535/tcp	192.168.102.253	0-65535/tcp
Enap Sipetrol AM3	port15/200.10.99.162	0-65535/tcp	192.168.103.253	0-65535/tcp
FTP_entrante_FTP_New_DMZ	port15/200.5.91.107	21/tcp	10.3.248.10	21/tcp
HTTPS_200.5.91.107	port15/200.5.91.107	443/tcp	192.168.1.1	443/tcp
test owa https	port15/200.5.91.107	30443/tcp	192.168.1.30	443/tcp

IP Address	Port	Weight	Max Connections	Mode
bld_HTTP_200.5.91.107				
bld_dns1_externo_200.5.91.107				
10.3.248.24	53	N/A	0	Active
10.3.248.30	53	N/A	0	Active
bld_dns2_externo_200.5.104.19				
10.3.248.24	53	N/A	0	Active
10.3.248.30	53	N/A	0	Active
camara_enapsipetro.com.ar				

Se procede con la baja del segmento 10.0.1.0/24, se cambia la dirección ip en el Firewall de borde, dejando la 10.3.248.1/24 como IP Principal, Ya que estaba como secundaria durante la transición:

Name	Type	IP/Netmask	Access	Administrative Status	Link Status
port11 (ARPETROL)	Physical	192.168.50.1 255.255.255.0	PING	↑	↑ 100Mbps/Full Duplex
port12	Physical	0.0.0.0 0.0.0.0		↑	↓
port13	Physical	0.0.0.0 0.0.0.0		↑	↓
port14	Physical	0.0.0.0 0.0.0.0		↑	↓
port15 (Internet Primario)	Physical	200.5.91.106 255.255.255.248	PING, HTTPS, SSH, SNMP	↑	↑ 1000Mbps/Full Duplex
port16 (Internet Backup)	Physical	146.82.228.114 255.255.255.248	PING, HTTPS, SSH	↑	↓
switch (Red Interna)	Physical	10.3.252.66 255.255.255.240	PING, HTTPS, SSH, SNMP	↑	↑ 100Mbps/Full Duplex
port9	Physical	5.5.5.5 255.255.255.0	PING, HTTPS, SSH, SNMP, HTTP, FMG-Access, AUTO-IPSEC, RADIUS-ACCT, PROBE-RESPONSE, CAPWAP	↑	↓
port10 (Red_10 - DMZ)	Physical	10.3.248.1 255.255.255.0	PING	↑	↑ 1000Mbps/Full Duplex

Prueba de conectividad a servidores OK y servicios funcionando correctamente.

2.2.3 Recomendaciones:

2.3 Implementar una alternativa tecnológica diferente al TMG, ya el servicio está discontinuado

2.3.1 Acciones:

- Adquisición de firewall UTM
- Relevar configuraciones de permisos de acceso en el TMG
- Migrar configuraciones de permisos de acceso a los firewalls UTM
- Pruebas de servicios

2.3.2 Datos y Evidencias:

- Se procede con la implementación de proxy Reverso y se migran los servicios que estaban en el TMG, OWA y LYNC pasan por proxy Reverso el cual se encuentra en la DMZ y el websense se reemplaza por un proxy implementado en el vdom de Proxy del fortigate 200D, realizando filtrado web.

Remitirse al anexo:

- **\\192.168.1.17\privado$\TI\ Proyecto Remediación\Informe del Proyecto/ CNP_CIPETROL_ANEXO 2 PROXY V2.doc**
  -\192.168.1.17\privado$\TI\ActiveSec - Proyecto Remediación\Informe del Proyecto/CNP_CIPETROL_ANEXO_PROXY_REVERSO\CNP_CIPETROL_Proxy_Reverso.doc

2.3.3 Recomendaciones:

3 Etapa III - Protección de Borde II

3.1 Realizar las adecuaciones para que los servicios sean publicados desde un único equipo y en forma directa

3.1.1 Acciones:

- Verificación de que servicios están publicados hacia internet desde el ISA Server y el TMG
- Creación y validación de las reglas de firewall en un entorno de prueba
- Migración de las reglas al nuevo firewall
- Realización de pruebas de funcionamiento de los servicios

3.1.2 Datos y Evidencias:

3.1.3 Recomendaciones:

3.2 Realizar las adecuaciones para que todos los servicios publicados en internet cuenten con protección de IPS, AV y DOS

3.2.1 Acciones:

- Creación de profiles de AV, IPS y Antivirus en el firewall
- Asignación de los profiles a los servicios publicados en internet
- Realización de pruebas de los servicios publicados en internet

3.2.2 Datos y Evidencias:

```
edit 57
    set srcintf "port15"
    set dstintf "switch"
    set srcaddr "all"
    set dstaddr "CNP CIPETROL AM3"
    set action accept
    set schedule "always"
    set service "ssh" "VPN1_IPSEC_encapsulation" "IPSEC Services" "ALL_ICMP" "AH" "IKE"
    set utm-status enable
    set logtraffic all
    set av-profile "AV-flow"
    set ips-sensor "default"
    set profile-protocol-options "default"
next
edit 56
    set srcintf "port15"
    set dstintf "switch"
    set srcaddr "all"
    set dstaddr "NAT_AM2_Arg"
    set action accept
    set schedule "always"
    set service "ALL_ICMP" "AH" "IKE" "VPN1_IPSEC_encapsulation" "ssh" "IPSEC Services"
    set utm-status enable
    set logtraffic all
    set av-profile "AV-flow"
    set ips-sensor "default"
    set profile-protocol-options "default"
next
edit 30
    set srcintf "port15"
```

```
    set dstintf "switch"
    set srcaddr "all"
    set dstaddr "NAT_192.168.1.4"
    set action accept
    set schedule "always"
    set service "HTTP" "HTTPS"
    set utm-status enable
    set logtraffic all
    set comments "192.168.1.4 IP del TMG"
    set av-profile "AV-flow"
    set ips-sensor "default"
    set profile-protocol-options "default"
  next
  edit 33
    set srcintf "port15"
    set dstintf "switch"
    set srcaddr "all"
    set dstaddr "Webmail_Arg2"
    set action accept
    set schedule "always"
    set service "HTTP" "HTTPS" "ALL_ICMP"
    set utm-status enable
    set logtraffic all
    set comments "192.168.1.38 IP del TMG"
    set av-profile "default"
    set ips-sensor "protect_http_server"
    set profile-protocol-options "default"
  next
  edit 35
    set srcintf "port15"
    set dstintf "switch"
    set srcaddr "all"
    set dstaddr "NAT_IMSS_Argentina"
    set action accept
    set schedule "always"
    set service "SMTP" "TCP_8445" "icmp-proto" "SSH"
    set utm-status enable
    set logtraffic all
    set av-profile "default"
```

```
    set ips-sensor "protect_email_server"
    set profile-protocol-options "default"
  next
  edit 59
    set srcintf "port15"
    set dstintf "port10"
    set srcaddr "all"
    set dstaddr "bld_dns2_externo_200.5.104.19"
    set action accept
    set schedule "always"
    set service "DNS"
    set utm-status enable
    set logtraffic all
    set comments "NAT DNS SECUNDARIO"
    set av-profile "AV-flow"
    set ips-sensor "default"
    set profile-protocol-options "default"
  next
  edit 66
    set srcintf "port15"
    set dstintf "port10"
    set srcaddr "all"
    set dstaddr "bld_dns1_externo_200.5.91.107"
    set action accept
    set schedule "always"
    set service "DNS"
    set utm-status enable
    set logtraffic all
    set comments "NAT DNS SECUNDARIO"
    set av-profile "AV-flow"
    set ips-sensor "default"
    set profile-protocol-options "default"
  next
  edit 40
    set srcintf "port15"
    set dstintf "port10"
    set srcaddr "all"
    set dstaddr "NAT_MVW2_ARG_10.0.1.18"
    set action accept
```

```
        set schedule "always"
        set service "HTTP" "HTTPS" "SIP" "sip_5061" "sip_any-tcp-ipv6" "sip_any-tcp" "udp_sip"
"ALL_ICMP"
        set utm-status enable
        set logtraffic all
        set av-profile "AV-flow"
        set ips-sensor "default"
        set profile-protocol-options "default"
    next
    edit 37
        set srcintf "port15"
        set dstintf "port10"
        set srcaddr "all"
        set dstaddr "NAT_MVW2_ARG_10.0.1.19:443"
        set action accept
        set schedule "always"
        set service "HTTPS"
        set utm-status enable
        set logtraffic all
        set av-profile "AV-flow"
        set ips-sensor "default"
        set profile-protocol-options "default"
    next
    edit 42
        set srcintf "port15"
        set dstintf "port10"
        set srcaddr "all"
        set dstaddr "NAT_MVW2_ARG_10.0.1.20"
        set action accept
        set schedule "always"
        set service "UDP3478" "HTTPS"
        set utm-status enable
        set logtraffic all
        set av-profile "AV-flow"
        set ips-sensor "default"
        set profile-protocol-options "default"
    next
    edit 41
        set srcintf "port15"
```

```
    set dstintf "port10"
    set srcaddr "all"
    set dstaddr "NAT_ARG_10.0.1.22:80"
    set action accept
    set schedule "always"
    set service "HTTP"
    set utm-status enable
    set logtraffic all
    set av-profile "AV-flow"
    set ips-sensor "default"
    set profile-protocol-options "default"
  next
  edit 61
    set srcintf "port15"
    set dstintf "switch"
    set srcaddr "all"
    set dstaddr "camara_CNPsipetro.com.ar"
    set action accept
    set schedule "always"
    set service "http"
    set utm-status enable
    set logtraffic all
    set comments "publicacion_camaras"
    set av-profile "AV-flow"
    set ips-sensor "default"
    set profile-protocol-options "default"
  next
  edit 65
    set srcintf "port15"
    set dstintf "switch"
    set srcaddr "all"
    set dstaddr "FTP_entrante_SIPARBUE00"
    set action accept
    set schedule "always"
    set service "ftp"
    set utm-status enable
    set logtraffic all
    set comments "Publicacion FTP Siparbue00"
    set av-profile "AV-flow"
```

```
        set ips-sensor "default"
        set profile-protocol-options "default"
    next
    edit 64
        set srcintf "port15"
        set dstintf "switch"
        set srcaddr "all"
        set dstaddr "bld_HTTP_200.5.91.107"
        set action accept
        set schedule "always"
        set service "HTTP"
        set utm-status enable
        set logtraffic all
        set comments "Publicacion HTTP"
        set av-profile "AV-flow"
        set ips-sensor "protect_http_server"
        set profile-protocol-options "default"
    next
end
```

3.2.3 Recomendaciones:

Cada vez que un servicio sea publicado en internet aplicar protección AV e IPS.

4 Etapa IV - Switch de LAN

4.1 Implementar segmentación por VLANs para red de usuarios y red de servidores. Configurar ruteo por capa 3 (nivel de red)

4.1.1 Acciones:

- Definición de rangos de red
- Configuración en Switchs, Vlans, puertos de Trunk
- Migración de equipos a nuevas redes, asignación de puertos de switch a nuevas Vlans
- Pruebas de funcionamiento

4.1.2 Datos y Evidencias:

A continuación de brinda el diseño de subnetting que se planteó, ya se asignaron segmentos a las vlan actuales: Segmento general utilizado para el diseño 10.3.0.0/16

Compañía Nacional del Petróleo

Prefijo	Red		Uso	Rango Asignado	Máscara	Bits	VLAN ID
172.3	111	0	Telefonía IP		255.255.255.0	24	**100**
192.168	1	0	Servers		255.255.255.0	24	1
192.168	6	0	Red WiFi Usuarios		255.255.255.0	24	**6**
192.168	70	0	Certelera Electronica		255.255.255.0	24	**70**
10.3	252	0	Vdom Root – Router TASA PPAL		255.255.255.248	29	**1200**
10.3	252	8	Vdom Root – Router TASA BKP		255.255.255.248	29	1208
10.3	252	32	Loopbak Telefonia TASA		255.255.255.240	30	**-**
10.3	252	64	Vdom root – FW Internet		255.255.255.240	28	**1264**
10.3	252	96	Vdom root – Router Level 3		255.255.255.248	29	1296
10.3	252	240	Test Proxy		255.255.255.240	28	**99**
10.3	253	240	Red VDOM_WiFi – Invitados		255.255.255.240	28	**999**
10.3	254	0	Networking		255.255.255.0	24	**1**
10.3	248		DMZ			24	Ruteada por FW Borde
10.3	244	0	WIFI Corporativo - NPS		255.255.255.0	24	(ruateada por VDOM WiFi)
10.3	242	0	Usuarios Cableados LAN		255.255.255.0	24	242
10.3	240	0	Usuarios Cableado Geologia		255.255.255.0	24	**240**

Se realiza la debida configuración de vlans en el CORE:

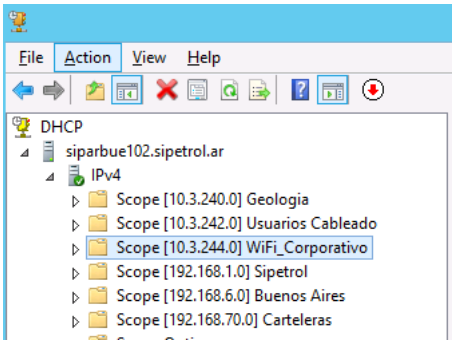
```
interface Vlan1
 ip address 10.3.254.1 255.255.255.0 secondary
 ip address 192.168.1.249 255.255.255.0 secondary
 ip address 192.168.1.186 255.255.255.0 secondary
 ip address 192.168.1.6 255.255.255.0 secondary
 ip address 192.168.1.251 255.255.255.0
!
interface Vlan6
 description Vlan WiFi
 ip address 192.168.6.251 255.255.255.0
 ip helper-address 192.168.1.161
 ip helper-address 192.168.1.158
!
interface Vlan70
 description Cartelera Electr.
 ip address 192.168.70.1 255.255.255.0
 ip helper-address 192.168.1.161
 ip helper-address 192.168.1.158
!
interface Vlan100
 description TOIP
 ip address 172.30.111.1 255.255.255.0
 ip helper-address 192.168.1.161
 ip helper-address 192.168.1.158
!
interface Vlan240
 description Usuarios Geologia
 ip address 10.3.240.1 255.255.255.0
 ip helper-address 192.168.1.161
 ip helper-address 192.168.1.158
!
interface Vlan242
 description Usuarios Cableado
 ip address 10.3.242.1 255.255.255.0
 ip helper-address 192.168.1.161
 ip helper-address 192.168.1.158
```

