Asunción, 13 de junio del 2025

Estimados UCP-MEF

Presente:

A quien corresponda:

Me dirijo a Uds. con el fin de entregar el compendio completo del proyecto la "Definición del Plan de Infraestructura Tecnológica" de la DNCP OBP Nro. P230707, en el marco del préstamo Nro. 4671/OC-PR que forma parte del Proyecto de Mejoramiento de las Finanzas Públicas para el Desarrollo Sostenible del Paraguay.

Los entregables en formato impreso son:

1- Diagnóstico de la situación actual
2- Revisión de procedimientos
3- Recomendación de procedimientos
4- Plan de infraestructura tecnológica

Los archivos adicionales, planillas, fotos, diagramas serán disponibilidades mediante un disco compartido en la nube.

Posteriormente seguiremos teniendo las reuniones de presentación y evaluación del informe con el equipo técnico como parte del cierre del proceso, así como los análisis pertinentes para cada proyecto evaluado.

Atentamente,

Victor Hugo Morel Cattebeke

Consultor CI: 1.204.808

RECIBIDO
UNIDAD COORDINADORA DE PROGRAMAS
13 JUN 2025
Programa "Mejoramiento de las Finanzas Públicas para el Desarrollo Sostenible del Paraguay"

Mario Ariel Bernal

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Contrato Nro 21/2024

Proyecto de Mejoramiento de las Finanzas Públicas para el Desarrollo Sostenible del Paraguay

Contrato de Préstamo N° 4671/OC-PR

"Definición del Plan de Infraestructura Tecnológica"

OBP N° P230707.

Diagnóstico de la situación actual

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

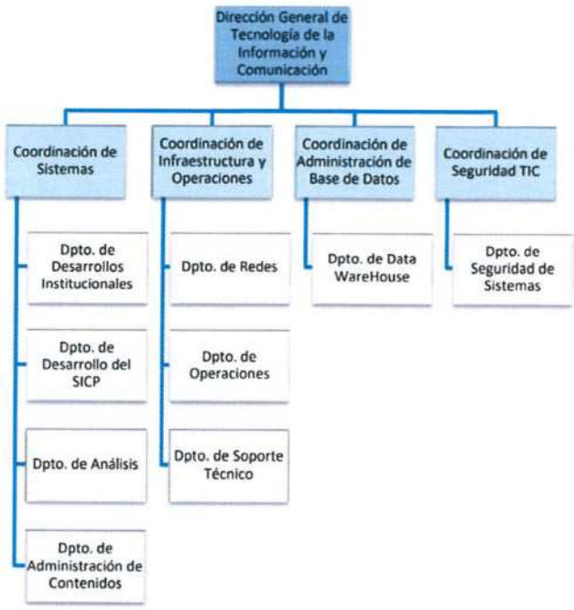
Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

2 Recursos humanos que dan soporte a la gestión de infraestructura.

2.1 Organigrama actual

El equipo humano está organizado de forma tradicional en cuatro áreas principales, esto está acorde a cómo van evolucionando las estructuras operativas de tecnologías en distintas instituciones, vemos que el equipo de tecnología se divide en cuatro grupos principales.

1. Desarrollo
2. Infraestructura
3. Base de Datos
4. Seguridad



Esto esta razonablemente alineado con el Decreto Nr 6234/2016 ***"POR EL CUAL SE DECLARA DE INTERÉS NACIONAL LA APLICACIÓN Y EL USO DE LAS TECNOLOGÍAS DE LA INFORMACION Y COMUNICACIÓN (TIC) EN LA GESTION PUBLICA, SE DEFINE LA ESTRUCTURA MINIMA CON LA QUE SE DEBERÁ CONTAR Y SE ESTABLECEN OTRAS DISPOSICIONES PARA SU EFECTIVO FUNCIONAMIENTO"***

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

El cual busca organizar las áreas de tecnología en 4 (cuatro) acorde al artículo nro. 5 de dicho documento:

> ***Art. 5°.-*** *El área de TIC deberá contar con una estructura mínima que le permita cumplir con sus funciones, pudiendo esta ser ampliada de acuerdo a las necesidades de cada institución. Dicha estructura contempla cuatro (4) áreas de trabajo: 1- Sistemas, 2- Infraestructura y Operaciones TIC, 3- Seguridad TIC y 4-Mesa de Ayuda, y adicionalmente un Staff Técnico y Administrativo.*
>
> *Además, el área de TIC con anuencia de la máxima autoridad deberá elaborar manual de organización y funciones, reglamentaciones y políticas de adquisición, administración y uso de las TIC.*

Estas áreas propuestas por el MITIC son las siguientes:

1. Sistemas
2. Infraestructura y Operaciones TIC
3. Seguridad TIC
4. Mesa de Ayuda

A esto se suma

- 1 (un) Staff técnico
- 1 (un) Staff Administrativo

Ya preparándonos para la revisión y evaluación posterior, procedemos a preparar un organigrama detallado completo, que posteriormente sirva para generar los organigramas tentativos a futuro, esto lo preparamos en formato pdf y xlsx editable.

La idea es posteriormente ir alineando la estructura actual vigente a las estructuras propuestas e ir creando el espacio de crecimiento y proyección de los recursos internos.

Ares que requieren evaluación posterior son:

- Mesa de ayuda
- Desarrollo
- Infraestructura Producción y Operación
- Seguridad
- Inteligencia de Negocios

A esto se suma la posterior resolución de MITIC nro. 733/2019 "***POR LA CUAL SE APRUEBA EL MODELO DE GOBERNANZA DE SEGURIDAD DE LA INFORMACION"*** en su ANEXO I

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

POR LA CUAL SE APRUEBA EL MODELO DE GOBERNANZA DE SEGURIDAD DE LA INFORMACIÓN.----------

- 4 -

ANEXO I
MODELO DE GOBERNANZA DE SEGURIDAD DE LA INFORMACIÓN

- *Área de Seguridad de la Información: Toda Institución Pública deberá contar con un Área de Seguridad de la Información, el cual deberá posicionarse en la estructura organizativa de manera a reportar a la Máxima Autoridad Institucional.*

- *Objetivo: el Área de seguridad de la información tiene como objetivo velar por la seguridad de todos los activos de información de la institución en cuanto a su confidencialidad, integridad y disponibilidad.*

- *Activos de información: los mismos incluyen, pero no se limitan a: los archivos de la Institución, ya sea en formato electrónico o no; los sistemas, equipos y redes en lo que se almacenan, procesan y/o transmiten la información institucional.*

- *Interdependencia del Área de Seguridad de la Información: el Área de Seguridad de la Información no debe depender del área de TIC o tecnología de las Instituciones; sin embargo, ambas áreas deben trabajar de manera conjunta y coordinada a fin de a garantizar el correcto funcionamiento de los sistemas de información y activos tecnológicos institucionales. El área de Seguridad de la Información no sustituye a las áreas de Seguridad TIC y/o otras áreas operativas, las cuales deberán igualmente trabajar de manera coordinada con los planes y lineamientos emitidos por el área de Seguridad de la Información.*

- *Responsabilidades del Área de Seguridad de la Información:*

    - *Identificar y evaluar los riesgos y las brechas que afectan a los activos de información de la institución y proponer planes y controles para gestionarlos.*
    - *Elaborar y velar por la implementación de un plan o estrategia de seguridad de la información en la Institución.*
    - *Elaborar, proponer y velar por el cumplimiento de las políticas de seguridad de la información de la Institución.*
    - *Proponer los planes de continuidad de negocio y recuperación de desastres en el ámbito de las tecnologías de la información.*
    - *Supervisar la administración del control de acceso a la información.*
    - *Supervisar el cumplimiento normativo de la seguridad de la información, incluido aquellas directrices y lineamientos dispuestas por el Ministerio de Tecnologías de la Información y Comunicación (MITIC) en su carácter de autoridad de prevención, gestión y control en materia de Ciberseguridad en resguardo del ecosistema digital nacional.*

Es importante tener en cuenta que durante el proceso de transición la mayoría de las instituciones públicas, estas irán formando sus respectivos equipos de seguridad hasta lograr la madurez solicitada por el MITIC, esto acorde al siguiente párrafo de la misma resolución nro. 733/2019

La cual dispone:

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

- *Disposiciones Transitorias: Las instituciones que, debido a factores ajenos a su control, se encuentren imposibilitadas de dar cumplimiento a la presente Resolución, igualmente deberá designar al menos un Responsable de Seguridad de la Información, de acuerdo a las directrices de la presente Resolución, hasta tanto sea posible realizar la adecuación definitiva.*

Podemos por ende asumir en conversaciones con el equipo Directivo de Tecnología que la DNCP está alineada con los requisitos de las distintas instituciones estatales reguladoras y en un proceso de transición para dar cumplimiento total a los mismos, se está evaluando las distintas áreas de la misma, referentes a sistemas, infraestructura, seguridad y mesa de ayuda.

Dicho eso, es importante tener en cuenta que la implementación de un Modelo de gobernanza de seguridad de la información posee tres partes.

1. Creación de las políticas de seguridad de la información.
2. Implementación de las políticas de seguridad.
3. Auditoría y control de estas.

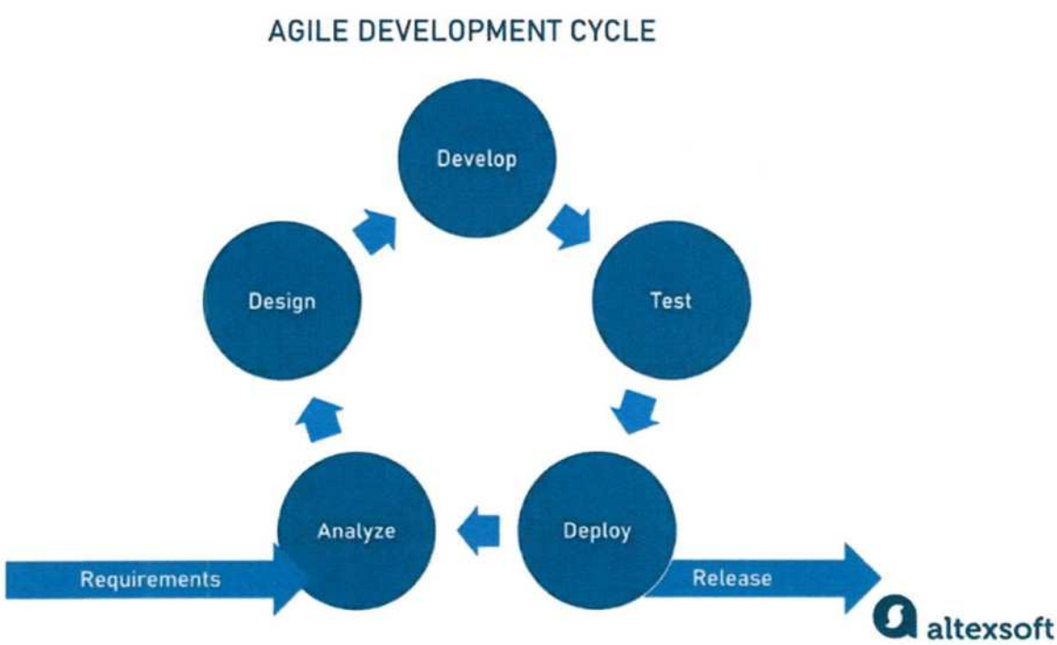
Los puntos observables de forma directa son:

- El equipo de tecnología posee una estructura magra y eficiente acorde a la cantidad de personal asignado a las tareas del área, es importante tener en cuenta que solo la tarea de llevar adelante el SICP es suficiente para copar de tareas al personal, no olvidar que a esto también se debe sumar el apoyo a los recursos internos de la institución, así como también procesos licitatorios eventuales que requieran evaluación.
- El equipo de mesa de ayuda hoy se encuentra dentro de la coordinación de infraestructura, si bien el equipo tiene basta capacidad para resolver los problemas, esto no está alineado con la estructura dispuesta por el MITIC.
- Se debe evaluar los tickets procesados por mesa de ayuda, ya que los mismos están colaborando con muchas tareas de ofimática (Word, Excel, PowerPoint) que si bien suman a la institución podrían ser resueltas con jornadas de capacitación ya que los mismos de por si no constituyen tareas técnicas informática sino de conocimientos que deben tener los personales en si para cumplir sus actividades.
- El área de seguridad informática se encuentra bajo la Dirección de Tecnología, esto es normal en sus inicios ya que el conocimiento necesario para construir las herramientas en dicha área nace de esta, a futuro puede irse alineado a las disposiciones del MITIC a la par que se van habilitando reformas en la estructura y las personas que puedan apoyar a plenitud dicha área.
-
- El equipo de planificación, diseño del SICP es mayormente interno, pero la ejecución del desarrollo, acompañamiento y asistencias en nuevas prácticas, modelado y tecnología es subcontratada, así que es muy importante que el sistema de desarrollo continuo e implementación continua sea implementado correctamente de manera de permitir que la DNCP

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

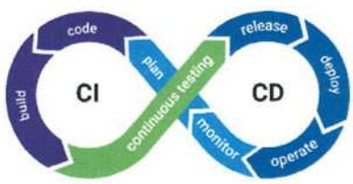
tenga gobernanza sobre el sistema SICP, su código fuente, puesta en productivo y posterior documentación los siclos tradicionales de desarrollo.

- Hoy en día dentro de tecnología ya se está evaluando la mejora de todo el ciclo de desarrollo de nuevas funcionalidades ya la creación de un proceso de control de calidad.



Dentro del equipo operativo actual como vemos más adelante tenemos varios componentes del ciclo de desarrollo, así como lo propone la metodología Ágil, hoy en día algunas áreas están cumpliendo una doble función, lograr esto nos daría el ciclo completo de desarrollo.

Ya contamos con un equipo de análisis, diseño y desarrollo, así como las pruebas internas, y potencialmente se debe evaluar separar las funciones de QA (Quality Assurance) que en la metodología ágil es conocida como TEST, pero se realizan de forma externa al equipo de desarrollo, y finalmente un grupo se encargue en forma externa de llevar a productivo las soluciones.



Hoy en día la infraestructura de apoyo, principalmente en la forma de la plataforma OpenShift y Git, ampliamente permiten esta mecánica, pero la cantidad de personal actual obliga a duplicar algunas funciones.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

2.2 Equipo operativo actual

Dirección General de Tecnología de la Información y Comunicación: David Reese

Coordinación de Sistemas: Nimia Garcia

Dpto. de Desarrollos Institucionales: Jonathan Marquez

Dpto. de Desarrollo del SICP: Jorge Miranda

Dpto. de Análisis: Ruth Maciel

Dpto. de Administración de Contenidos: Roldolfo Cazal

Coordinación de Infraestructura y Operaciones: Hugo Araujo

Dpto. de Redes:Christian Garay

Dpto. de Operaciones: Jorge Javier

Dpto. de Soporte Técnico: Martha Caceres

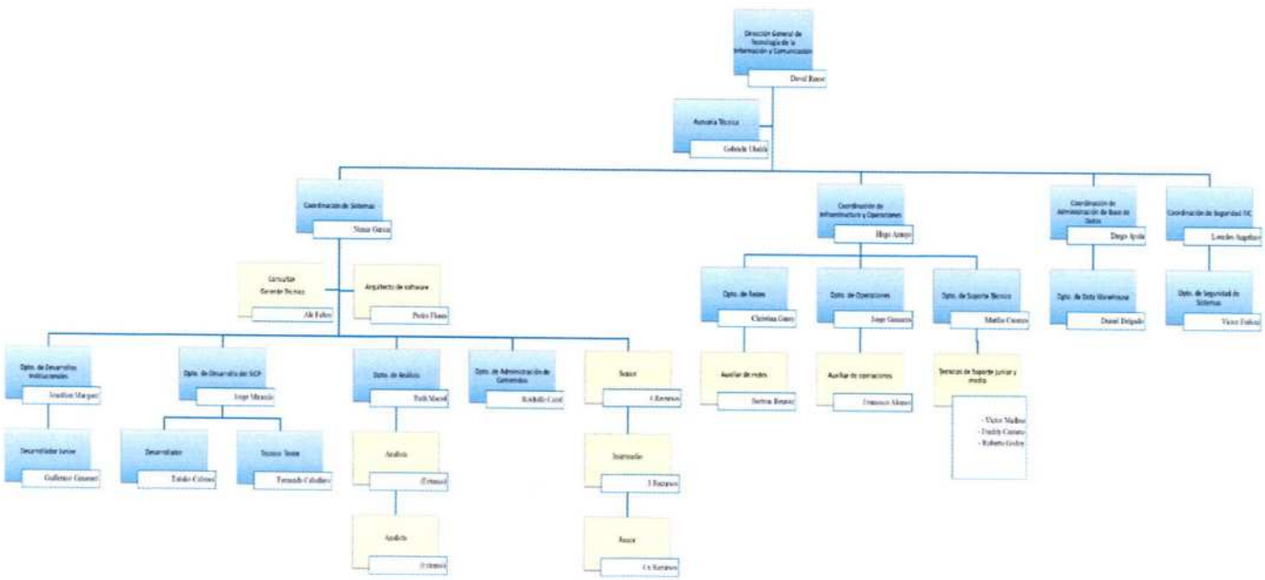
Coordinación de Administración de Base de Datos: Diego Ayala

Dpto. de Data WareHouse: Daniel Delgado

Coordinación de Seguridad TIC: Lourdes Angelino

Dpto. de Seguridad de Sistemas: Victor Ferloni

2.3 Organigrama expandido contemplando todo el equipo permanente, comisionados y contratados.



Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

2.4 Situación General del Personal de TIC

2.4.1 Perfil del Personal

El equipo de TIC está conformado por personas cuyas edades están entre 26 y 48 años, desempeñando diversos roles tales como las áreas de Redes y Operaciones, Base de datos, seguridad, mesa de ayuda. En términos de nivel educativo, la mayoría cuenta con títulos universitarios, aunque algunos todavía se encuentran estudiando.

Un punto importante es tocar es que, si bien el organigrama actual responde a necesidades tecnológicas a presente, tenemos que ir preparando al personal para que la DNCP vaya adecuándose a la criticidad de las operaciones a las cuales está siendo exigida, la operación 24/7 que se está volviendo una realidad y adicionalmente ir adecuándonos a las necesidades de seguridad, así como inteligencia de negocios que deben ir planificándose para que conformen parte de la estructura a futuro.

Para lo cual es fundamental que dentro de las descripciones de cargo vayamos preparando al personal que nos servirá de respaldo para los lideres actuales de la operativa, hacia donde estarán yendo dichos roles y quienes podrán colaborar con los mismos en su crecimiento.

Adicionalmente debemos contemplar que la operativa va a requerir de roles de producción y operación que son fundamentales en la administración de servicios 24/7, estos cada uno con sus responsabilidades criticas dentro de la operación.

2.4.2 Experiencia y Alineación Profesional

Años de experiencia: La experiencia laboral en el sector TIC de los funcionarios varía significativamente, desde 3 hasta más de 20 años. Los roles de mayor responsabilidad tienden a estar ocupados por quienes tienen entre 11 y 20 años de trayectoria.

Alineación académica: El personal considera que su formación está mayoritariamente alineada con las demandas del puesto, aunque existe la percepción de que hay áreas de mejora, especialmente en capacitación técnica.

Obsolescencia de conocimientos: Se detecta que existe personal que precisa actualizar sus conocimientos.

2.4.3 Competencias Técnicas

- Herramientas tecnológicas: Varios miembros indican un nivel bajo de familiaridad con las herramientas utilizadas por la institución, lo cual podría impactar en la eficiencia.
- Seguridad informática: Una gran parte tiene conocimientos generales, pero carece de experiencia práctica en temas críticos como prácticas OWASP, firewalls, y gestión de vulnerabilidades.
- Administración de redes/servidores: Algunos no cuentan con experiencia, mientras que otros poseen conocimientos técnicos pero poca o nula experiencia práctica.

2.4.4 Manejo de Problemas e Incidentes

- Resolución técnica: Los funcionarios suelen abordar problemas desconocidos mediante investigación, consulta con colegas o recopilación de datos para comprender mejor la situación.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

- Incidentes críticos: La mayoría no ha enfrentado incidentes críticos en sus áreas, pero cuando lo han hecho, han tomado medidas sistemáticas como diagnósticos iniciales, comunicación con el equipo y seguimiento del problema.

2.4.5 Fortalezas y Áreas de Mejora

- Fortalezas: Se destacan la posibilidad de capacitación constante, habilidades de investigación y conocimiento especializado en áreas como bases de datos.
- Aspectos para mejorar: El personal identifica la necesidad de fortalecer conocimientos técnicos, familiarizarse con más herramientas y mejorar procesos específicos como la atención en mesa de ayuda. Se identifica que especialmente en el área de ciberseguridad se precisa mayor nivel de conocimiento.

2.5 Necesidades de Recursos

Capacitaciones adicionales: Cursos en áreas específicas como seguridad informática, herramientas tecnológicas (Microsoft, Apple) para el personal de soporte helpdesk, bases de datos no sql ejemplo Elastic search, Linux, servidores, virtualizaciones minería de datos.

- Equipos y personal: Recursos humanos suficientes para cumplir con las demandas operativas, mejorar la atención y distribución de cargas de trabajo.
- Herramientas: software para gestión de inventarios de hardware y software,
- Actualización del sistema de control de acceso.
- Equipos servidores para realizar pruebas.

