Gobierno Regional Junín

¡Trabajando con la fuerza del pueblo!

RESOLUCIÓN GERENCIAL GENERAL REGIONAL

N° 144 -2020-GRJ/GGR

Huancayo, 31 AGO. 2020

EL GERENTE GENERAL REGIONAL DEL GOBIERNO REGIONAL JUNÍN

VISTO:

El Memorando N° 1318-2020-GRJ/GGR del 27 de agosto de 2020; Reporte N° 252-2020-GRJ/GGR-ORDITI del 14 de agosto de 2020; Memorando N° 1236-2020-GRJ/GGR del 13 de agosto de 2020; Reporte N° 159-2020-GRJ-ORAJ del 03 de agosto de 2020; Informe Legal N° 290-2020-GRJ/ORAJ del 31 de julio de 2020; Informe Técnico N° 14-2020-GRJ/GGR-ORDITI del 22 de julio de 2020; Informe Técnico N° 14-2020-GRJ/GGR-ORDITI del 22 de junio de 2020 y, demás documentos adjuntos;

CONSIDERANDO:

Que, de acuerdo al artículo 191° de la Constitución Política del Perú de 1993, modificada por la Ley N° 27680 – Ley de la Reforma Constitucional del Capítulo XIV, respecto a la descentralización, establece que: *"Los Gobiernos Regionales tiene autonomía política, económica y administrativa en los asuntos de su competencia (…)"*;

Que, la autonomía de los Gobierno Regionales se define como la facultad de adoptar y concordar las políticas, planes y normas en los asuntos de su competencia, aprobar y expedir sus normas, decidir a través de sus órganos de gobierno y desarrollar las funciones que le son inherentes conforme a lo establecido en la Ley N° 27783 - Ley de Bases de la Descentralización;

Que, de conformidad a las facultades y atribuciones conferidas en el literal b) del numeral 1 del artículo primero de la Resolución Ejecutiva Regional Nº 018-2020-JUNIN/GR del 27 de enero de 2020, que establece: "*La facultad de aprobar, modificar, derogar, reordenar, directivas, circulares y/o manuales, así como todo documento de carácter normativo que permita la racionalización del gasto y el manejo adecuado de los recursos asignados por toda fuente de financiamiento durante la ejecución del Ejercicio Fiscal correspondiente, así como los que regulen actos de administración interna, Clasificador de Cargos, el Cuadro para Asignación de Personal Provisional (CAP-P), el Presupuesto Analítico de Personal (PAP), así* ***como otros documentos de gestión susceptibles de delegación, trámites internos, lineamientos técnico normativos y metodológicos, orientados a optimizar los procedimientos y procesos administrativos de carácter interno, a cargo de los órganos de apoyo y asesoramiento****; así como dejar sin efecto toda normativa interna o documento de gestión que se le oponga*"; corresponde al Gerente General Regional, la suscripción del presente acto resolutivo;

Que, de conformidad a lo establecido en el artículo 56° del Reglamento de Organizaciones y Funciones del Gobierno Regional de Junín, aprobado mediante

GERENCIA GENERAL
DOC. Nº 4277614
EXP. Nº 2902336

Ordenanza Regional N° 304-GRJ/CR, compete a la Oficina Regional de Desarrollo Institucional y Tecnología de la Información, entre otros, formular, proponer y ejecutar el Plan Estratégico de Tecnologías de la Información y Gobierno Electrónico, en concordancia con los objetivos estratégicos institucionales y las necesidades de los órganos de la entidad;

Que, mediante Informe Técnico N° 14-2020-GRJ/GGR-ORDITI, de fecha 27 de julio del año 2020, elaborado por el Director Regional de Desarrollo Institucional y Tecnologías de la Información, se sustenta la propuesta del "Plan de Transición al Protocolo IPv6 del Gobierno Regional de Junín". Así como se solicita la aprobación de dicho plan;

Que, el Plan de Transición al Protocolo IPv6 del Gobierno Regional Junín, propuesto por la Oficina Regional de Desarrollo Institucional y Tecnología de la Información, tiene como objetivo mejorar la seguridad y calidad de los servicios informáticos que el Gobierno Regional Junín brinda a la ciudadanía y público en general, incorporando nuevas tecnologías compatibles con el protocolo de comunicación en la Internet IPv6;

Que, mediante Ley Nº 27658 - Ley Marco de Modernización de la Gestión del Estado, publicada el 30 de enero de 2002, se declaró al Estado Peruano en proceso de modernización en sus diferentes instancias, dependencias, entidades, organizaciones y procedimientos, con la finalidad de mejorar la gestión pública, disponiendo su aplicación en todas las dependencias de la Administración Pública a nivel nacional;

Que, mediante Decreto Supremo Nº 081-2017-PCM, publicado el 9 de agosto de 2017, se aprobó la formulación de un "Plan de Transición al Protocolo IPv6 en las entidades de la Administración Pública", el cual indica que las entidades de la Administración Pública deben elaborar un Plan de Transición al Protocolo IPv6;

Que, la norma establece que las entidades de la Administración Pública que adquieran hardware o software que reciba, transmita o procese información por medio del protocolo IP, a partir de la fecha de la entrada en vigencia del referido Decreto Supremo, deben asegurar que estos soporten el Protocolo IPv6 con compatibilidad o soporte al Protocolo IPv4;

Que, el Decreto Supremo Nº 066-2011- PCM, publicado el 27 de julio de 2011, aprobó el Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0, que dispone la aplicación para todas las entidades que conforman el Sistema Nacional de Informática, siendo una de ellas el Gobierno Regional de Junín, por cuyo mérito la Entidad se encargará de adoptar las acciones necesarias para el cumplimiento y ejecución del referido Plan;

Que, al considerarse necesario propiciar un entorno que garantice la adopción del Protocolo IPV6, y ante el inminente agotamiento de las direcciones IPV4, resulta necesario aprobar el Plan de Transición al Protocolo IPV6 del Gobierno Regional de Junín;

Que, de conformidad con lo establecido en la Ley 27867 - Ley Orgánica de los Gobiernos Regionales; el Decreto Supremo N° 081-2017-PCM - Decreto Supremo que

aprueba la formulación de un Plan de Transición al Protocolo IPV6 en las Entidades de la Administración Publica; y la Ordenanza Regional N° 304-GRJ/CR, que aprueba el Reglamento de Organización de Funciones del Gobierno Regional Junín;

Que, estando al sustento técnico y a los fundamentos legales corresponde a la Entidad aprobar el "Plan de Transición al Protocolo IPv6 del Gobierno Regional Junín" que propicie un entorno que garantice la adopción de dicho protocolo de conformidad con la Resolución Nº 180 correspondiente a la Conferencia de Plenipotenciarios de la Unión Internacional de Telecomunicaciones;

De conformidad con las facultades y atribuciones dispuestas por la Ley N° 27867 - Ley Orgánica de Gobiernos Regionales y sus modificatorias, y la Resolución Ejecutiva Regional Nº 018-2020-JUNIN/GR; contando con la visación de la Directora de la Oficina Regional de Asesoría Jurídica y Oficina Regional de Desarrollo Institucional y Tecnología de la Información del Gobierno Regional Junín,

SE RESUELVE:

ARTICULO PRIMERO.- APROBAR el **"PLAN DE TRANSICIÓN AL PROTOCOLO IPV6 DEL GOBIERNO REGIONAL JUNÍN",** de conformidad con los fundamentos expuestos.

ARTICULO SEGUNDO.- ENCARGAR a la Oficina Regional de Desarrollo Institucional y Tecnología de la Información del Gobierno Regional Junín, la difusión y cumplimiento del referido "Plan de Transición al Protocolo IPv6 del Gobierno Regional Junín".

ARTÍCULO TERCERO.- NOTIFICAR, el presente acto administrativo a los órganos competentes del Gobierno Regional de Junín, de acuerdo a las disposiciones del TUO de la Ley N° 27444, aprobado con Decreto Supremo N° 004-2019-JUS; para conocimiento, cumplimiento y difusión.

REGÍSTRESE, COMUNÍQUESE Y PUBLÍQUESE.

GOBIERNO REGIONAL JUNÍN
LIC. CLEVER RICARDO UNTIVEROS LAZO
GERENTE GENERAL REGIONAL

GOBIERNO REGIONAL JUNÍN
Lo que transcribo a Ud. para su conocimiento y fines pertinentes
HYO. 31 AGO. 2020
Abog. Helen S. Díaz Herrera
SECRETARÍA GENERAL

PLAN DE TRANSICIÓN AL PROTOCOLO IPV6

¡Trabajando con la fuerza del pueblo!

Gobierno Regional Junín

Oficina Regional de Desarrollo Institucional y Tecnología de la Información

ÍNDICE

I. Introducción

Dado el crecimiento de la demanda de usuarios en la Internet, se requiere asignar una identificación única o dirección IP para cada equipo de los usuarios. La dirección IP es una numeración en un formato específico como **a.b.c.d**, el cual permite que la información vaya de un lugar de origen a un destino y es el principal recurso técnico para que los dispositivos logren conectarse a Internet.

El protocolo de Internet versión 4 (IPv4) que usa el formato antes indicado es el que actualmente y globalmente se emplea e identifica cerca de 4,300 millones de direcciones IP (aproximadamente 2^{32}) de los dispositivos de los usuarios. Sin embargo, éstas no son suficientes para abastecer la demanda actual, por el auge de los teléfonos móviles con acceso a Internet, redes sociales y el interés de interconectar cada uno de los diversos dispositivos tecnológicos.

En junio del año 2014 se anunció oficialmente que las direcciones IP del protocolo IPv4 han entrado en fase de agotamiento final. Para resolver esta situación crítica de escasez de las direcciones IPv4 se ha desarrollado un nuevo protocolo de Internet de conectividad, denominado **IPv6 con una capacidad de asignar 340 sextillones** de direcciones. A nivel mundial, para la asignación de direcciones IP existen organismos jerárquicos siendo el principal IANA (Internet Assigned Numbers Authority) que es la entidad que supervisa la asignación global de direcciones IP, sistemas autónomos, servidores raíz de nombres de dominio DNS y otros recursos relativos a los protocolos de Internet. También podemos mencionar a la Corporación de Internet para la Asignación de Nombres y Números (ICANN). Estos organismos delegan los recursos de internet bajo ciertas políticas al Registro Regional de Internet (RIR) el cual es una organización que supervisa la asignación y el registro de recursos de números de Internet dentro de una región particular del mundo las cuales realizan una posterior subdelegación de recursos a sus clientes principales que incluyen a los proveedores de servicios de Internet (ISP) .

Esta nueva versión del protocolo provee nuevas e importantes características en las conexiones tales como:

La capacidad de direccionamiento extendida.

Mayor seguridad, puesto que al tener suficientes direcciones IP se podrá identificar con mayor facilidad a cada dispositivo en la red, porque cada uno tendrá su propia dirección IP.

Encriptación de los datos, de tal manera que la comunicación entre dos puntos será realmente privada y nadie podrá intervenirla.

Etiquetar los paquetes de datos para realizar una mejor gestión del tráfico de las comunicaciones.

Paquetes IP eficientes y extensibles, sin que haya fragmentación en los enrutadores, alineados a 64bits (preparados para su procesado óptimo con los nuevos procesadores de 64bits), y con la cabecera de longitud fija, más simple, que agiliza su procesado por parte del enrutador.

- Simplificación del formato de cabecera.
- Autoconfiguración de direcciones.
- Procesamiento simplificado en los routers.
- Mejor soporte para las extensiones y opciones.
- Adelantos en Multicast y Anycast.
- Calidad de Servicio (QoS) y clase de Servicio(CoS).

El protocolo IPv6 cubrirá la necesidad de asignar el nuevo direccionamiento a todos los dispositivos tecnológicos usados para la conexión a internet, lo cual facilitará la conectividad en banda ancha, poniéndolos al alcance de toda la población a fin de estimular y ofrecer mejores oportunidades para el desarrollo mundial.