Estas son las Vlan y asignación de ips en el Vdom Root Fortigate 200D:

Compañía Nacional del Petróleo

	Status	Name	VLAN ID	Members	IP/Netmask	Type	Access	Virtual Domain	Ref.
Aggregate (8)									
	↑	LACP_ROOT		port9, port10, port11 ...	10.3.252.142 255.255.255.240	802.3ad Aggregate (4)	PING HTTPS SSH	root	19
		root_internet	1264		10.3.252.65 255.255.255.240	VLAN	PING HTTPS SSH	root	9
		wan_level3	1296		10.3.252.97 255.255.255.248	VLAN	PING	root	8
		wan_telefonica1	1200		10.3.252.1 255.255.255.248	VLAN	PING	root	3
		wan_telefonica2	1208		10.3.252.9 255.255.255.248	VLAN	PING	root	3
	↑	LACP_WIFI		port14, port15, port16	10.3.254.13 255.255.255.0	802.3ad Aggregate (3)	PING HTTPS SSH CAPWAP	WiFi	10
		WIFI_CORP	6		192.168.6.254 255.255.255.0	VLAN	PING	WiFi	2
		WIFI_INVITADOS	999		10.3.255.253 255.255.255.248	VLAN	PING	WiFi	5
Physical (14)									
	↓	dmz1			0.0.0.0 0.0.0.0	Physical Interface	PING HTTPS HTTP FMG-Access CAPWAP	root	0
	↓	dmz2			0.0.0.0 0.0.0.0	Physical Interface	PING FMG-Access CAPWAP	root	0
	↑	mgmt			10.3.254.9 255.255.255.0	Physical Interface	PING HTTPS SSH SNMP HTTP		2
	↑	port1 (HA1)			0.0.0.0 0.0.0.0	Physical Interface		root	2
	↑	port2 (HA2)			0.0.0.0 0.0.0.0	Physical Interface		root	1
	↓	port3			0.0.0.0 0.0.0.0	Physical Interface		root	0
	↓	port4			0.0.0.0 0.0.0.0	Physical Interface		root	0
	↓	port5			0.0.0.0 0.0.0.0	Physical Interface		root	0
	↓	port6			0.0.0.0 0.0.0.0	Physical Interface		root	0
	↓	port7			0.0.0.0 0.0.0.0	Physical Interface		root	0
	↓	port8			0.0.0.0 0.0.0.0	Physical Interface		root	0
		port13			0.0.0.0 0.0.0.0	Physical Interface	PING HTTPS SSH CAPWAP	WiFi	0
	↓	wan1			0.0.0.0 0.0.0.0	Physical Interface		root	0
	↓	wan2			0.0.0.0 0.0.0.0	Physical Interface		root	0
VDOM Link (3)									
		root_proxy				VDOM Link		root, Proxy	0
		root_proxy0			10.3.252.241 255.255.255.240	VDOM Link Interface	PING	root	3
		root_proxy1			10.3.252.242 255.255.255.240	VDOM Link Interface	PING	Proxy	2
WiFi (3)									
		intf-privado (SSID: privada)	6		N/A	WiFi SSID		WiFi	2
		invitados_porta (SSID: Enap_invitados)			172.31.243.1 255.255.255.0	WiFi SSID	PING	WiFi	6
		nps2 (SSID: Enap_privado)			10.3.244.1 255.255.255.0	WiFi SSID	PING	WiFi	5

Los pool´s de direcciones se encuentran en los servidores DHCP respectivos:



Configuracion Ruteo por Capa 3: Remitirse al documento

- **\\192.168.1.17\privado$\TI\ActiveSec - Proyecto Remediación\Informe del Proyecto\CNP_CIPETROL_ANEXO ROUTING 2018**

4.1.3 Recomendaciones:

4.2 Realizar las adecuaciones para utilizar otro puerto de backup en caso de falta en el puerto que está en uso

4.2.1 Acciones:

- Configuración port channel en cada uno de los switch
- Pruebas de puertos de backup y continuidad de servicio

4.2.2 Datos y Evidencias:

A continuación de detallan los portchannel que se tienen actualmente:

- Portchannel entre CORE-STACK-3850 y Fortigate 200D VDOM ROOT, contra Master y Slave
- Portchannel entre CORE-STACK-3850 y Fortigate 200D VDOM WIFI, contra Master y Slave
- Portchannel entre CORE-STACK-3850 y Switch siparbuesw05 previo a la migración de equipos al Stack, para que se tenga mayor capacidad.

CORE-STACK-3850#show etherchannel summary
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2

U - in use f - failed to allocate aggregator

M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port

Number of channel-groups in use: 5
Number of aggregators: 5

Group	Port-channel	Protocol	Ports
11	Po11(SU)	LACP	Gi8/0/43(P) Gi8/0/44(P) Gi8/0/45(P) Gi8/0/46(P)
12	Po12(SU)	LACP	Gi7/0/43(P) Gi7/0/44(P) Gi7/0/45(P) Gi7/0/46(P)
21	Po21(SU)	LACP	Gi8/0/38(P) Gi8/0/39(P) Gi8/0/40(P)
22	Po22(SU)	LACP	Gi7/0/38(P) Gi7/0/39(P) Gi7/0/40(P)
99	Po99(SU)	LACP	Gi4/0/45(P) Gi4/0/46(P) Gi4/0/47(P) Gi4/0/48(P)

CORE-STACK-3850#show run int po11
Building configuration...

Current configuration : 135 bytes
!
interface Port-channel11
description PortChannel Fortigate Primario
switchport trunk allowed vlan 1,99
switchport mode trunk
end

CORE-STACK-3850#show run int po12
Building configuration...

Current configuration : 133 bytes
!
interface Port-channel12

```
 description PortChannel Fortigate Backup
 switchport trunk allowed vlan 1,99
 switchport mode trunk
end

CORE-STACK-3850#show run int po21
Building configuration...

Current configuration : 138 bytes
!
interface Port-channel21
 description PortChannel FortiWiFi Primario
 switchport trunk allowed vlan 1,6,999
 switchport mode trunk
end

CORE-STACK-3850#show run int po22
Building configuration...

Current configuration : 140 bytes
!
interface Port-channel22
 description PortChannel FortiWiFi Secundario
 switchport trunk allowed vlan 1,6,999
 switchport mode trunk
end

CORE-STACK-3850#show run int po99
Building configuration...

Current configuration : 97 bytes
!
interface Port-channel99
 description Interfaz LACP a siparbuesw05
 switchport mode trunk
end
```

4.2.3 Recomendaciones:

4.3 Realizar las adecuaciones para utilizar acceso SSH (secure shell) encriptado

4.3.1 Acciones:

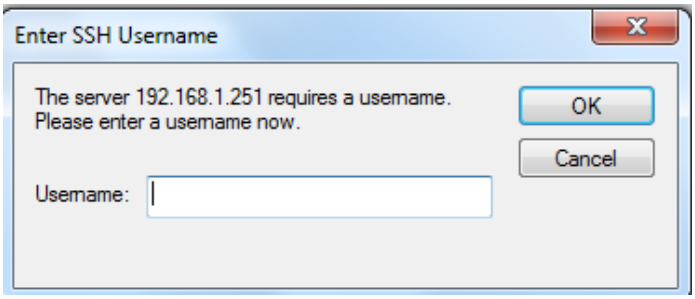
- Configuración de acceso por secure shell a los switchs
- Cancelación la configuración para acceder por telnet
- Pruebas de acceso por shh a los equipos

4.3.2 Datos y Evidencias:

Se implementa acceso SSH para todos los dispositivos Firewalls y CORE stack Cisco en la red de CNP.

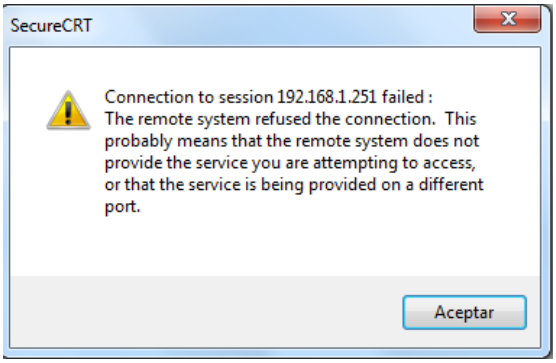
Ingreso al Fortigate:200D por SSH:

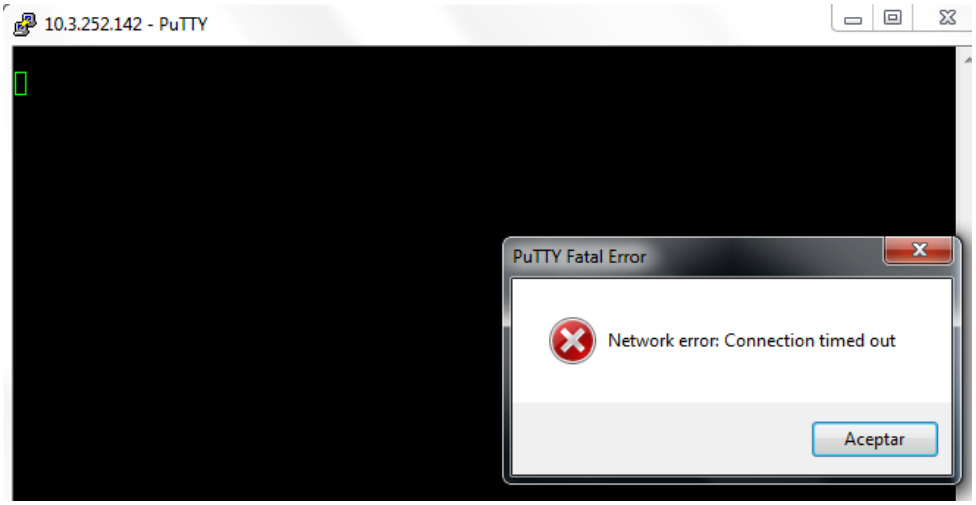
Ingreso al Core Cisco por SSH:



Denegación al acceer por telnet:

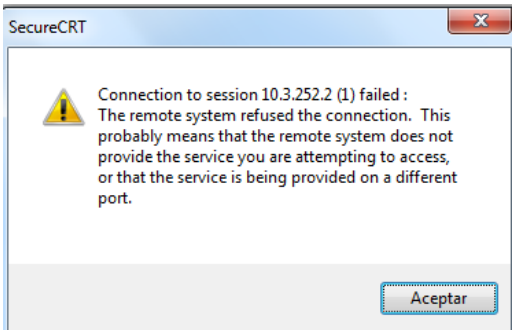
Compañía Nacional del Petróleo

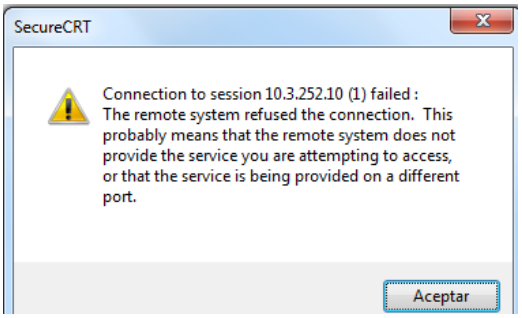




4.3.3 Recomendaciones: se le sugiere a los proveedores configurar los routers y equipos ara acceder solo por SSH:

Compañía Nacional del Petróleo





4.4 Realizar las adecuaciones para no utilizar la vlan nativa para tráfico de red

4.4.1 Acciones:

- Configuración de VLAN para gestión de dispositivos de red
- Asignación de direcciones ip de la nueva vlan a los dispositivos
- Pruebas de acceso

4.4.2 Datos y Evidencias:

Se tiene configurada la vlan 1 con direccionamiento 192.168.1.0/24 y 10.3.254.0/24, donde se encuentra el Stack Core 3850 y el Firewall Fortinet 200D donde se encuentran los vdom root, wifi y proxy:

Prefijo	Red		Uso	Rango Asignado	Máscara	Bits	VLAN ID
192.168	1	0	Servers		255.255.255.0	24	1
10.3	254	0	Networking		255.255.255.0	24	**1**

interface Vlan1
ip address 10.3.254.1 255.255.255.0 secondary
ip address 192.168.1.249 255.255.255.0 secondary

ip address 192.168.1.186 255.255.255.0 secondary
ip address 192.168.1.6 255.255.255.0 secondary
ip address 192.168.1.251 255.255.255.0
end

4.4.3 Recomendaciones:

4.5 Realizar las adecuaciones para asignar una red exclusiva para las impresoras

4.5.1 Acciones:

- Configurar VLAN para impresoras y asignar puertos
- Configurar la nueva dirección IP en las impresoras
- Pruebas de funcionamiento

4.5.2 Datos y Evidencias:

Se configura la vlan para impresoras:

CORE-STACK-3850#show run int vlan 1234
Building configuration...

Current configuration : 92 bytes
!
interface Vlan1234
 description Red_Impresoras
 ip address 10.3.234.1 255.255.255.0
end

Se prueba desde el Server en la red **192.168.1.0,** se alcanza correctamente

PS C:\Users\jvallejo> ping 10.3.234.1

Pinging 10.3.234.1 with 32 bytes of data:
Reply from 10.3.234.1: bytes=32 time=2ms TTL=255
Reply from 10.3.234.1: bytes=32 time=3ms TTL=255
Reply from 10.3.234.1: bytes=32 time=2ms TTL=255
Reply from 10.3.234.1: bytes=32 time=2ms TTL=255

Ping statistics for 10.3.234.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms

4.5.3 Recomendaciones:

Se deben migrar las impresoras actuales, actualizar el print server y aplicaciones relacionadas.