2.6 Colaboración Interdepartamental

El personal recomienda:

- Fortalecer la comunicación: Mejorar la coordinación entre áreas y fomentar una cultura de comunicación efectiva.

- Capacitación cruzada: Promover actividades donde todos conozcan las funciones y retos de otras áreas dentro de la institución.

2.7 Observaciones

1. Experiencia diversificada: Existe una amplia gama de conocimientos y experiencia, pero también una necesidad significativa de capacitación técnica específica.

2. Desafíos en herramientas: Es fundamental aumentar la familiaridad del equipo con las tecnologías utilizadas en la institución.

3. Colaboración: Una mejor comunicación y capacitación cruzada podrían optimizar la integración entre áreas.

4. Recursos limitados: Es necesario invertir en formación y equipamiento para atender las demandas del personal y de los puestos.

Este informe refleja los aspectos más relevantes derivados del formulario de relevamiento y sirve como punto de partida para planificar acciones de mejora en la DGTIC.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

2.8 Capacitaciones recomendadas

De acuerdo con las necesidades identificadas en el informe, los cursos que deberían tomar el personal de TIC incluyen:

2.8.1 Seguridad Informática

- Introducción a OWASP y gestión de vulnerabilidades.
- Configuración y gestión de firewalls.
- Detección y prevención de intrusos.
- Criptografía aplicada.

2.8.2 Administración de Redes y Servidores

- Configuración de redes y protocolos avanzados.
- Gestión y monitoreo de servidores.
- Implementación y administración de ruteadores.
- Curso de Linux avanzado para creación de scripts.
- Power automate.
- Open shift.

2.8.3 Herramientas Específicas

- Uso avanzado de herramientas Microsoft (Office 365, Azure, etc.).
- Gestión y configuración de equipos Apple.
- Linux, openshift.

2.8.4 Bases de Datos

- Administración y optimización de bases de datos.
- Herramientas de minería de datos y análisis avanzado.
- Base de Datos SQL.

2.8.5 Atención y Soporte Técnico

- Mejora en procedimientos de mesa de ayuda.
- Comunicación efectiva con usuarios finales.
- Resolución de problemas técnicos comunes.

2.8.6 Capacitación Cruzada

- Conocimiento de las funciones y retos de otras áreas dentro de la institución.
- Talleres de colaboración interdisciplinaria.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

2.9 Conclusiones y Recomendaciones:

Los resultados indican que, si bien el personal de TIC cuenta con experiencia relevante y competencias adecuadas, es necesario abordar áreas clave como familiaridad con tecnologías institucionales, fortalecimiento de capacidades técnicas específicas, y mejora en la comunicación interdepartamental. Se recomienda:

1. Diseñar un plan integral de capacitación técnica enfocado en las necesidades identificadas.

2. Incrementar los recursos humanos y materiales en áreas críticas.

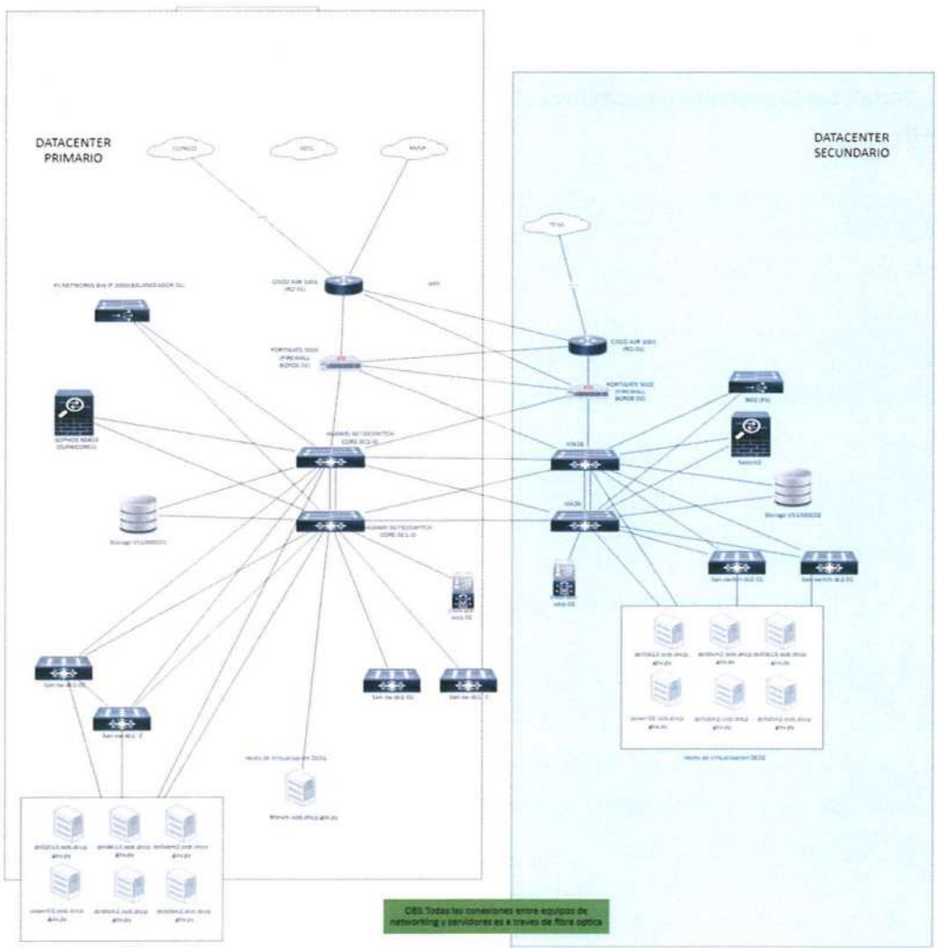
3. Fortalecer los canales de comunicación interna para evitar duplicidad de esfuerzos y mejorar la eficiencia.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

3 Diagrama de red.

El diagrama actual de red utilizado por la DNCP contempla la estructura distribuida en dos datacenter, uno primario y otro secundario.

Dentro de cada datacenter dicha infraestructura está distribuida en una línea de equipos de CORE, representados por los equipos Huawei S6730 al cual se conecta la infraestructura de virtualización, y una serie de equipos de distintos proveedores que representan la línea de distribución y posterior agregación.

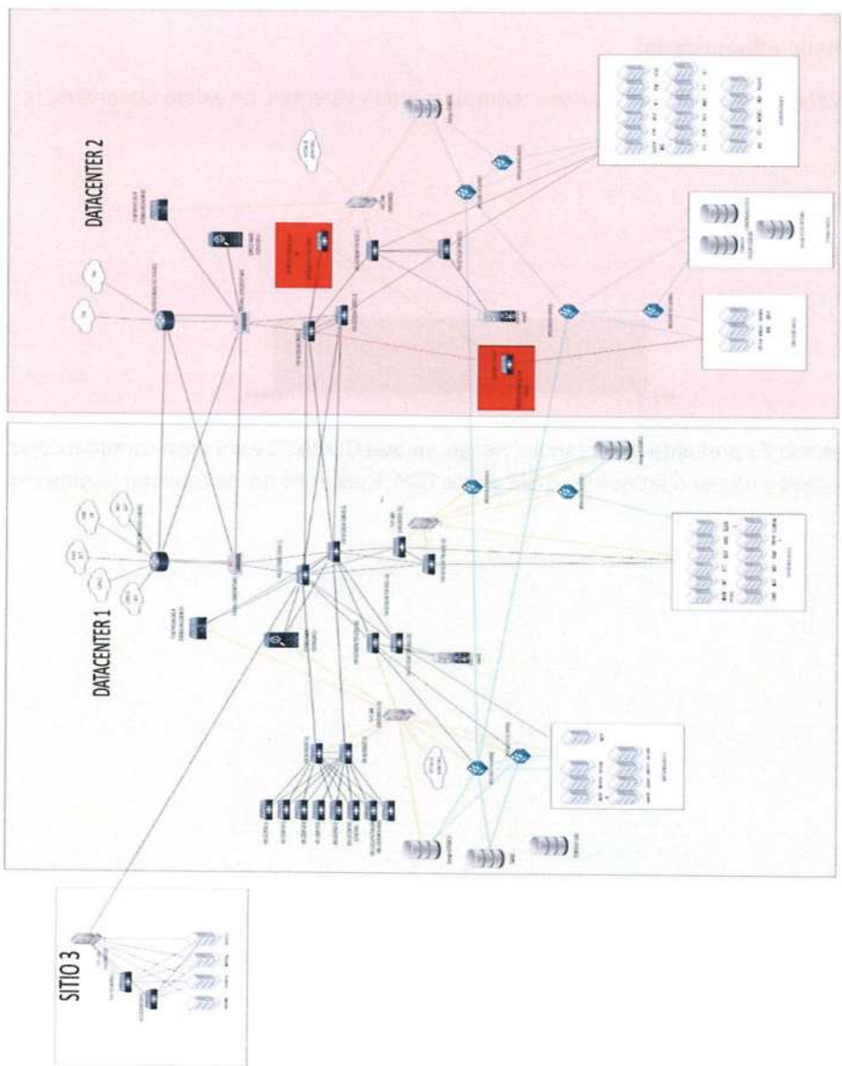


Acorde a las mejores prácticas se procedió a la preparación de un nuevo diagrama actualizado contemplando todos los equipos en cada sitio, actuales en uso y potenciales cambios, así como tener en cuenta la infraestructura de virtualización de OpenSwift que contempla un tercer sitio como sitio de gestión, estos fueron preparados en el formato Microsoft Visio de manera que el equipo de redes tenga a disposición el mismo para su uso, y/o modificación

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

3.1 Diagrama de red actualizado

El diagrama nuevo fue actualizado con todos los equipos y nombres de servidores, así como los proveedores, existe una estructura en proceso de implementación y todas las fuentes fueron serán entregadas en formato Visio editable para que el equipo técnico pueda seguir actualizando los datos.



3.2 Proveedores de Internet y VPN

La estructura de proveedores esta distribuida entre servicios primarios y secundarios acorde a las reglamentaciones vigentes.

Los proveedores de Internet son

- En el sitio primario COPACO
- En el sitio Secundario TEISA

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Bajo esta premisa podemos asumir que los enlaces están segurizados, es importante validar la estructura de conectividad y DNS para brindar el servicio, así como pruebas de fail-over para ambos proveedores.

Los accesos de VPN son los siguientes:

- RMSP SET
- RMSP SII
- RMSP SIF
- FO (Primario – Secundario)

Los enlaces de VPN todos están con equipos reemplazables y vigentes, no existe observación.

Enlaces de Telefonía

- Enlace E1 FO

El enlace de telefonía E1 presenta un potencial riesgo, ya que COPACO está empezando a dejar de dar soporte a los mismos y migrar a tecnologías SIP sobre TCP/IP, es importante tener en cuenta eso como punto de riesgo.

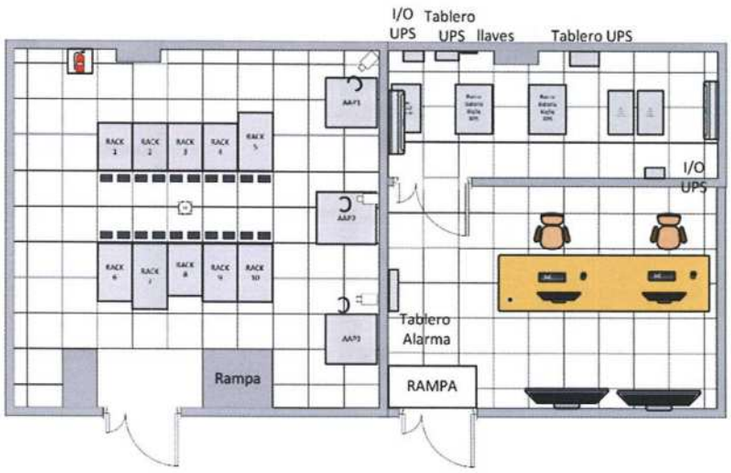
Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

4 Diagrama de servidores y equipos en racks

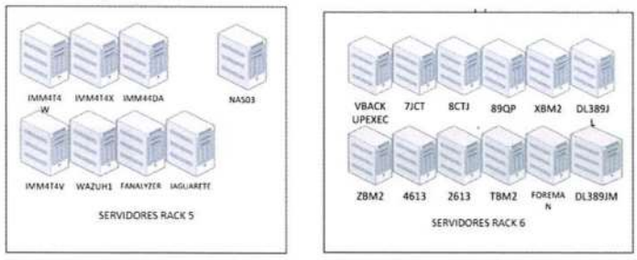
4.1 DATACENTER PRIMARIO

El datacenter primario contiene unos 10 racks de confrontados en dos hileras de 5 racks cada uno, el sistema de soplado es mediante rejillas en el piso falso frontales y no existe sistema de aislamiento de pasillos y los equipos primordialmente presentan un flujo FRONT TO BACK.

La solución de enfriamiento está conformada por 3 unidades de aire acondicionado de 25, 25 y 30 kw respectivamente.



Infraestructura de servidores, rack 5 y 6



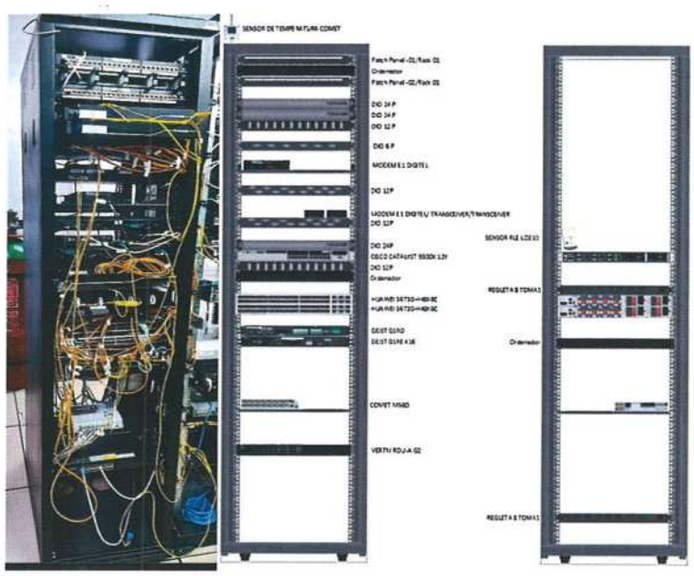
La estructura de storage está repartidas entre soluciones de varios proveedores.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

4.1.1 RACK 1

Este rack tiene como funcionalidad concentradora de FO, también tiene las conexiones E1 de telefonía.

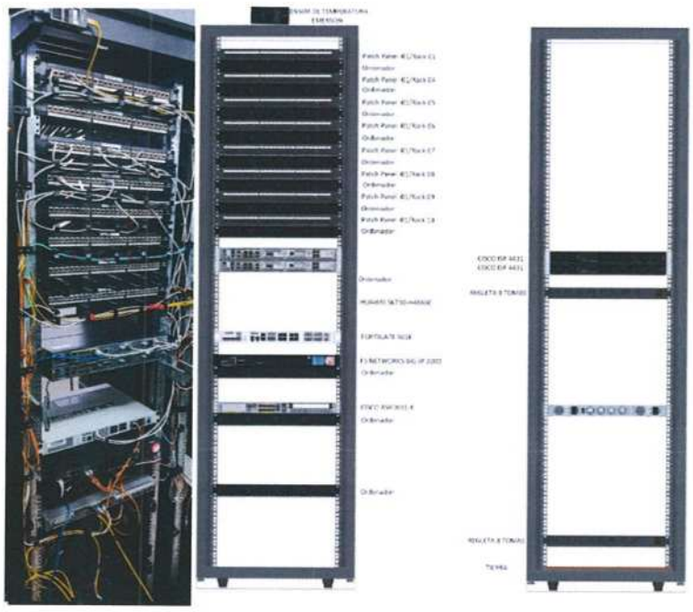
USO: 70%



4.1.2 RACK 2

Este rack tiene patcheras de distribución de UTP con baja utilización y la solución de ISR de Cisco y Seguridad de Fortigate 501E

USO: 50%

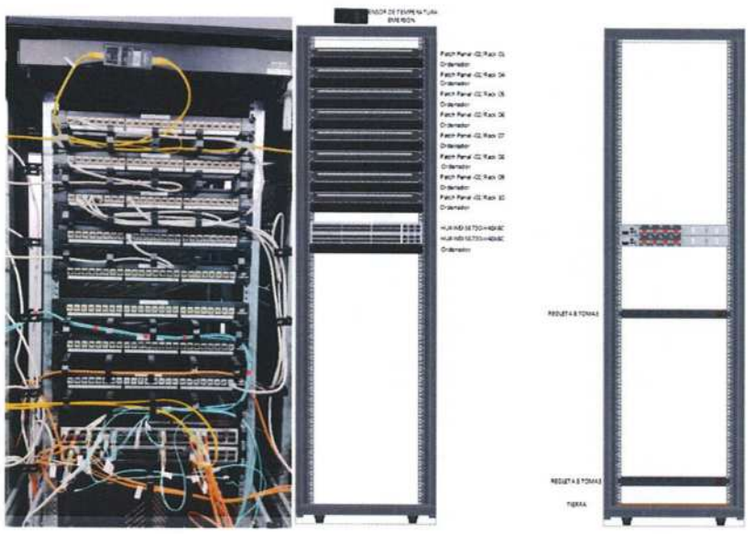


Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

4.1.3 RACK 3

Este rack contiene distribución de Cableado UTP y dos interconexión de TOR de Huawei.

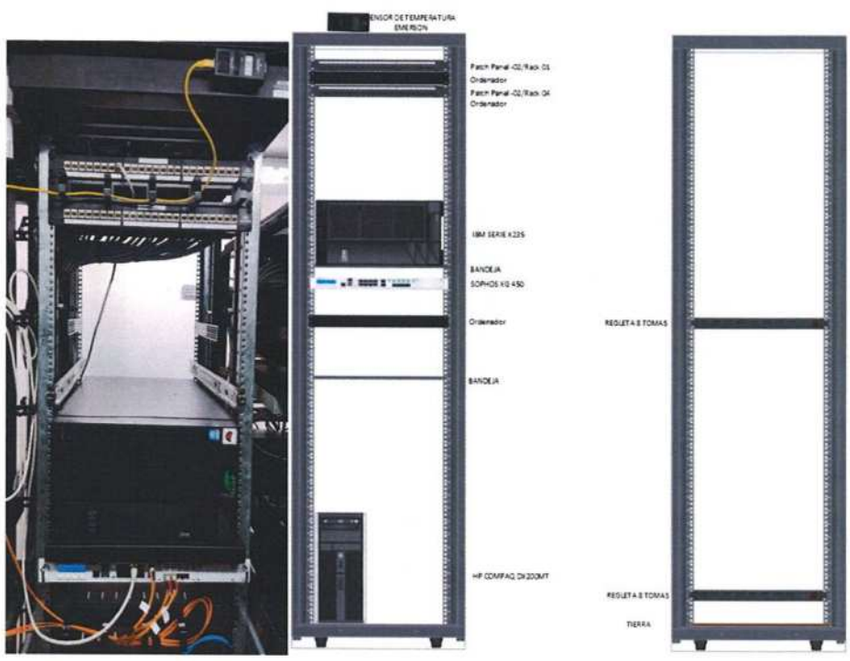
USO: 45%



4.1.4 RACK 4

Dentro de este rack se tiene una solución de IBM Serio X235 y una solución de gabinete legacy HP Compaq DX200MT

USO: 35%



Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

RACK 5

Rack de servidores y de equipos de storages.

USO: 90 %

4.1.5 RACK 6

Este rack es de servidores principalmente, relacionados a la solución de Virtualización/Openshift y adicionalmente la arquitectura de red SAN.

USO: 90%

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

4.1.6 RACK 7

Arquitectura de servidores y UPS locales.

USO: 40%

4.1.7 RACK 8

Rack de FO y UTP

USO: 14 %

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

4.1.8 RACK 9

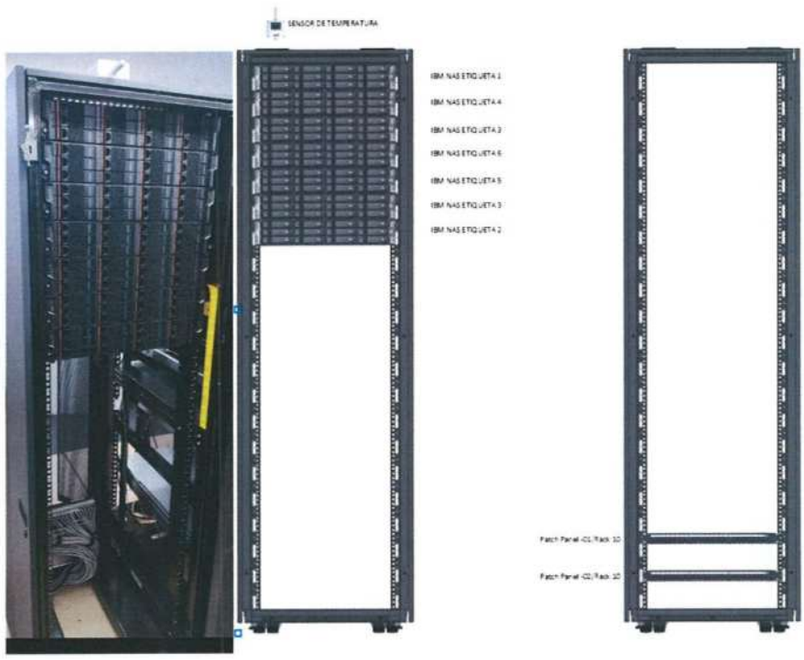
Este rack presenta la solución de Tape Backup, la misma se encuentra en proceso de poner en funcionamiento.