En los últimos años se ha manifestado que el despliegue de IPv6 es relativamente lento en el mundo, considerando que varios de los RIR ya han iniciado la última fase de asignación de sus últimos bloques (prefijo /8s) de direcciones IPv4, por lo que resulta importante dinamizar la implementación del protocolo IPv6 (Ver tabla 1).

REGISTRO REGIONAL DE INTERNET (RIR)	Direcciones IPv4 disponible Set. 2017 Cada bloque /8 equivale aprox. a 16 millones de direcciones IP.
APNIC (Asia/Pacifico)	0.35/8s
ARIN (América del Norte y parte del Caribe)	0.00/8s
AFRINIC (África y parte Océano Indico)	0.79/8s
LACNIC (América Latina y parte del Caribe)	0.24/8s
RIPE NCC (Europa, centro y medio de Asia)	0.72/8s

Tabla 1: Registro Nacional de Internet, Fuente www.nro.net

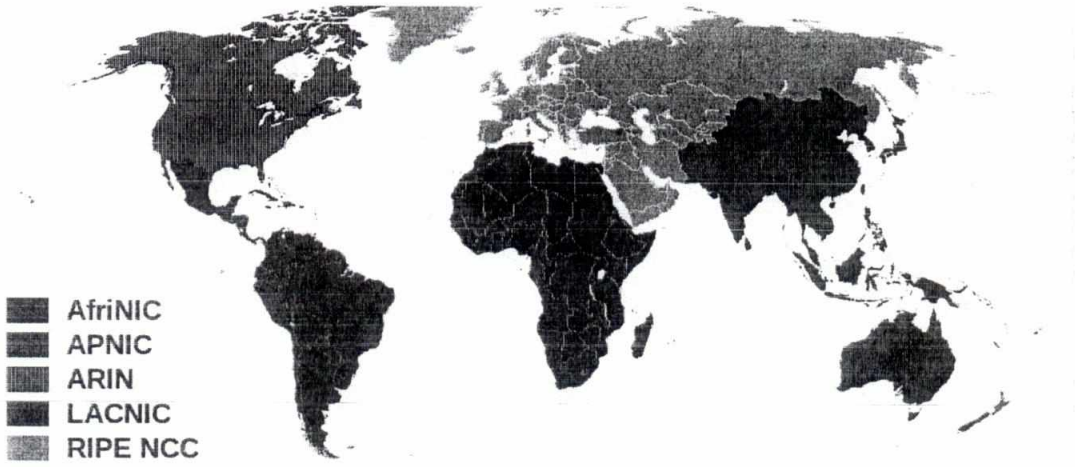

Gráfico 1: Distribución Geográfica del Registro Regional de Internet (RIR), Fuente: Wikipedia

La transición no va a ser fácil y pasarán años hasta completar el tránsito a IPv6, un tiempo en el que los proveedores, los sitios web y los fabricantes de dispositivos deberán ir adaptando sus infraestructuras a este cambio.

Sin embargo, surgen otros inconvenientes como el hecho de llevar a cabo la respectiva transición de un protocolo a otro (IPv4 a IPv6) de una manera práctica en organizaciones que cuentan con infraestructura tecnológica, sin afectar los servicios, tecnologías y procesos que actualmente gestionan. Es por ello que es necesario realizar los estudios y evaluaciones preliminares con el fin de elaborar un Plan de Transición al protocolo IPv6 en el **Gobierno Regional Junín (GRJ).**

II. Base Legal

- Decreto Supremo 081-2017-PCM, que aprueba la formulación de un Plan de Transición al Protocolo IPV6 en las entidades de la Administración Pública.
- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
- Decreto Legislativo N° 604,
- Ley N° 29158, Ley Orgánica del Poder Ejecutivo.
- Ley N° 30225, Ley de Contrataciones del Estado.
- Decreto Legislativo N° 1017, Decreto Legislativo que aprueba la Ley de Contrataciones del Estado, y su Reglamento, aprobado con Decreto Supremo N° 184-2008-EF, de aplicación hasta la entrada en vigencia de la Ley N° 30225.
- Resolución de Contraloría N° 163-2015-CG, aprueba la Directiva N° 007-2015CG/PROCAL, Directiva de los Órganos de Control Institucional.
- Decreto Supremo Nº 066-2011-PCM, que aprueba el Plan de Desarrollo de la Sociedad de la Información - La Agenda Digital Peruana 2.0.
- Decreto Supremo N° 004-2013-PCM, que aprueba la Política Nacional de Modernización de la Gestión Pública.
- Decreto Supremo N° 081-2013-PCM, que aprueba la Política Nacional de Gobierno Electrónico.
- Decreto Supremo N° 004-2019-JUS, que aprueba el Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General.
- Decreto Supremo N° 350-2015-EF, que aprueba el Reglamento de la Ley de
- Contrataciones del Estado y norma modificatoria.
- Decreto Legislativo N° 1353 que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el Régimen de Protección de Datos Personales y la Regulación de la Gestión de Intereses.
- Ley N° 30225 – Ley de Contrataciones del Estado y normas modificatorias.
- Resolución Ministerial N° 246-2007-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de Buenas Prácticas para la gestión de la Seguridad de la Información. 2da. Edición" en todas las entidades integrantes del Sistema Nacional de Informática.

III. Objetivos del Plan de Transición

- ✓ Analizar y desarrollar el plan de diagnóstico.
- ✓ Realizar el despliegue del nuevo direccionamiento IPv6 en las redes, dispositivos, servicios y aplicaciones con que cuenta el Gobierno Regional Junín para Internet.

IV. Alcance del Plan de Transición

El Gobierno Regional Junín cuenta con una infraestructura propia e interna (Data Center) en el cual permite ofrecer los siguientes servicios:

- Sistema de trámite documentario.
- Aplicaciones administrativas
- Intranet.
- Correo institucional.
- Telefonía IP.
- Videoconferencia.

- Video vigilancia.
- Repositorios de archivos.

El presente plan de transición contempla como alcance toda la infraestructura, plataforma y servicios públicos digitales que estén bajo control del Gobierno Regional al protocolo IPv6."

4.1. TOPOLOGIA ACTUAL DE LA RED DEL GOBIERNO REGIONAL

El modelo jerárquico de conectividad que se emplea se muestra a continuación

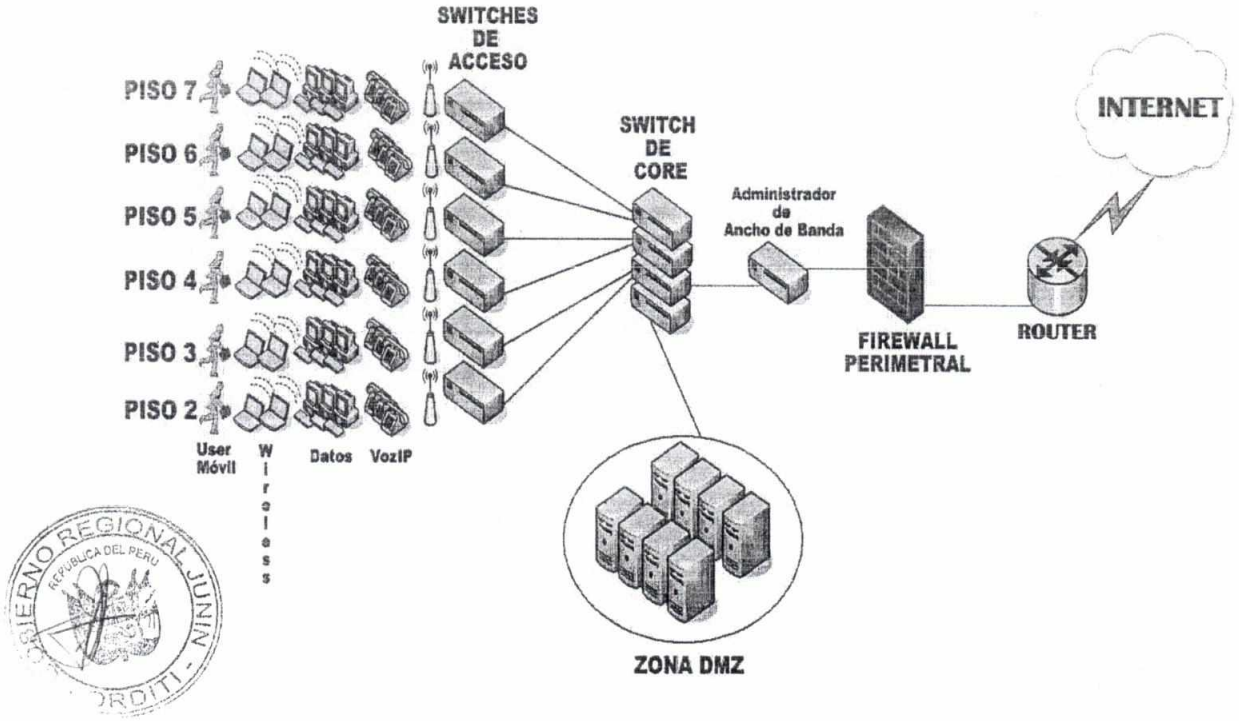

Gráfico 2: Topología actual del Gobierno Regional Junín, Fuente: Propia de la ORDITI

En la gráfica anterior se describe el equipamiento de la infraestructura tecnológica del Gobierno Regional: Router, Firewall, Controlador de Ancho de Banda, Swtiches de acceso, Servidores, teléfonos IP, equipos inalámbricos. La configuración de VLAN (segmento o redes virtuales) se realiza en los switches principales (CORE) y tiene por objetivo administrar el flujo de datos entre un segmento a otro.

V. Riesgos de no adopción del Protocolo IPv6

5.1. Riesgos Identificados

En la tabla 2, se identificó los riesgos sobre un proceso crítico en el Gobierno Regional Junín, el cual influye en las actividades diarias y el giro del negocio, en la columna: Cod_Riesgo se puede mostrar los riesgos identificados. Para la adopción del protocolo IPv6 se debe de realizar una nueva gestión de riesgos y ver que activos de información se ven afectados con dicha implementación. El cual ya está en desarrollo.