5 Etapa V - Protección de Redes Internas

5.1 Realizar las adecuaciones para que todo el tráfico entre redes de la empresa pase a través del firewall

5.1.1 Acciones:

- Adquisición de firewall UTM
- Ajustes de firewall UTM en la topología de red
- Ajustes de configuración en reglas de acceso
- Pruebas y testeos de conexión entre las distintas redes

5.1.2 Datos y Evidencias:

5.1.3 Recomendaciones:

Se implementa el vdom_root en el Fortigate 200_D, todo el tráfico entrante a la LAN en Buenos Aires, pasará por ahí, el acceso a servidores, de igual forma el tráfico saliente, internet, otras sedes etc.

Se implementan políticas para permitir los accesos necesarios, estas se mencionan en el documento anexo:

\\192.168.1.17\privado$\TI\ActiveSec - Proyecto Remediación\Informe del Proyecto\ CNP_CIPETROL_ANEXO 3 ROUTING.doc

Compañía Nacional del Petróleo

5.2 Aplicar IPS, AV, restricciones de ancho de banda para el tráfico LAN to LAN y LAN to WAN

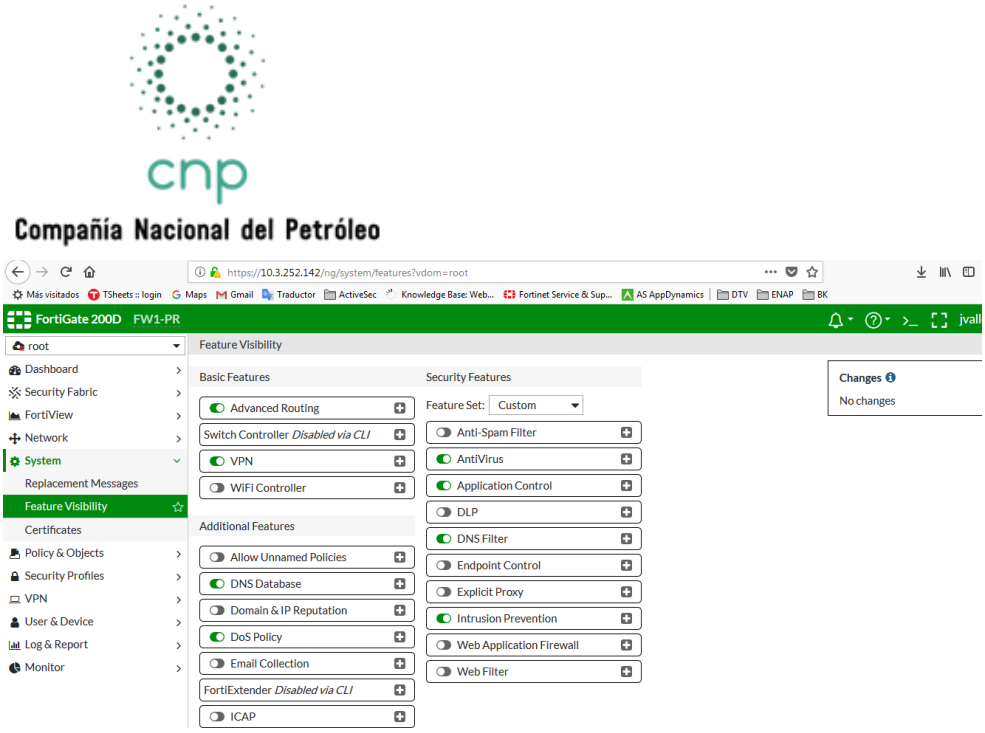
5.2.1 Acciones:

- Aplicación de IPS, AV, restricciones de ancho de banda para el tráfico LAN to LAN y LAN to WAN

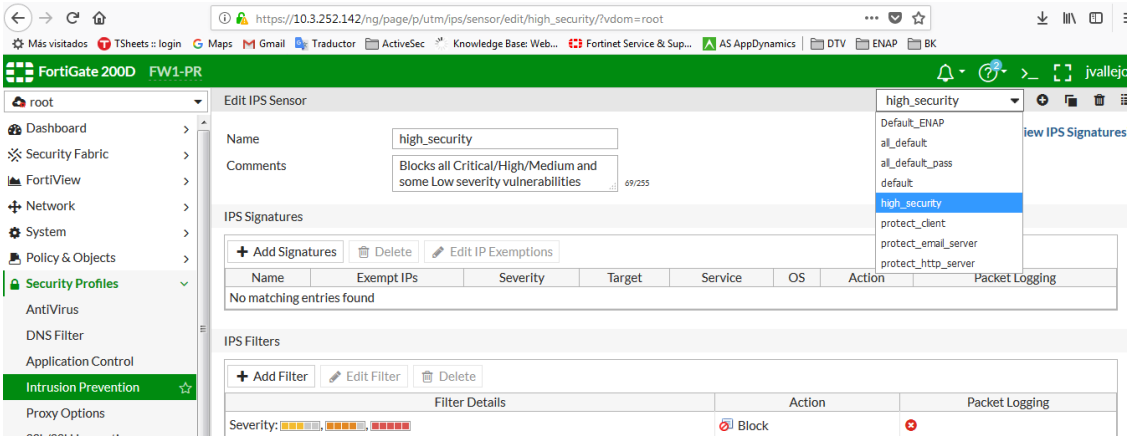
5.2.2 Datos y Evidencias:

Se implementa IPS en el Vdom_root del Fortigate 200D:

Se habilita el Feature respectivo:

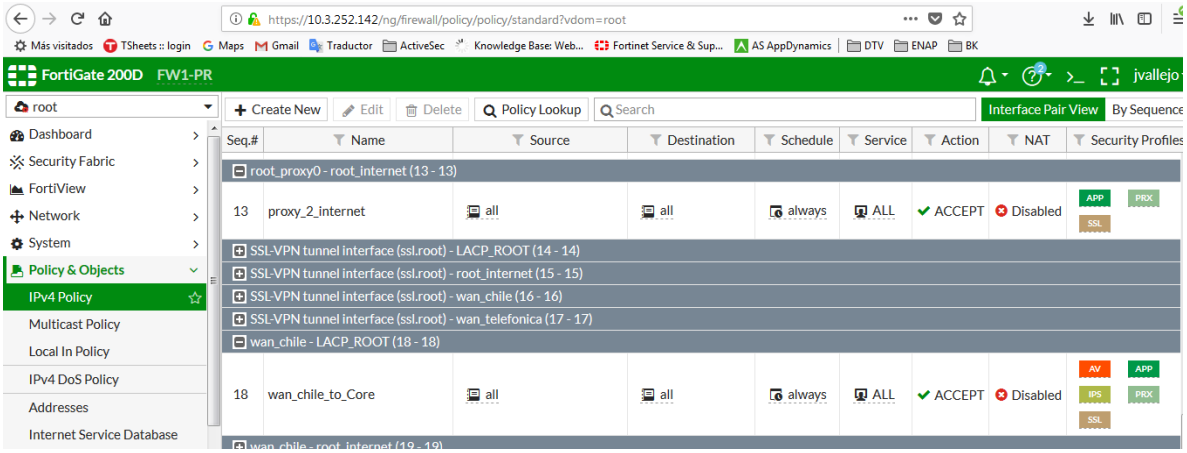


Se Crean siferentes perfiles para aplicar según corresponda:



En este momento se tiene habilitado el IPS para el tráfico entrante a Buenos Aires:

Compañía Nacional del Petróleo



Conf vdom
Edit root
config firewall policy
edit 4
set ips-sensor "Default_CNP"
end

edit 14
set ips-sensor "Default_CNP"
end

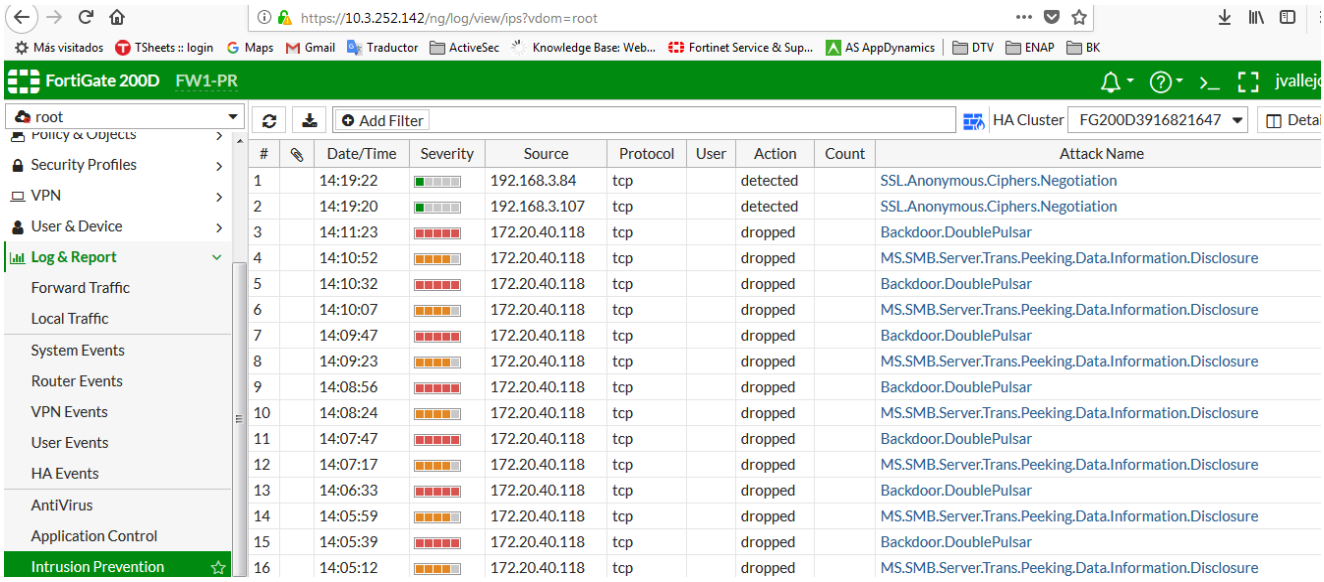
edit 2
set ips-sensor "Default_CNP"
end

edit 13
set ips-sensor "Default_CNP"
end

edit 17
set ips-sensor "Default_CNP"
end

end

- En el Firewall se pueden obervsar lo logs de eventos relacionados y la accion a tomar de acuerdo al perfil aplicado:



5.2.3 Recomendaciones:

5.3 Permitir el acceso a la infraestructura tecnológica solo desde la red de informática.

5.3.1 Acciones:

- Permiso de acceso a la infraestructura tecnológica solo desde la red de informática.

5.3.2 Datos y Evidencias:

Se implementa el vdom_root en el Fortigate 200_D, todo el tráfico entrante a la LAN en Buenos Aires, pasará por ahí, el acceso a servidores, de igual forma el tráfico saliente, internet, otras sedes etc.

Se implementan políticas para permitir los accesos necesarios, estas se mencionan en el documento anexo:

\\192.168.1.17\privado$\TI\ActiveSec - Proyecto Remediación\Informe del Proyecto\ CNP_CIPETROL_ANEXO 3 ROUTING.doc

Compañía Nacional del Petróleo

5.3.3 Recomendaciones:

6 Etapa VI - Webfiltering, Antispam y Procedimientos

6.1 Implementar un esquema de WebFiltering en alta disponibilidad

6.1.1 Acciones:

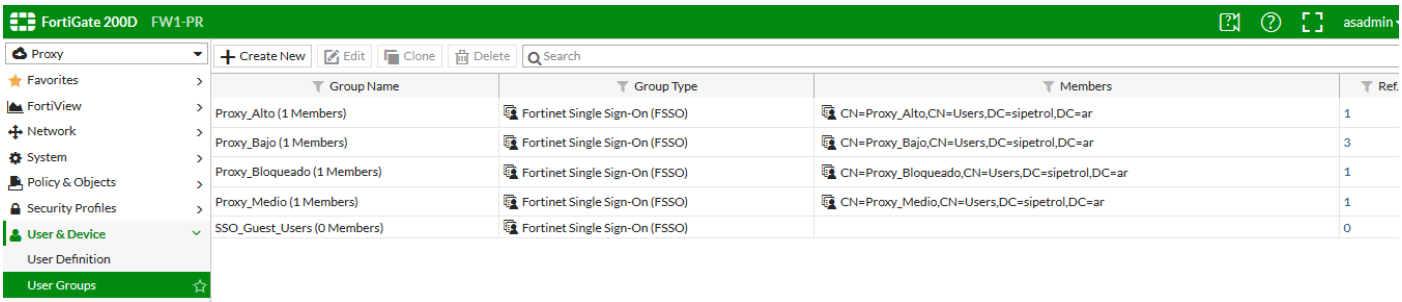
- Adquisición de firewall UTM (con funcionalidad de WebFilter)
- Configuración inicial del equipo y del servicio de webfiltering
- Relevamiento de configuración del WebSense
- Migración de configuración al nuevo equipo
- Pruebas del servicio de Webfiltering