USO: 30%

4.1.9 RACK 10

Este presenta una solución de NAS en proceso de poner a producción, más las pancheras necesarias.

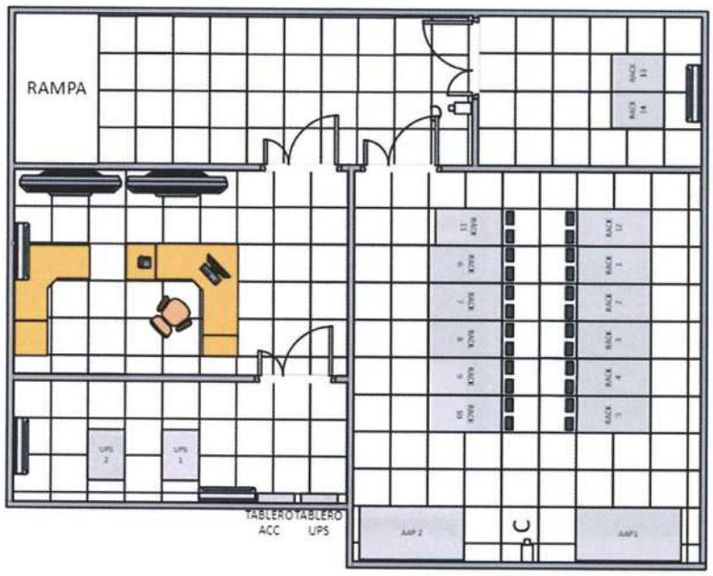
USO: 40%



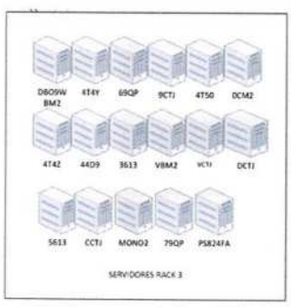
Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

4.2 DATACENTER SECUNDARIO

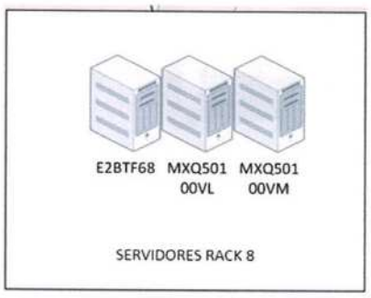
El datacenter secundario tiene una conformación de 10 racks en la Sala IT y dos racks en la sala de proveedores, la refrigeración de este esta data por aires Emerson Power, lieber de 60kw cada uno, la solución de refrigeración de la sala secundaria por un aire de confort de 18000 BTU



Estructura de servidores, rack 3



Estructura de servidores rack 8



Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

4.2.1 RACK 1

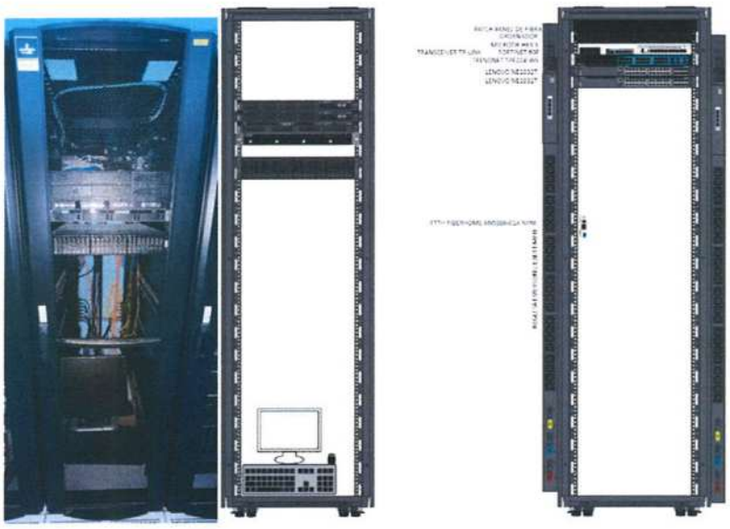
El mismo sirve principalmente de estructura de redes, adicionalmente de equipos de firewall, también un Cisco Catalyst 4500

USO: 50%

4.2.2 RACK 2

Este mismo presenta una solución básica de conectividad

USO: 30%



Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

4.2.3 RACK 3

Rack de servidores principal del sitio secundario.

USO 90%

4.2.4 RACK 4

Rack de sensores

USO: 20%

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

4.2.5 RACK 5

Rack de solución de seguridad, Fortigate 501E principalmente, adicionalmente equipos de CORE y DIOs.

USO: 30%

4.2.6 RACK 6

Rack de CISCO UCS 5108, colaboración, y equipos NEXUS

USO: 50%

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

4.2.7 RACK 7

Rack de storage HUS 110 solución HITACHI
USO: 70%

4.2.8 RACK 8

Rack de servidores y switches SAN

USO: 40%

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

4.2.9 RACK 9

Rack de Servidores

USO: 20%

4.2.10 RACK 10

Rack de Seguridad, Sophos, Nexus, y ASR

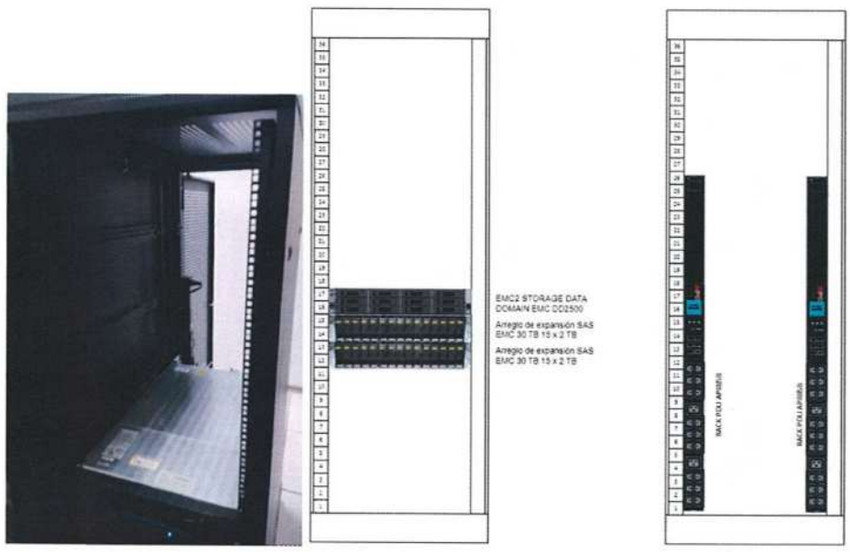
USO: 40%

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

4.2.11 RACK 11

Racj de servidores y SAS

USO: 20%



4.2.12 RACK 12

Rack de Servidores y NAS

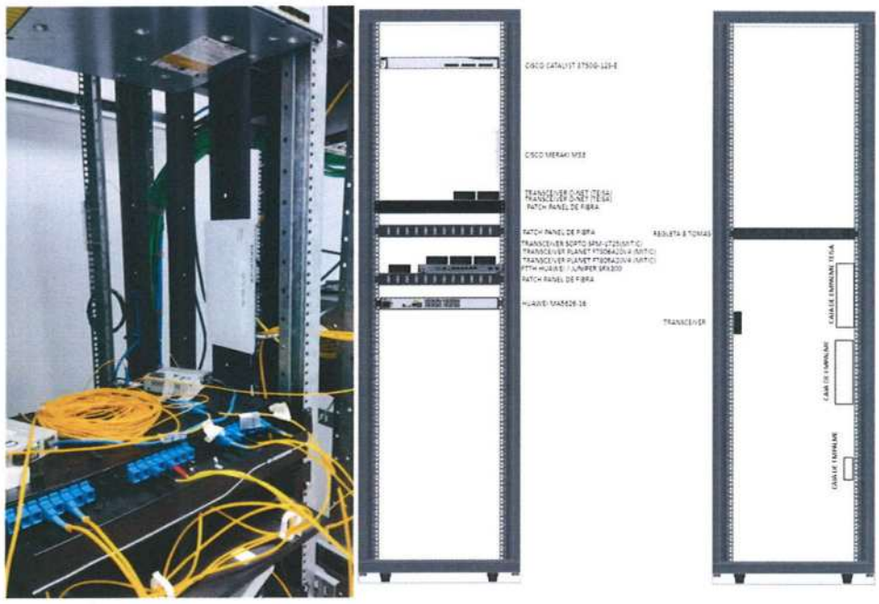
USO: 40%

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

4.2.13 RACK 13

Rack de FO y MC

USO: 30%



4.2.14 RACK 14

Racks de FO y Wireless

USO: 20%

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

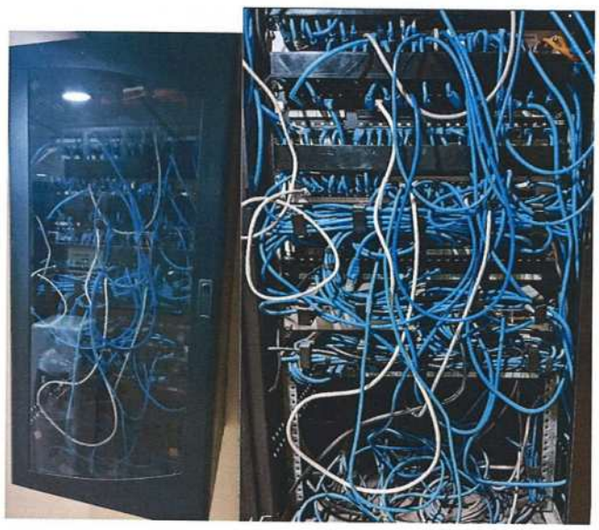
5 Racks de edificio

Estos racks todos contienen conexiones a puestos de usuario.

Planta Baja

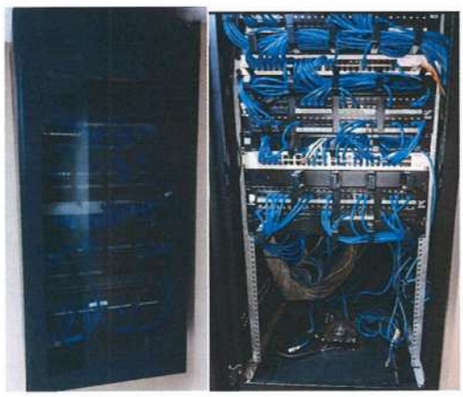
Verificación, capacitación P1, y capacitación P2

Piso 1

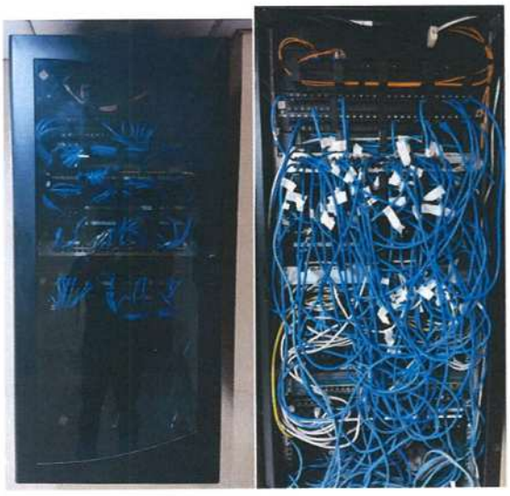


Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

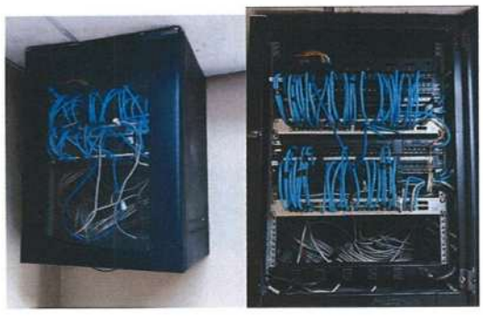
Piso 2



Piso 3



Piso 4



Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Piso 5

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

6 Diagrama de aplicaciones críticas.

El sistema principal de la DNCP es el SICP alrededor del cual se encuentran todas las aplicaciones críticas operativas de la institución.

Estas proveer el servicio a las DNCP, las instituciones contratantes, así como los proveedores.

6.1 Software

Acorde al MITIC en su Resolución 699/2019 todo software en uso en las instituciones públicas debe regirse por las siguientes premisas básicas basas en buenas practicas

Soporte y gestión continua del software:

1. *Todo el software desarrollado debe contar con soporte de software del fabricante. Al momento de la adquisición se debe establecer claramente el tiempo de vida mínimo que se requiere para el software o sistema, y el fabricante debe ofrecer un tiempo de soporte igual o superior a dicho tiempo de vida.*
2. *En caso de que no sea posible contar con soporte de software del fabricante, el modelo de licenciamiento y la disponibilidad del código fuente debe ser tal, que permita a la institución o a otra empresa o desarrollador de software nacional asumir dicho soporte.*
3. *El fabricante o servicio de soporte debe tener un canal de comunicación y/o mecanismo de reporte de vulnerabilidades o bugs de programación, de manera a que el cliente pueda contactarlo en caso de descubrimiento de vulnerabilidades. En caso de que el reporte ocurra dentro de la ventana de tiempo de vida solicitado, el fabricante o servicio soporte debe ser capaz de proporcionar una corrección a la vulnerabilidad de manera oportuna, según el acuerdo del nivel del servicio (por sus siglas en inglés, Service Level Agreement o SLA) especificado en el contrato o pliego de bases y condiciones.*
4. *El software debe poder ser inventariado por herramientas estándar automatizadas de inventario de software basados en el estándar Common Platform Enumeration (CPE), debiendo incluir como mínimo la información del nombre, versión, autor y fecha de instalación del mismo.*

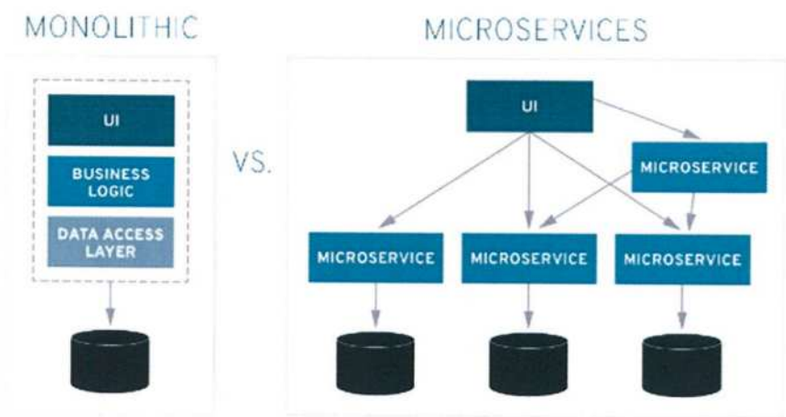
Hoy en día la DNCP tiene como software principal en uso el SICP, o Sistema de Información de Contrataciones Públicas hoy regida por la Ley 7021/2022 "De Suministro y Contrataciones Públicas".

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Dicho software hoy está siendo realizado por el equipo interno con la colaboración de equipos externos, ya sea consultores y/o desarrolladores para lograr el mejor resultado.

Dicho software está siendo documentado vía GitHub, donde los equipos van generando el código para posteriormente ser llevado a producción.

La DNCP se encuentra en la actualidad con tecnología de primer nivel y ha tomado las decisiones correctas con referencia a arquitecturas de desarrollo y virtualización al contar con la solución licenciada de OpenSwift los caminos de desarrollo están alineados con las nuevas tecnologías, de parte de infraestructura debemos acompañar para dotar a dicha plataforma de una correcta implementación in situ



7 Evaluación de los planes de contingencia.

Dentro de los planes de contingencia el equipo de tecnología tiene diseñada una matriz de riesgo donde establecen distintas áreas y sus controles, las áreas actualmente abarcadas son:

- Gestión de Sistemas
- Gestión de la Plataforma tecnológica
- Gestión de Datos y Generación de Información
- Gestión de la Seguridad de la Información

En el proceso de relevamiento recabamos la información sobre los potenciales puntos críticos y los estaríamos revisando como estos se convierten en procedimientos y como los mismos luego se convierten en acciones acorde a lo sugerido por la matriz de riesgo.

Estaremos trabajando sobre esta matriz posteriormente para ir agregando recomendaciones sobre las mismas, esto alineado con las capacidades actuales del personal y de ser necesario sugerir actualizaciones.

Adjuntamos la matriz de riesgos que es como sigue:

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

7.1 Gestión de Sistemas

1. Gestion de Sistemas	Fallas de software: funcionamiento anormal del sistema operativo o aplicaciones.	Actualizaciones, control de cambios no establecidos.	Daño de la información, pérdida económica, interrupción de servicio, daño de imagen.	10	2	20	MODERADO	Correcto relevamiento y entendimiento de los requerimientos solicitados. Uso de metodologías para ordenamiento en el desarrollo y mantenimiento de Sistemas informáticos. Actualización constante de los cambios en el repositorio de control de versiones. Se utiliza un ambiente separado de desarrollo. (Controles contemplados en el PG-DTI-02). Pruebas de funcionalidad y de seguridad para la detección de fallas. Gestión de vulnerabilidades de activos para la detección y corrección de vulnerabilidades.
	Ausencia del personal clave: cantidad de funcionarios no acorde con las necesidades.	Enfermedad y problemas personales, lesiones, vacaciones, permisos	Atrasos en los desarrollos de corrección en los proyectos de software.	10	1	10	TOLERABLE	Reasignacion de tareas / Documentacion de convenciones / Contratación de personal / Preparación y capacitación en base a procedimientos establecidos
	Falta de documentación sobre configuración de sistemas para una respuesta rápida.	Poca implementacion de estándares para manejo de control de cambios y configuraciones.	Atrasos en los desarrollos de corrección en los proyectos de software.	20	1	20	MODERADO	Documentaciones internas elaboradas y/o proveidas por el fabricante. Portal de desarrollo.
	Atrasos en los desarrollos de corrección en los proyectos de software.	Imprevistos durante el desarrollo de los proyectos.	Interrupción del servicio. Daño de imagen.	20	1	20	MODERADO	Contratación de nuevos empleados. Seguimiento y medición de procesos. Contrato abierto de Desarrolladores. Control de versionado de código.
	Fallas de copia de seguridad: imposibilidad de recuperacion de datos a partir de copias de seguridad.	Falla en los medios de almacenamiento.	Retraso en los trabajos de desarrollos de corrección de software. Pérdida de información. Interrupción del servicio.	20	1	20	MODERADO	Procedimiento para backup y recuperación de datos. Monitoreo de la herramientas utilizada para el proceso de backup y recuperación. Copias de trabajo de los desarrolladores

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

7.2 Gestión de la plataforma tecnológica

2. Gestión de la Plataforma tecnológica	Fallas de software: funcionamiento anormal del sistema operativo o aplicaciones.	Actualizaciones, control de cambios no establecidos.	Daño de la información, pérdida económica, interrupción de servicio, daño de imagen.	20	1	20	MODERADO	Pruebas de funcionalidad y de seguridad para la detección de fallas. Gestión de vulnerabilidades de activos para la detección y corrección de vulnerabilidades.
	Ausencia del personal clave: cantidad de funcionarios no acorde con las necesidades.	Enfermedad, problemas particulares, permisos o vacaciones, renuncia, traslado.	Degradación del servicio brindado en cuanto a tiempos de respuesta. Retraso en las tareas del usuario afectado.	10	2	20	MODERADO	Reasignación de tareas / Contratación de nuevos empleados.
	Fallas de copia de seguridad, imposibilidad de recuperación de datos a partir de copias de seguridad	Falla en los medios de almacenamiento.	Interrupción del servicio. Pérdida de información. Retraso en el servicio brindado.	20	1	20	MODERADO	Procedimiento para backup y recuperación de datos. Monitoreo de la herramientas utilizada para el proceso de backup y recuperación.
	Falta de documentación sobre configuración de sistemas para una respuesta rápida.	Poca implementación de estándares para manejo de control de cambios y configuraciones.	Degradación en la calidad del servicio. Altos tiempos de respuesta.	20	1	20	MODERADO	Documentaciones internas elaboradas y/o las provistas por el fabricante. Biblioteca de manuales y configuraciones basado en normativas y mejores prácticas.
	Falla del servicio de internet.	Externas	Aumento de reclamos y solicitudes de asistencia debido a la imposibilidad de acceder al portal. Posible daño de imagen.	20	1	20	MODERADO	Enlaces a varios proveedores de internet. Monitoreo del estado de los enlaces de internet. Establecer SLA mas estrictos en los contratos con los diferentes proveedores de internet.
	Ausencia del personal clave: cantidad de funcionarios no acorde con las necesidades.	Enfermedad, problemas particulares, permisos o vacaciones, renuncia, traslado.	Degradación del servicio brindado en cuanto a tiempos de respuesta. Daño de imagen. Leve impacto en la operativa de otra área de la DTI.	20	1	20	MODERADO	Reasignación de tareas / Contratación de nuevos empleados.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