Amenaza	Principales ACTIVOS afectados	MECANISMOS DE PROTECCIÓN EXISTENTES						Vulnerabilidades	Riesgo Existente				
		Confidencialidad	Integridad	Disponibilidad	Preventivos	Detectivos	Correctivos		Probabilidad	Impacto	Riesgo	Tolerancia	Cod_Riesgo
RIESGOS COMUNES A LAS CATEGORIAS DE ACTIVOS													
Incendio	**DATOS:** Documentos físicos y digitales. **SOFTWARE**: Sistemas informáticos en funcionamiento y respectivamente sus bases de datos, aplicaciones en desarrollo. **EQUIPOS:** Computadoras, servidores, laptops, impresoras, teléfonos, swchites, access point(s), antenas PTP, UPS, equipos del sistema eléctrico, equipos del data center, cableado estructurado, cableado de fibra óptica, equipos del sistema de distribución de agua potable. **PERSONAL:** Muertes de personal por asfixia. **INSTALACIONES:** Oficinas con dificiencia de acceso para la evacuación.		X	X	Charlas y capacitación por la INDECI, instalación de extintores manuales (portátiles) y/o automáticos (rociadores) en algunas oficinas, utlización de aire acondicionado esta no debe de sobrepasar los 20° C y el límite de humedad no debe de superar el 70% para evitar deterioro. No sé permite fumar dentro de las oficinas del GRJ, Plan de contingecia.	Sistemas de Detección (Sensores de Humo)	Utilización de muebles incombustibles en algunas oficinas, uso de cestos métalicos para el almacenamiento de basura, uso de extintores contra incendio.	Fallas de instalaciones eléctricas defectuosas, presencia de material inflamable, no existe procedimientos planeados para recibir y almacenar el abastecimiento de papel, utilización de supresor de picos para varias instalaciones eléctricas.	3	4	12		R01-TI-ACT

Inundaciones	**DATOS:** Documentos físicos y digitales. **SOFTWARE**: Sistemas informáticos en funcionamiento y respectivamente sus bases de datos, aplicaciones en desarrollo. **EQUIPOS:** Computadoras, servidores, laptops, impresoras, teléfonos, swchites, access point(s), antenas PTP, UPS, equipos del sistema eléctrico, equipos del data center, cableado estructurado, cableado de fibra óptica, equipos del sistema de distribución de agua potable. **PERSONAL:** Muertes de personal por ahogo. **INSTALACIONES:** Oficinas con dificiencia de acceso paa la evacuación.		X	X	Charlas y capacitación por la INDECI, Plan de contingencia.	No existe.	No existe	Falta de canales de drenaje artificial, presencia de lluvias torrenciales con probabilidad de desborde de laguna aledaña (Huaytapallana)	2	2	4	RT	R02-TI-ACT

Terremoto	**DATOS:** Documentos físicos y digitales. **SOFTWARE**: Sistemas informáticos en funcionamiento y respectivamente sus bases de datos, aplicaciones en desarrollo. **EQUIPOS:** Computadoras, servidores, laptops, impresoras, teléfonos, swchites, access point(s), antenas PTP, UPS, equipos del sistema eléctrico, equipos del data center, cableado estructurado, cableado de fibra óptica, equipos del sistema de distribución de agua potable. **PERSONAL:** Muertes de personal por asfixia. **INSTALACIONES:** Oficinas con dificiencia de acceso paa la evacuación.		X	X	Charlas y capacitación por la INDECI, simulacros de sismo, marcado y señalización de zonas de seguridad, Plan de contingencia.	Se identificarón zonas seguras ante sismos en la sede del Gobierno Regional de Junín.	Capacitación contínua de buen uso de las zonas de marcado y señalización.	Ubicación de la sede del GRJ en el cinturón de fuego del Pacífico	3	3	9		R03-TI-ACT
RIESGOS DE LOS DOCUMENTOS													

Robo de información por parte del personal interno	Orden de compra, orden de servicio, contrato de locación de servicios, contrato de entrega de bienes, orden electrónicas (convenio marco), pedidos de compra (convenio marco), documentos para la adquisición de bienes y servicios mayores a 3 UIT, cotizaciones, documentos administrativos (memorandos, informes, reportes, etc), pecosas, requerimientos de bienes y servicios, requerimientos de bienes / servicios / mantenimiento, pedidos de insumo.	X	X	X	Establecimiento de políticas de seguridad, reglamento interno de trabajo, normativa de la ley del Procedimiento Administrativo General LEY Nº 27444, Normativa Código Penal Art. 207-A, Art-B, Art-C.	Grabación de cámaras de video vigilancia.	Aplicación de establecimiento de políticas de seguridad, reglamento interno de trabajo, normativa de la ley del Procedimiento Administrativo General LEY Nº 27444, Normativa Código Penal Art. 207-A, Art-B, Art-C.	No se cumplen plenamente las sanciones que estan establecidas en el Reglamento Interno de la Institución, Política de Seguridad de Información, normativa de la ley del Procedimiento Administrativo General LEY Nº 27444, Normativa Código Penal Art. 207-A, Art-B, Art-C., recelo político, adversarios politicos, prensa sensasionalista, guerra sucia, etc	3	2	6	RT	R01-TI-DOC

Robo de información por parte criminales (asalto)	Orden de compra, orden de servicio, contrato de locación de servicios, contrato de entrega de bienes, orden electrónicas (convenio marco), pedidos de compra (convenio marco), documentos para la adquisición de bienes y servicios mayores a 3 UIT, cotizaciones, documentos administrativos (memorandos, informes, reportes, etc), pecosas, requerimientos de bienes y servicios, requerimientos de bienes / servicios / mantenimiento, pedidos de insumo.	X	X	X	Monitoreo con cámaras de video vigilancia	Grabación de cámaras de video vigilancia.	Denuncias	Falta de capacitación y entrenamiento al personal de seguridad , falta de armamento de contingencia, falta de coordinación con la policia	1	2	2	TI	R02-TI-DOC

Robo de información por parte criminales informáticos (Hackers)- Externo	Orden de compra, orden de servicio, contrato de locación de servicios, contrato de entrega de bienes, orden electrónicas (convenio marco), pedidos de compra (convenio marco), documentos para la adquisición de bienes y servicios mayores a 3 UIT, cotizaciones, documentos administrativos (memorandos, informes, reportes, etc), pecosas, requerimientos de bienes y servicios, requerimientos de bienes / servicios / mantenimiento, pedidos de insumo.	X	X	X	Establecimiento de políticas de seguridad, implantación de seguridad perimetral (Firewall con Módulos UTM: Antispam, webfilter, antivirus; IPS)	Monitoreo de sucesos (log), registro de actividades, encriptación, control de accesos, ingenieria forense, etc	Pruebas de vulnerabilidad, post explotación y corregir vulnerabilidades encontradas	Incremento de técnicas y herramientas de hacking, adversarios politicos, retos, etc.	3	2	6	RT	R03-TI-DOC

Fuga/Divulgación de información por parte del personal interno	Orden de compra, orden de servicio, contrato de locación de servicios, contrato de entrega de bienes, orden electrónicas (convenio marco), pedidos de compra (convenio marco), documentos para la adquisición de bienes y servicios mayores a 3 UIT, cotizaciones, documentos administrativos (memorandos, informes, reportes, etc), pecosas, requerimientos de bienes y servicios, requerimientos de bienes / servicios / mantenimiento, pedidos de insumo.	X	X	X	Establecimiento de políticas de seguridad, reglamento interno de trabajo, normativa de la ley del Procedimiento Administrativo General LEY N° 27444, Normativa Código Penal Art. 207-A, Art-B, Art-C.	No existe.	Aplicación de establecimiento de políticas de seguridad, reglamento interno de trabajo, normativa de la ley del Procedimiento Administrativo General LEY N° 27444, Normativa Código Penal Art. 207-A, Art-B, Art-C.	Recelo político, insatisfación del ciudadano, adversarios políticos, prensa sensasionalista, guerra sucia, etc	4	2	8		R04-TI-DOC

Fuga/Divulgación de información por parte de los proveedores de servicios	Orden de compra, orden de servicio, contrato de locación de servicios, contrato de entrega de bienes, orden electrónicas (convenio marco), pedidos de compra (convenio marco), documentos para la adquisición de bienes y servicios mayores a 3 UIT, cotizaciones, documentos administrativos (memorandos, informes, reportes, etc), pecosas, requerimientos de bienes y servicios, requerimientos de bienes / servicios / mantenimiento, pedidos de insumo.	X	X	X	Establecimiento de políticas de seguridad, reglamento interno de trabajo, normativa de la ley del Procedimiento Administrativo General LEY N° 27444	Incidendia de conductas en el proveedor	Aplicación de establecimiento de políticas de seguridad, reglamento interno de trabajo, Normativa Código Penal Art. 207-A, Art-B, Art-C.	Recelo político, insatisfación del ciudadano, adversarios politicos, prensa sensasionalista, guerra sucia, etc	2	2	4	RT	R05-TI-DOC

Código malicioso que borre y/o elimine archivos digitales que tenga relación con documentos importantes	Orden de compra, orden de servicio, contrato de locación de servicios, contrato de entrega de bienes, orden electrónicas (convenio marco), pedidos de compra (convenio marco), documentos para la adquisición de bienes y servicios mayores a 3 UIT, cotizaciones, documentos administrativos (memorandos, informes, reportes, etc), pecosas, requerimientos de bienes y servicios, requerimientos de bienes / servicios / mantenimiento, pedidos de insumo.		X	X	Utilización de antivirus, antispam, webfilter, backup(s)	Diagnóstico de archivos infectados con código malicioso	Uso de antivirus, antispam, webfilter, backup(s)	Mantenimiento correcitvo de computadoras de la institución, tareas de antivirus, filtro de antispam, filtro de páginas web, backup(s) semanal-mensual	3	1	3	RT	R06-TI-DOC

Vandalismo que exponga documentos importantes	Orden de compra, orden de servicio, contrato de locación de servicios, contrato de entrega de bienes, orden electrónicas (convenio marco), pedidos de compra (convenio marco), documentos para la adquisición de bienes y servicios mayores a 3 UIT, cotizaciones, documentos administrativos (memorandos, informes, reportes, etc), pecosas, requerimientos de bienes y servicios, requerimientos de bienes / servicios / mantenimiento, pedidos de insumo.		X	X	Capacitación y entrenamiento al personal de seguridad en temas de violencia y vandalismo.	Anticipos a la coyuntura política: anticipar y pronosticar disturbios.	Coordinación de eventos de violencia y vandalismo con la Policia Nacional del Perú	Recelo político, insatisfación del ciudadano, adversarios politicos, prensa sensasionalista, guerra sucia, etc	1	3	3	RT	R07-TI-DOC

Fraude/alteración de documentos	Orden de compra, orden de servicio, contrato de locación de servicios, contrato de entrega de bienes, orden electrónicas (convenio marco), pedidos de compra (convenio marco), documentos para la adquisición de bienes y servicios mayores a 3 UIT, cotizaciones, documentos administrativos (memorandos, informes, reportes, etc), pecosas, requerimientos de bienes y servicios, requerimientos de bienes / servicios / mantenimiento, pedidos de insumo.		X	X	Establecimiento de políticas de seguridad, reglamento interno de trabajo, normativa de la ley del Procedimiento Administrativo General LEY Nº 27444	Auditoria.	Aplicación de establecimiento de políticas de seguridad, reglamento interno de trabajo, normativa de la ley del Procedimiento Administrativo General LEY Nº 27444, Normativa Código Penal Art. 207-A, Art-B, Art-C.	Recelo político, insatisfación del ciudadano, adversarios politicos, prensa sensasionalista, guerra sucia, etc	4	2	8		R08-TI-DOC

Deterioro de información debido a Contaminación (Meriendas, polvo, suciedad, humedad, insolación)	Orden de compra, orden de servicio, contrato de locación de servicios, contrato de entrega de bienes, orden electrónicas (convenio marco), pedidos de compra (convenio marco), documentos para la adquisición de bienes y servicios mayores a 3 UIT, cotizaciones, documentos administrativos (memorandos, informes, reportes, etc), pecosas, requerimientos de bienes y servicios, requerimientos de bienes / servicios / mantenimiento, pedidos de insumo.		X	X	Selección de la información	Clasificación de la información	Almacenamiento de la información.	Neglicencia de personal, no cumplimiento de roles y funciones	1	1	1	T	R09-TI-DOC
RIESGOS DEL SOFTWARE													
Fallas en los Sistemas de Información	Sistema de adquiciones, sistema de almacen, sistema del portal del seace, SIAF (Sistema integrado de administración financiera), SISGEDO (Sistema de trámite documentario), DNS, WEB, CORREO, FTP	X	X	X	Pruebas de análisis de vulnerabilidades	Explotación de vulnerabilidades encontradas	Correción de vulnerabilidades encontradas, aplicación de actualización o parches	No se sigue metodológias de programación adecuadas, configuración sin patrones de seguridad	3	3	9	T	R01-TI-SOF