6.1.2 Datos y Evidencias:

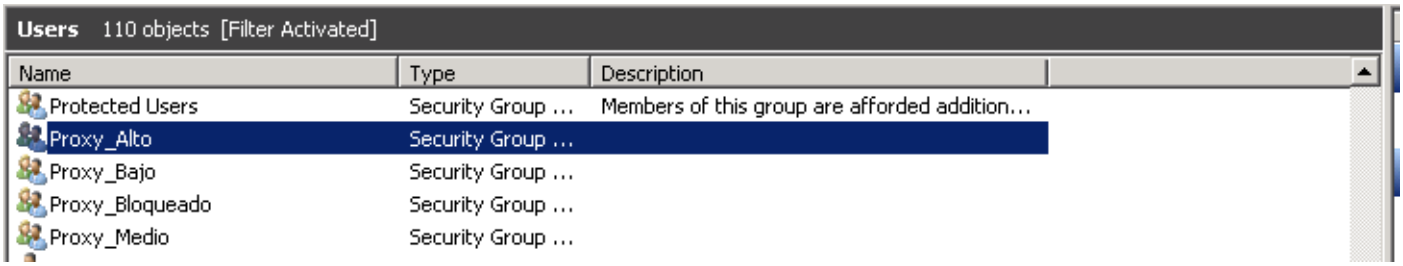
Se creó un Vdom de proxy (Se configura Proxy Explícito) en el Fortigate 200D, allí se habilitó la funcionalidad de webfiltering, a continuación se describen las políticas y configuración realizadas:

Compañía Nacional del Petróleo

- Se crean 4 grupos en el Fortigate, para identificar a los usuarios:

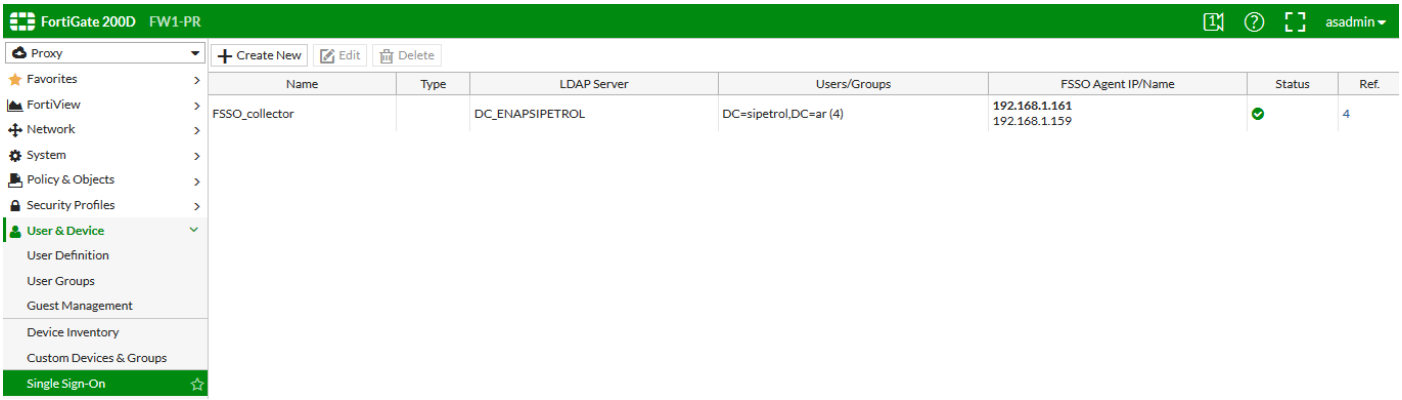


De igual forma, se tienen 4 grupos definidos en el Active Directory:

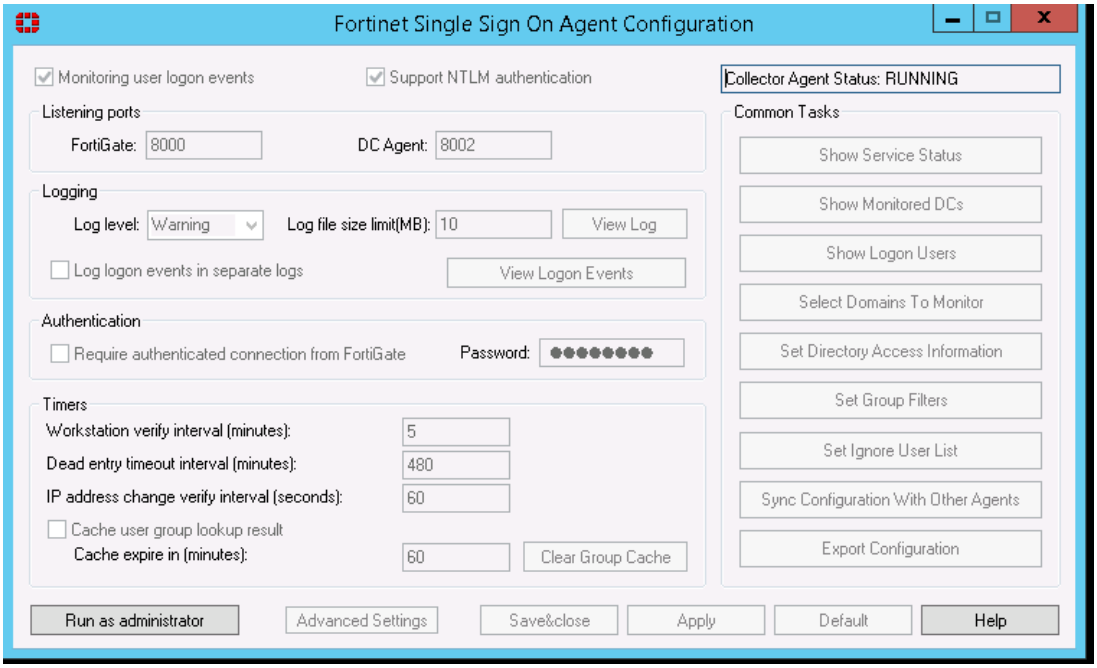


Ahora la forma en que se relacionan es la siguiente:

Desde el Fortigate mediante FSSO: Se consulta a los servidores NPS 10.161.1.158 y 10.161.1.161

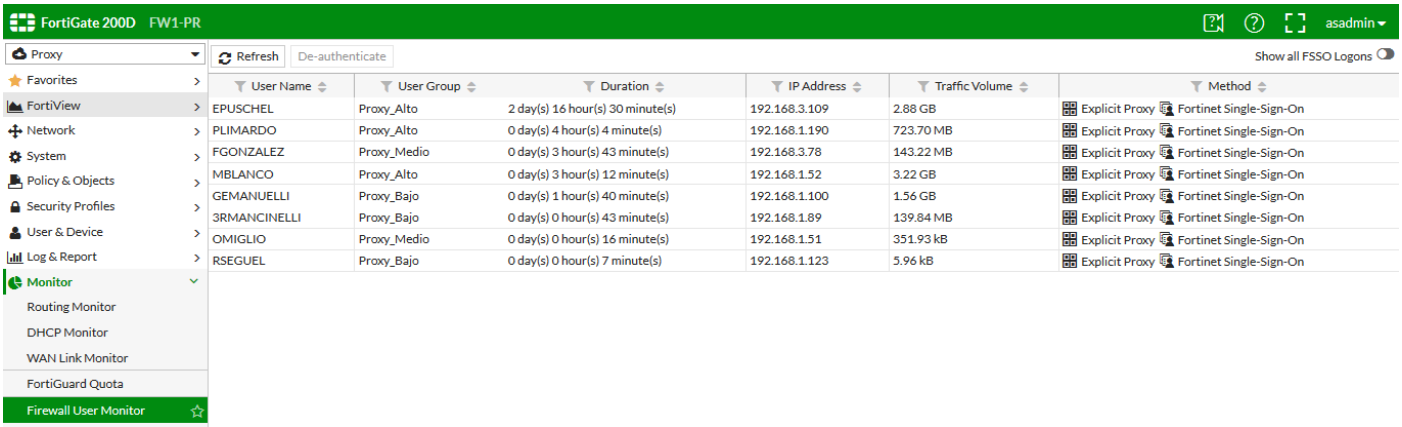


A su vez en este servidor se tiene configurado el Agente FSSO Collector, el cual escanea los usuarios que cuentan con sesión activa en el Directorio Activo.

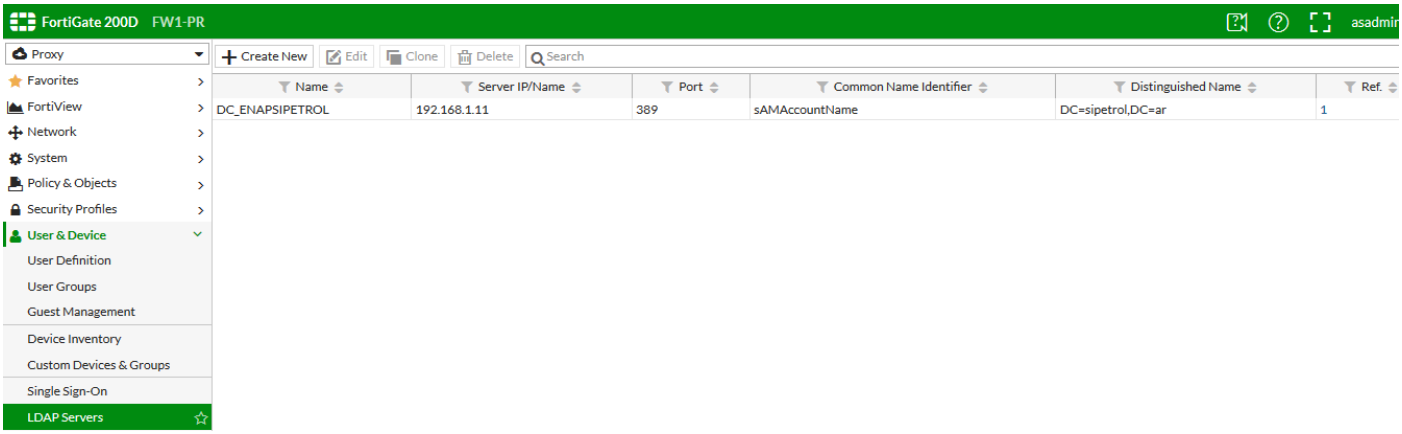


Para validar los usuarios que se encuentran activos, lo puedo hacer en la opcion Firewall Users monitor; allí me arroja la informacion de usuaros, grupo al que pertenece, tiempo de conexión, direccion ip y demás datos requeridos.

Compañía Nacional del Petróleo

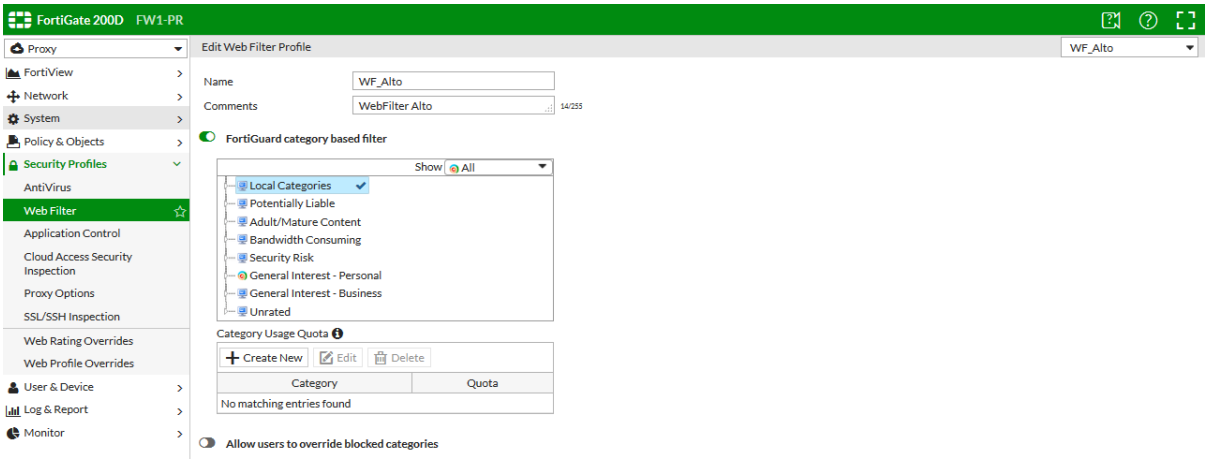


El fortigate vdom Proxy también llama al AD por LDAP, para tarer la demás información requerida:

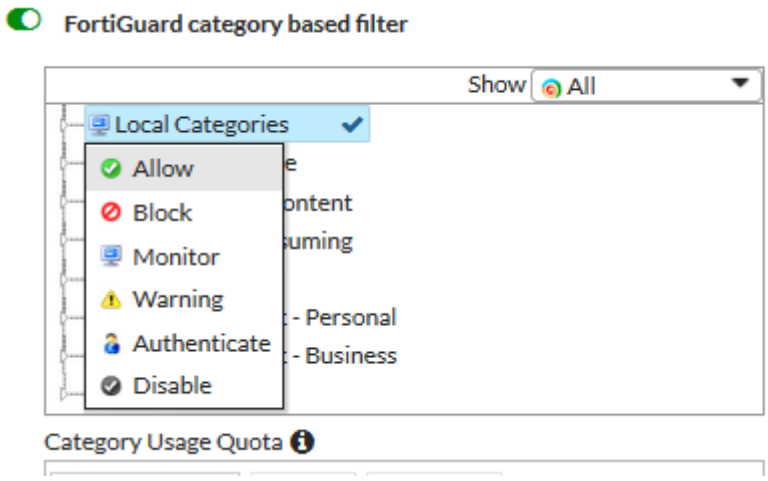


- se observan los perfiles creados, en el menú que despliega en la parte superior derecha:

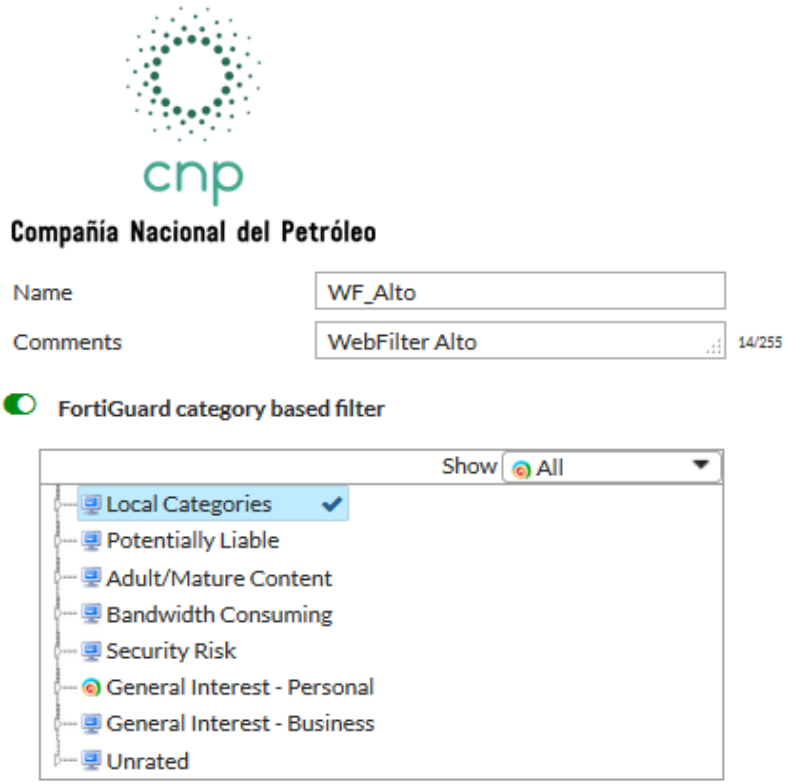
Compañía Nacional del Petróleo



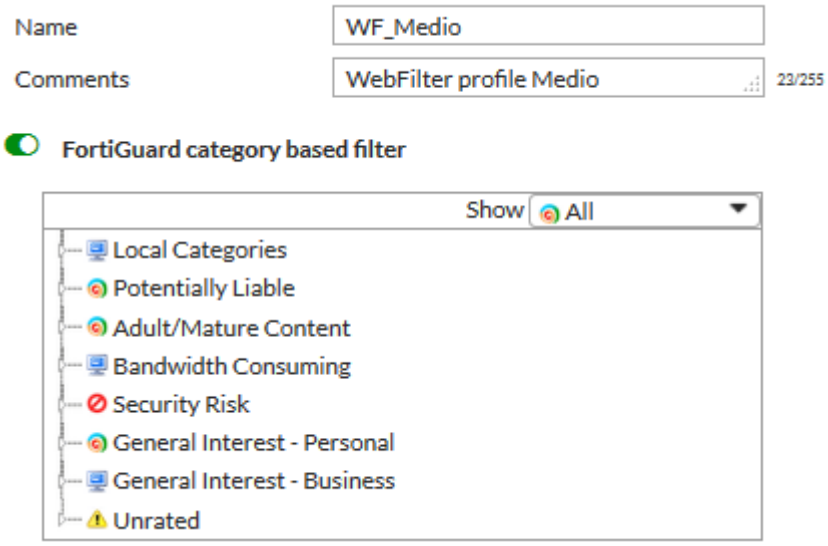
- Ahora en webfiltering, podemos definir en cada categoría la acción a tomar, ya sea permitir, resringuir, insertar warning o permitir:



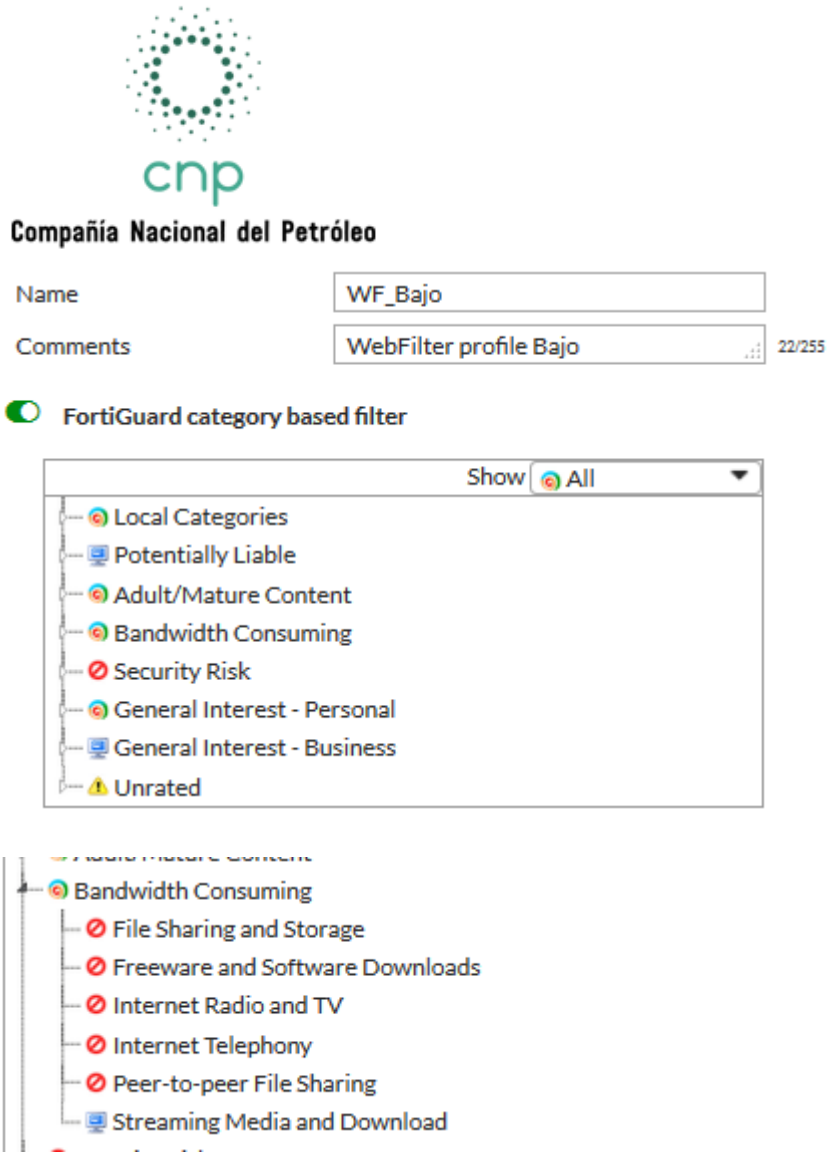
Profile WebFilter Alto: Cuenta con todas las categorias en modo Monitor, solo reatrea la navegación pero permite el acceso a todas las categorias:



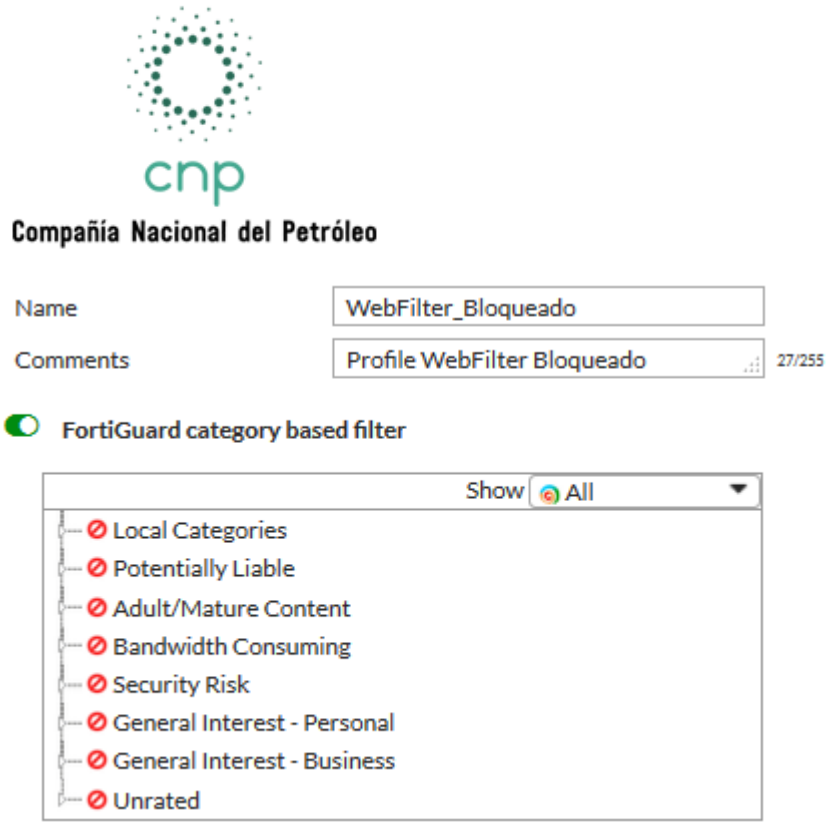
Profile WEbfilter medio: Se restingue la categoria riesgos de seguridad y la navegacion es un poco mas restringuida:



Profile WEbfilter bajo: Se encuentra mas restringuido aún, ya que son usuarios que no requiern acceso total y se debe evitar generar tráfico innecesario.



Profile WEbfilter Bloqueado: no puede navegar, todas las categorias restringuidas:



Se debe desplegar en todos los navegadores el proxy para proceder con el filtrado web, reatrear el tráfico y evitar accesos indebidos y saturación

6.1.3 Recomendaciones:

Se puede encontrar el detalle de configuración de proxy y funcionamiento en el siguiente anexo:

\\192.168.1.17\privado$\TI\ActiveSec - Proyecto Remediación\Informe del Proyecto\ CNP_CIPETROL_ANEXO 2 PROXY V2.doc

6.2 Desarrollar las directrices de un procedimiento backup y control de cambios sobre el equipamiento de TI

6.2.1 Acciones:

- Indicación de recomendaciones para generar un procedimiento de backup
- Indicación de recomendaciones para generar un procedimiento de control de cambios

6.2.2 Datos y Evidencias:

Se generan los respectivos procedimientos:

6.2.3 Recomendaciones:

6.3 Implementar un esquema de Antispam en alta disponibilidad

6.3.1 Acciones:

- Gestión la adquisición del equipamiento
- Configuración inicial del equipamiento
- Relevamiento de configuración actual
- Migración de configuración
- Pruebas de servicio

6.3.2 Datos y Evidencias:

6.3.3 Recomendaciones: Esta parte queda a consideración de CNP

6.4 Desarrollar las directrices de un procedimiento diferencial para el ABM de cuentas de administrador de domino

6.4.1 Acciones:

- Indicar recomendaciones para generar un procedimiento para ABM de cuentas de administrador de dominio

6.4.2 Datos y Evidencias:

Se generan los respectivos procedimientos:

\\192.168.1.17\privado$\TI\ActiveSec - Proyecto Remediación\Procedimientos

6.4.3 Recomendaciones:

7 Etapa VII - RED WiFi, MPLS y Backup Satélital

7.1 Implementar cifrado WPA2 o WPA2/Enterprise, SSID Corporativo y SSID Invitados, ajustes de seguridad

7.1.1 Acciones:

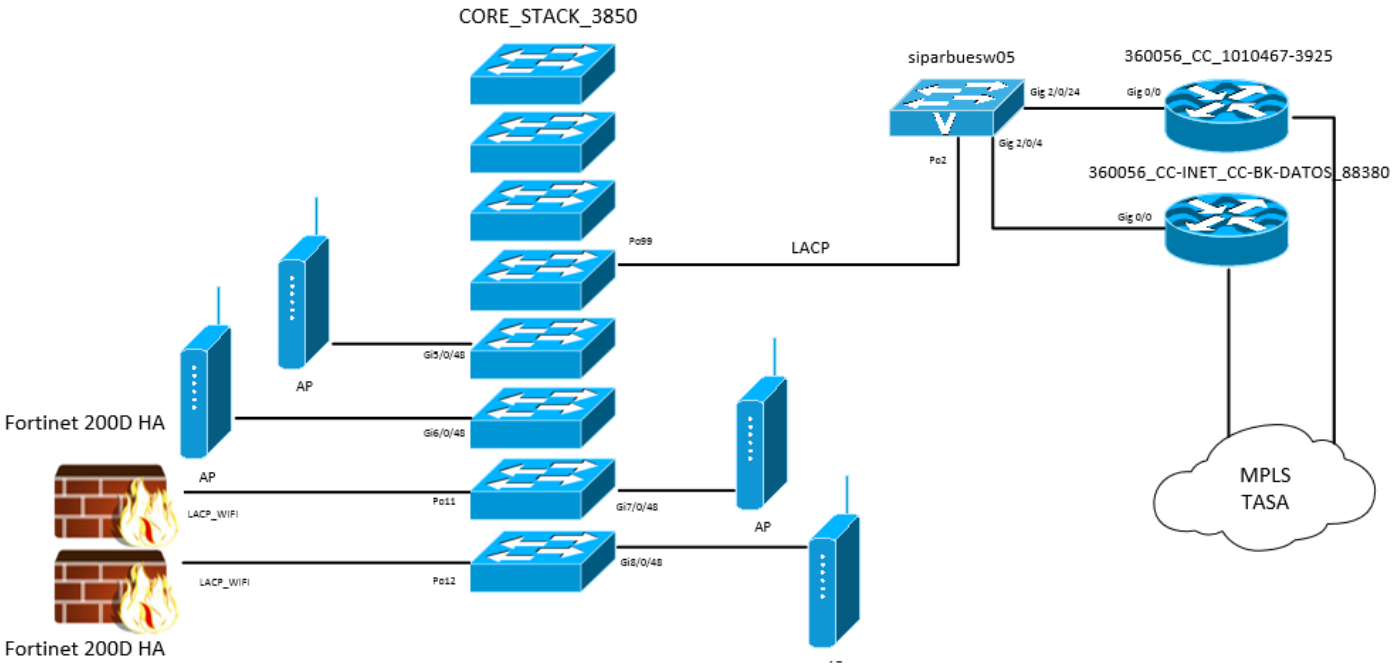
- Sincronizar wireless controller con usuarios active directory

Compañía Nacional del Petróleo

- Configurar cifrado WPA2/Enterprise con autenticación para SSID Corporativo
- Configurar cifrado WPA2
- Definir red vlan de red WiFi corporativa y vlan de red WiFi invitados
- Ajustes en red LAN
- Documentación, pruebas y test de conexión

7.1.2 Datos y Evidencias:

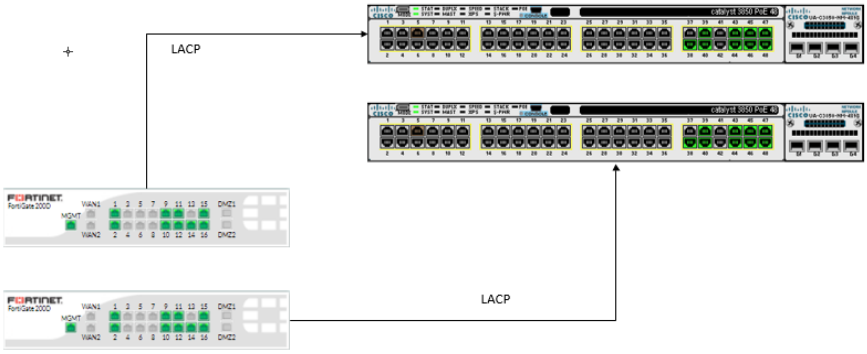
Despliegue Red Wifi:



La conexión desde El Fortigate 200D hacia el Core Cisco 3850, se realiza simetricamente, mediante portchannel:

Fortinet 200D MASTER (LACP_WIFI: port 14, port 15, port 16) → CORE_STACK_3850 (po11)

Fortinet 200D SLAVE (LACP_WIFI: port 14, port 15, port 16) → CORE_STACK_3850 (po12)



CORE-STACK-3850#show run int po11
Building configuration...