7.3 Gestión de datos y generación de información

3. Gestión de Datos y Generación de Información	Fallas de software: funcionamiento anormal del sistema operativo o del sistema gerenciador de base de datos	Falta de actualización / Falla en el disco / Control de cambios no establecidos	Daño de la información, interrupción de servicio, daño de imagen	20	1	20	MODERADO	Pruebas de funcionalidad y de seguridad para la detección de fallas. Gestión de vulnerabilidades de activos para la detección y corrección de vulnerabilidades.
	Fallas de hardware	Falta de actualización / Componente obsoletos	Daño de la información, interrupción de servicio, daño de imagen	20	1	20	MODERADO	Se cuenta con un sistema y equipos de replicacion.
	Falta de personal clave	Vacancia / Vacaciones / Permisos particulares	Sobrecarga de trabajo para los demás funcionarios del área / Retraso en la ejecución de los procesos	5	1	5	ACEPTABLE	Reasignación de tareas / Guias operativas / Contratación de personal
	Falla del servicio de internet	Externas	Retraso en la ejecución de los procesos	20	1	20	MODERADO	Enlaces a varios proveedores de internet. Monitoreo del estados de los enlaces de internet.
	Fallas de copia de seguridad: imposibilidad de recuperación de datos a partir de copias de seguridad.	Falla en los medios de almacenamiento	Pérdida de información	20	1	20	MODERADO	Procedimiento para backup y recuperación de datos. Pruebas semanales de restauración de copias de seguridad

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

7.4 Gestión de Seguridad de la Información

4. Gestión de Seguridad de la información	Fallas de software: funcionamiento anormal del sistema operativo o aplicaciones.	Actualizaciones, control de cambios no establecidos, falta de documentación	Daño de la información, pérdida económica, interrupción de servicio, daño de imagen	20	1	20	MODERADO	Pruebas de funcionalidad y de seguridad para la detección de fallas. Gestión de vulnerabilidades de activos para la detección y corrección de vulnerabilidades.
	Existe el riesgo de interrupción de un servicio o proceso, posterior a la actualización de un activo de TI	Debilidad en el analisis de impacto sobre otros servicios al planificar una actualizacion	Interrupción del servicio / interrupción de procesos operativos manuales	20	1	20	MODERADO	Realizar un análisis exhaustivo de impacto sobre otros servicios al momento de planificar la actualización, identificando y evaluando todas las dependencias y conexiones con otros activos y servicios Validar el analisis con las demas coordinaciones Realizar una verificacion post actualización del estado de las dependencias y conexiones a otros activos y servicios.
	Existe el riesgo que las copias de seguridad se infecten con algun tipo de codigo malicioso	Medios local de almacenamiento logico utilizados como repositorio final de las copias de seguridad y crecimiento de los tipos y metodos de ataques a través de codigo malicioso.	Daño de la información, interrupción de servicio, daño de imagen	20	1	20	MODERADO	Asegurese que todas las copias de respaldo se almacénen en al menos un destino que no esté disponible si es alcanzable de manera continua a través de llamadas del sistema operativo
	Perdida de información sensible o confidencial almacenada en dispositivos moviles	Extravió, hurto o daños fisicos del dispositivo movil.	Daño de la información, perdida de información sensible o confidencial	20	1	20	MODERADO	Las informaciones confidenciales que son procesados por el SICP son almacenados en los Data Center de la institución Disponibilizar plataformas institucionales como repositorio de información sensible que pudieran recibir y manejar los funcionarios. Copias de seguridad de los principales directorios de los Directores, Asesores, Coordinadores. Utilizar herramientas de encriptación de discos duros.
	Ausencia de Politicas especificas de seguriad acordes a los lineamientos operativos actuales, relacionadas a gestión de activos, gestion de vulnerabilidades, gestion de cambios y continuidad de TI	Insuficiente dotación de personal en la Coordinación de Seguridad TICs	Retraso en la ejecución de los procesos. Daño en la imagen de la institución. Interrupción en el servicio.	10	2	20	MODERADO	Solicitud de ampliación de dotación personal. Contratación de servicios terceirizados para apoyo.
	Fallas de copia de seguridad: imposibilidad de recuperación de datos a partir de copias de seguridad.	No están claramente establecidos los lineamientos para realizar las copias de seguridad	Interrupción del servicio / Pérdida de información	10	2	20	MODERADO	Procedimiento para backup y recuperación de datos. Monitoreo de la herramientas utilizada para el proceso de backup y recuperación.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

7.5 Gestión de riesgos combinados

1.Gestión de Sistemas 2. Gestion de la plataforma tecnológica 3. Gestion de datos y Generación de información 4. Gestion de Seguridad de la información	Corte de energía eléctrica por parte de la ande	Externas: constantes fallas de la ANDE	interrupción del servicio, pérdida de imagen de la institución	10	1	10	TOLERABLE	Sistema de Alimentacion ininterrumpidad (UPS) para estaciones de trabajo, equipos de comunicacion y datos. Grupos generadores tanto para todo el Data Center como para las estaciones de trabajos de los funcionarios, equipos de iluminación y refrigeracion de areas de trabajo. Mantenimiento preventivo, correctivo y periodico de los grupos generadores y de las UPS.
	Robo sustraccion de todos o algun equipo del Data Center	Complicidad de funcionarios responsables o personal de seguridad, vandalismo	Daño de la información, pérdida económica, interrupción del servicio daño de imagen.	20	1	20	MODERADO	Inventario de equipos. Control de acceso fisico al datacenter y a las inmediaciones de la DTI. Control mediante videovigilancia dentro del datacenter y en sus inmediaciones. Auditoria de interna de patrimonio.
	Fallas humanas (operacion, mantenimiento, respuestas) errores humanos cometidos durante la realizacion de tareas especificas y que pueden producirse de manera casual o no	Riesgo inherente	Sanciones, daño de la información, interrupción del servicio, daño de imagen	20	1	20	MODERADO	Deteccion de capacitacion para los cargos, manual de funciones, descripcion de cargos, evaluación de desempeño. Procedimientos establecidos e implementados.
	Fallas de Hardware funcionamiento anormal de equipos	Término de la vida útil tecnológica de los equipos, fallas de fábrica en componentes electrónicos, cadena de suministro eléctrico deficiente	Pérdida de datos, interrupción del servicio, pérdida de imagen de la institución.	20	1	20	MODERADO	Mantenimiento preventivo de los equipos, extensión de garantía de equipos críticos. Renovacion periodica de la infraestructura tecnológica.
	Falta de recursos financieros: imposibilidad de adquisición de repuestos (memoria, disco, fuente, dispositivos de red, etc.), contratación de personal técnico especializado.Aplica a todos los procesos de la DTI.	imprevistos, crisis.	interrupción del servicio y daño de imagen	10	1	10	TOLERABLE	Previsión presupuestaria
	Destrucción o deterioro del Data Center o equipos del mismo. Deterioro de las instalaciones y los repositorios de datos por incendio, inundación, fallas eléctricas, falta de climatización, robos.	Equipos tecnológicos obsoletos, fallas estructurales, instalaciones eléctricas deterioradas. Fallas en los Sistema de cañerías	interrupción del servicio, pérdida de imagen de la institución.	20	1	20	MODERADO	Data Center Alternativo

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

8 Evaluación de plataformas de prestación de servicios

8.1 Arquitectura OpenShift

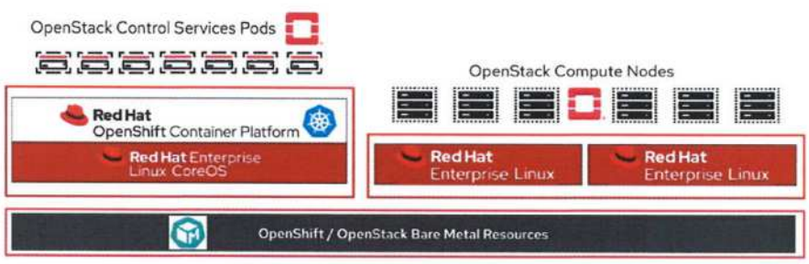
La plataforma principal para la prestación de servicios para la DNCP actualmente es Red Hat OpenShift Platform Plus y Data Foundation Advance, además de acceso ilimitado para invitados que son los que acceden a los servicios varios.

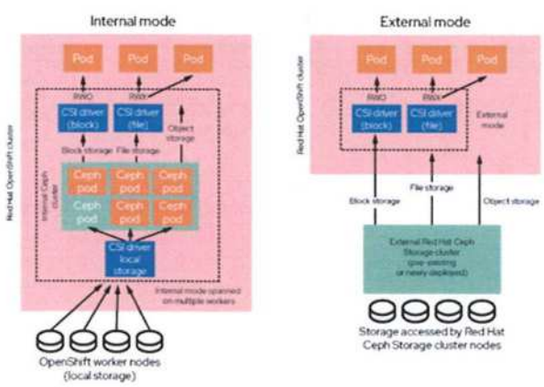
- Red Hat OpenShift Platform Plus with Red Hat OpenShift Data Foundation Advanced (Bare Metal Node) Subscription Standard por el periodo del 15/12/2024 al 14/12/2025 (1-2 sockets up to 64 cores)ma utilizada es RE
- Red Hat Satellite for Unlimited Guest por el periodo del 15/12/2024 al 14/12/2025

La misma está bajo soporte y licencia hasta diciembre 2025 como podemos ver.

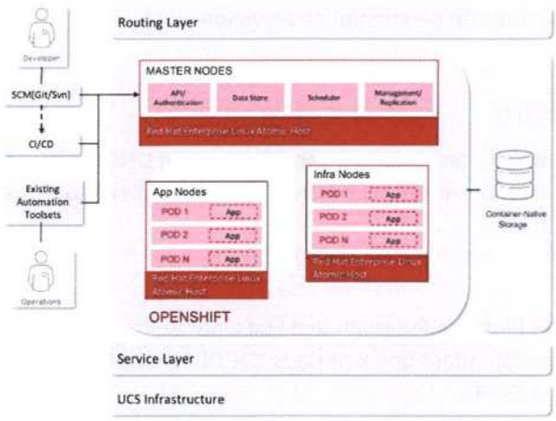
OpenShift Container Platform (OCP) requiere como mínimo tres (tres) paneles de control, esto es algo observado y ya en cuenta por el equipo actual de infraestructura, por el momento dichos paneles están distribuidos entre el sitio primario (dos) y el sitio secundario(uno) pero se está evaluando una mejor arquitectura para mejorar la capacidad de redundancia.

Arquitectura Openshift

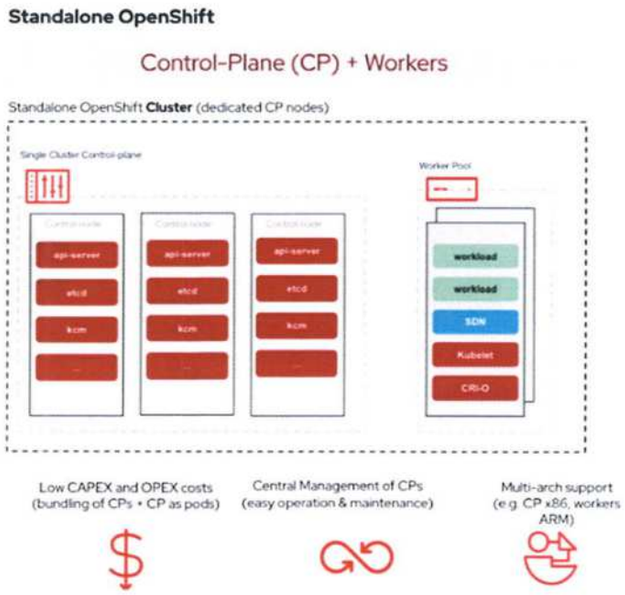




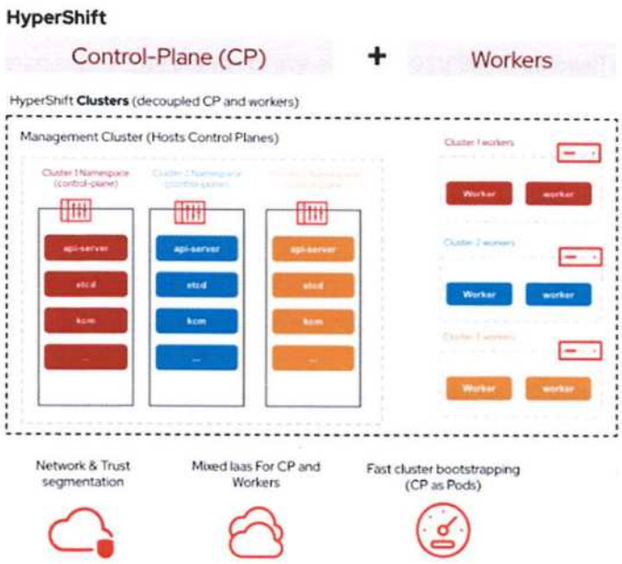
Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030



Esta infraestructura contiene un plano de control para los Clusters para lo cual en conversación con el equipo técnico vemos que requiere unos tres nodos, en la actualidad dicha solución esta situada en dos sitios, a futuro, una vez que la arquitectura esté consolidada se podrán usar recursos de Nube-Py o el futuro datacenter de MITIC para acompañar esta infraestructura, por hoy, es la DNCP que está ayudando con su infraestructura a otras entidades.



Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030



8.2 Sistema de backup

Si nos vamos al concepto de alta disponibilidad y las mejores prácticas de resguardo de datos debemos seguir la filosofía conocida como 3-2-1, que nos pide como mínimo 3 copias, en dos medios distintos y un sitio alternativo externo a nuestra plataforma.

Podemos asumir que nuestra copia primaria corre en los servidores en producción, y estos tienen un sitio secundario, así mismo, todos guardan sus respaldo en una arquitectura Fibre-Channel en raid, y por ultimo esto esta diseñado para guardar todo en Cinta Magnetica.

IBM Storwize V3700, HP STOREEASY 1660, Tape Library HP Storage Works MSL 4048



Es importante tener en cuenta que en el siguiente documento a ser entregado estaremos evaluando los procedimientos de backup y si está la mecánica para que el NOC realice periódicamente todos estos, así mismo en conversaciones con el equipo está en estudio el uso de una copia de seguridad inmutable, pero todavía en preparación.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

8.3 Gestión de usuarios, sesiones y privilegios.

Acorde al MITIC, en su Resolución 699/2019, estos son los datos requeridos para el proceso de gestión de usuarios de los usuarios.

Gestión de usuarios, sesiones y privilegios:

1. *El software debe permitir una gestión de usuarios de acuerdo a los requerimientos de la institución, con niveles de privilegios en conformidad a los roles que éstos requieran (administrador, editor, usuario, etc.), basados en el principio de mínima necesidad de conocimiento.*
2. *El software debe permitir la revocación de acceso de usuarios, mediante un estado "desactivado" o similar.*
3. *Debe ser posible establecer una fecha de expiración para las cuentas de usuarios, a partir de la cual la cuenta deberá entrar a un estado "desactivado" o similar, hasta tanto se apruebe la continuidad de la misma. El parámetro de fecha de expiración podrá ser fijo o configurable por la institución, de acuerdo a sus requerimientos de negocio.*
4. *El software debe contemplar la expiración de sesiones conforme a parámetros temporales. Estos parámetros pueden ser fijos o configurables por la institución, de acuerdo a sus requerimientos de negocio.*

Hoy en día las plataformas que están acompañando estas se dividen entre plataformas de gestión de usuarios de Windows AD, y plataformas de equipos diversos para la gestión de otros usuarios, en el caso de los usuarios internos de la institución se recomienda una utilización de una plataforma única para realizar single sign-on, y para las plataformas de provisión servicio externo, como el SICP se puede utilizar una plataforma gestionada por los administradores de dicha plataforma.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

8.4 Autenticación y gestión de credenciales

En este sentido la DNCP con su sistema SICP ha adoptada una mecánica de delegación de permisos a cada cabeza de institución para el mismo realice las altas, bajas y modificaciones pertinentes de sus usuarios, posteriormente se recomienda a la DNCP seguir las recomendaciones de la Resolución 699/2019 respetando los criterios de esta. Posiblemente se deba empezar a evaluar la utilización del factor de autenticación doble para ir reduciendo los riesgos de robo de usuarios.

Autenticación y gestión de credenciales:

1. *El software debe permitir la gestión individual eficaz de credenciales, debiendo permitir que cada usuario sea capaz de cambiar su propia contraseña. Se debe contemplar también mecanismos de recuperación de contraseñas, ya sea a través de un usuario de mayores privilegios o de mecanismos de auto-gestión por parte del usuario. Preferentemente, debe ser posible que al momento de la creación de cuentas permita forzar el cambio de contraseña luego del primer inicio de sesión.*
2. *El software que almacene y/o procese información crítica y/o que se utilice para un proceso crítico de la institución debe soportar autenticación de doble factor para los usuarios de privilegios elevados.*
3. *El software debe permitir establecer políticas de contraseña, que incluyan, como mínimo, la posibilidad de establecer los siguientes parámetros:*
    a. *Longitud mínima de la contraseña*
    b. *Complejidad de contraseña (mayúsculas, minúsculas, números y caracteres especiales, etc.)*

    Los mencionados parámetros serán configurables por la institución, preferentemente, o en su defecto, deberán ajustarse a los lineamientos y estándares mínimos indicados por la institución.
4. *Las contraseñas no deben almacenarse en texto claro, sino mediante la aplicación de funciones hash o funciones resumen. Para el almacenamiento de las contraseñas se debe utilizar funciones criptográficas seguras no reversibles de hash combinadas con salt aplicadas a las contraseñas. Algoritmos aprobados son los siguientes:*
    a. *Argon2*
    b. *PBKDF2*
    c. *scrypt*
    d. *bcrypt*
5. *De manera alternativa, se puede cifrar las contraseñas utilizando técnicas criptográficas reversibles únicamente en aquellos casos en que la clave secreta y/o privada de cifrado quede bajo el poder exclusivo del usuario dueño de la contraseña.*

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

8.5 Registros de auditoria

Acorde al MITIC en su reglamentación 699/2019, estos son los delineamientos que se debe seguir en el registro de auditoría para las distintas plataformas utilizadas, es importante tener en cuenta que hoy la DNCP se encuentra en utilización de la herramienta wazuh, la cual sirve de funcionalidad extendida para registro de todos los eventos de plataformas y usuarios, estos registrado lo solicitado por la resolución.

Gestión de registros de auditoría:

1. *El software debe ser capaz de generar registros de auditoría de todos los eventos relevantes, con los detalles suficientes para permitir una trazabilidad adecuada, que abarque como mínimo los siguientes eventos:*
   a. *Inicios de sesión de usuarios (exitosos y fallidos)*
   b. *Delegación/impersonificación de cuentas de usuarios*
   c. *Modificación de parámetros del sistema*
   d. *Gestión de usuarios (cambio de contraseña, creación/eliminación/modificación de usuarios y/o grupos)*
   e. *Acciones críticas llevadas a cabo por usuarios en el marco del proceso de negocio del sistema (edición de datos sensibles, eliminación de datos, etc.)*
2. *El software debe contemplar un mecanismo configurable de rotación de registros de auditoría, de acuerdo al parámetro de cantidad de tiempo (diario, semanal, mensual, etc.), como mínimo.*

La DNCP cuenta con un servicio de seguridad bajo la licitación "412176 - SERVICIO DE SEGURIDAD DE LA INFORMACION Y AUDITORIA EN GESTIÓN DE TECNOLOGÍA DE LA INFORMACIÓN" con duración de 26 meses a partir de la fecha de inicio de ejecución de 26-09-2023 de la mano de la consultora "ERNST & YOUNG PARAGUAY AUDITORES Y ASESORES DE NEGOCIOS"

Cuyos objetivos son:

Los objetivos que se pretenden alcanzar mediante la ejecución del contrato son:

- Establecer el nivel de seguridad, detectar los bugs de seguridad existentes en las aplicaciones web y móviles,

- servicios y la infraestructura tecnológica con la que cuenta la DNCP.
- Proponer las soluciones generales y específicas a todos los hallazgos y potenciales vulnerabilidades, independientes
- de las fuentes de origen, de modo tal a mitigar el riesgo que ello representa reduciendo el potencial impacto a corto mediano o largo plazo.
- Revalidar los hallazgos mitigados.
- Fortalecer el Sistema de Gestión de Seguridad de la Información mediante el diseño y desarrollo de todas las documentaciones relacionadas a ella como, por ejemplo: planes de seguridad, políticas, guías, procedimientos, formularios, entre otros.
- Proponer o implementar soluciones tecnológicas que sirvan de soporte operativo para el cumplimiento de las políticas y controles de Seguridad de la Información.
- Apoyar en el proceso de Gestión de Incidentes, mediante el análisis de eventos, sugerencias para la recolección y salvaguarda de evidencias, y propuestas de mejora.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

8.6 Cifrado

La DNCP se encuentra en cumplimiento de las reglas de cifrado para sitios y su certificado es emitido por USERTrust RSA Certification Authority, como esta sección escapa al alcance de este proyecto, nos remitimos meramente a la verificación de la herramienta principal que es el SICP.

Cifrado:

1. *El software debe cifrar toda la información sensible en tránsito, especialmente aquella información de carácter confidencial y/o cuya integridad deba asegurarse. Para tal efecto, se deberán utilizar protocolos de red cifrados, tales como HTTPS, SSH, SCP, SFTP/FTPS, etc.*
2. *Para sistemas basados en web, se adoptará el modelo SSL/TLS para el cifrado del tráfico. Los protocolos aprobados son TLS v.1.2 o superiores. Los protocolos TLS v.1.1 e inferiores y SSLv3 e inferiores no deben ser utilizados. Se deben seleccionar suites de cifrado robustos; una guía de referencia es:https://cheatsheetseries.owasp.org/cheatsheets/TLS_Cipher_String_Cheat_Sheet.html*
   Se deben evitar las suites de categoría C o inferiores.
3. *Las claves de cifrado deben ser robustas. Se recomienda una longitud de 2048 bits para RSA o equivalente, de acuerdo al estándar NIST SP 800-57. La clave privada debe quedar en poder de la institución, exclusivamente.*

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9 Evaluación de infraestructura de datacenter.