Fallas en software de ofimática	Word, excel, power point, vizio. Outlook			X	Copias de seguridad de los instaladores de software de ofimática	Fallas en el performance del software de ofimática	Reinstalación del software de ofimática	Desconfiguración de sistema operativo, virus informático	2	1	2	RT	R02-TI-SOF
Alteración y/o modificación de configuración de los sistemas de información	Sistema de adquiciones, sistema de almacen, sistema del portal del seace, SIAF (Sistema integrado de administración financiera), SISGEDO (Sistema de trámite documentario), DNS, WEB, CORREO, FTP	X	X	X	Revision de código fuente de desarrollo y configuración	Compilación y pruebas de código fuente	Corrección de código fuente en desarrollo y configuración	No se sigue metodológias de programación adecuadas, configuración sin patrones de seguridad	3	1	3	RT	R03-TI-SOF
Virus informáticos	Sistema de adquiciones, sistema de almacen, sistema del portal del seace, SIAF (Sistema integrado de administración financiera), SISGEDO (Sistema de trámite documentario), DNS, WEB, CORREO, FTP	X	X	X	Utilización de antivirus, recolección de código malicioso	Análisis de código malicioso	Neutralizar código malicioso	Infección y propagación de código malicioso por dispositvos externos, spam, dafecement, etc	3	1	3	RT	R04-TI-SOF

Accesos no autorizados a los sistemas de información	Sistema de adquiciones, sistema de almacen, sistema del portal del seace, SIAF (Sistema integrado de administración financiera), SISGEDO (Sistema de trámite documentario), DNS, WEB, CORREO, FTP	X	X	X	Se aplica de modalidades de acceso: lectura, escritura, ejecución, borrado.	Monitoreo de sucesos (log), registro de las actividades de control de accesos	Control sobre las modalidades de acceso: lectura, escritura, ejecución, borrado.	Sincronización de password, caducidad de password, facilidad de password	2	2	4	RT	R05-TI-SOF
Ataques activos (DDoS, Injection SQL/java, Backdoor, etc) a los sistemas de información	Sistema de adquiciones, sistema de almacen, sistema del portal del seace, SIAF (Sistema integrado de administración financiera), SISGEDO (Sistema de trámite documentario), DNS, WEB, CORREO, FTP	X	X	X	Aplicación de controles externos(IPS, Firewall)	Monitoreo de sucesos (log), registro de las actividades	Aplicación de politicas de seguridad	Criminalidad informática, adversarios politicos, guerra sucia, etc	3	2	6	RT	R06-TI-SOF
Ataques pasivos	Sistema de adquiciones, sistema de almacen, sistema del portal del seace, SIAF (Sistema integrado de administración financiera), SISGEDO (Sistema de trámite documentario), DNS, WEB, CORREO, FTP		X	X	Aplicación de controles internos(IDS, Radius)	Monitoreo de sucesos (log), registro de las actividades	Aplicación de politicas de seguridad	Actividades fraudulentas, robo de información, spoofing, intrusión a los sistemas, etc	2	1	2	T	R07-TI-SOF
RIESGOS DE LOS EQUIPOS													

Fallas de equipos	Servidores, computadoras, laptops, impresoras, fotocopiadoras, teléfonos, etc.		X	X	Mantenimientos preventivos y correctivos cada 3 meses	Atención de servicios de soporte técnico	Adquición de nuevos equipos por depreciación	Expuesto a daños fisícos debido a su ubicación	3	1	3	RT	R01-TI-EQ
Robo de equipos	Servidores, computadoras, laptops, impresoras, fotocopiadoras, teléfonos, etc.	X	X	X	Inventario de hardware anual	Mantenimiento preventivo	Mantenimiento correctivo	Expuesto a robo debido a su ubicación, no se utiliza cable de seguridad, acceso a otras personas a los equipos	1	1	1	TT	R02-TI-EQ
Fallas en la infraestructura de Red (dificulta comunicación y operación)	Servidores, computadoras, laptops, impresoras, fotocopiadoras, teléfonos, etc.		X	X	Servicio de internet alterno (fibra óptica: 8MB y cobre: 2MB)	pruebas de testeo	Uso de servicio de internet alterno por cobre: 2MB	Problemas de cobertura externa o de planta con el proveedor (mantenimiento, fallas, etc)	3	3	9		R03-TI-EQ
Falla en la infraestructura de telefonía (interna y externa)	Servidores, computadoras, laptops, impresoras, fotocopiadoras, teléfonos, etc.		X	X	No existe	No existe	No existe	Problemas de cobertura externa o de planta con el proveedor (mantenimiento, fallas, etc)	2	1	2	TT	R04-TI-EQ
RIESGOS A LOS SERVICIOS													
Falla del servicio de Telefonía Fija	Telefonía fija			X	No existe	No existe	No existe	Problemas de cobertura externa o de planta con el proveedor (mantenimiento, fallas, etc)	1	1	1	TT	R01-TI-SE

Corte del suministro eléctrico	Suministro de energía eléctrica		X	X	Implementación de sistema eléctrico alterno automático (grupo electrógeno) y de UPS	Avisos de corte de servicio emitidos por el proveedor	Uso de sistema eléctrico alterno automático (grupo electrógeno) y de UPS	Problemas de cobertura externa o de planta con el proveedor (mantenimiento, fallas, etc)	3	1	3	RT	R02-TI-SE
Falla del servicio de Internet	Internet			X	Servicio de internet alterno (fibra óptica: 8MB y cobre: 2MB)	pruebas de testeo	Uso de servicio de internet alterno por cobre: 2MB	Problemas de cobertura externa o de planta con el proveedor (mantenimiento, fallas, etc)	3	2	6	RT	R03-TI-SE
RIESGOS DEL PERSONAL													
Desidia del personal		X	X	X	Capacitación a personal alterno	Interrelación de personal con jefe y colegas	Contratación de personal alterno	No cumplimiento del ciclo de proceso de adquición del bien y servicio	1	1	1	TT	R01-TI-PE
Remuneraciones bajas				X	Pruebas de desempeño	MOF (manual de organización y funciones)	Incentivos por función	Ausencia de personal capacitado	1	1	1	TT	R02-TI-PE
RIESGOS INTANGIBLES (IMAGEN Y REPUTACION DE LA EMPRESA)													
Mala reputación de la institución	Burocracia de documentos			X	Implementación de sistema de gestión documentaria (SISGEDO) para la agilización del trámite documentario	Bloqueo de procesos documentarios en el SISGEDO	Filtro de documentos en mesa de partes	Ineficiencia de la gestión	4	3	12	IT	R01-TI-RI

Desinformación	Transparecia			X	Actualizar constantemte el portal de transparecia (resoluciones, normatividad, remuneración de personal, dietas, viáticos, procesos de selección, etc)	Indicadores de desempeño de trasparecia (ONGEI), Estádisticas de encuestas	Campañas publicitarias y prensa	Corrupción en al gestión	4	2	8	R02-TI-RI

Tabla 2: Riesgos identificados para un proceso crítico, Fuente: Elaboración propia.

MATRIZ DE RIESGOS

PROBABILIDAD	IMPACTO			
	Crítico -4	Serio -3	Medio -2	Mínimo -1
Alta (4)				
Media (3)			R06-TI-SW	
Baja (2)		R02-TI-ACT		
Muy baja (1)	R10-TI-SER			

CRITERIOS			
NT	Valor igual: 16 a 8	RT	Valor igual: 3 a 6
	Valor igual: 1 a 2		

Tabla 3: Matriz de riesgos para un proceso crítico, Fuente: Elaboración propia.

CUADRO PARA LA EVALUACIÓN DE RIESGOS	
Descripción del contenido	
CONTENIDO	

Riesgo efectivo

Riesgo efectivo de activos sometidos a amenazas, considerando los mecanismos de protección existentes

Probabilidad

Estimación de la probabilidad de ocurrencia de la amenaza

4 **Alta (Una vez al mes)**

3 Media (Una vez al año)

2 **Baja (Una vez cada 5 años)**

1 **Muy baja (Una vez cada 20 años)**

Impacto

Estimación del impacto que las amenazas pueden producir en los activos

4 **Crítico: afecta irreversiblemente (Mayor a S/.150,000)**

3 **Serio: afecta seriamente (Entre S/.50,000 a S/.150,000)**

2 Medio (Entre S/.15,000 a S/. 50,000)

1 **Mínimo (Menor a S/.15,000)**

Riesgo

Estimar el riesgo multiplicando los valores de estimación de probabilidad por impacto

Tolerancia

Identicar el nivel de tolerancia del riesgo

TT **Totalmente tolerable (De 1 a 2)**

RT Regularmente tolerable (De 3 a 6)

NT **No tolerable (De 7 a más)**

Tabla 4: Cuadro para la elaboración de riesgos, Fuente: Elaboración propia.

VI. Diagnóstico de la Infraestructura Tecnológica

6.1 Hardware

En la infraestructura del Gobierno Regional Junín se cuenta con varios equipos networking, los más importantes se menciona a continuación:

6.1.1 ROUTER

En el GRJ cuenta con router modelo SRX210 CPE (Customer Premise Equipament), de máximum concurrentsessions: 16 K (512 MB DRAM) / 32 K (1 GB DRAM), con 8 x 10/100 puertos.

El cuál es utilizado para la habilitación del servicio dedicado a Internet, ambos enlaces principal y respaldo terminan en este CPE.

4.2.1.1 Características técnicas del Router

Las características principales del router son:

CANTIDAD	Nº DE PARTE	DESCRIPCIÓN
1	SRX210B	SRX Services Gateway 210 with 2xGE + 6xFE ports, 1xMini-PIM slot, 1xExpressCard slot, and base memory (512 Mb RAM, 1GB Flash). Externalpowersupply and cordincluded.
1	SV3-ND-SRX100	J-Care 3YR PrepaidNextDaySupportfor SRX100

Tabla 5: Características del router, Fuente: Elaboración propia.

Overbooking[1]: La tabla siguiente muestra los valores de concentración (overbooking), aplicables para cada uno de los tramos (nacional e internacional) asociados a los enlaces solicitados asociados al servicio de Transmisión de Datos y Acceso a Internet que ofrece GTD.

ENLACE	CARACTERÍSTICAS DEL SERVICIO	VALOR SOLICITADO POR EL GRJ	VALOR OFERTADO POR TELMEX
Acceso a Internet enlace principal	Overbooking del tramo local	1:1	**1:1**
	Overbooking del tramo internacional	1:1	**1:1**

Tabla 6: Overbooking tramo local e internacional, Fuente: Elaboración propia.

El servicio se implementa utilizando como medio: Fibra Óptica canalizada desde el punto de presencia del proveedor (GTD) hasta la sede del cliente (GRJ).

6.1.2 FIREWALL

El FIREWALL es de la marca Palo Alto modelo PA – 820, es una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la información perimetral que incluye filtro de paquetes, control de aplicaciones, administración de ancho de banda (QoS), VPN IPSec y SSL, IPS, prevención contra amenazas de virus, spyware y malware "Zero Day", bien como controles de transmisión de datos y acceso a internet componiendo una plataforma de seguridad integrada y robusta. Por plataforma de seguridad se entiende hardware y software integrados de tipo appliance.

6.1.2.1 Características esenciales técnicas del Firewall a IPv6

Las características principales del Firewall son:

[1]**Overbooking:** Es el nivel de sobreventa de un enlace, es decir cuántos usuarios van a estar compartiendo los recursos de un enlace.

Performance and Capacities[1]	PA-820
Firewall throughput (App-ID)[2,4]	940 Mbps
Threat prevention throughput[3,4]	610 Mbps
IPsec VPN throughput[2,4]	400 Mbps
New sessions per second[5]	8,300
Max sessions	128,000

[1] Performance and capacities are measured under ideal testing conditions running PAN-OS 8.0

[2] Firewall and IPsec VPN throughput are measured with App-ID and User-ID features enabled

[3] Threat prevention throughput is measured with App-ID, User-ID, IPS, Antivirus and Anti-Spyware features enabled

[4] Throughput is measured with 64Kb HTTP transactions

[5] New sessions per second is measured with 4Kb HTTP transactions

Tabla 7: Características técnicas del Firewall, Fuente: Elaboración propia.