Current configuration : 135 bytes
!
interface Port-channel11
description PortChannel Fortigate Primario
switchport trunk allowed vlan 1,99
switchport mode trunk
end

CORE-STACK-3850#show run int po12
Building configuration...

Current configuration : 133 bytes
!
interface Port-channel12
description PortChannel Fortigate Backup
switchport trunk allowed vlan 1,99
switchport mode trunk
end

En la troncal se permite la vlan de Wifi e invitados:

Vlan 1: Nativa
Vlan 6: Datos Wireless
Vlan 999: Wifi Invitados.

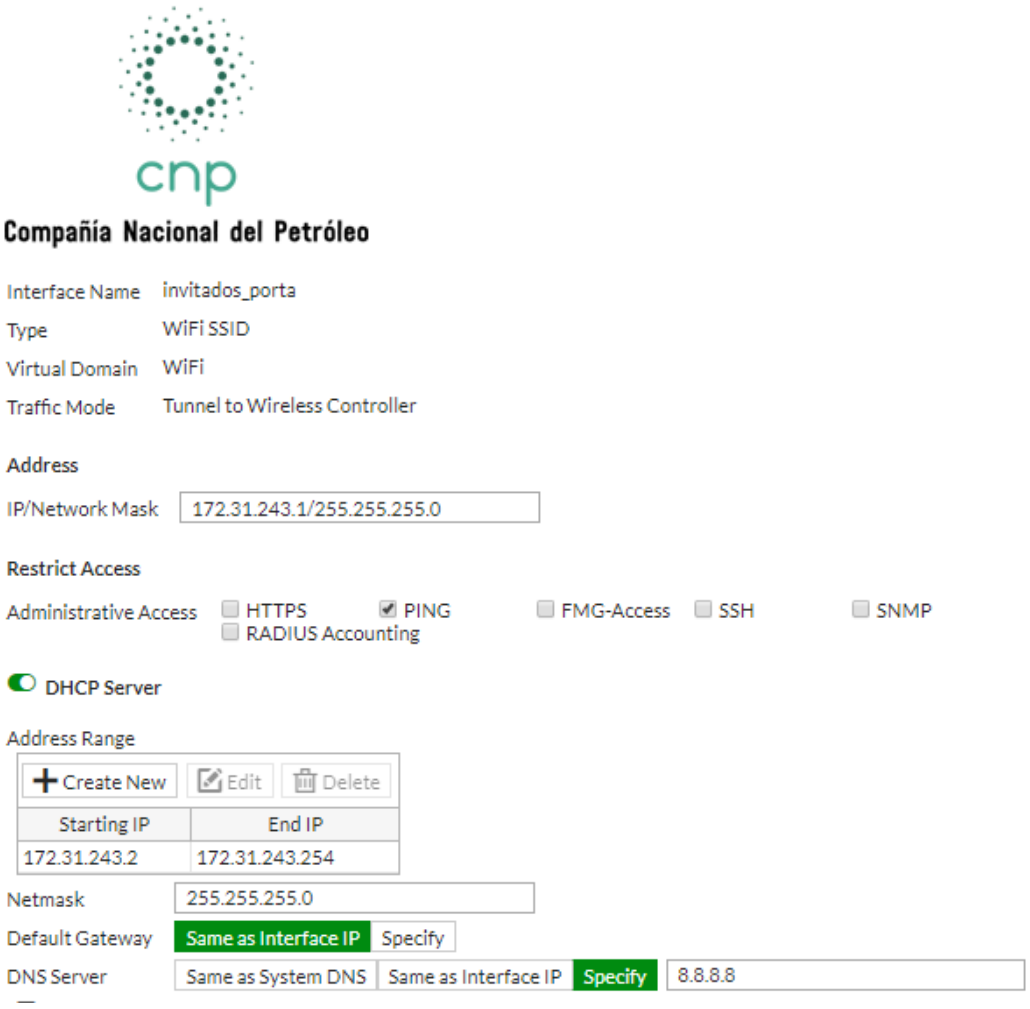
Se tienen 4 APS Configurados en el Fortigate 200D:

Access Point	State	Connected Via	SSIDs	Channel	Clients
FP223C3X17000408	✔	10.3.254.24	Radio 1: new_invitados, privada, portal, nps2 Radio 2: new_invitados, privada, portal, nps2	Radio1: 1 Radio2: 149	Radio 1: 15 Radio 2: 0
FP223C3X17000671	✔	10.3.254.23	Radio 1: new_invitados, privada, portal, nps2 Radio 2: new_invitados, privada, portal, nps2	Radio1: 1 Radio2: 52	Radio 1: 7 Radio 2: 0
FP223C3X17003199	✔	10.3.254.22	Radio 1: new_invitados, privada, portal, nps2 Radio 2: new_invitados, privada, portal, nps2	Radio1: 6 Radio2: 149	Radio 1: 9 Radio 2: 0
FP223C3X17003238	✔	10.3.254.21	Radio 1: new_invitados, privada, portal, nps2 Radio 2: new_invitados, privada, portal, nps2	Radio1: 11 Radio2: 161	Radio 1: 18 Radio 2: 0

La conexión contra los AP, se encuentra en los siguientes puertos:

CORE-STACK-3850#show int desc | inc Access
Gi5/0/48 up up Conexion Access Point, IP: 10.3.254.23
Gi6/0/48 up up Conexion Access Point, IP: 10.3.254.21
Gi7/0/48 up up Conexion Access Point, IP: 10.3.254.22
Gi8/0/48 up up Conexion Access Point, IP: 10.3.254.24

Se define el SSID ***CNP_invitados*** se tiene configurado el Scope DHCP 172.31.243.0/24, se asigna Direccionamiento desde la 172.31.243.2 hasta 172.31.243.254



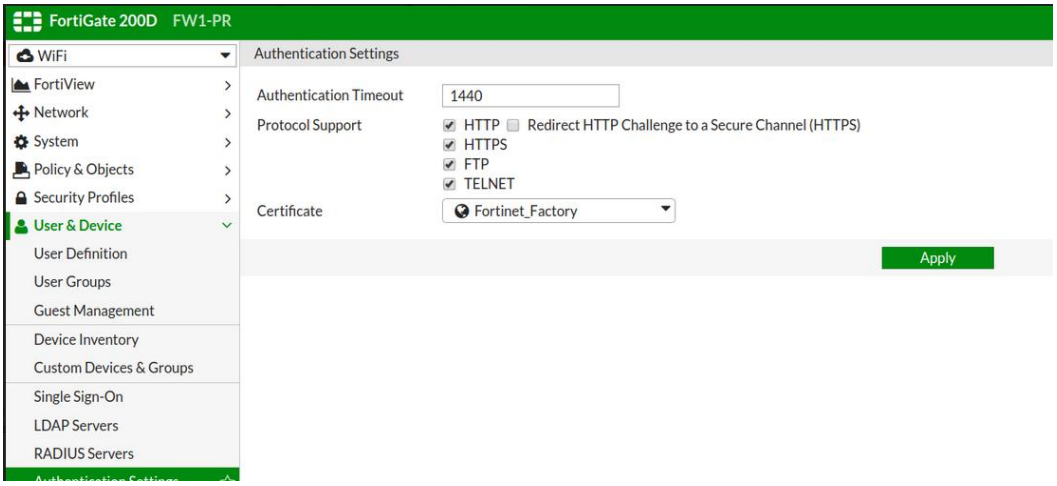
Se prueba la red de Invitados GUEST en el VDOM de Wifi, después de la intervención de TASA habilitando en su router la salida hacia Internet mediante la interfaz requerida; Se define el acceso a esta red mediante Captive portal, Además se podrán autenticar dispositivos Móviles mediante Usuario de AD

Interface Name	SSID	Traffic Mode	Security Mode
SSIDs (4)			
intf-invitados	new_invitados	Tunnel	WPA2 Personal
intf-privado	privada	Local Bridge	WPA2 Personal
invitados_porta	portal	Tunnel	Captive Portal
nps2	nps2	Local Bridge	WPA2 Enterprise

Este es el banner que arrojará a los usuarios invitados autorizados:

Compañía Nacional del Petróleo

Se define un tiempo de un 24 hrs en el Captive portal:



- Se genera politica de traffic Shaping, sobre la red de invitados:
  20Mbps tráfico de recepcion
  5 Mbps tráfico de transmisión:

Name	Type	Guaranteed Bandwidth	Max Bandwidth	Bandwidth Utilization	Dropped Bytes	Priority	Ref.
5MB	Shared		5000 Kbps	0 bps	2.34 MB	High	1
20MB	Shared		20000 Kbps	0 bps	6.02 MB	High	1

cnp

Compañía Nacional del Petróleo

Matching Criteria

Source	all
Destination	all
Service	ALL

Apply shaper

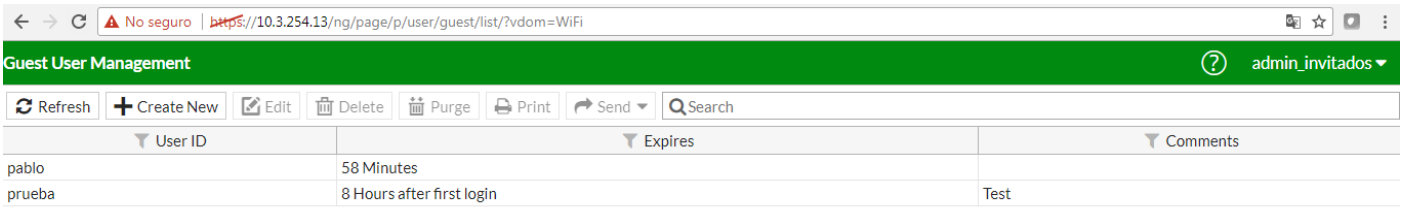
Outgoing Interface	WIFI_INVITADOS (port13)
Shared Shaper	5MB
Reverse Shaper	20MB
Per-IP Shaper	

Enable this policy

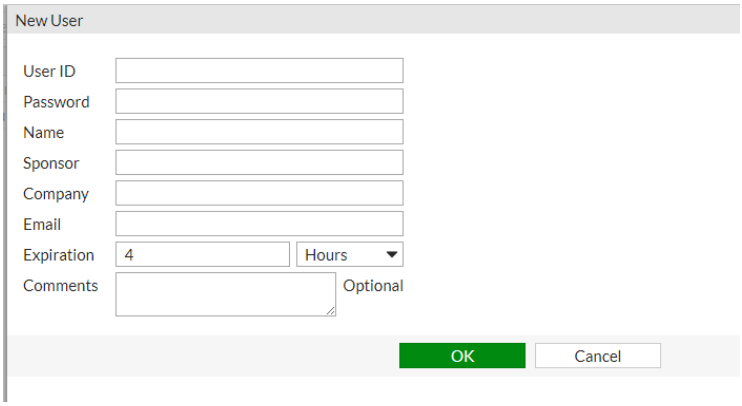
Se realiza tests de velocidad confirmando el limite configurado:

La solicitud para conexión a la red wifi de invitados se tramitará mediante la mesa de ayuda, Se genera en el Firewall el usuario **admin_invitados**, El personal de mesa de servicio accederá mediante el siguiente link: https://portalinvitados.CIPETROL.ar/ o https://10.3.254.13

Compañía Nacional del Petróleo



Sólo cuentan con la posibilidad de crear usuarios y parámetros de la conexión wifi Guest;



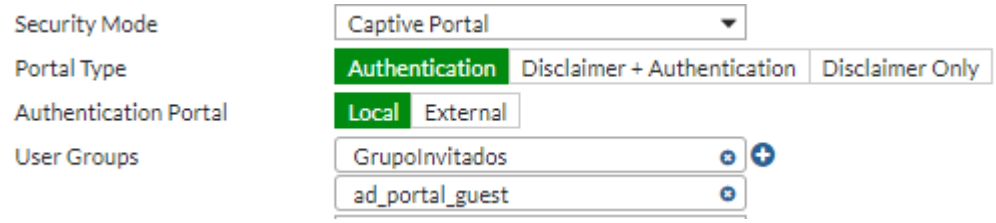
Al incluir la informacion de Email del sponsor, a él, le llegará un correo con la informacion de conexión requerida para el usuario:

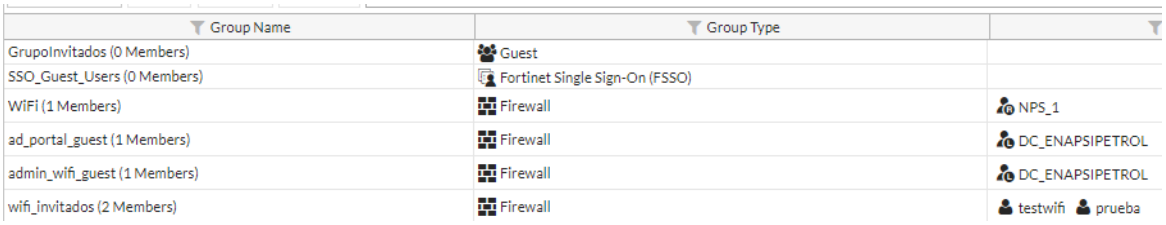
-----Mensaje original-----
De: forti@enapsipetrol.com.ar [mailto:forti@enapsipetrol.com.ar]
Enviado el: martes, 08 de agosto de 2017 11:51 a.m.
Para: Limardo, Pablo
Asunto: Guest User Account: prueba

User ID=prueba
Password=123456
Expires=Tue Aug 8 14:58:00 2017
User Name=Prueba
Mobile Phone=none
Sponsor=Prueba
Company=AS
Email=pablo.limardo-externo@enapsipetrol.com.ar

Compañía Nacional del Petróleo

- Para la autenticacion de usuarios, se consulta mediante LDAP el AD, alcanzando el grupo requerido para acceder al VDOM de wifi

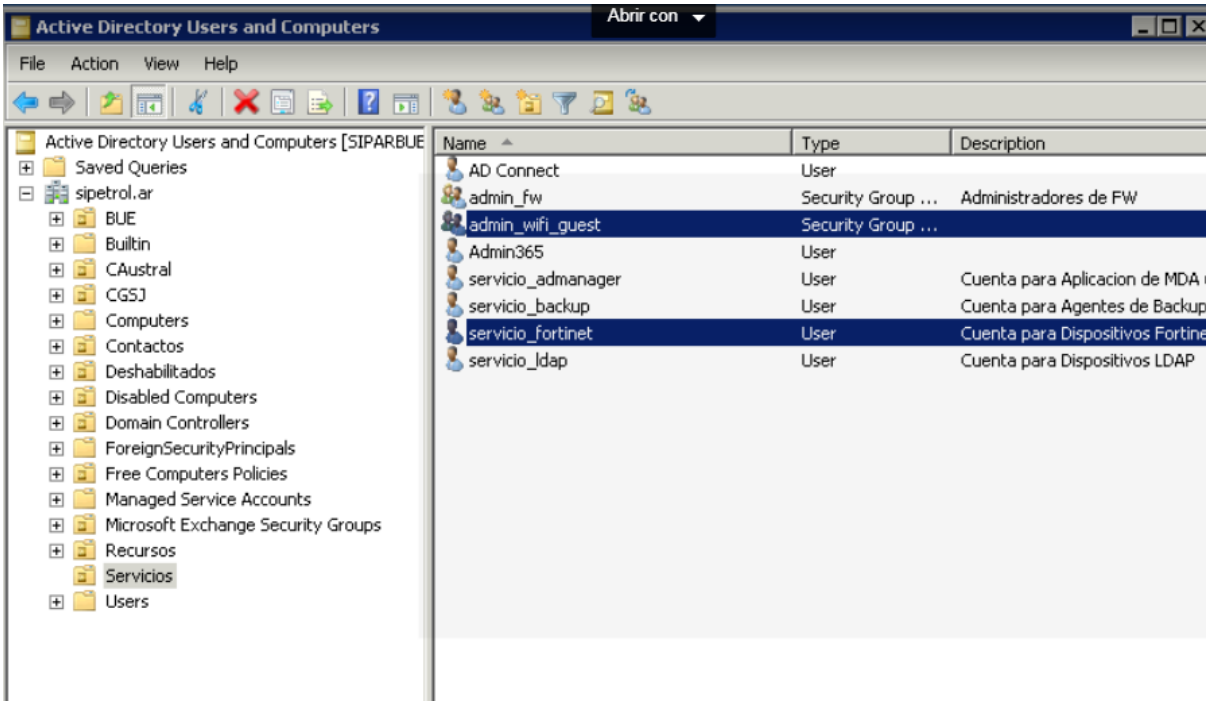




Group Name	Group Type	
GrupoInvitados (0 Members)	Guest	
SSO_Guest_Users (0 Members)	Fortinet Single Sign-On (FSSO)	
WIFI (1 Members)	Firewall	NPS_1
ad_portal_guest (1 Members)	Firewall	DC_ENAPSIPETROL
admin_wifi_guest (1 Members)	Firewall	DC_ENAPSIPETROL
wifi_invitados (2 Members)	Firewall	testwifi prueba

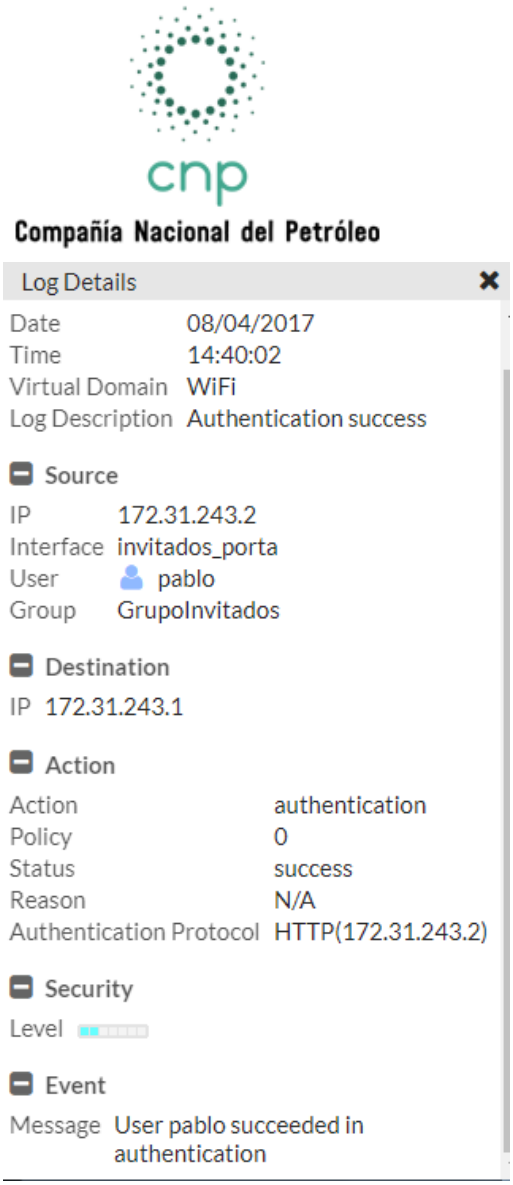
Por parte de CNP, en el Directorio activo podrán agregar los usuarios requeridos al grupo de gestion admin_wifi_guest, y así loguearse al Fortinet para la gestion de usuarios invitados.

Compañía Nacional del Petróleo



- Se valida la informacion en los logs del firewall, evidenciando todos los datos de conexión, ademas se realizan pruebas con el personal de soporte en sitio confirmando acceso correcto a internet

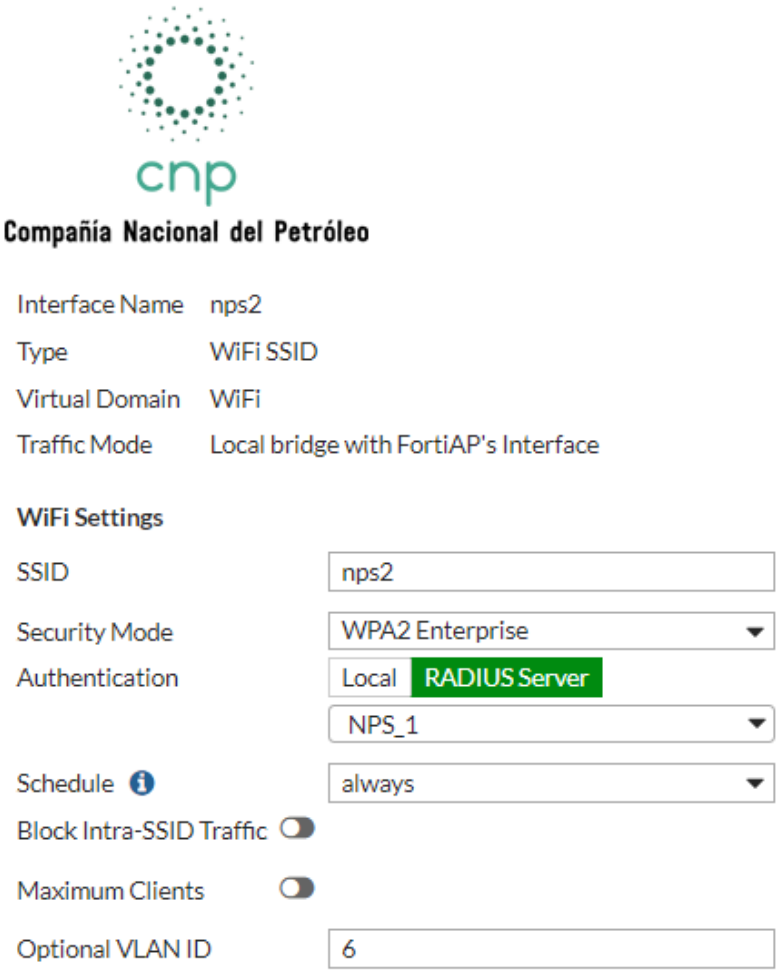
#	Date/Time	Level	User	Action	Messages	Group
1	16:11:43		pablo	authentication	User from 172.31.243.3 was timed out	GrupoInvitados
2	16:02:31		pablo	authentication	User pablo succeeded in authentication	GrupoInvitados
3	15:25:27		pablo	authentication	User from 172.31.243.3 was timed out	GrupoInvitados
4	15:02:16		pablo	authentication	User pablo succeeded in authentication	GrupoInvitados
5	15:01:41		pablo	authentication	User from 172.31.243.2 was timed out	GrupoInvitados
6	14:40:02		pablo	authentication	User pablo succeeded in authentication	GrupoInvitados
7	14:33:20		testwifi	authentication	User testwifi failed in authentication	N/A



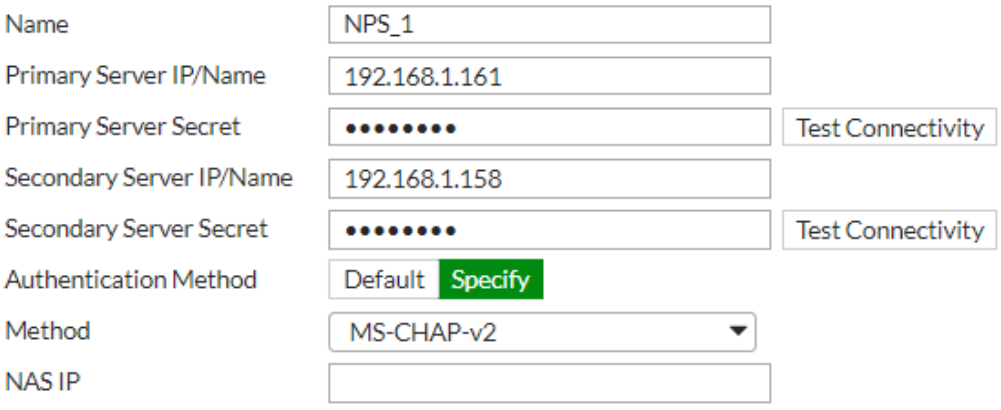
WIFI Corporativo:

Para el Acceso a Internet Corporativo, se configura un SSID ***CNP_privado*** con autenticacion por RADIUS:

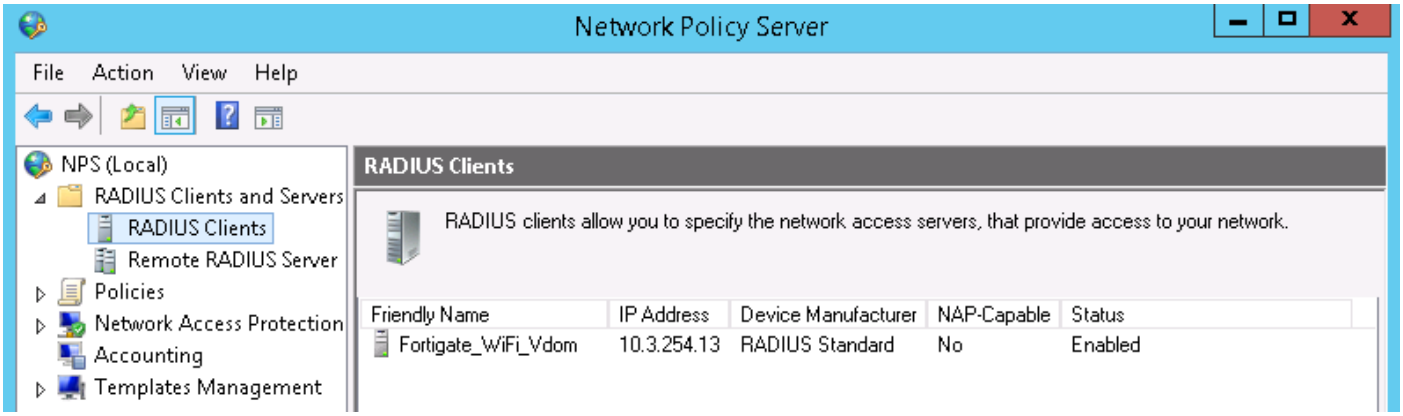
Compañía Nacional del Petróleo



El Firewall hace el llamado al RADIUS en el servidor de dominio donde se tiene configurado un NPS: 192.168.1.161 con Ip secundaria 192.168.1.158