9.1 Generadores

Acorde al Uptime Institute, entidad que se dedica a la certificación de profesionales y centros de datos los generadores se dividen en dos tipos, los generadores se dividen en dos grupos:

Generadores continuos: Estos son para sitios donde NO hay electricidad, y deben funcionar 24 horas.

Generadores stand-by: Generadores que se activan ante un corte eventual de electricidad.

Los datacenter mayormente hacen utilización de generadores stand-by ya que los mismos en su mayoría se encuentran en zonas donde existe disponibilidad de electricidad en forma permanente, y estos generadores se usan ante el eventual corte de electricidad.

La estimativa que utiliza el uptime para determinar la capacidad continua de un generador tradicional stand-by es como sigue:

Uptime Institute®

Standby units—allowed to run for limited durations at constrained capacities—do not afford the data center owner the capability to run the engine-generator plant at capacity for extended periods to support operations during critical events

"**Prime Power:** The maximum power for which an engine-generator is capable of delivering continuously with a variable load for an unlimited number of hours. The allowable average power output over a 24-hour run period is 70% of the prime rating unless otherwise agreed to by the RIC manufacturer."

"**Continuous Power:** The maximum power for which an engine-generator is capable of delivering continuously for a constant load for an unlimited number of hours."

In practice, when applying these definitions and the requirement for no runtime limitations at N demand, standby-rated units (as defined) with limited run hours do not comply with Tier III and IV. Standby units—allowed to run for limited durations at constrained capacities—do not afford the data center owner the capability to run the engine-generator plant at capacity for extended periods to support operations during critical events, and therefore do not meet Tier III or Tier IV requirements. Some manufacturers allow only up to 500 hours of capacity operation per year for certain units. However, a standby-rated unit can comply with Tier III and Tier IV requirements if there is proper manufacturer documentation that establishes the unlimited run hour capacity of the unit at the site conditions.

Prime-rated units, per their definition, have more robustness than standby units. Many manufacturers offer the same unit with both standby and prime ratings. However, to comply with the no runtime limitations at N-load requirement, these units must be de-rated to 70% of their prime (nameplate) rating. Note, however, that some manufacturers will offer a derating of more or less than 70% of the prime rating. It is important to work with the manufacturer and obtain commitments in writing of the specific allowance for runtimes and capacities. Continuous is the only rating that complies with the requirement without any derating.

9.1.1 Generadores DC1

El grupo electrógeno asignado al Datacenter 1 es un equipo de la marca WEG, 200kVA stand-by el cual nos da una potencia de 160kwe, y si hacemos el calculo acorde a la recomendación del UPTIME Institute tenemos que convertir esto a prime capacity y posteriormente tenemos que normalizar de Standby a uso continuo de 24 horas, calculando al 70% de uso del mismo, adjuntamos documento de UPTIME para su referencia, el mismo nos provee una potencia adecuada para sostenter los 10 racks del datacenter primario a 20A cada uno, en su alimentación lado A y Lado B.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030


9.1.2 Generadores DC2

El grupo electróngeno asignado al Datacenter 1 es un equipo de la marca STAMFORD, 230kVA stand-by, el cual nos da una potencia de 184kwe, y si hacemos el cálculo acorde a la recomendación del UPTIME Institute tenemos que convertir esto a prime capacity y posteriormente tenemos que normalizar de Standby a uso continuo de 24 horas, calculando al 70% de uso del mismo, adjuntamos documento de UPTIME para su referencia, el mismo nos provee una potencia adecuada para sostenter los 14 racks del datacenter secundario a 20A cada uno, en su alimentación lado A y Lado B.


Como nuestro data center no está certificado, no nos regimos por el UPTIME, pero en caso que lo estuviéramos estaríamos entre un TIER II y un TIER III acorde al tipo de elementos que vamos a evaluar, la siguiente tabla habla de lo esperado de cada equipo generador y las condiciones generales.

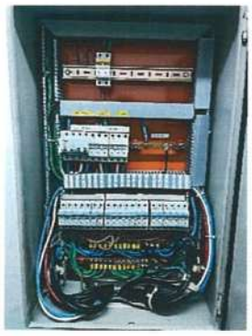
Engine-Generator Requirements	Tier I	Tier II	Tier III	Tier IV
Rating to Support Design Load	Any; up to nameplate rating to support design load	Any; up to nameplate rating to support design load	Capable of supporting design load for unlimited hours at site conditions	Capable of supporting design load for unlimited hours at site conditions
Continuous	No additional requirement for hours of operation limitations		Full nameplate capacity	
Prime			Option 1: 70% of nameplate capacity Option 2: Larger capacity than Option 1 with manufacturer letter	
Standby			Can be used for Tier III and Tier IV with manufacturer letter; Tier Certification capacity dependent on manufacturer letter	
Derating for Site Conditions	Additional derating may be required due to site conditions (e.g., ambient temperatures, elevation)—consult manufacturer requirements			

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9.2 Tableros

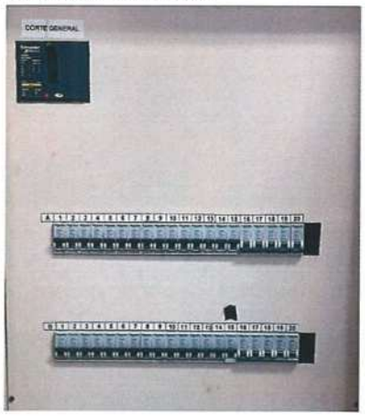
9.2.1 Tableros DC1

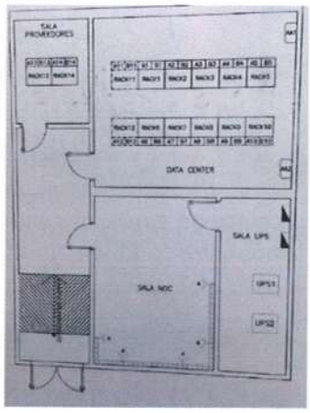
Con el tablero principal de las UPS podemos identificar que cada rack puede soportar una corriente de 20A según llave, lo cual nos da unos 4,4 Kw por rack, el mismo permite levantar un máximo de datacenter de 44 KW para los 10 racks instalados.



9.2.2 Tableros DC2

Con el tablero principal de las UPS podemos identificar que cada rack puede soportar una corriente de 20A según llave, lo cual nos da unos 4,4 Kw por rack, el mismo permite levantar un máximo de datacenter de 61,6 KW para los 14 racks instalados.

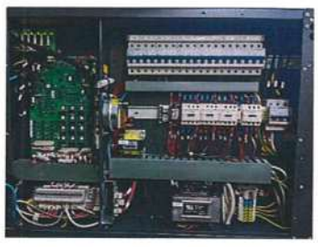




9.3 Controladoras AC

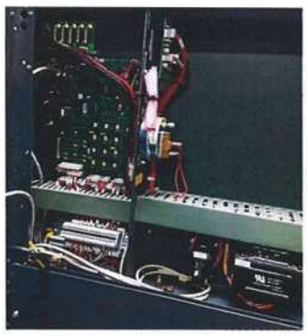
9.3.1 Controladora DC1

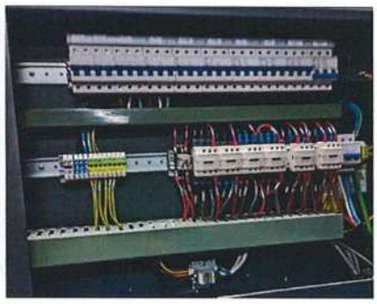
La solución contempla un tablero de distribución de aire acondicionado intermitente.



Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9.3.2 Controladora DC2





9.4 UPS

9.4.1 UPS DC1

Observación muy importante es que las 2 (dos) UPS Vertiv Liebert son de 30KVA

A Estas acompaña una tercera UPS de la marca Riello, de 80kVA, para apoya a la primera y cargas no críticas y salas NOC, esta podría ser utilizada en un plan de contingencia opcional

9.4.2 UPS DC2

Observación muy importante es que las 2 (dos) UPS Emerson Power Liebert son de 30KVA, esto quiere decir que la potencial carga del datacenter podría exceder las capacidades de las UPS instaladas

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9.5 Baterías DC1

Esta solución representa baterías en un formato 20 + 20 x 12 Vdc, a un amperage de 40Ah, el cual daría una autonomía de.....

9.6 Enfriamiento

9.6.1 Enfriamiento DC1

El sistema de refrigeración de la sala IT está configurado en una solución 2N+1 de tres aires acondicionales, dos de 25KW primarios los cuales proveen un enfriamiento aproximado de 85000 BTU cada una y una tercera unidad de 30KW, la cual permite un enfriamiento de 100.000 BTU que sirve de respaldo a las anteriores.

Esto permite mantener los ciclos 12 + 12 horas y posteriormente en caso de tener que hacer mantenimiento concurrente se cuenta con un equipo adicional.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

De la misma manera los compresores externos acompañan en la solución 2N+1

9.6.2 Enfriamiento DC2

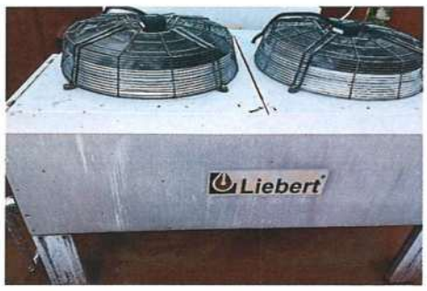
El sistema de refrigeración de la sala IT está configurado en una solución 2N de dos aires acondicionadores, dos de 57,9KW primarios los cuales proveen un enfriamiento aproximado de 200000 BTU cada una.

Esto permite mantener los ciclos 12 + 12 horas y posteriormente en caso de tener que hacer mantenimiento concurrente se cuenta con un equipo adicional.

Type		Model(mm×H/W/D)					
		P030DA/D	P032DA/D	P035DA/D	P038DA/D	P040DA/D	P050DA/D
Cooling Capacity (kW)	Total (kW)	19.4	22.1	29.2	32.4	44.6	52
	Sensible (kW)	18.3	20.7	25.9	28	40.7	46.1
Fan	Standard flow volume (m³/h)	5400	6300	7066	7920	11810	13032
	Fan number	1	1	1	1	2	2
Electric heater	Power (kW)	6	6	6	6	9	9
Infrared humidifier	Capacity (kg/h)	4.5	4.5	4.5	4.5	10	10
Dimensions	W×D×H (mm)	853×874×1970				1704×874×1970	
Net weight	kg	320	330	340	350	580	670
Condenser water supply requirement (32.3°C)	Quantity of water intake (32°C)m	1.15	1.32	1.73	1.9	2.58	3.05
	Pressure drop (kPa)	45.5	60.9	54.4	50	92.1	101.3
	Plate exchanger water in/out line (mm)	28	28	35	35	35	35
Electrical	FLA (A)	23.1	25.2	30.4	32.3	46.5	53.5
	Breaker (A)	32	32	40	40	63	63

De la misma manera los compresores externos acompañan en la solución 2N

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030



9.7 Prevencion de Incencio

9.7.1 Prevención de incendio DC1

Los sistema de extinción si bien son adecuados y cumplen ambas normativas para DC y PCI requieren un control más periódico, el tiempo de vida de los extintores de datacenter suele ser fácilmente superior a 30 años, pero requiere control periódico.

Si bien están en instalación de nuevos equipos, es importante que posterior a dicho periodo se retiren cualquier elemento ajeno a los Datacenter.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9.7.1 Prevención de incendio DC2

Es importante tener en cuenta que el datacenter respeta ambas normas, de datacenter y PCI municipal, pero un detalle importante a observar es que los equipos de extinción requieren seguimiento para evaluar sus condiciones ya que requieren validaciones periódicas. La estructura física de extinción es adecuada, posteriormente estaremos revisando los procedimientos operativos alrededor de los mismos. Es un importante que dentro de los

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9.8 NOC

La DNCP contiene dos NOC operacionales los cuales dan servicio a los sitios primarios y secundarios, ambos contienen instalaciones adecuadas para proveer los servicios de monitoreo y seguimiento de sucesos.

Hoy en día se cuenta con distintos tipos de herramientas como Zabbix y Wazuh que nos permiten monitorear y registrar los eventos en distintos sistemas, a la par a estos luego el personal debe convertirlos en acciones basadas en procedimientos operativos convertidos a tickets o eventos que registren una acción o respuesta ante el incidente.

Es importante que todas estas herramientas luego se conviertan en métricas las cuales pueden ser evaluadas y luego basadas en datos medir la calidad de servicio, la atención y si finalmente contamos o no con el personal adecuado para la operación.

Nuestro gran desafío en estos tiempos es la posibilidad de brindar servicios con operación continua 24/7, pero este desafío no viene sin sus complicaciones, cada puesto que deba ser cubierto requiere por lo menos 5 personas.

Hoy en día la DNCP se ha organizado para responder a esta necesidad 24/7, pero a un tremendo costo de personal, ya que parte del equipo está cumpliendo guardias permanentes a disposición 24 horas, si bien el personal siempre está dispuesto a colaborar es importante tener en cuenta los permisos, vacaciones y necesidades adicionales que vayan sucediendo.

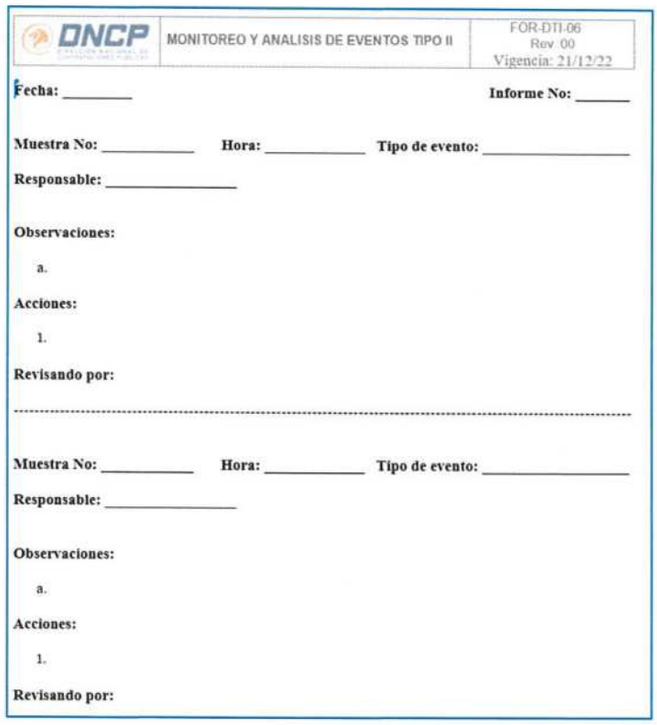
Hoy en día contamos con los siguientes materiales para documentar los eventos.

FOR-DGTIC-16 Informe de Monitoreo y análisis de Eventos tipo I

DNCP	Informe de Monitoreo y Análisis de Eventos tipo I			FOR-DTI-16 Rev.:01 Vigencia: 04/11/2020
Fecha:				
Muestra Nº:				
Rango de tiempo:				
Parámetros:	Nivel de criticidad Nivel de acción Tipo de firma		Origen Destino Otro	
Observaciones y detalles	1. 2.			
Análisis	1. 2.			
Recomendación	1. 2.			
Datos Adjuntos		Obs.:		
Comunicación	Externa	Obs.:		
Responsables	Realizado por:		Validado por:	

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

- FOR-DGTIC-06 Informe de Monitoreo y Analisis de Eventos tipo II



DNCP	MONITOREO Y ANALISIS DE EVENTOS TIPO II	FOR-DTI-06 Rev .00 Vigencia: 21/12/22

Fecha: _____ **Informe No:** _____

Muestra No: _____ **Hora:** _____ **Tipo de evento:** _____

Responsable: _____

Observaciones:

a.

Acciones:

1.

Revisando por:

Muestra No: _____ **Hora:** _____ **Tipo de evento:** _____

Responsable: _____

Observaciones:

a.

Acciones:

1.

Revisando por:

Estos a su vez están siendo manejados ya en formato digital, uno de los más importantes objetivos de un NOC para darle valor a toda la estructura y al trabajo realizado por los mismos es la documentación de cada evento y/o actividad.

La DNCP tiene un equipo operativo en ambos sitios con personal propio y contratado.

Las funcionalidades del NOC pueden ser distribuidas entre las siguientes:

Monitoreo: El NOC monitorea la red, los servidores y las aplicaciones para garantizar su rendimiento y salud.

Respuesta a incidentes: Si el NOC detecta un problema, responde para corregirlo y restaurar el funcionamiento normal.

Gestión de la seguridad: El NOC gestiona el firewall, el sistema de prevención de intrusiones (IPS) y otros sistemas de seguridad.

Gestión del sistema: El NOC implementa, administra y retira los servidores y dispositivos de red.

Administración de parches: El NOC identifica sistemas vulnerables y aplica parches y actualizaciones para corregirlos.

Automatización de procesos: El NOC automatiza tareas repetitivas para que el equipo de TI pueda gestionar otros servicios.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Este proceso de relevamiento de infraestructura posteriormente nos va a llevar al proceso de relevamiento de procedimientos.

Es importante tener en cuenta que a la par que vamos elevando el nivel del equipo de monitoreo van aligerando la carga al equipo operativo, de ahí podemos determinar que el equipo de monitoreo tiene varios niveles posibles.

1- Nivel Básico
- Monitoreo
- Respuesta a incidentes

2- Nivel Intermedio
- Gestión de seguridad
- Gestión de sistemas

3- Nivel avanzado
- Administración de parches
- Automatización de procesos

Un nivel avanzado de NOC prácticamente realiza las funciones de OPERACIONES mientras que el plantel realiza las funciones de PRODUCCIÓN.

9.8.1 NOC DC1

La sala de NOC está bien distribuida y los equipos de monitoreo están a distancias correcta, mesas y disposiciones de monitores adecuados.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Observación: Requiere un espacio técnico para ir armando equipos y otros ya que potencialmente la sala puede llenarse, esto es respetando una recomendación del estándar TIA 942 donde se designa una salade montaje especial

9.8.2 NOC DC2

El Sitio Secundario está correctamente distribuido y los monitores colocados a una distancia razonable, posteriormente con el proceso de relevamiento de procedimientos, se encuentra en situación similar al DC1.

10 Evaluación de infraestructura de cableado.

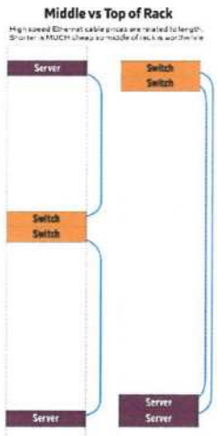
El cableado estructurado del datacenter contiene una combinación de cables UTP de distintas categorías 5A, 6A, así como cableado de FO de varios tipos, SM, MM, OM4.

Un detalle muy importante a la hora de organizar el cableado es que se debe definir que mecánica de interconexión de racks utilizar, ya sea para servicios o gestión, la ubicación de los equipos debe ser consistente entre los racks y los mismos deben interconectarse mediante cables largos utilizando la estructura del piso falso, de la misma manera que la infraestructura de O&M

Un detalle importante al evaluar la situación actual es que se encontraban en proceso de instalación de nuevos equipos, lo cual deja muchos cables temporales durante el proceso de instalación, esta situación debe ser reevaluada en un momento posterior.

Las estructuras tradicionales de TOR (Top of rack), o Middle rack o la menos común (Bottom of rack) deben ser preparadas en cada rack, independiente de su uso o no, y los switches de gestión, independiente de que estos sean rack de servidores, telco, storage, seguridad, UTP o FO ya que no prepararlas ocasiona que distintos técnicos, proveedores o en momentos de apuro o emergencia estas posiciones sean utilizadas sin consideración.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

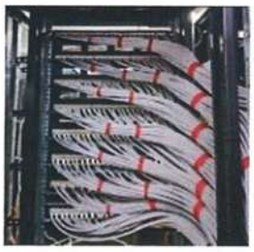


Dependiendo del rack se deben elegir que lados utilizar para los cables UTP y cuales para la FO ya que estas son mucho más frágiles, en caso de racks de uso especifico se puede permitir el acceso por ambos lados. Alimentación, todo debe realizarse por la parte posterior, especialmente si estamos hablando de ventilación FRONT to BACK, para que las fuentes soplen hacia la parte trasera del rack.

10.1 Estructura UTP

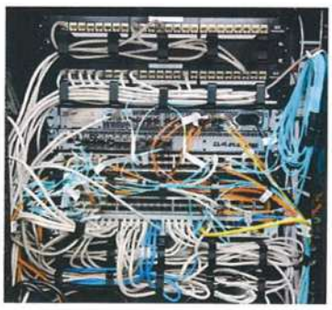
10.1.1 Rack to Outlet

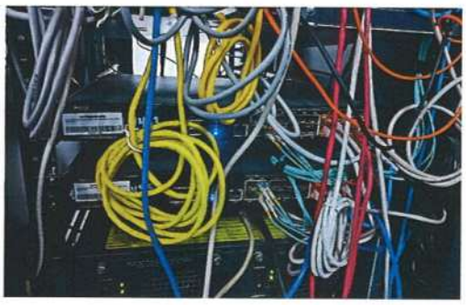
La infraestructura de cableado estructurado al edificio está compuesta de Cableado UTP CAT color gris, esta se encuentra ordenada y terminada en patcheras.