- El dispositivo soporta VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub-interfaces ethernet lógicas, NAT de origen y destino.
- Soporta enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2);
- Soporta las siguientes funcionalidades en IPv6: SLAAC (address auto configuration), NAT64, Identificación de usuarios a partir de LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Reglas de seguridad contra DoS (Denial of Service), Descifrado SSL/TLS y SSH, PBR (Policy Base Routing) o PBF (Policy Based Forwarding), OSPFv3, QoS, DHCPv6 Relay, SNMP, NTP, NTP autenticado, SYSLOG, DNS y control de aplicaciones;
- **Soporta IPv6 en modos de alta disponibilidad, tanto Activo/Activo como Activo/Pasivo.**
- Modo Sniffer, para inspección vía puerto espejo del tráfico de datos de la red.
- Modo Capa – 2 (L2), para inspección de datos en línea y tener visibilidad del control del tráfico en nivel de aplicación.
- Modo Capa – 3 (L3), para inspección de datos en línea y tener visibilidad del control del tráfico en nivel de aplicación operando como default gateway de las redes protegidas;
- Modo Transparente, para poder inspeccionar datos en línea y tener visibilidad del control de tráfico a nivel de aplicación sobre 2 puertos en modo bridge/transparente.
- Modo mixto de trabajo Sniffer, Transparente, L2 y L3 simultáneamente en diferentes interfaces físicas del mismo equipo;

6.1.3 ADMINISTRADOR DE BANDA ANCHO DE BANDA

El tráfico de señal se distribuye por el equipo Sinefa modelo 150, dicho equipo es un administrador inteligente de tráfico LAN que permite asegurar protección a servicios críticos a través de políticas de control de calidad de servicio (QoS) aplicando tecnologías de inspección profunda de paquetes (Deep Packet Inspection: DPI) y restringir el acceso a internet de las aplicaciones que no sea de interés para la sede central del Gobierno Regional Junín.

El sistema provee un tráfico optimizado, así también es una herramienta para el Administrador de Red.

6.1.3.1 Características técnicas del Administrador de Ancho de Banda

Las características principales del administrador de ancho de banda son:

Model	SF150
Status	Available for purchase
Pictures	SF150 pics
Maximum Bandwidth	100 Mbps
Packets Per Second	40k
Flows	400k
In-Line Deployment	YES
SPAN Support	YES
Layer 7 DPI Visibility	YES
High Availability (Active/Active or Active/Passive)	YES
Ethernet Ports	3
Ethernet Bypass Pairs (2 ports each)	1
Ethernet NIC Speeds	10/100/1000 Mbps
Serial Console	YES
Secure Shell (SSH) Console	YES
Approvals and Compliance	CE emission, FCC Class A, RoHS
Disk Capacity	8G (CF)

Tabla 7: Características técnicas del Controlador de Ancho de Banda,
Fuente: Elaboración propia.

6.1.4 SWITCH DE CORE EX4200-48P

Se cuentan con 4 equipos Switch de Core EX4200-48P. El equipo EX4200-48P permite la consolidación de la formación de un chassis virtual para la administración centralizada de toda la red del GRJ, agrupando 3 equipos similares EX4200-48P y 1 equipo EX4200-24F mediante un backplane de 128Gbps, cuenta con interfaces de 10GE en el Uplink, y permite múltiples LAGs (Link Aggregation Group) para la interconexión con el acceso, las interfaces 10/100/1000 Base-T, el elevado nivel de performance y las funcionalidades de capa 3. Son las características que permitirán la flexibilidad y escalabilidad en infraestructura de Red orientada al acceso y núcleo.

6.1.4.1 Características técnicas de los Switch de Core EX4200-48P

Las características principales de los switch de core EX4200-48P son:

CARACTERÍSTICAS	MÉTRICAS
Date rate	136Gbps

Throughput	101Mbps
10/100/1000 Base- T Port Densites	48
100 Base-SX (SFP) uplink	4 per switch (four-portGbEuplink module)
10GBase-X	2 per switch (viaoptionaltwo-port 10GbE uplink module)
BackplaneSpeed	128 Gbps (Virtual Chassis)
Powerover Ethernet (IEEE 802.3af)	8 by default (also Full PoE)
QoSQueues/Port	8
MAC Addresses	8,000
Jumbo Frames	9216 Bytes
IPv4 Unicast/MulticastRoutes	6,500/0
Number of VLANs	4,096
ARP Entries	2,000
Compatibility	IPv6

Tabla 8: Características técnicas del switch de core EX4200-48P, Fuente: Elaboración propia.

6.1.5 SWITCH DE CORE EX4200-24F

Se cuentan con 10 equipos Switch de Core EX4200-24F, se utilizó dichos equipos en interfaces 1000Base-SX para la interconexión con los conmutadores de core de acceso, ubicados en los gabinetes secundarios de cada piso para la distribución horizontal de acceso a Internet a los usuarios del GRJ.

6.1.5.1 Características técnicas de los Switch de Core EX4200-24F

A continuación, se hace el detalle de las principales características del conmutador de core EX4200-24F.

CARACTERÍSTICAS	MÉTRICAS
Date rate	88Gbps
Throughput	65Mbps

10/100/1000 Base- T Port Densites	24
100 Base-SX (SFP) uplink	4 per switch (four-portGbEuplink module)
10GBase-X	2 per switch (viaoptionaltwo-port 10GbE uplink module)
BackplaneSpeed	128 Gbps (Virtual Chassis)
Powerover Ethernet (IEEE 802.3af)	8 by default (also Full PoE)
QoSQueues/Port	8
MAC Addresses	8,000
Jumbo Frames	9216 Bytes
IPv4 Unicast/MulticastRoutes	6,500/0
Number of VLANs	4,096
ARP Entries	2,000
Compatibility	IPv6

Tabla 9: Características técnicas del Conmutador EX4200-24F, Fuente: Elaboración propia.

6.1.6 VIRTUAL CHASSIS: SWITCH DE CORE EX2200- 48P (3) & SWITCH DE CORE EX2200-24F (1)

Se usaron (04) conmutadores EX4200 para formar un virtual chassis, mediante la interconexión de sus puertos de virtual chassis de backplane. Este virtual chassis interconectará a los diferentes nodos de la red y también a los otros conmutadores ubicados en los gabinetes secundarios.
Los Swithes 4200 tienen la posibilidad de interconectarse entre sí para formar un virtual chassis que llega a operar como una red única. En este esquema la implementación de estos Switches son usados para formar el virtual chassis y que este escenario sea usado como red de alto desempeño. El virtual chassis se requerirá de (03) tres equipos EX4200-48P y (01) un equipo EX4200-24F con (10) diez interfaces 1000Base-SX con fuente redundante por cada equipo.
Los equipos conmutadores de core, cuentan con licenciamiento base que incluye funcionalidades avanzadas de ruteo como RIPv1/v2 y OSPF.
La administración es centralizada del virtual chasis (core):

	EQUIPOS		CANTIDAD DE PUERTOS	
PISO	MODELO	CANTIDAD	SOLICITADO	PROPUESTO
5 (Administración centralizada)	EX4200-48P	3	120	144
	EX4200-24F	1	10	10

Tabla 10: Distribución de Switch de Core y los puertos propuestos,
Fuente: Elaboración propia.

PISO	EQUIPOS		CANTIDAD DE PUERTOS
	MODELO	CANTIDAD	
2	EX2200-48P	2	96
3	EX2200-48P	1	72
	EX2200-24P	1	
4	EX2200-48P	2	96
6	EX2200-48P	2	96
7	EX2200-48P	1	72
	EX2200-24P	1	

Tabla 11: Distribución de Switch de Acceso en cada piso y los puertos propuestos,
Fuente: Elaboración propia

SEGMENTO DE RED	CLASE	ZONA
10/8	A	Red Interna
192.168/16	B	Redes DMZ
172.16/12	B	VLAN internas o redes

Tabla 12: Segmentación de Red, Fuente: Elaboración propia

- El Switch de Core tiene las siguientes configuraciones de VLAN:

#VLAN	NOMBRE DE LA VLAN
8	GESTION
104	INFORMATICA
26	VIDEO
98	ORAF
56	PISO 1
62	PISO 2
68	PISO 3
74	PISO 4
80	PISO 5
86	PISO 6
92	PISO 7
32	VOZ

46	WIRELESS-EXTERNO
44	WIRELESS-INTERNO
2	PRUEBA

Tabla 13: Segmentación de VLAN, Fuente: Elaboración propia

6.2 Equipamiento de Comunicaciones:

N°	Descripción	Soporte IPv4	Soporte IPv6	Riesgo
1	ROUTER	X	X	*2
2	FIREWALL	X	X	*
3	SWITCH CORE (4)	X	X	*
4	SWITCH ACCESO	X	X	*
5	CONTROLADOR DE ANCHO DE BANDA	X	X	*

Tabla N° 14: Equipamiento de comunicaciones

6.3 Equipamiento de Telefonía:

N°	Descripción	Soporte IPv4	Soporte IPv6	Riesgo
1	CENTRAL AVAYA	X	X	*

Tabla N° 15: Equipamiento de Telefonía

6.4 Equipamiento de Servidores – Físicos:

N°	Descripción	Soporte IPv4	Soporte IPv6	Riesgo
1	HP Proliant DL 560	X	X	*
2	HP Proliant DL 560	X	X	*
3	HP Proliant DL 160	X	X	*
4	HP Proliant DL 160	X	X	*
5	HP Proliant DL 180	X	X	*
6	HP Proliant DL 120	X	X	*
7	HP Proliant DL 120	X	X	*
8	HP Proliant DL 380	X	X	*
9	HP Proliant DL 120	X	X	*
10	HP Proliant DL 120	X	X	*
11	Dell Power Edge R720	X	X	*

Tabla N° 16: Equipamiento de Servidores –Físicos

6.5 Equipamiento de Servidores – Sistema Operativo:

N°	Descripción	Sistema Operativo	Soporte IPv4	Soporte IPv6	Riesgo
1	SIAF	WINDOWS SERVER 2016	X	X	*
2	SIGA	WINDOWS SERVER 2008 R2	X	X	*
3	WEB	CENTOS 7	X	X	*
4	CORREO	CENTOS 7	X	X	*

[2] (*) Ya mencionados en el análisis de riesgos

5	SISTEMASWEB	WINDOWS SERVER 2019	X	X	*
6	SISDORE	WINDOWS SERVER 2019	X	X	*
7	SIAR	UBUNTU SERVER 19	X	X	*
8	GEOSIAR	CENTOS 7	X	X	*
9	ANTIVIRUS	WINDOWS SERVER 2019	X	X	*
10	DNS (DIRECTORIO ACTIVO 1)	WINDOWS SERVER 2019	X	X	*
11	DNS (DIRECTORIO ACTIVO 2)	WINDOWS SERVER 2019	X	X	*

Tabla N°17: Equipamiento de Servidores – Sistema Operativo

6.6 Equipamiento de Usuarios – Sistema Operativo:

N°	Descripción	Sistema Operativo	Soporte IPv4	Soporte IPv6	Riesgo
1	EQUIPOS DE USUARIOS	WINDOWS 10	X	X	Bajo
2	EQUIPOS DE USUARIOS	WINDOWS 8	X	X	Medio
3	EQUIPOS DE USUARIOS	WINDOWS 7	X		Medio
4	EQUIPOS DE USUARIOS	WINDOWS XP	X		Alto

Tabla N° 18: Equipamiento de usuarios PC

6.7 Equipamiento de Video Vigilancia:

N°	Descripción	Soporte IPv4	Soporte IPv6	Riesgo
1	VIDEO VIGILANCIA	X	X	Bajo

Tabla N° 19: equipamiento de CCTV

6.8 Equipamiento de Control de Asistencia:

N°	Descripción	Soporte IPv4	Soporte IPv6	Riesgo
1	CONTROL DE ASISTENCIA 1	X	X	Bajo
2	CONTROL DE ASISTENCIA 2	X	X	Bajo
3	CONTROL DE ASISTENCIA 3	X	X	Bajo