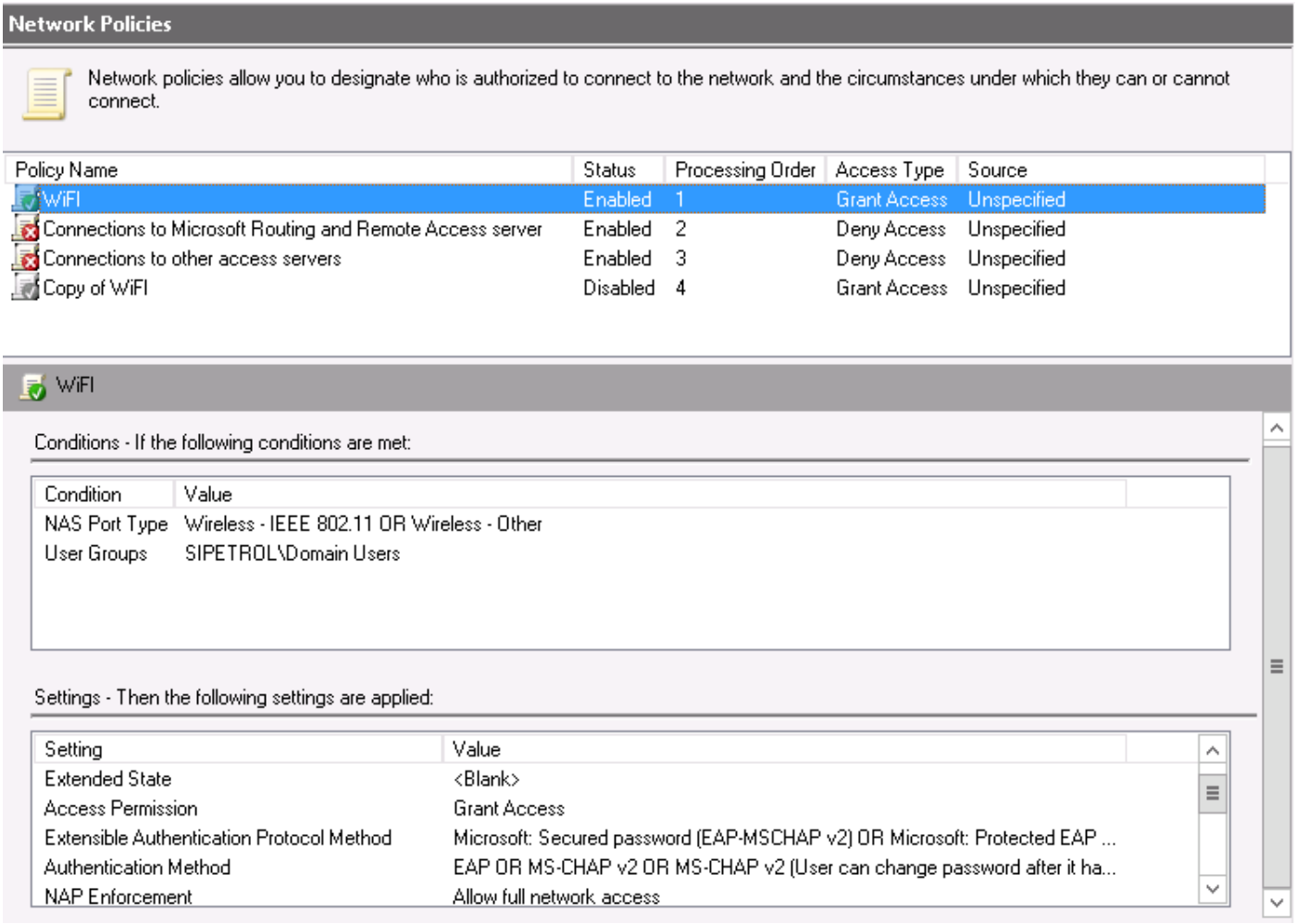


Compañía Nacional del Petróleo



Allí se tiene configurada la politica de red, donde se define el Metodo de autenticacion, y el grupo de usuarios del dominio desde donde se podrá acceder:

Compañía Nacional del Petróleo

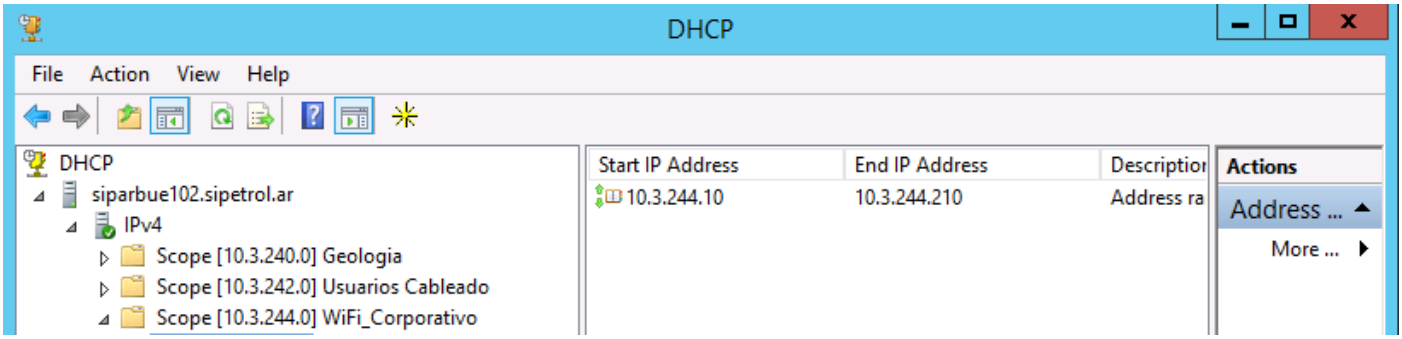


Se debe renovar el certificado para autenticación en la red Wifi corporativa, ya que si llegase a expirar, los usuarios perderán conectividad, esta es la fecha de expiración actual 09/12/2018

Para la asignacion de direcciones ip se tiene configurado un Pool dentro del servidor DHCP, el cual es llamado desde el VDOM de wifi del Firewall:

El segmento de red para los Usuarios de esta red es el siguiente: **10.3.244.0/24**

Compañía Nacional del Petróleo



- En cuanto a la red Wifi Corporativa se realizan pruebas de conexión en las instalaciones de CNP, atraves de usuario de dominio, donse se observa funcionamiento correcto.

7.1.3 Recomendaciones:

- Se debe renovar el certificado para autenticación en la red Wifi corporativa, ya que si llegase a expirar, los usuarios perderán conectividad, esta es la fecha de expiración actual 09/12/2018
- Se genera manual de gestión de red Wifi para personal de Soporte y mesa de ayuda en la siguiente ruta:

  \\192.168.1.17\privado$\TI\ActiveSec - Proyecto\Remediación\CNP_CIPETROL_Manual_Wifi.doc

- **El Anexo de configuracion de red Wifi se encuentra en la siguiente ruta: \\192.168.1.17\privado$\TI\ActiveSec - Proyecto Remediación\Informe del Proyecto \CNP_CIPETROL_ANEXO 4 WIFI.doc**

7.2 Desarrollar un procedimiento para implementar conmutación de enlace MPLS y Backup Satelital

7.2.1 Acciones:

- Desarrollo de directivas de un procedimiento para implementación de conmutación de enlace MPLS y Backup Satelital

7.2.2 Datos y Evidencias:

7.2.3 Recomendaciones: CNP, y proveedores analizan cambiar la solución

7.3 Interactuar con el proveedor y coordinar implementación de conmutación automática de enlace principal a enlace backup y viceversa

7.3.1 Acciones:

- Interacción con el proveedor y coordinación de implementación de conmutación automática de enlace principal a enlace backup y viceversa

7.3.2 Datos y Evidencias:

7.3.3 Recomendaciones: CNP, y proveedores analizan cambiar la solución

CNP Argentina S.A.

Propuesta de relevamiento y análisis de Servicios Básicos de Red y Seguridad Informática

Tycon tech

Objetivo

- Determinar el estado actual de las configuraciones de los servicios básicos de IT.
- Hallazgos de configuraciones que no estén alineados con las buenas prácticas recomendadas en el mercado de IT.
- Vulnerabilidades y riesgos existentes asociadas a la seguridad informática.

Alcance

- Relevamiento de la infraestructura informática de ES.
- Identificación de eventuales desvíos en la organización de la arquitectura de TI.
- Detección de desvíos en las configuraciones de los servicios básicos de la red.
- Análisis de los resultados.
- Identificación y cuantificación de los riesgos asociados a los desvíos.
- Propuesta de plan de acción para la corrección de las observaciones.
- Organización de las prioridades.

Etapa I - Grupo de trabajo, acuerdo de cronograma y definición de herramientas.

- **Tareas**
  - Presentación grupo de trabajo
  - Definición de contraparte ES
  - Propuesta cronograma
  - Requerimientos tareas relevamiento

- **Entregable Parcial**
  - Equipo de trabajo conformado
  - Cronograma de a tarea a nivel de detalle (GANTT)

Etapa II - Relevamiento de infraestructura IT

Relevamiento:

- Equipamiento seguridad Informática
- Conectividad WAN/LAN/WIFI
- Servicios Básicos de Red
- Aplicaciones
- Infraestructura Servidores Microsoft
- Infraestructura de Virtualización
- Infraestructura de Storage
- Procedimientos y Compliance

Entregable Parcial

- Inventario detallado de equipamiento de red LAN, WIFI, WAN, MAN y seguridad perimetral

Etapa III - Mapa y categorización de activos

Tareas

- Análisis de activos categorizados
- Análisis de recursos/activos relacionados a aplicaciones y servicios de negocio

Entregable Parcial

- Mapa de activos de IT para cada uno de los sitios.
- Sistemas críticos para el negocio.
- Sistemas fundamentales para realizar tareas diarias.

Etapa IV - Gap Análisis

Tareas

- Análisis de los puntos de desvíos detectados
- Categorización de criticidad y prioridad

Entregable parcial

- Mapa de activos especificando desvíos para activos críticos.

Etapa V - Propuesta de Mejoras

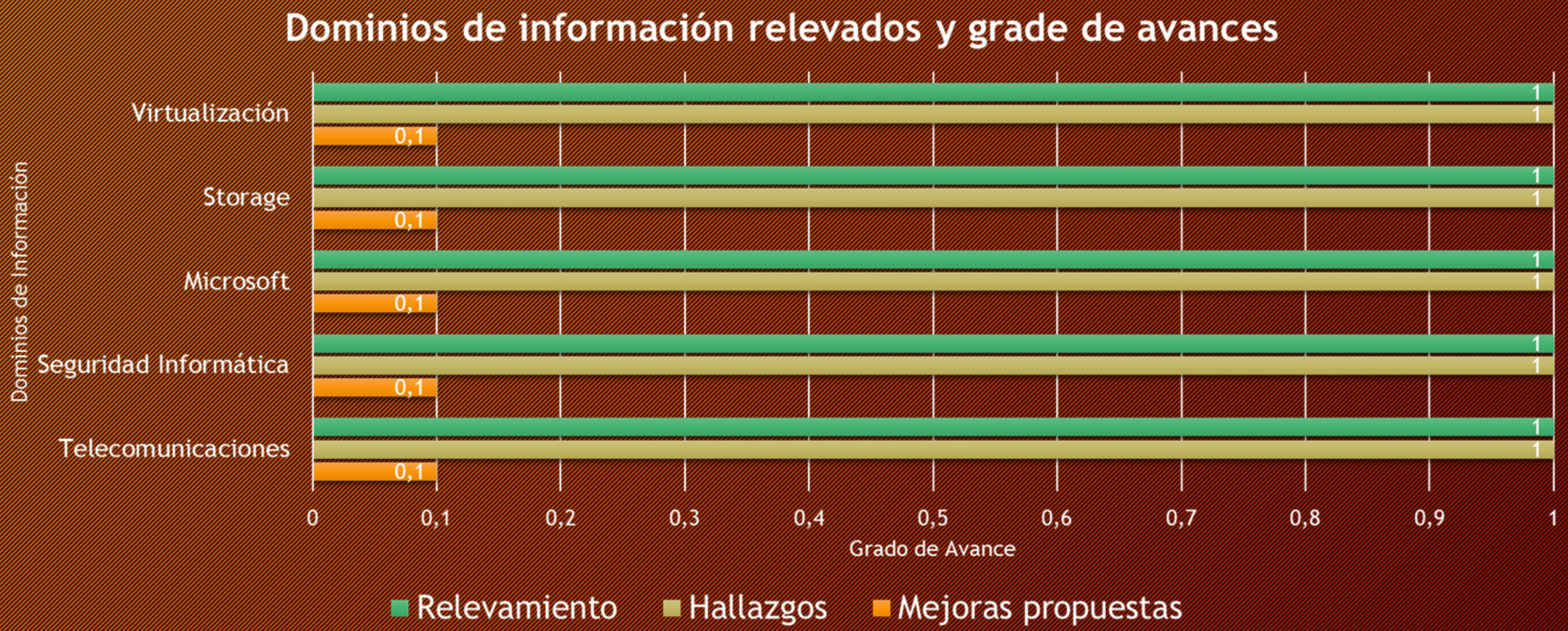
Tareas

- Análisis de propuestas de mejora para cada uno de los desvíos identificados

Entregable parcial

- Lista priorizada de vulnerabilidades encontradas, acciones correctivas y recomendaciones.
- Informe de networking, vulnerabilidades en red perimetral, redes internas cableadas e inalámbricas.
- Informe de virtualización, storage y tecnologías de Microsoft
- Alternativas de solución para mitigación de riesgos, de tal forma que ES pueda optar por la más conveniente para sus objetivos.

Dominios de información y grado de avances



Cantidad de hallazgos por domino de información

Criticidad	Infraestructura	Seguridad	Monitoreo	Networking
Alta	3	18	7	21
Media	5	14	0	18

Criticidad	Microsoft	Virtualización	Storage
Alta	18	10	12
Media	6	6	5

CNP – Arquitectura – Conexión WAN L3 - Of. CABA