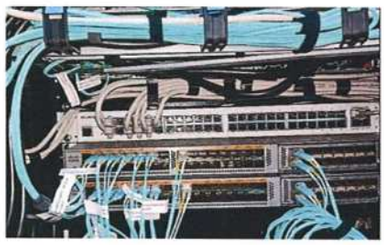
10.1.2 Inner – rack

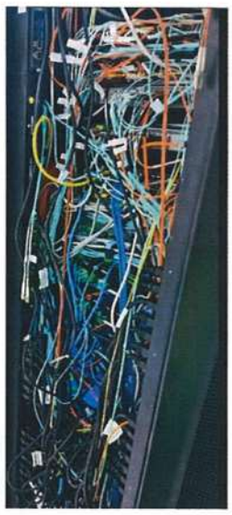
El cableado interno de los racks es adecuado ,pero requiere mayor ordenamiento, vemos que se requiere la utilización adicional de ordenadores de cables así como ordenar FO, UTP, Power.





Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

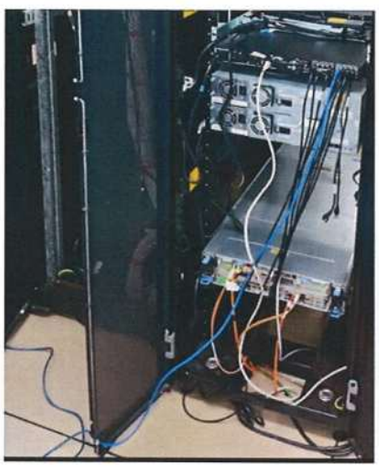


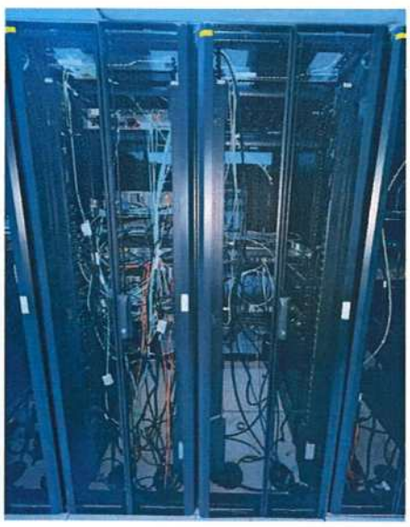


10.1.3 Cross – Rack

Es importante reducir al mínimo las interconexiones entre racks que no sean vía el TOR (top of the rack) o vía el switch de la red de gestión.

Esto complica bastante al generar las zonas diferenciadas de seguridad, servidores, storage, pisos, telefonía etc.





10.1.4 Cableado FO

La estructura de cableado de fibra óptica está dividida de la siguiente manera:

- Cableado SM (Amarillo)

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

- Cableado MM (Naranjado)
- Cableado (OM4, MM) Celeste

Lo ideal es la separación del tipo de cableado por el tipo de longitud de onda, así como el uso, lo ideal sería tener un color separado para la infraestructura de ethernet, así como la infraestructura de fibre channel, vemos que el uso del cableado OM4 celeste es de uso generalizado en nuevos proyectos.

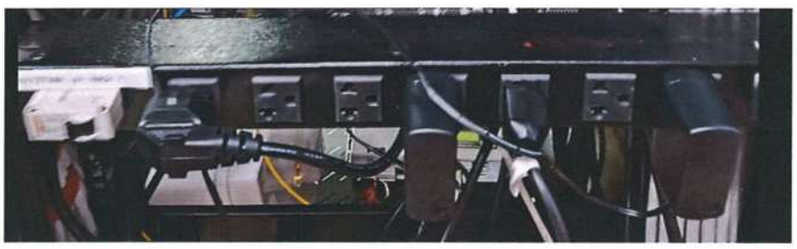
Adicionalmente para las recomendaciones estaremos trabajando para la diferenciación de los enlaces locales (normalmente MM) versus los enlaces remotos (SM)

E internamente se debe diferenciar las terminaciones locales de las remotas.

Cableado cross-rack

10.1.5 PDU

El datacenter primario consta mayormente de PDUs horizontales, lo cual conlleva a tener que realizar una mejor distribución del cableado eléctrico, la norma TIA -568 nos pide que mantengamos una separación razonable, en racks altamente poblados esto no es fácil, de manera que sugerimos el uso de PDUs verticales.



Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

El datacenter 2 presenta una mejor estructura de PDU, si bien no existe una obligación de usar PDUs horizontales o verticales, con la nueva densidad de equipos el uso de PDUs verticales es mucho más eficiente, sin contar que permite una mayor cantidad de equipos conectados, una mejora sustancial para el DC1 sería la instalación de este tipo de PDU.

Para continuar la evaluación se ha detectado equipos que poseen fuente simple, para dichos equipos se recomienda usar PDUs inteligentes de doble fuente, o equipos ATS que permitan conectar los mismos, ya que sin esa infraestructura será imposible realizar el mantenimiento de cualquiera de los brazos de las UPS.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

11 Evaluación de herramientas de seguridad física y lógica

11.1 Acceso físico y lógico

El sistema de acceso físico cuenta con las siguientes capas:

1- Acceso a edificio principal, personal físico, y llaves físicas, registro en papel, toma de datos nombre, cedula, empresa.
2- Acceso a espacios operativos de tecnología, recepcionista que toma los detalles y anota en papel nombre, cedula, empresa.
3- Acceso a datacenter mediante tarjeta magnética, solo personal autorizado, salida mediante puertas de seguridad de empuje (incendio) así como botones de patico.
4- Racks abiertos abiertos en su mayoría DC1, cerrados DC2.
5- cámaras de seguridad CCTV.



11.1.1 Señalética en general


Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Bibliografía

MITIC 2022, Plan Nacional TIC, URL= https://drive.mitic.gov.py/index.php/s/xWyPqZQ99Jm8zYL

MITIC CERTPY 2017, Plan Nacional de Cyberseguridad,
URL= https://gestordocumental.mitic.gov.py/share/s/zkKW1CkKScSvapqlB7UhNg

MITIC 2019, Res 733/2019 Modelo de Gobernanza de la Seguridad de la Información,
URL: https://www.cert.gov.py/wp-content/uploads/2022/07/RESOLUCION_MITIC_N_733-2019_-_Modelo_de_Gobernanza-1.pdf

Ministerio Interior 2016, Dec 6234/2016, Estructura mínima TICS con la que se deberá contar y se establecen otras disposiciones.
URL: https://www.cert.gov.py/wp-content/uploads/2022/07/DECRETO6234_-_Estructura_TICS_GOB.pdf

MITIC 2019, Reso 699/219, Criterios Mínimos para el desarrollo y adquisición de Software
URL= https://drive.mitic.gov.py/index.php/s/P6MpFDLNMRR3cq6

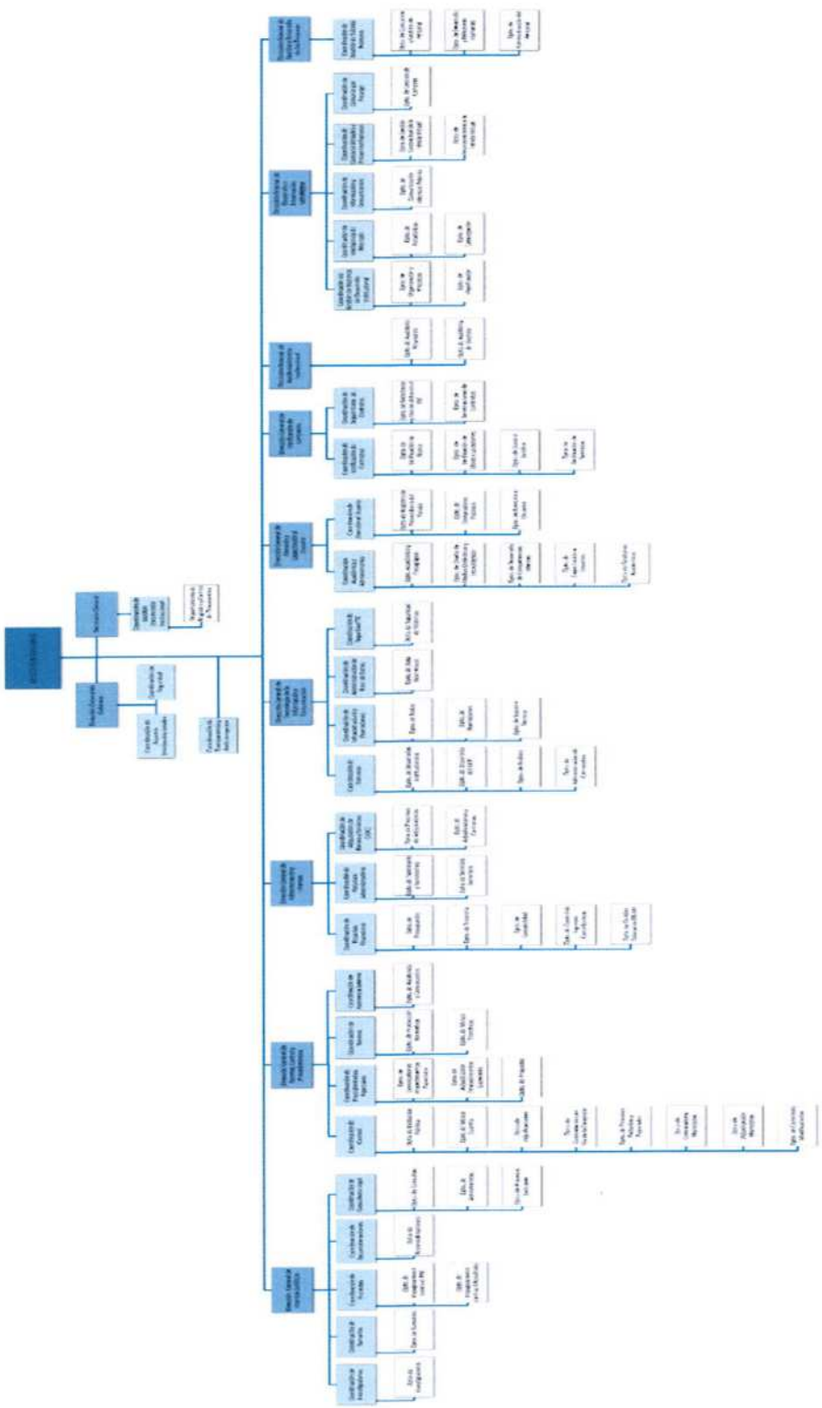
TIA 942, Telecommunications Industry Association, Estándar que rige la certificación de datacenters
URL= https://tiaonline.org/products-and-services/tia942certification/ansi-tia-942-standard/
URL= https://en.wikipedia.org/wiki/TIA-942
URL= https://tiaonline.org/942-datacenters/

UPTIME INSTITUTE, Entidad privada que certifica data centers acorde a la TIA-942 y otras practicas propias de la institución.
URL= https://uptimeinstitute.com/

TIA-568
URL= https://en.wikipedia.org/wiki/ANSI/TIA-568

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

13 ANEXO 1: Organigrama completo



Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

14 ANEXO 2: Encuestas

14.1 Respuestas Organizadas por Nombre y Apellido

14.1.1 Roberto Godoy

Cargo: Técnico en Soporte
Nivel educativo: Estudiante universitario
¿Cuánto tiempo llevas trabajando en el sector de TIC?: Entre 4 y 6 años
Considero que mi experiencia previa en TIC es suficiente para desempeñar mi rol actual.:5
Estoy familiarizado con las herramientas y tecnologías que utiliza la institución.:3
Siento que mi formación académica o técnica está alineada con las demandas del puesto.:5.0
¿Tienes experiencia en la administración de redes o servidores?
Conocimientos sobre protocolos, configuración de routers, y gestión de servidores. Especifica cual no es tu área de expertiz y cual si es.:
No tengo experiencia, pero tengo conocimiento sobre protocolos TCP/IP, configuración básica de router cisco, Sobre Gestión de Servidores no tengo conocimiento.
¿Qué nivel de experiencia tienes en seguridad informática?
Conocimiento en prácticas OWASP, firewalls, detección de intrusos, cifrado, y gestión de vulnerabilidades. Especificar en cual no.:
Tengo los conocimientos, pero no tengo las herramientas necesarias para llevar a cabo alguna prueba de laboratorio o aplicar el conocimiento adquirido.
¿Puedes describir un incidente crítico que hayas manejado? ¿Qué pasos seguiste?:
En el área que estoy actualmente todos los incidentes Tienen solución y si un incidente es crítico se deriva al área correspondiente ej: Sistemas, NOC, SOC
¿Cómo manejas un problema técnico que no conoces?:
Lo primero que hago es relevar todos los datos correspondientes para así poder investigar, consultar y aplicar la mejor solución para ese problema técnico específico.
¿Cuál consideras que es tu mayor fortaleza como profesional de TIC?:
La capacitación constante, las ganas de aprender cosas nuevas y la honestidad en el trabajo, sobre todo.
¿Qué aspecto de tu trabajo crees que podrías mejorar?:
Capacitación Técnica y conocimientos de otras áreas
¿Qué herramientas o recursos adicionales crees que necesitas para desempeñar mejor tu trabajo? (mencionar cursos, herramientas, equipos, personal, etc.):
Necesitaría Cursos intensivos para desempeñar mejor mi trabajo:
Cursos y herramientas para administrar servidores
Cursos de Microsoft
Cursos de Redes
Curso de Electrónica y herramientas para reparación de placas.
¿Qué recomendarías para mejorar la colaboración entre TI y otras áreas de la institución? incluso con otras áreas dentro de la DGTIC.:
Con otras áreas de la DGTIC recomendaría compartir el conocimiento adquirido en cada área
¿Hay algo más que te gustaría compartir sobre tu experiencia en el área de TI?:
Ninguna

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

14.1.2 Martha Cáceres

Cargo: Jefa Soporte Técnico
Nivel educativo: Titulo Universitario
¿Cuánto tiempo llevas trabajando en el sector de TIC?: Entre 15 y 20 años
Considero que mi experiencia previa en TIC es suficiente para desempeñar mi rol actual.: 4
Estoy familiarizado con las herramientas y tecnologías que utiliza la institución.: 2
Siento que mi formación académica o técnica está alineada con las demandas del puesto.: 5.0
¿Tienes experiencia en la administración de redes o servidores?
Conocimientos sobre protocolos, configuración de routers, y gestión de servidores. Especifica cual no es tu área de expertiz y cual si es.:
No tengo experiencia en la administración de redes o servidores
¿Qué nivel de experiencia tienes en seguridad informática?
Conocimiento en prácticas OWASP, firewalls, detección de intrusos, cifrado, y gestión de vulnerabilidades. Especificar en cual no.:
No poseo experiencia en seguridad informática.
¿Puedes describir un incidente crítico que hayas manejado? ¿Qué pasos seguiste?:
Debido a la tarea que desempeño los incidentes procesados en mi área poseen solución, los incidentes críticos comunicamos a coordinación que corresponda, por ejemplo, si el portal está abajo inmediatamente comunicamos al NOC, y al coordinador de Infraestructura.
¿Cómo manejas un problema técnico que no conoces?:
Como primera acción, consulto con mi equipo de trabajo e investigo en internet para identificar posibles soluciones al problema técnico. Si el inconveniente está relacionado con otra área, como redes, me pongo en contacto con el departamento correspondiente para verificar si pueden resolverlo. En caso afirmativo, solicito que compartan la información necesaria para evaluar si la solución podría ser aplicada por el equipo de soporte en el futuro.

Si no logro encontrar una solución, informo a mi coordinador y, en paralelo, busco posibles alternativas, como consultar a expertos externos, investigar costos de repuestos y mano de obra, o explorar opciones de consultoría. Posteriormente, presento a mi superior las soluciones propuestas para que, en conjunto, podamos determinar cuál es la más viable y aplicable.
¿Cuál consideras que es tu mayor fortaleza como profesional de TIC?:
Mi mayor fortaleza como profesional de TIC es mi capacidad para coordinar eficazmente el trabajo en equipo, asegurar la formación continua de los técnicos encargados de la atención al usuario y gestionar de manera proactiva la adquisición de herramientas y recursos necesarios para que mi departamento pueda desempeñar sus funciones
¿Qué aspecto de tu trabajo crees que podrías mejorar?:
El procedimiento de mesa de ayuda, la atención y seguimiento a las consultas de los usuarios.
¿Qué herramientas o recursos adicionales crees que necesitas para desempeñar mejor tu trabajo? (mencionar cursos, herramientas, equipos, personal, etc.):

Lo principal es contar con recursos humanos de la casa, y una herramienta que permita gestionar los activos y servicios de TI, como ser inventarios de hardware y software, incidentes, problemas, tareas, etc.

¿Qué recomendarías para mejorar la colaboración entre TI y otras áreas de la institución? incluso con otras áreas dentro de la DGTIC.:

Mayor comunicación, y coordinación en las tareas, mesas de trabajo en conjunto, pero no solo de los directores, ya que al momento de aplicar lo acordado entre direcciones, se detectan acciones que no serán posible realizar.

¿Hay algo más que te gustaría compartir sobre tu experiencia en el área de TI?:

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

El equipo de trabajo que tengo actualmente se capacita constantemente, y gracias a ello el departamento de soporte puede enfrentar y solucionar como primer frente desde problemas sencillos a complejos, es por ello que considero super importante ver la posibilidad de incluirles a ellos en el plantel de la DNCP

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

14.1.3 Víctor Hugo Medina Ruíz

Cargo: Soporte IT senior
Nivel educativo: No estoy estudiando ahora en la universidad
¿Cuánto tiempo llevas trabajando en el sector de TIC?: Entre 15 y 20 años
Considero que mi experiencia previa en TIC es suficiente para desempeñar mi rol actual.: 5
Estoy familiarizado con las herramientas y tecnologías que utiliza la institución.: 2
Siento que mi formación académica o técnica está alineada con las demandas del puesto.: 5.0
¿Tienes experiencia en la administración de redes o servidores?
Conocimientos sobre protocolos, configuración de routers, y gestión de servidores. Especifica cual no es tu área de expertiz y cual si es.:
Conocimientos tengo, pero falta experiencia para poder aplicar.
¿Qué nivel de experiencia tienes en seguridad informática?
Conocimiento en prácticas OWASP, firewalls, detección de intrusos, cifrado, y gestión de vulnerabilidades. Especificar en cual no.:
Conocimientos tengo pero falta experiencia para poder aplicar.
¿Puedes describir un incidente crítico que hayas manejado? ¿Qué pasos seguiste?:
Debido a mi área de trabajo los problemas críticos fueron subsanados.
¿Cómo manejas un problema técnico que no conoces?:
Se basa en investigación del problema, materiales en la web, foros, fabricantes.
¿Cuál consideras que es tu mayor fortaleza como profesional de TIC?:
Mi mayor fortaleza es la investigación técnica y el trato con el usuario final.
¿Qué aspecto de tu trabajo crees que podrías mejorar?:
Adquirir mayor conocimientos de otras áreas por ej. administración de servidores.
¿Qué herramientas o recursos adicionales crees que necesitas para desempeñar mejor tu trabajo? (mencionar cursos, herramientas, equipos, personal, etc.):
Acceso a capacitaciones: Microsoft, Apple.
¿Qué recomendarías para mejorar la colaboración entre TI y otras áreas de la institución? incluso con otras áreas dentro de la DGTIC.:
Fomentar una cultura de comunicación efectiva entre las demás áreas: reuniones informativas del rol dela DITIC para entender el impacto actual de la tecnología a nivel laboral e incluso personal.
¿Hay algo más que te gustaría compartir sobre tu experiencia en el área de TI?:
Una estrategia clave es invertir en la formación y el desarrollo continuo del personal. Los programas de capacitación interna, las certificaciones y el desarrollo de nuevas habilidades son esenciales para mantener equipos productivos y motivados.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

14.1.4 Freddy Cantero

Cargo: Técnico
Nivel educativo: No estoy estudiando ahora en la universidad
¿Cuánto tiempo llevas trabajando en el sector de TIC?: Entre 1 y 3 años
Considero que mi experiencia previa en TIC es suficiente para desempeñar mi rol actual.: 3
Estoy familiarizado con las herramientas y tecnologías que utiliza la institución.: 2
Siento que mi formación académica o técnica está alineada con las demandas del puesto.: 3.0
¿Tienes experiencia en la administración de redes o servidores?
Conocimientos sobre protocolos, configuración de routers, y gestión de servidores. Especifica cual no es tu área de expertiz y cual si es.:
No tengo experiencias en estos campos.
¿Qué nivel de experiencia tienes en seguridad informática?
Conocimiento en prácticas OWASP, firewalls, detección de intrusos, cifrado, y gestión de vulnerabilidades. Especificar en cual no.:
Conocimientos pero no experiencia. en el campo de Seguridad
¿Puedes describir un incidente crítico que hayas manejado? ¿Qué pasos seguiste?:
De momento no tuve un incidente critico
¿Cómo manejas un problema técnico que no conoces?:
A través de investigación del caso o de consultas a un experimentado del área.
¿Cuál consideras que es tu mayor fortaleza como profesional de TIC?:
De momento no tengo fortaleza especifica en el campo ya estoy aprendiendo y capacitándome
¿Qué aspecto de tu trabajo crees que podrías mejorar?:
Adquirir mayor conocimiento en el proceso de otras áreas
¿Qué herramientas o recursos adicionales crees que necesitas para desempeñar mejor tu trabajo? (mencionar cursos, herramientas, equipos, personal, etc.):
Capacitaciones y cursos
¿Qué recomendarías para mejorar la colaboración entre TI y otras áreas de la institución? incluso con otras áreas dentro de la DGTIC.:
Capacitación cruzada para que los empleados de TI entiendan mejor las funciones de otras áreas, y viceversa.
¿Hay algo más que te gustaría compartir sobre tu experiencia en el área de TI?:
Ninguna