Tabla N° 20: equipamiento de Control de Asistencia

6.9 Servicios

6.9.1 Servicio de Internet

N°	Descripción	Soporte IPv4	Soporte IPv6	Riesgo
1	GTD, 41 MBPS	X	X	Bajo

Tabla N° 21: Servicio de internet

6.9.2 Servicio de alojamiento de dominio:

N°	Descripción	Soporte IPv4	Soporte IPv6	Riesgo
1	regionjunin.gob.pe	X	X	Bajo

Tabla N° 22: Servicio de dominio

6.9.3 Servicio de correo electrónico:

N°	Descripción	Soporte IPv4	Soporte IPv6	Riesgo
1	RoundCube	X	X	Bajo
2	Zimbra 8.15	X	X	Bajo

Tabla N° 23: Servicio de correo electrónico

6.9.4 Servicio de hosting [Nube]:

N°	Descripción	Soporte IPv4	Soporte IPv6	Riesgo
1	www.regionjunin.gob.pe	X	X	Bajo

Tabla N° 24: Servicio de hosting [Nube]

6.9.5 Otros comprendidos en el alcance

6.10 Aplicaciones

N°	Descripción	Sistema Operativo	Soporte IPv4	Soporte IPv6	Riesgo
1	SIAF	WINDOWS SERVER 2016	X	X	*
2	SIGA	WINDOWS SERVER 2008 R2	X	X	*
3	WEB	CENTOS 7	X	X	*
4	CORREO	CENTOS 7	X	X	*
5	SISTEMASWEB	WINDOWS SERVER 2019	X	X	*
6	SISDORE	WINDOWS SERVER 2019	X	X	*
7	SIAR	UBUNTU SERVER 19	X	X	*
8	GEOSIAR	CENTOS 7	X	X	*
9	ANTIVIRUS	WINDOWS SERVER 2019	X	X	*
10	DNS (DIRECTORIO ACTIVO 1)	WINDOWS SERVER 2019	X	X	*
11	DNS (DIRECTORIO ACTIVO 2)	WINDOWS SERVER 2019	X	X	*

Tabla 25: Aplicaciones

VII. Implementación del Protocolo IPv6

7.1 Características generales del protocolo IPv6

Las *direcciones IPv6 tienen una longitud de 128 bits*, lo que equivale a 16 octetos que son escritos en una secuencia de 8 grupos de 4 dígitos hexadecimales, debido a que los diseñadores del protocolo optaron por representarlas de esta manera para permitir una representación más compacta que un grupo de unos y ceros. A pesar de esto, continúa siendo bastante complicada de manipular y recordar. En la tabla 9 se muestra algunos ejemplos de formatos como la reducción de ceros, el direccionamiento IP en su forma abreviada y las clases de direcciones.

	FORMATO COMPLETO	FORMATO ABREVIADO
REPRESENTACIÒN	x:x:x:x:x:x:x:x	Valor hexadecimal de 16 bits
EJEMPLOS	FEDC:DA98:7654:3210:FEDC:BA98:7654:3210	
	1080:0:0:0:8:800:200C:417A	
DIRECCION UNICAST	**1080:0:0:0:8:800:200C:417A**	1080::8:800:200C:417A
DIRECCION MULTICAST	FF01:0:0:0:0:0:0:101	FF01::101
DIRECCION DE LOOPBACK	0:0:0:0:0:0:0:1	::1(similar en IPv4 a 127.0.0)
DIRECCION NO ESPECIFICADA	0:0:0:0:0:0:0:0	::
EJEMPLO DE PREFIJOS DE 60 BITS	2AB:0000:0000:CD30:0000:0000:0000/60	2AB:CD30:0:0:0/60
NOTACION DECIMAL	0:0:0: 0:192.168.0.2	::192.168.0.2
	0:0:0:0:0:0:C0A8:2	::C0A8:2
DIRECCION COMPLETA	12AB:0:0:CD30:123:4567:89AB:CDEF/60	12AB::CD30:123:4567:89AB:CDEF/60

Tabla 26: Características generales del IPv6

Una de las nuevas características que presenta el protocolo IPv6 es la capacidad de dar soporte a direcciones IP que utilizan el protocolo IPv4; esto es de gran importancia para la coexistencia de los dos protocolos en infraestructuras de las redes actuales y las redes futuras.

Dirección IPv4	Dirección Ipv6	Definición
IP públicas	Direcciones Globales	Direcciones ruteables en Internet
10.0.0/8,192.168.0.0/16, 172.16.0.0/12	fec0::/48	Direcciones del tipo privado
127.0.0.1	::1	Dirección Loopback.
224.0.0.0/4	ff00::/8	Direcciones multicast.
0.0.0.0	::	Dirección no especificada
169.254.0.0/16	fe80::/64(link local)	Direcciones de autoconfiguración.
146.83.206.114	::ffff:146.83.206.114	Direcciones IPv4 compatibles.

Tabla 27: Configuración de servicios de Internet con IPv6

7.1.1 Tipos de direcciones en IPv6

a) **Unicast:** Identifican a una interfaz única; esto quiere decir que un paquete destinado a una dirección unicast será entregado únicamente a la interfaz identificada con dicha dirección.
b) **Anycast:** Estas direcciones identifican a un conjunto de interfaces, de tal manera que un paquete enviado a una dirección anycast será entregado a un miembro que pertenezca a este grupo, que generalmente es el más cercano según la distancia asignada en el protocolo de encaminamiento.
c) **Multicast:** Igual que las direcciones anycast, con la diferencia de que un paquete que sea enviado a una dirección multicast, es entregado a todas las interfaces del grupo. Las direcciones de broadcast no existen en IPv6; en reemplazo se han creado este tipo de direcciones.

Una de las características para resaltar es la*capacidad de autoconfiguración de IPv6*, pues ahorra a los administradores de la red mucho trabajo, su instalación e implementación es fácil y sencilla, debido a que ha sido diseñada con el fin de garantizar que la configuración manual no sea necesaria.

7.1.2 Seguridad en IPv6

La seguridad se da a través del IPsec, el cual es un concepto que se aplica cuando el paquete está listo y antes de ser enviado por la red; es obligatorio en IPv6 y su uso es opcional con IPv4. El IPsec fue diseñado para proporcionar seguridad en modo transporte (extremo a extremo) del tráfico de paquetes y en modo túnel (puerta a puerta) en el que la seguridad del tráfico de paquetes es proporcionada a varias máquinas por un único nodo.

IPv4	IPv6
Las direcciones tanto de origen como de destino son de 32 bits de longitud (4 Bytes).	Las direcciones de origen y destino son de 128 bits de longitud (16 Bytes).
IPSec es un protocolo opcional.	IPSec es una obligatoriedad.
No existe identificación de paquetes QoS que manejen los routers en sus cabeceras.	Con la utilización del campo flow label se tiene entendido que se está manejando QoS.
La fragmentación de un paquete lo realiza el host como el router, que produce retardos.	La fragmentación en IPv6 lo realiza únicamente el host porque el paquete es
Su cabecera tiene un cheksum.	Es eliminado el campo cheksum.
Se emplean solicitudes ARP para resolver direcciones IPv4 en una dirección de capa física.	Las tramas ARP son reemplazadas con mensajes multicast neighbor Discovery.
Usan registros A para la resolución de direcciones IPv4 a dominios.	Usan registros AAAA para la resolución de las direcciones IPv6.
Se utilizan las direcciones Broadcast para enviar un paquete a todos los nodos de las subredes.	Se utiliza una dirección multicast para poder enviar la información a los nodos de un ámbito local del vínculo.
Se debe configurar las direcciones de manera manual o utilizando DHCP.	No requiere de configuraciones manuales o utilizar DHCP.

Tabla 28: Cuadro de diferencias entre IPv6 y IPv4

7.1.3 Los mecanismos de transición del protocolo IPv6

Podemos agruparlos en tres categorías o estrategias que se han definido hasta la actualidad:

- **Doble Pila (Dual-Stack):** Este mecanismo de transición soporta ambas versiones del protocolo IP (IPv4/IPv6). Para su implementación se tiene que configurar todos los nodos con ambas pilas de protocolos (IPv4/IPv6), soportando direccionamiento (estático, DHCPv4, SLAAC o DHCPv6) y los protocolos de enrutamiento especificadas para cada versión (OSPFv3, RIPng, BGP4, IS-IS, entre otros).

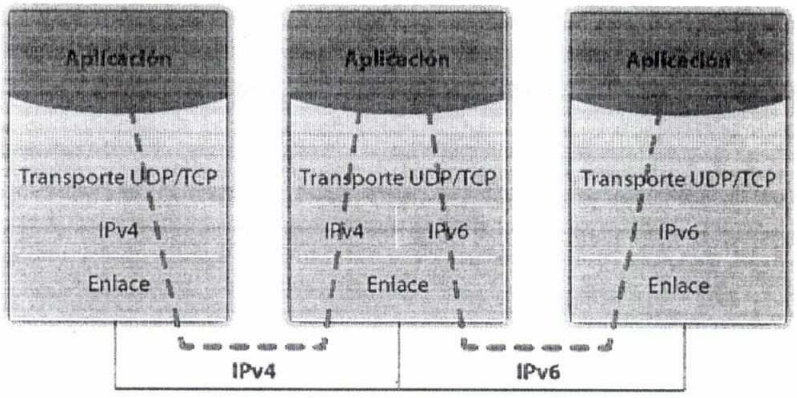

Gráfico 3: Modelo de transición doble pila

- **Túneles/Encapsulamiento**: Las técnicas que se agrupan en este mecanismo de transición parten del principio de establecer un túnel virtual de comunicación entre dos redes IPv6 a través de una red con IPv4. La red IPv6 envía un paquete con el formato IPv6 hasta su enrutador de borde, este enrutador encapsula el protocolo IPv6 en una cabecera IPv4 con valor de campo de protocolo 41, el cual indica que está encapsulando un paquete IPv6. Cuando el paquete es encapsulado por el protocolo IPv4 es importante verificar los valores configurados del MTU (Máximum Transfer Unit) y del MRU (Máximum Receive Unit) y la conversión de los mensajes ICMPv4/ICMPv6.

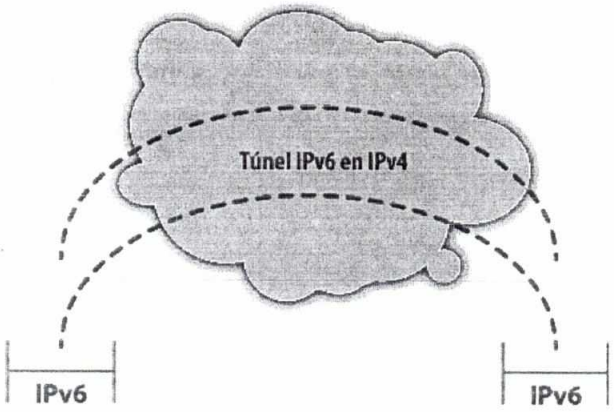

Gráfico 4: Modelo de transición túnel

- **Traducción (Translation):** Esta técnica permite traducir direcciones IPv6 en direcciones IPv4 y viceversa. En el escenario en el que una red IPv4 inicie el proceso de comunicación hacia una red IPv6 utilizando alguna técnica de traducción, la red IPv4 deberá utilizar doble pila (IPv4/IPv6) desde el host que quiera comunicarse.