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Daniel Delgado
Cargo: Jefe Departamento de Base de Datos
Nivel educativo: Titulo Universitario
¿Cuánto tiempo llevas trabajando en el sector de TIC?: Entre 11 y 15 años
Considero que mi experiencia previa en TIC es suficiente para desempeñar mi rol actual.: 5
Estoy familiarizado con las herramientas y tecnologías que utiliza la institución.: 4
Siento que mi formación académica o técnica está alineada con las demandas del puesto.: 5.0
¿Tienes experiencia en la administración de redes o servidores?
Conocimientos sobre protocolos, configuración de routers, y gestión de servidores. Especifica cual no es tu área de expertiz y cual si es.:
Base de datos es mi área, no tengo experiencia en administrar redes o servidores
¿Qué nivel de experiencia tienes en seguridad informática?
Conocimiento en prácticas OWASP, firewalls, detección de intrusos, cifrado, y gestión de vulnerabilidades. Especificar en cual no.:
No tengo experiencia en seguridad informática a parte de las buenas prácticas que son de sentido común, hay compañeros que se dedican a ese aspecto
¿Puedes describir un incidente crítico que hayas manejado? ¿Qué pasos seguiste?:
Incidente critico en mi área seria la des sincronización de la alta disponibilidad de algunas bases de datos... detectar las bases de datos des sincronizadas y meterlas a la alta disponibilidad y hacer controles periódicos para que detectar esto y solucionarlo de la manera más rápida
¿Cómo manejas un problema técnico que no conoces?:
Acudo a los compañeros del área necesaria, recurro a material de internet a paginas especializadas en el tema que no conozco
¿Cuál consideras que es tu mayor fortaleza como profesional de TIC?:
Conocer la estructura de datos que maneja la institución
¿Qué aspecto de tu trabajo crees que podrías mejorar?:
Conocer más herramientas de mi área
¿Qué herramientas o recursos adicionales crees que necesitas para desempeñar mejor tu trabajo? (mencionar cursos, herramientas, equipos, personal, etc.):
Cursos de herramientas de minería de datos o de inteligencia de negocio BI
¿Qué recomendarías para mejorar la colaboración entre TI y otras áreas de la institución? incluso con otras áreas dentro de la DGTIC.:
Creo que la comunicación es buena, seguir teniendo un dialogo constante para buscar mejorar los procesos con todas las áreas
¿Hay algo más que te gustaría compartir sobre tu experiencia en el área de TI?:
Nada en particular

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

14.1.5 Diego Ayala

Cargo: Coordinador Adm. base de datos
Nivel educativo: Titulo Universitario
¿Cuánto tiempo llevas trabajando en el sector de TIC?: Entre 15 y 20 años
Considero que mi experiencia previa en TIC es suficiente para desempeñar mi rol actual.: 5
Estoy familiarizado con las herramientas y tecnologías que utiliza la institución.: 4
Siento que mi formación académica o técnica está alineada con las demandas del puesto.: 4.0
¿Tienes experiencia en la administración de redes o servidores?
Conocimientos sobre protocolos, configuración de routers, y gestión de servidores. Especifica cual no es tu área de expertiz y cual si es.:
servidores si, redes no
¿Qué nivel de experiencia tienes en seguridad informática?
Conocimiento en prácticas OWASP, firewalls, detección de intrusos, cifrado, y gestión de vulnerabilidades. Especificar en cual no.:
nivel basico en casi todo.
¿Puedes describir un incidente crítico que hayas manejado? ¿Qué pasos seguiste?:
desincronización del servidor de db de producción por problemas de red. Seguimos los pasos requeridos para volver a poner sincronizados los equipos
¿Cómo manejas un problema técnico que no conoces?:
recurro a los técnicos que creo que conocen o a san google
¿Cuál consideras que es tu mayor fortaleza como profesional de TIC?:
Responsabilidad y serenidad para tomar decisiones que requieren tranquilidad por la criticidad de las mismas.
¿Qué aspecto de tu trabajo crees que podrías mejorar?:
creo que algo que falta mejorar dentro de la dti, es la de la comunicación, principalmente entre los coordinadores.
¿Qué herramientas o recursos adicionales crees que necesitas para desempeñar mejor tu trabajo? (mencionar cursos, herramientas, equipos, personal, etc.):
cursos, analisis de datos, data lake, IA, seguridad, BI, actualizaciones sobre bases de datos no sql ejemplo Elasticsearch, linux, servidores, virtualizaciones, me interesaría saber más sobre las herramientas con las que contamos
¿Qué recomendarías para mejorar la colaboración entre TI y otras áreas de la institución? incluso con otras áreas dentro de la DGTIC.:
creo que la mayor problemática es la comunicación, se debe mejorar y optimizar para que todos manejemos la misma información, principalmente dentro de TI, y eso ayudaría con las otras áreas de la institución.
¿Hay algo más que te gustaría compartir sobre tu experiencia en el área de TI?:
creo que somos un equipo que viene trabajando hace mucho tiempo juntos, y ya conocemos las mañas de cada uno, pero como comente, falta algo mas, y creo que es la comunicación, para que sepamos los proyectos que lleva cada uno y que eso del alguna manera no permita colaborar mejor, buscando siempre la optimización de los servicios que brindamos dentro toda la TI con las demás direcciones.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Francisco Alonso
Cargo: Técnico del NOC
Nivel educativo: Estudiante universitario
¿Cuánto tiempo llevas trabajando en el sector de TIC?: Entre 11 y 15 años
Considero que mi experiencia previa en TIC es suficiente para desempeñar mi rol actual.: 4
Estoy familiarizado con las herramientas y tecnologías que utiliza la institución.: 4
Siento que mi formación académica o técnica está alineada con las demandas del puesto.: 4.0
¿Tienes experiencia en la administración de redes o servidores?
Conocimientos sobre protocolos, configuración de routers, y gestión de servidores. Especifica cual no es tu área de expertiz y cual si es.:
No es configuración de router y si gestión de servidores
¿Qué nivel de experiencia tienes en seguridad informática?
Conocimiento en prácticas OWASP, firewalls, detección de intrusos, cifrado, y gestión de vulnerabilidades. Especificar en cual no.:
OWASP
¿Puedes describir un incidente crítico que hayas manejado? ¿Qué pasos seguiste?:
Una funcionaria había borrado archivos críticos de auditoría del FS, me comunique con la funcionaria y consulte cual era la ubicación del archivo borrado y el nombre del archivo borrado. Le comenté que podríamos recuperar el archivo, pero solo hasta un día antes del borrado. Procedí a restaurar el archivo e informe por correo lo sucedido a mi superior y puse en copia a los involucrados.
¿Cómo manejas un problema técnico que no conoces?:
Cuando me llegan casos de ese tipo lo primero que digo es "ok déjame voy a verificar el caso". Me pongo a investigar cuales serian las causas y los posibilidades de solución
¿Cuál consideras que es tu mayor fortaleza como profesional de TIC?:
Trabajo en equipo, comunicación efectiva, gestión de tiempo y organización
¿Qué aspecto de tu trabajo crees que podrías mejorar?:
Actualización de tareas y gestión de tiempo
¿Qué herramientas o recursos adicionales crees que necesitas para desempeñar mejor tu trabajo? (mencionar cursos, herramientas, equipos, personal, etc.):
Actualmente contamos con herramientas para monitoreo y gestión de activos, pero estoy seguro de que no estamos explotando al 100% dichas herramientas. Entonces diría que lo ideal sería pulir un poco más esas herramientas para que será de mejor utilidad. También sería muy bueno cambiar todo el sistema de acceso físico ya están viejos y con inconvenientes.
¿Qué recomendarías para mejorar la colaboración entre TI y otras áreas de la institución? incluso con otras áreas dentro de la DGTIC.:
Promover la capacitación entre departamentos.
¿Hay algo más que te gustaría compartir sobre tu experiencia en el área de TI?:
En mi experiencia sería fantástico poder tener capacitaciones para mejorar el conocimiento sobre el OpenShift, tener la posibilidad de involucrarnos si es posible en los proyectos o cambios que deseen realizar para poder dar una visión diferente desde el punto de vista cliente/servicios.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

14.1.6 Christian Garay Irala

Cargo: Jefe de Redes
Nivel educativo: Título Universitario
¿Cuánto tiempo llevas trabajando en el sector de TIC?: Entre 11 y 15 años
Considero que mi experiencia previa en TIC es suficiente para desempeñar mi rol actual.: 5
Estoy familiarizado con las herramientas y tecnologías que utiliza la institución.: 5
Siento que mi formación académica o técnica está alineada con las demandas del puesto.:
nan
¿Tienes experiencia en la administración de redes o servidores?
Conocimientos sobre protocolos, configuración de routers, y gestión de servidores. Especifica cual no es tu área de expertiz y cual si es.:
Tengo experiencia en ambos
¿Qué nivel de experiencia tienes en seguridad informática?
Conocimiento en prácticas OWASP, firewalls, detección de intrusos, cifrado, y gestión de vulnerabilidades. Especificar en cual no.:
tengo conocimiento un poquito de todo
¿Puedes describir un incidente crítico que hayas manejado? ¿Qué pasos seguiste?:
Corte de fibra óptica entre datacenter, los pasos fue medir, detectar el corte, y solicitar de manera urgencia la fusión y arreglo mediante un contrato abierto que tengo
¿Cómo manejas un problema técnico que no conoces?:
Con calma, consulto con mi superior o lo investigo.
¿Cuál consideras que es tu mayor fortaleza como profesional de TIC?:
Mi mayor fortaleza es mi capacidad para combinar un enfoque técnico sólido con habilidades estratégicas de resolución de problemas
¿Qué aspecto de tu trabajo crees que podrías mejorar?:
podria mejorar con la parte documental.
¿Qué herramientas o recursos adicionales crees que necesitas para desempeñar mejor tu trabajo? (mencionar cursos, herramientas, equipos, personal, etc.):
CCNA
¿Qué recomendarías para mejorar la colaboración entre TI y otras áreas de la institución? incluso con otras áreas dentro de la DGTIC.:
nan
¿Hay algo más que te gustaría compartir sobre tu experiencia en el área de TI?:
nan

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

14.1.7 Hugo Araujo

Cargo: Coordinador de Infraestructura
Nivel educativo: Título Universitario
¿Cuánto tiempo llevas trabajando en el sector de TIC?: Entre 15 y 20 años
Considero que mi experiencia previa en TIC es suficiente para desempeñar mi rol actual.: 4
Estoy familiarizado con las herramientas y tecnologías que utiliza la institución.: 4
Siento que mi formación académica o técnica está alineada con las demandas del puesto.: 4.0
¿Tienes experiencia en la administración de redes o servidores?
Conocimientos sobre protocolos, configuración de routers, y gestión de servidores. Especifica cual no es tu área de expertiz y cual si es.:
Tengo conocimientos en configuración de routers, y gestión de servidores, pero no tengo conocimientos profundos en administración de contenedores y filesystem ceph
¿Qué nivel de experiencia tienes en seguridad informática?
Conocimiento en prácticas OWASP, firewalls, detección de intrusos, cifrado, y gestión de vulnerabilidades. Especificar en cual no.:
Falta de conocimiento en prácticas OWASP y gestión de vulnerabilidades
¿Puedes describir un incidente crítico que hayas manejado? ¿Qué pasos seguiste?:
Caída de Cluster de Almacenamiento Ceph, se recupero backup de archivos y se volvió a levantar las aplicaciones en plataforma Openshift y posteriormente se migraron los archivos a los volúmenes persistentes de cada aplicación
¿Cómo manejas un problema técnico que no conoces?:
Intento no reaccionar de forma impulsiva, trato de recaudar toda la información disponible como por ejemplo que ocurrió y cuando empezó, que cambios recientes pudieron ocasionarlo, trato de identificar los síntomas y empiezo a buscar logs o registros en lo que se o sino trato de investigar lo que desconozco.
¿Cuál consideras que es tu mayor fortaleza como profesional de TIC?:
Adaptarme a los cambios
¿Qué aspecto de tu trabajo crees que podrías mejorar?:
Tiempo de respuesta y organización
¿Qué herramientas o recursos adicionales crees que necesitas para desempeñar mejor tu trabajo? (mencionar cursos, herramientas, equipos, personal, etc.):
Metodologías para mejorar el tiempo de respuesta en las tareas, sistema de inventarios fiables para elaboración de informes y un mejor planeamiento de compras.
¿Qué recomendarías para mejorar la colaboración entre TI y otras áreas de la institución? incluso con otras áreas dentro de la DGTIC.:
Mejor comunicación entre las áreas, procedimientos de cambios y procedimiento compras
¿Hay algo más que te gustaría compartir sobre tu experiencia en el área de TI?:
Ninguna

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

14.1.8 Jorge Javier Gamarra

Cargo: Jefe de operaciones
Nivel educativo: Estudiante universitario
¿Cuánto tiempo llevas trabajando en el sector de TIC?: Entre 11 y 15 años
Considero que mi experiencia previa en TIC es suficiente para desempeñar mi rol actual.: 4
Estoy familiarizado con las herramientas y tecnologías que utiliza la institución.: 4
Siento que mi formación académica o técnica está alineada con las demandas del puesto.: 4.0
¿Tienes experiencia en la administración de redes o servidores?
Conocimientos sobre protocolos, configuración de routers, y gestión de servidores. Especifica cual no es tu área de expertiz y cual si es.:
falta mas configuración de routers
¿Qué nivel de experiencia tienes en seguridad informática?
Conocimiento en prácticas OWASP, firewalls, detección de intrusos, cifrado, y gestión de vulnerabilidades. Especificar en cual no.:
falta OWASP
¿Puedes describir un incidente crítico que hayas manejado? ¿Qué pasos seguiste?:
cuando un sistema informático no podía levantarse, revise los log de la aplicación y resultaba ser que era problemas de permisos con la base de datos
¿Cómo manejas un problema técnico que no conoces?:
busco en las distintas plataformas para poder resolverlo
¿Cuál consideras que es tu mayor fortaleza como profesional de TIC?:
La forma de investigar las distintas novedades que hay en el área TIC
¿Qué aspecto de tu trabajo crees que podrías mejorar?:
Y tengo varias cosas que puedo ir mejorando
¿Qué herramientas o recursos adicionales crees que necesitas para desempeñar mejor tu trabajo? (mencionar cursos, herramientas, equipos, personal, etc.):
cursos sobre openshift
¿Qué recomendarías para mejorar la colaboración entre TI y otras áreas de la institución? incluso con otras áreas dentro de la DGTIC.:
La comunicación entre las áreas
¿Hay algo más que te gustaría compartir sobre tu experiencia en el área de TI?:
nada mas

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

14.1.9 David Savaje

Cargo: Técnico Noc
Nivel educativo: Titulo Universitario
¿Cuánto tiempo llevas trabajando en el sector de TIC?: Entre 4 y 6 años
Considero que mi experiencia previa en TIC es suficiente para desempeñar mi rol actual.: 5
Estoy familiarizado con las herramientas y tecnologías que utiliza la institución.: 5
Siento que mi formación académica o técnica está alineada con las demandas del puesto.: 5.0
¿Tienes experiencia en la administración de redes o servidores?
Conocimientos sobre protocolos, configuración de routers, y gestión de servidores. Especifica cual no es tu área de expertiz y cual si es.:
Experiencia en Servidores y en redes nivel medio
¿Qué nivel de experiencia tienes en seguridad informática?
Conocimiento en prácticas OWASP, firewalls, detección de intrusos, cifrado, y gestión de vulnerabilidades. Especificar en cual no.:
Si
¿Puedes describir un incidente crítico que hayas manejado? ¿Qué pasos seguiste?:
Restauración de documento de fs01 borrado, Restauración de BD del Reloj marcador
¿Cómo manejas un problema técnico que no conoces?:
La investigación y posible solución del problema
¿Cuál consideras que es tu mayor fortaleza como profesional de TIC?:
Mi capacidad para resolver problema complejo mediante el conocimiento adquirido, y mi mayor fortaleza es adaptarme rápidamente a nuevas tecnologías y aprender constantemente.
¿Qué aspecto de tu trabajo crees que podrías mejorar?:
Capacitación de personal en las plataformas que administramos
¿Qué herramientas o recursos adicionales crees que necesitas para desempeñar mejor tu trabajo? (mencionar cursos, herramientas, equipos, personal, etc.):
Curso openshift, redhat
¿Qué recomendarías para mejorar la colaboración entre TI y otras áreas de la institución? incluso con otras áreas dentro de la DGTIC.:
Socialismo
¿Hay algo más que te gustaría compartir sobre tu experiencia en el área de TI?:
Me gustaria destacar que lidera la actualización de la plataforma moodle que redujo el procesamiento de datos y mejoras al sistema.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

14.1.10 Victor Ferloni

Cargo: Encargado de Despacho del Departamento Seguridad de Sistemas.
Nivel educativo: Estudiante universitario
¿Cuánto tiempo llevas trabajando en el sector de TIC?: Entre 11 y 15 años
Considero que mi experiencia previa en TIC es suficiente para desempeñar mi rol actual.: 4
Estoy familiarizado con las herramientas y tecnologías que utiliza la institución.: 4
Siento que mi formación académica o técnica está alineada con las demandas del puesto.: 5.0
¿Tienes experiencia en la administración de redes o servidores?
Conocimientos sobre protocolos, configuración de routers, y gestión de servidores. Especifica cual no es tu área de expertiz y cual si es.:
No tengo experiencia práctica directa en la administración de redes o servidores. Sin embargo, tengo conocimientos teóricos sobre protocolos de red.
¿Qué nivel de experiencia tienes en seguridad informática?
Conocimiento en prácticas OWASP, firewalls, detección de intrusos, cifrado, y gestión de vulnerabilidades. Especificar en cual no.:
OWASP
¿Puedes describir un incidente crítico que hayas manejado? ¿Qué pasos seguiste?:
Por el momento ninguno
¿Cómo manejas un problema técnico que no conoces?:
Investigo, consulto documentación, pruebo soluciones y busco ayuda.
¿Cuál consideras que es tu mayor fortaleza como profesional de TIC?:
Mi mayor fortaleza es la capacidad de aprender rápidamente y adaptarme a nuevas tecnologías.
¿Qué aspecto de tu trabajo crees que podrías mejorar?:
Creo que podría mejorar mi capacidad para resolver problemas técnicos más complejos de manera más rápida y eficaz.
¿Qué herramientas o recursos adicionales crees que necesitas para desempeñar mejor tu trabajo? (mencionar cursos, herramientas, equipos, personal, etc.):
Creo que podría beneficiarme de cursos adicionales sobre Linux y ciberseguridad, así como de herramientas más avanzadas para la automatización y monitoreo de sistemas. También sería útil contar con equipos de prueba más específicos y un equipo de apoyo técnico con más experiencia.
¿Qué recomendarías para mejorar la colaboración entre TI y otras áreas de la institución? incluso con otras áreas dentro de la DGTIC.:
Recomendaría fomentar la comunicación regular, capacitación cruzada y utilizar herramientas colaborativas para mejorar la coordinación y comprensión entre áreas.
¿Hay algo más que te gustaría compartir sobre tu experiencia en el área de TI?:
Ninguna

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

14.1.11 Lourdes Angelino

Cargo: Encargado de Despacho Coordinación de Seguridad TIC
Nivel educativo: Título Universitario
¿Cuánto tiempo llevas trabajando en el sector de TIC?: Entre 15 y 20 años
Considero que mi experiencia previa en TIC es suficiente para desempeñar mi rol actual.: 3
Estoy familiarizado con las herramientas y tecnologías que utiliza la institución.: 2
Siento que mi formación académica o técnica está alineada con las demandas del puesto.: 2.0
¿Tienes experiencia en la administración de redes o servidores?
Conocimientos sobre protocolos, configuración de routers, y gestión de servidores. Especifica cual no es tu área de expertiz y cual si es.:
la experiencia que tengo ya está desactualizada
¿Qué nivel de experiencia tienes en seguridad informática?
Conocimiento en prácticas OWASP, firewalls, detección de intrusos, cifrado, y gestión de vulnerabilidades. Especificar en cual no.:
sólo conceptual y manejo de reportes
¿Puedes describir un incidente crítico que hayas manejado? ¿Qué pasos seguiste?:
Si el responsable directo no está y tengo los conocimientos básicos para resolverlo me pongo manos a la obra. Si soy el responsable directo, a) si tengo los conocimientos manos a la obra (ver metodología en sgte respuesta) b) si no tengo los conocimientos busco quien los tiene y sgtes pasos.
¿Cómo manejas un problema técnico que no conoces?:
respiro profundo para mantener la calma. Verifico la gravedad, urgencia, importancia. Busco apoyo interno o externo de entendidos. Analizo todas las aristas posibles y las alternativas de solución con sus costos / beneficios y elijo hasta 3 alternativas en un nivel de prioridades (si da el tiempo) y se las presento y justifico a mi superior, para obtener la mejor decisión posible.
¿Cuál consideras que es tu mayor fortaleza como profesional de TIC?:
Relevamiento, análisis, implementación, seguimiento de proyectos, en especial los mas engorrosos
¿Qué aspecto de tu trabajo crees que podrías mejorar?:
comunicación verbal
¿Qué herramientas o recursos adicionales crees que necesitas para desempeñar mejor tu trabajo? (mencionar cursos, herramientas, equipos, personal, etc.):
rrhh, cursos de los temas: seguridad de la información, seguridad TIC, ciberseguridad, redes, actualizar administración de servidores
¿Qué recomendarías para mejorar la colaboración entre TI y otras áreas de la institución? incluso con otras áreas dentro de la DGTIC.:
reunión global de trabajo de todos los colaboradores (no solo jefes) de toda la DGTI en general con libertad de expresión total para recibir quejas y sugerencias sin enojos, para mejorar
¿Hay algo más que te gustaría compartir sobre tu experiencia en el área de TI?:
Uso varias técnicas: 1) esponja selectiva (incorporo cosas buenas o positivas y dejo de lado las negativas de las personas o situaciones 2) Hago muchas preguntas y preguntas tontas para aprender siempre y más. 3) Hago simulaciones de situaciones y hago de abogado del diablo. Así consigo mucha información de una situación y sobre los conocimientos para encarar su solución