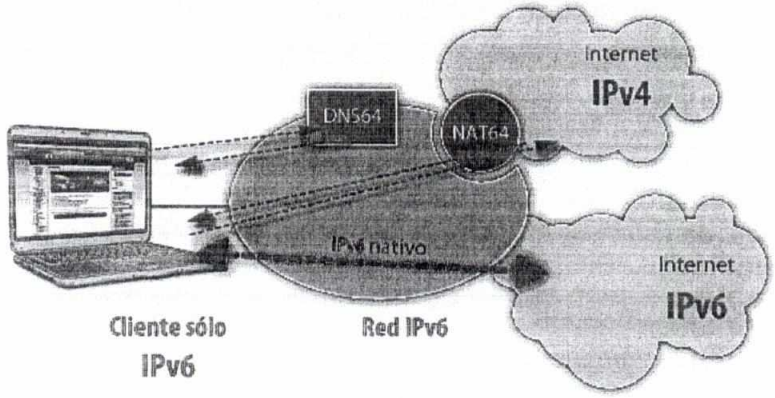

Gráfico 5: Modelo de transición traducción

TIPO	CONSUMO RECURSOS	COSTO OPERATIVO	COMPLEJIDAD
Doble Pila	Alto	Alto	Bajo
Túneles	Mediano	Mediano	Mediano
Traducción(NAT64/DNS64)	Alto	Alto	Alto

Tabla 29: Mecanismos de Transición de IPv6

VIII. Implementación del Protocolo IPv6

El objetivo principal en el despliegue es lograr la utilización de los estándares IPv4 e IPv6 en una infraestructura común proporcionando al usuario una experiencia que no requiera estar al tanto de qué protocolo se está utilizando.

Debemos remarcar que la parte más crítica a solventar es la coexistencia entre ambos estándares debido a su incompatibilidad. A largo plazo IPv4 se desvanecerá, pero como el proceso podría tardar algunos años más no debemos perder de vista tres requisitos esenciales en cualquier planificación para el despliegue de IPv6:

- ✓ La integración de IPv4 e IPv6 no debe afectar a los servicios y aplicaciones existentes.
- ✓ No debe haber ninguna reducción en la seguridad de la red derivada de la migración hacia IPv6.
- ✓ Se reutilizará la infraestructura existente, capacidades, contenidos y entornos de aplicación siempre que sea posible.

Para adaptar una red a IPv6 manteniendo la interoperabilidad con IPv4, podemos seguir una metodología genérica basada en las siguientes fases:

Fase 1: Formulación de Plan y Políticas vinculadas con la Transición al Protocolo IPV6

Tener un plan de enrutamiento para IPv6 no debe variar demasiado sobre lo que ya se hace en IPv4. En general para el Gobierno Regional Junín ya tiene sentido que en IPv6 se mantenga la misma topología que en IPv4, pues el mantener dos topologías significaría incrementar el costo de operación del encaminamiento de la red y el aumento de incidentes.

Nuestras opciones de enrutamiento en IPv6 son:

- Enrutamiento estático.
- Enrutamiento dinámico, en éste existen distintas categorías, como protocolos de vector distancia ó RIPNG (RIP Next Generation), protocolos de vector camino ("path vector") ó BGPv4 y protocolos de estado de enlaces: ISIS o u OSPFv3.

Con todas estas opciones, debemos considerar especialmente el enrutamiento ya existente en el Gobierno Regional Junín. Para OSPFv2 en la red IPv4, tiene sentido utilizar OSPFv3 en IPv6, al igual que utilizar BGPv4 para el encaminamiento externo. En caso de utilizar direccionamiento estático para IPv4, se puede utilizar las mismas configuraciones para IPv6.
No aplicaremos el uso de RIPNG ya que imposibilita el uso de técnicas modernas de ingeniería de tráfico.

La versión 6 del Protocolo de Internet ha sido diseñada para que su implementación se realice en coexistencia con IPv4. Por lo tanto, describimos algunos de los principales trabajos a realizar.

- Uso de Doble pila: Tanto en nodos como en enrutadores se tendrá un soporte IPv4 e IPv6, por lo tanto, tienen la habilidad de enviar y recibir paquetes de los dos protocolos. Se va operar de las siguientes maneras:
  - Con la pila IPv4 habilitada pero la pila IPv6 deshabilitada.
  - Con la pila IPv6 habilitada pero la pila IPv4 deshabilitada.
  - Con las dos pilas habilitadas.
- Uso de túneles: Cada túnel puede ser implementado de diferente manera:
  - Enrutador a enrutador. Los enrutadores IPv6/IPv4 interconectados por una infraestructura IPv4 pueden tunelizar paquetes IPv6 entre ellos.
  - Host a enrutador: Los host IPv6/IPv4 pueden tunelizar paquetes IPv6 a un enrutador IPv6/IPv4 por medio de una infraestructura IPv4.
  - Host a host. Los host IPv6/IPv4 que están conectados por una infraestructura IPv4 pueden tunelizar paquetes IPv6 entre ellos mismos.
  - Enrutador a host. Los enrutadores IPv6/IPv4 pueden tunelizar hacia sus destinos finales que son host IPv6/IPv4.

Fase 2: Definición y Diseño

Plan de Numeración IPv6: Por temas de administración y simplificación, a la configuración, los servidores y equipamiento de red ("switch", "router", "firewall", entre otros) se les asignará su dirección IPv6 de forma manual.
En una primera fase, habilitar el direccionamiento IPv6 para cada uno de los componentes de hardware y software de los servicios de: DNS, DHCP, Portal Web.
Es conveniente utilizar mecanismos de autoconfiguración existentes en IPv6, como el DHCPv6, que permite centralizar toda la asignación de direcciones de los equipos pertenecientes a un sitio o sede, como es el caso de las estaciones de trabajo y equipos periféricos.

#	Equipo	Siglas	Ejemplo IPv6
1	Router (LAN)	ROU	2001:1388:1::1:x
2	Server	SRV	2001:1388:1::2:x
3	Central Telefónica	PBX	2001:1388:1::3:x
4	Gateway	GWY	2001:1388:1::4:x
5	Impresoras	PRT	2001:1388:1::5:x
6	Print Server	PRS	2001:1388:1::6:x
7	Wireless	WIF	2001:1388:1::7:x
8	Eq. Seguridad	SEC	2001:1388:1::8:x
9	IDS	IDS	2001:1388:1::9:x
10	Cámaras IP	CIP	2001:1388:1::10:x
11	Administrador de Ancho de Banda	AAB	2001:1388:1::11:x

Tabla 30: Plan de numeración de IPv6

Protocolos de enrutamiento IPv6: En cuanto al enrutamiento interno, el uso de IPv6 no implica cambios significativos en la forma en que operan los protocolos de enrutamiento en las redes IP. Para aprovechar nuevas características del IPv6 se han desarrollado nuevas versiones o complementos de enrutamientos:

Protocolo de	Versión IPv6
OSPF	OSPFv3
BGP	BGP-MP
EIGRP	EIGRP for IPv6

Tabla 31: Protocolos de enrutamiento de IPv6

Asignar las rutas en los switches core y de accesos de la red, ruteadores internos y firewalls.

- Dado que IPv6 es un protocolo capa 3, su uso es transparente para todos los dispositivos capa 2; es decir, no habrá un impacto en la configuración de los "switches" de acceso que se encuentran a lo largo de los pisos del Gobierno Regional.
- Una vez configurada la red IPv6 en el Gobierno Regional Junín es necesario avanzar con el despliegue en los servicios básicos de red como el DHCP, DNS.

Fase 3: Migración de Servicios orientados a Internet y otros

PARA HARDWARE Y SOFTWARE:

Actualmente no se cuenta con un inventario de Software y Hardware en el Gobierno Regional. Por tal motivo se empezó a trabajar en ello.

Si bien todos los equipos existentes pueden estar en el proceso de transición a IPv6, se debe realizar actualizaciones y/o cambios en los equipos cuyas versiones sean Windows XP o Windows Vista, pues son versiones desarrolladas hace una década o más y probablemente presenten problemas con algunas configuraciones necesarias, además, Microsoft ya no brinda ningún tipo de soporte para Windows XP, lo que eventualmente puede presentar un gran inconveniente en el proceso de migración a IPv6.

La cantidad de equipos con sistema operativo Windows XP y Windows Vista no supera el 35% del total, además el cambio de éstos no es necesario de manera simultánea ni para el momento exacto en el que se empiece la migración, ya que los métodos de transición lo posibilitan así; debido a esto se hace factible el hecho de reemplazar dichos dispositivos por nuevos equipos que cuenten con versiones recientes de sistemas operativos Windows, Macintosh o Linux, que muy probablemente no presentarían ninguna dificultad en la transición.

PARA IMPRESORAS

Actualmente no se cuenta con un inventario de Impresoras en el Gobierno Regional. Por tal motivo se empezó a trabajar en ello.

Las principales marcas de impresoras usadas en el Gobierno Regional Junín son: HP, Konica Minolta, Canon y Epson, Brother.

Una vez analizadas las fichas técnicas de algunas impresoras, se encontró que fabricantes como HP, Konica Minolta, Canon, Epson y Brother señalan en ciertos modelos y tecnologías de impresoras láser que soportan IPv6, pero al revisar el software de administración de la impresora no se encuentra la opción para habilitar y configurar el protocolo IPv6; por tal razón se deduce que aún hace falta apropiación en temas de implementación del protocolo por parte de los fabricantes para indicar al usuario final cómo se activa. Por ello, alguno de los equipos de impresión es compatible con IPv6, y el resto no, por lo tanto, no existe el soporte que permita configurar de manera automática y/o manual el nuevo protocolo. En este caso se debe trabajar con la pila IPv4 habilitada pero la pila IPv6 deshabilitada para dichos equipos o caso contrario si tiene un buen perfonmance sustituir dicha impresora por otra que si realmente soporte IPv6.

PARA LOS EQUIPOS DE COMUNICACIÓN

Para los equipos de comunicación no se tendría muchos problemas ya que implicaría actualizar el sistema operativo de los Switch (16 total) de marca Juniper y Sistema Operativo JunOS. De la versión 12 a la última versión 18.4. Dichos equipos soportan dicha actualización. Cabe mencionar que algunas cosas pueden modificarse, como el uso de la sintaxis en JunOS a razón de ello se tendría que coordinar con los patner o soporte del IPS ya que dentro del contrato de servicio ofrece un servicio de soporte técnico a dichos equipos.

PARA LOS SERVIDORES

El total de servidores con la cuenta el Gobierno Regional Junín tiene soporte IPv6 debido a que los Sistemas Operativos en los que se encuentran operando son compatibles con el nuevo protocolo, por lo que sugieren una fácil implementación de cualquier mecanismo de transición, Doble Pila y/o Tunelización.

PARA LAS APLICACIONES

Con los aplicativos que corren sobre servidores con Sistemas Operativos compatibles con IPv6 no se tiene problema alguno en la implementación de técnicas para la coexistencia de los dos protocolos, por el contrario, como no se tiene potestad alguna sobre alguno de los aplicativos, se recomienda trabajarlos como "nodos IPv4 Only", en donde se implementen métodos de traducción para que puedan soportar la técnica Doble Pila, esto mientras dura el proceso de migración y se tiene una comunicación directa con las entidades responsables de dichos aplicativos para saber cuándo éstos empiecen a trabajar sobre IPv6, si es el caso de que aún no estén implementados y/o trabajando ya con el nuevo protocolo.

Fase 4: Migración de la (WAN)

Esta fase es importante y requiere la colaboración de profesionales involucrados en la materia.

- Se debe contar con personal calificado con conocimiento en todas las áreas necesarias para el desarrollo del proyecto: nociones y conceptos sobre IPv6.
- Trabajar en conjunto con proveedores de servicio internet- ISP al momento del diseño de la red tanto interna como externa de la entidad. En este caso se consultó al actual proveedor de servicio internet GTD, el cuál manifestó que cuentan con infraestructura lista de servicios internet con IPv6.
- Se requiere coordinar con los proveedores de servicios internet para lograr la conectividad integral de IPv6 con el exterior.
    - Habilitación y configuración de los ruteadores de internet.
    - Estructurar el esquema de direccionamiento.
    - Armar un esquema de diseño lógico de Red con IPv6.

Fase 7: Migración completa a IPv6

EQUIPOS DE COMUNICACIÓN

- Diseño de la red con el nuevo esquema IPv6:
- Plan de Numeración IPv6
- Por temas de administración y simplificación, a la configuración, los servidores y equipamiento de red ("switch", "router", "firewall", entre otros) se les asignará su dirección IPv6 de forma manual.
- En una primera fase, habilitar el direccionamiento IPv6 para cada uno de los componentes de hardware y software de los servicios de: DNS, DHCP, Portal Web.
- Es conveniente utilizar mecanismos de autoconfiguración existentes en IPv6, como el DHCPv6, que permite centralizar toda la asignación de direcciones de los equipos pertenecientes a un sitio o sede, como es el caso de las estaciones de trabajo y equipos periféricos.
- Establecer los protocolos de enrutamiento IPv6 adecuadamente: En cuanto al enrutamiento interno, el uso de IPv6 no implica cambios significativos en la forma en que operan los protocolos de enrutamiento en las redes IP. Para aprovechar nuevas características del IPv6 se han desarrollado nuevas versiones o complementos de enrutamientos:
- Asignar las rutas en los switches core de la red, ruteado interno y firewall. Dado que IPv6 es un protocolo capa 3, su uso es transparente para todos los dispositivos capa 2; es decir, no habrá un impacto en la configuración de los "switches" de acceso que se encuentran a lo largo del edificio del Gobierno Regional Junín.
- Una vez configurada la red IPv6 configurar DHCPv6 y DNS.

SERVIDORES DE PRODUCCIÓN

La configuración de los Servidores de Producción es considerada la última etapa que se considera para la configuración IPv6 entre ellos cabe nombrar:

- Bases de datos.
- Sistemas de almacenamiento.
- Sistema de Call Center.
- Comunicaciones unificadas y dispositivos end-point.

Es probable que exista remanentes de dispositivos **end-point** que aun cuenten con direcciones IPv4 tales como: impresoras, computadoras antiguas, equipos inalámbricos y otros, que pueden tomar un poco más de tiempo en

estandarizar y habilitarlos al IPv6. Para ellos son los switches y routers los elementos base de soportar el esquema doble pila IPv6; es decir, de soportar ambos protocolos IPv4/IPv6, garantizando la migración de manera controlada.

APLICACIÓN DE POLÍTICAS DE SEGURIDAD DEL PROTOCOLO IPV6 EN LOS EQUIPOS DE SEGURIDAD Y COMUNICACIONES.

Se debe aplicar Estrategias de monitoreo, el monitoreo de la red y de los servicios que hay implementados sobre ella cobran importancia cuanto más críticos nos resultan estos servicios o vínculos de la red.

- Actualizar las herramientas y procesos de seguridad.
- Obtener equipos certificados es decir su licencia debe estar activa y válida.
- Desarrollar prácticas de programación adecuadas para IPv6.
- Contar con auditorias que conozcan IPv6.
- Incluir en la herramienta de monitoreo las nuevas direcciones IPv6 y validaciones de los servicios mediante ambos protocolos (recordar que IPv4 no se elimina).
- Detectar y prevenir problemas. Diagnosticar causas de fallas.
- Determinar las acciones que solucionarán el problema y documentarlas.
- Conformar planes de contingencia.
- Realización de pruebas y monitoreo de la funcionalidad del protocolo IPv6 en los sistemas de información, sistemas de almacenamiento, sistemas de comunicaciones y servicios de la entidad, generando tráfico de IPv6 desde la entidad hacia el internet y viceversa.
- Realización de pruebas de funcionalidad del protocolo IPv6 con respecto a las políticas de seguridad perimetral de servidores de cómputo, servidores de comunicaciones y demás equipos de comunicaciones.
- Realización del afinamiento de las configuraciones de hardware, software y servicios de la entidad, tomando como referencia el informe de configuraciones del protocolo IPv6 de la fase pasada.
- Elaboración de un inventario final de servicios, aplicaciones y sistemas de comunicaciones bajo el esquema de funcionamiento del protocolo IPv6.

IX. Realización de Pruebas

Es recomendable iniciar la implementación de manera parcial, teniendo en cuenta las aplicaciones más críticas con las que cuenta EL Gobierno Regional Junín. Para ello es preciso contar con un segmento de red alterno para realizar las pruebas antes de iniciar la producción y así evitar la interrupción de cualquiera de los servicios y aplicaciones.
La realización de pruebas es importante para el funcionamiento correcto de la implementación de IPV6 ello implica:

- Realizar las configuraciones, monitoreo y las pruebas de acceso con clientes IPv6 e IPv4.
- Elaborar informes técnicos indicando recursos, secuencias que fueron necesarias, conclusiones y recomendaciones para la configuración de IPv6.
- Comprobar la funcionalidad del protocolo IPv6 frente a las políticas de seguridad perimetral (firewalls) de la entidad.
- Afinamiento de las configuraciones de hardware, software y servicios de la entidad.
- Aplicar los criterios de seguridad IPv6 en la plataforma configurada.
- Elaborar un inventario final de servicios, aplicaciones y sistemas migrados.

X. Capacitación y Sensibilización

Una de las tareas fundamentales para la implementación de IPv6 es la capacitación del personal técnico quien se encargará de la implementación. Esto tiene el propósito de que el personal se familiarice con los conceptos y lógica de funcionamiento del protocolo.

- Elección de los ingenieros y/o profesionales que trabajan en las áreas técnicas de ORDITI de la entidad, para cumplir con todas las actividades que este proyecto demanda.
- Talleres de entrenamiento al personal técnico sobre conceptos, configuraciones, seguridad de redes IPv6 (equipos de redes, servidores).
- Reforzar las capacidades para revisar las opciones técnicas y ver cuál es la apropiada relacionado al proceso de migración del protocolo IPv6.

XII. Anexos

ANEXO: Cronograma Diagnóstico de la Infraestructura

Ítem	Responsable	Actividad	Producto	Fecha inicio	Duración	Fecha fin
1	ORDITI	Inventario	Inventario de comunicaciones	01/06/2020	90	03/09/2020
	ORDITI		Inventario de telefonía	01/06/2020	90	03/09/2020
	ORDITI		Inventario de servidores - hardware	01/06/2020	30	01/07/2020
	ORDITI		Inventario de servidores - sistema operativos físicos y virtuales	01/06/2020	30	01/07/2020
	ORDITI		Inventario de equipamiento - usuarios	01/06/2020	90	03/09/2020
	ORDITI		Inventario de equipamiento - Varios	01/06/2020	90	08/06/2020
	ORDITI		Inventario de servicios - Internet	01/06/2020	30	01/07/2020
	ORDITI		Inventario de servicios - Dominio	01/06/2020	30	01/07/2020
	ORDITI		Inventario de servicios - Correo electrónico	01/06/2020	30	01/07/2020
	ORDITI		Inventario de servicios - Hosting	01/06/2020	30	01/07/2020
	ORDITI		Inventario de aplicaciones	01/06/2020	30	01/07/2020
	ORDITI		Entregable de Inventario	01/06/2020	30	01/07/2020
2	ORDITI	Diagnostico	Diagnóstico de comunicaciones	01/06/2020	60	01/08/2020
	ORDITI		Diagnóstico de telefonía	01/06/2020	60	01/08/2020
	ORDITI		Diagnóstico de servidores - hardware	01/06/2020	30	01/07/2020
	ORDITI		Diagnóstico de servidores - sistema operativos físicos y virtuales	01/06/2020	30	01/07/2020
	ORDITI		Diagnóstico de equipamiento - usuarios	01/06/2020	90	03/09/2020
	ORDITI		Diagnóstico de equipamiento - Varios	01/06/2020	90	03/09/2020
	ORDITI		Diagnóstico de servicios - Internet	01/06/2020	30	01/07/2020
	ORDITI		Diagnóstico de servicios - Dominio	01/06/2020	30	01/07/2020
	ORDITI		Diagnóstico de servicios - Correo electrónico	01/06/2020	30	01/07/2020
	ORDITI		Diagnóstico de servicios - Hosting	01/06/2020	30	01/07/2020
	ORDITI		Diagnóstico de aplicaciones	01/06/2020	30	01/07/2020
	ORDITI		Entregable de diagnostico	01/06/2020	90	03/09/2020
3	ORDITI	Evaluación de Riesgo	Medición de Riesgo - Infraestructura Tecnológica	01/06/2020	90	03/09/2020
	ORDITI		Medición de Riesgo - Servicios	01/06/2020	90	03/09/2020
	ORDITI		Medición de Riesgo - Aplicaciones	01/06/2020	90	03/09/2020
	ORDITI		Entregable de Medición de Riesgo	01/06/2020	90	03/09/2020

ANEXO: Cronograma Implementación del protocolo IPv6

Ítem	Responsable	Producto	Fecha inicio	Duración	Fecha fin
1	Oficial de Seguridad ORDITI | Jefatura ORDITI	Formulación de política de seguridad	01/06/2020	30	01/07/2020
2	Oficial de Seguridad ORDITI | Jefatura ORDITI	Definición y diseño	01/06/2020	90	03/09/2020
3	Infraestructura ORDITI	Migración de Servicios orientados a Internet	01/02/2021	180	02/08/2021
		Contratación del servicio de internet vía IPV6 para servicios publicados	01/02/2021	180	02/08/2021
		Adquisición de equipamiento requerido para soporte IPV6	01/02/2021	180	02/08/2021
4	Infraestructura ORDITI	Migración del acceso a internet desde usuarios internos mediante IPv6	01/02/2021	180	02/08/2021
		Contratación del servicio de internet vía IPV6, de salida hacia internet	01/02/2021	180	02/08/2021
		Adquisición de equipamiento requerido para soporte IPV6	01/02/2021	180	02/08/2021
5	Infraestructura ORDITI	Migración de la WAN	01/02/2021	180	02/08/2021
		Contratación del servicio de WAN/MPLS/VPN vía IPV6	01/02/2021	180	02/08/2021
		Adquisición de equipamiento requerido para soporte IPV6	01/02/2021	180	02/08/2021
6	Infraestructura ORDITI | Sistemas de Información ORDITI	Migración de las aplicaciones	01/02/2021	240	01/10/2021
		Adquisición de equipamiento requerido para soporte IPV6	01/02/2021	240	01/10/2021
7	Infraestructura ORDITI | Oficial de Seguridad ORDITI | Jefatura ORDITI	Migración completa a IPv6	01/02/2021	240	01/10/2021
		Adquisición de equipamiento requerido para soporte IPV6	01/02/2021	240	01/10/2021

ANEXO: Cronograma Realización de Pruebas

Ítem	Responsable	Producto	Fecha inicio	Duración	Fecha fin
3	Infraestructura ORDITI	Pruebas: Migración de servicios orientados a Internet Optimización	01/02/2021	240	01/10/2021
4	Infraestructura ORDITI	Pruebas. Migración del acceso a internet desde usuarios internos mediante IPv6 Optimización	01/02/2021	240	01/10/2021
5	Infraestructura ORDITI	Pruebas: Migración de la WAN Optimización	01/02/2021	240	01/10/2021
6	Infraestructura ORDITI Sistemas de Información ORDITI	Pruebas: Migración de las aplicaciones Optimización	01/02/2021	240	01/10/2021
7	Infraestructura ORDITI Oficial de Seguridad ORDITI Jefatura ORDITI	Pruebas: Migración completa a IPv6 Optimización	01/02/2021	240	01/10/2021

ANEXO: Cronograma Capacitación y sensibilización

Ítem	Responsable	Producto	Fecha inicio	Duración	Fecha fin
1	Infraestructura ORDITI Oficial de Seguridad ORDITI Jefatura ORDITI	Capacitación: Personal Técnico	04/01/2021	90	01/04/2021
2	Infraestructura ORDITI Oficial de Seguridad ORDITI Jefatura ORDITI	Capacitación: Usuario Final	04/01/2021	60	29/01/2021