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

14.1.12 Bertrán Benítez

Cargo: Redes
Nivel educativo: No estoy estudiando ahora en la universidad
¿Cuánto tiempo llevas trabajando en el sector de TIC?: Entre 4 y 6 años
Considero que mi experiencia previa en TIC es suficiente para desempeñar mi rol actual.: 4
Estoy familiarizado con las herramientas y tecnologías que utiliza la institución.: 4
Siento que mi formación académica o técnica está alineada con las demandas del puesto.: 5.0
¿Tienes experiencia en la administración de redes o servidores?
Conocimientos sobre protocolos, configuración de routers, y gestión de servidores. Especifica cual no es tu área de expertiz y cual si es.:
Experiencia en Redes en configuración de routers : Nateo , Segmentos , Ruteos , configuración de troncales , designaciones de vlans
¿Qué nivel de experiencia tienes en seguridad informática?
Conocimiento en prácticas OWASP, firewalls, detección de intrusos, cifrado, y gestión de vulnerabilidades. Especificar en cual no.:
en cuanto a firewall realizo acceso a salida a internet de ips asignadas a funcionarios y elaboración de web filter
¿Puedes describir un incidente crítico que hayas manejado? ¿Qué pasos seguiste?:
El incidente critico que maneje fue , sobre los switches de distribución que se apagaron por que se bajo la llave por un inconveniente de corto circuito , se realizo la conexión a otra zapatilla de otro rack para volver a encender el equipo
¿Cómo manejas un problema técnico que no conoces?:
1 - realizo una retroalimentación
2 - pido ayuda a mi superior
3 - desgloso el problema
4 - me comunico con claridad
5 - Intento aprender e investigo
¿Cuál consideras que es tu mayor fortaleza como profesional de TIC?:
mi mayor fortaleza es la experiencia , realizando un troubleshooting de cada paso que realizo en cuanto para mi y compañeros
¿Qué aspecto de tu trabajo crees que podrías mejorar?:
La organización
¿Qué herramientas o recursos adicionales crees que necesitas para desempeñar mejor tu trabajo? (mencionar cursos, herramientas, equipos, personal, etc.):
Elaborar cursos de administración de Routers , Switches CORE , Switches SAN , Switches TOR y Firewall de servidores
¿Qué recomendarías para mejorar la colaboración entre TI y otras áreas de la institución? incluso con otras áreas dentro de la DGTIC.:
se recomendaría trabajar de forma sincronizada con otros sectores , adquirir mas herramientas como canaletas y fichas disponer todo a mano
¿Hay algo más que te gustaría compartir sobre tu experiencia en el área de TI?:
La elaboración de ordenamiento de racks , con esto se logra la identificación de usuarios y equipos de cada piso en cuanto a inconvenientes de conexión de telefonos , aps , cámaras.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

15Glosario

AC: Air Conditioner (Aire Acondicionado)
AC: Alternating Current (Corriente Alterna)
ACL: Access Control List (Lista de Control de Acceso)
AES: Advanced Encryption Standard (Estándar de Encriptación Avanzada)
ANDE: Administración Nacional de Electricidad
ANEAES Agencia Nacional de Evaluación y Acreditación de la Educación Superior
API: Application Programming Interface (Interfaz de Programación de Aplicaciones)
APP Asociación Público Privada
ARP: Address Resolution Protocol (Protocolo de Resolución de Direcciones)
BA: Banda Ancha
BCP: Banco Central de Paraguay
BGP: Border Gateway Protocol (Protocolo de Puerta de Enlace Fronteriza)
BIOS: Basic Input/Output System (Sistema Básico de Entrada/Salida)
BMC: Baseboard Management Controller (Controlador de Gestión de Placa Base)
BPS: Bits Per Second (Bits Por Segundo)
BYOD: Bring Your Own Device (Trae Tu Propio Dispositivo)
CaaS: Container as a Service (Contenedor como Servicio)
CAF: Corporación Andina de Fomento
CAPEX: Capital Expenditure (Gasto de Capital)
CDN: Content Delivery Network (Red de Entrega de Contenidos)
CERT-PY: Centro de Respuestas a Incidentes Cibernético
CIFS: Common Internet File System (Sistema de Archivos Común en Internet)
CISO: Chief information security officer (Oficial de Seguridad de la Información)
CLI: Command Line Interface (Interfaz de Línea de Comandos)
CNAME: Canonical Name (Nombre Canónico)
CONACYT: Compañía Nacional de Ciencia y Tecnología
CONATEL: Comisión Nacional de Telecomunicaciones
CONES: Consejo Nacional de Educación Superior
COPACO: Compañía Paraguaya de Comunicaciones
CPU: Central Processing Unit (Unidad Central de Procesamiento)
CRM: Administración de Relaciones del Ciudadano con el Estado
CRUD: Create, Read, Update, Delete (Crear, Leer, Actualizar, Eliminar)
DAC: Discretionary Access Control (Control de Acceso Discrecional)
DBMS: Database Management System (Sistema de Gestión de Bases de Datos)
DCIM: Data Center Infrastructure Management (Gestión de Infraestructura de Centro de Datos)
DDoS: Distributed Denial of Service (Denegación de Servicio Distribuida)
DFS: Distributed File System (Sistema de Archivos Distribuido)
DGCPI: Dirección General de Ciberseguridad y Protección de la Información
DGGE: Dirección General de Gobierno Electrónico
DGIC: Dirección General de Infraestructura y Conectividad
DGIDTE: Dirección General de Inclusión Digital y TIC en la Educación

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

DGIPED: Dirección General de Innovación Productiva y Economía Digital
DHCP: Dynamic Host Configuration Protocol (Protocolo de Configuración Dinámica de Host)
DIMM: Dual In-Line Memory Module (Módulo de Memoria de Línea Doble)
DINAPI Dirección Nacional de Propiedad Intelectual
DNP: Departamento Nacional de Planeación de Colombia
DNS: Domain Name System (Sistema de Nombres de Dominio)
DR: Disaster Recovery (Recuperación ante Desastres)
DRAM: Dynamic Random-Access Memory (Memoria de Acceso Aleatorio Dinámica)
DSL: Digital Subscriber Line (Línea de Suscriptor Digital)
DWDM: Dense Wavelength Division Multiplexing (Multiplexación por División en Longitudes de Onda Densa
EAI: Enterprise Application Integration (Integración de Aplicaciones Empresariales)
EAP: Extensible Authentication Protocol (Protocolo de Autenticación Extensible)
EBD Emprendimiento de Base Digital
ECC: Error-Correcting Code (Código de Corrección de Errores)
ECI Entidad consumidora de la información
EDR: Endpoint Detection and Response (Detección y Respuesta de Puntos de Extremo)
EIGRP: Enhanced Interior Gateway Routing Protocol (Protocolo de Enrutamiento de Puerta de Enlace Interic
ENCONEC: Estrategia Nacional de Conectividad
EOL: End of Life (Fin de Vida Útil)
EPI: Entidad productora de la información
ERP: Enterprise Resource Planning (Planificación de Recursos Empresariales)
ESXi: Elastic Sky X Integrated (Versión de VMware de su Hipervisor)
FCoE: Fibre Channel over Ethernet (Canal de Fibra sobre Ethernet)
FEEI Fondo para la Excelencia de la Educación y la Investigación
FO: Fibra Óptica
FONTED: Fondo Nacional de Tecnologías en la Educación
FONTIC: Fondo Nacional de Tecnologías de la Información
FTP: File Transfer Protocol (Protocolo de Transferencia de Archivos)
Gbps: Gigabits Per Second (Gigabits Por Segundo)
GDL: Gestor de Documentos en Línea
GPU: Graphics Processing Unit (Unidad de Procesamiento Gráfico)
HBA: Host Bus Adapter (Adaptador de Bus de Host)
HIS: Sistema de Información en Salud
HTTP: HyperText Transfer Protocol (Protocolo de Transferencia de Hipertexto)
HTTPS: HyperText Transfer Protocol Secure (Protocolo Seguro de Transferencia de Hipertexto)
HVAC: Heating, Ventilation, and Air Conditioning (Calefacción, Ventilación y Aire Acondicionado)
I+D+i: Investigación, Innovación y Desarrollo
IA: Inteligencia Artificial
IaaS: Infrastructure as a Service (Infraestructura como Servicio)
IAEE: Instituto de Altos Estudios Estratégicos
ICMP: Internet Control Message Protocol (Protocolo de Mensajes de Control de Internet)
ICT: Information and Communication Technology (Tecnología de la Información y Comunicación)
IDS: Intrusion Detection System (Sistema de Detección de Intrusos)
IDU: Impuesto a los Dividendos y a las Utilidades

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

IGEP: Internet Gratuito en Espacios Públicos
INCUNI: La Incubadora de Empresas de la Universidad Nacional de Itapúa
INE: Instituto Nacional de Estadística
INR: Impuesto a la Renta de No Residentes
IoT: Internet de las cosas
IoT: Internet of Things (Internet de las Cosas)
IP: Internet Protocol (Protocolo de Internet)
IPMI: Intelligent Platform Management Interface (Interfaz de Gestión de Plataforma Inteligente)
IPS: Instituto de Previsión Social
IPS: Intrusion Prevention System (Sistema de Prevención de Intrusiones)
IR: Incident Response (Respuesta a Incidentes)
IRE: Impuesto a la Renta Empresarial
IRP: Impuesto a la Renta Personal
ISCSI: Internet Small Computer System Interface (Interfaz de Sistema de Computadora Pequeña por Inter
ISP: Internet Service Provider (Proveedor de Servicios de Internet)
ITIL: Information Technology Infrastructure Library (Biblioteca de Infraestructura de Tecnología de la Infor
ITU International Telecommunication Union
IXPy Punto de Intercambio de Internet de Paraguay
JSON: JavaScript Object Notation (Notación de Objetos de JavaScript)
KVM: Kernel-based Virtual Machine (Máquina Virtual Basada en Núcleo)
IaaS: Infraestructura como Servicio
LAN: Local Area Network (Red de Área Local)
LDAP: Lightweight Directory Access Protocol (Protocolo Ligero de Acceso a Directorios)
LUN: Logical Unit Number (Número de Unidad Lógica)
MAC: Media Access Control (Control de Acceso al Medio)
MADES: Ministerio del Ambiente y Desarrollo Sostenible
MAG: Ministerio de Agricultura y Ganadería
Mbps: Megabits Per Second (Megabits Por Segundo)
MEC: Ministerio de Educación y Ciencias
MEF: Ministerio de Economía y Finanzas
MH: Ministerio de Hacienda
MIC: Ministerio de Industria y Comercio
MIPYMES: Pequeñas y Medianas Empresas
MITIC: Ministerio de Tecnologías de la Información y Comunicación
MPLS: Multiprotocol Label Switching (Conmutación de Etiquetas Multiprotocolo)
MSPBS Ministerio de Salud Pública y Bienestar Social
MTBF: Mean Time Between Failures (Tiempo Medio Entre Fallos)
MTTR: Mean Time to Repair (Tiempo Medio para Reparar)
MUVH Ministerio de Urbanismo, Vivienda y Hábitat
NAS: Network Attached Storage (Almacenamiento Conectado a la Red)
NAT: Network Address Translation (Traducción de Direcciones de Red)
NOC Centro de Operación y Atención al Cliente
NOC: Network Operations Center (Centro de Operaciones de Red)
Nube Py: Nube del Estado

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

NVMe: Non-Volatile Memory Express (Interfaz de Memoria No Volátil)
OAuth: Open Authorization (Autorización Abierta)
ODS: Objetivos de Desarrollo Sostenible
ONG: Organización No Gubernamental
OPEX: Operating Expense
OPEX: Operational Expenditure (Gasto Operativo)
OS: Operating System (Sistema Operativo)
OSI: Open Systems Interconnection (Interconexión de Sistemas Abiertos)
OTP: One-Time Password (Contraseña de Un Solo Uso)
PaaS: Platform as a Service (Plataforma como Servicio)
PBX: Private Branch Exchange (Central Telefónica Privada)
PCI: Peripheral Component Interconnect (Interconexión de Componentes Periféricos)
PCI-DSS: Payment Card Industry Data Security Standard (Estándar de Seguridad de Datos de la Industria de
PDU: Power Distribution Unit (Unidad de Distribución de Energía)
PDU: Protocol Data Unit (Unidad de Datos de Protocolo)
PIB: Producto Interno Bruto
PNC: Plan Nacional de Ciberseguridad
PND: Plan Nacional de Desarrollo
PNT: Plan Nacional de Telecomunicaciones
PNTE: Plan Nacional de Transformación Educativa 2030
PNTIC: Plan Nacional de Tecnologías de la Información y la Comunicación
PROINNOVA: Programa de Innovación en Empresas Paraguayas
QA: Quality Assurance
QoS: Quality of Service (Calidad de Servicio)
RAID: Redundant Array of Independent Disks (Matriz Redundante de Discos Independientes)
RDP: Remote Desktop Protocol (Protocolo de Escritorio Remoto)
RFID: Radio-Frequency Identification (Identificación por Radiofrecuencia)
RIPC: Red Integrada de Infraestructura Pública de Conectividad
RMM: Remote Monitoring and Management (Monitoreo y Gestión Remotos)
RMSP Red Metropolitana del Sector Público
ROE Reglamento Operativo Específico
ROM: Read-Only Memory (Memoria de Solo Lectura)
RPM: Revolutions Per Minute (Revoluciones Por Minuto)
RTC: Real-Time Clock (Reloj en Tiempo Real)
RTO: Recovery Time Objective (Objetivo de Tiempo de Recuperación)
RUE Registro Único del Estudiante
SaaS: Software as a Service (Software como Servicio)
SAN: Storage Area Network (Red de Área de Almacenamiento)
SAS: Serial Attached SCSI (SCSI Conectado en Serie)
SATA: Serial Advanced Technology Attachment (Interfaz de Tecnología Avanzada en Serie)
SDN: Software-Defined Networking (Redes Definidas por Software)
SENAC: Secretaría Nacional Anticorrupción
SENATIC: Secretaría Nacional de Tecnologías de la Información y Comunicación
SET: Subsecretaría de Estado de Tributación

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

SFP: Secretaría de la Función Pública
SFTP: Secure File Transfer Protocol (Protocolo Seguro de Transferencia de Archivos)
SICOM: Secretaría de Información y Comunicación para el Desarrollo
SII: Sistema de Intercambio de Información
SIIS: Sistema Integrado de Información Social
SIP: Sistema de Información Policial
SLA: Service Level Agreement (Acuerdo de Nivel de Servicio)
SLB: Server Load Balancing (Equilibrio de Carga de Servidores)
SMTP: Simple Mail Transfer Protocol (Protocolo Simple de transferencias de correos)
SNC: Servicio Nacional de Catastro
SNMP: Simple Network Management Protocol (Protocolo Simple de Gestion de Redes)
SOC: Centro de Operaciones de Seguridad
STEAM: Ciencia, Tecnología, Ingeniería, Arte y Matemáticas
STP: Secretaría Técnica de Planificación del Desarrollo Económico y Social
TA: Tecnologías Adaptativas
TI: Tecnología e Información
TIC: Tecnologías de la Información y las Comunicaciones
UAT: User Acceptance Testing
UGPR: Unidad de Gestión de la Presidencia de la República
UIS: Instituto de Estadística de la UNESCO
UNA: Universidad Nacional de Asunción
USF: Unidades de Salud Familiar
VPN: Virtual Private Network

Victor Morel
Consultor

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Contrato Nro 21/2024

Proyecto de Mejoramiento de las Finanzas Públicas para el Desarrollo Sostenible del Paraguay

Contrato de Préstamo N° 4671/OC-PR

"Definición del Plan de Infraestructura Tecnológica"

OBP N° P230707.

Revisión de procedimientos

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

1 Contenido

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

2 Objetivos del relevamiento de procedimientos.

El objetivo del análisis de procedimientos tiene por objetivo trabajar con la institución para ir evaluando los procedimientos vigentes aprobados, así como los procedimientos actualmente siendo realizados por el personal de la institución.

Es importante tener en cuenta que muchas instituciones realizan un sin número de trabajos de un valor crítico para la institución y lo hacen de manera natural en su día a día, en muchos casos el staff asignado para dichas tareas es muy reducido, así que el objetivo principal del mismo es avocarse a la ejecución de la tarea en sí, a la par que la institución va contando con un equipo acorde a la institución a esas actividades se pueden ir sumando otras adicionales que nos permitan organizar y documentar las actividades de cada personal,

Para que estos procedimientos puedan ser diseñados, elaborados, aprobados y posteriormente comunicados al personal operativo es importante que se debe tener un equipo de trabajo que constantemente esté acompañando los mismos y sean ellos los que juntamente con el personal existen puedan ir acomodando los mismos.

Adicionalmente dichos procesos deben ajustarse al organigrama y a la cantidad de personal existente, y en caso de necesidad ir creando nuevos roles que puedan ir ejecutando las tareas críticas, a la par que todos los servicios del estado están convirtiéndose en servicios 24/7 el sector tecnológico se está encontrando en un enorme desafío de poder acompañar dichos tiempos, no sin tener en cuenta que debemos acompañar de cerca dicho crecimiento del personal para lograr que la DNCP siga siendo una institución eficiente y referente de la calidad del personal.

Un punto importante a tener en cuenta es que a la par que la institución decida acomodar más tareas o responsabilidades y el personal no sea suficiente el mismo se mantendrá primordialmente realizando actividades IMPORTANTES y URGENTES acorde a la matriz Eisenhower.

Hoy en día la institución está priorizando aquellas personas que HACEN las cosas y sus respectivas tareas.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

A la par que vayamos creciendo en los servicios y la disponibilidad de estos, así como la documentación pertinente para permitir una continuidad de negocios debemos empezar a focalizarnos en la planificación de como estas tareas deben ser resueltas por personal propio o tercerizado.

Todo aquello que esté dentro de la MISION y VISION de la institución y requiera continuidad en el tiempo debe ser realizado por personal interno, con gente de respaldo que permita que la institución se proyecte.

Misión

"Somos la entidad reguladora responsable de la gestión de contrataciones públicas, orientada a promover la eficiencia, la transparencia y la optimización de los recursos públicos"

Visión

"Ser la institución líder en optimización de los procesos de adquisiciones públicas, destacándose a nivel internacional por la innovación y excelencia en los sistemas de compras públicas"

Todo aquello que no esté dentro de la MISION y VISION, y/o no afecte directamente puede ser delegado a terceros.

Para poder delegar a terceros debemos crear procedimientos, formas y la documentación necesaria para el cumplimiento de las normas más adelante citadas que adicionalmente requieren que la institución tenga recursos asignados a dichas tareas administrativas de la organización en forma continua y permanente, ya que sino estaremos sacando un valioso tiempo de recursos asignados a tareas críticas.

Adicionalmente es importante la medición de la productividad de los recursos actuales de manera a poder justificar correctamente con indicadores, KPIs, OKRs o formas de medida similar que nos permitan identificar si estamos logrando los resultados esperados.

Dejamos a continuación una opción de potenciales recursos que se presentan en el PGN para ordenar las finanzas del estado.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

2.1 Potenciales recursos

Pongo a evaluación del equipo de la DNCP la situación atípica sobre la disponibilidad de recursos potencialmente utilizables del sector de la tecnología y telecomunicaciones de COPACO en el marco de ordenamiento operativo de dicha institución, vía Decreto 3248 del Ministerio de Economía y Finanzas, POR EL CUAL SE REGLAMENTA LA LEY N° 7408 DEL 30 DE DICIEMBRE DE 2024, "QUE APRUEBA EL PRESUPUESTO GENERAL DE LA NACIÓN PARA EL EJERCICIO FISCAL 2025".

Explícitamente el Art 195 mencionado siguientemente:

Art. 195.- Traslado de empleados de COPACO. Para el traslado definitivo de los empleados de la Compañía Paraguaya de Comunicaciones S.A. (COPACO S.A.) a los Organismos y Entidades del Estado (OEE), se realizará las siguientes acciones:

1. La Compañía Paraguaya de Comunicaciones S.A. (COPACO S.A.) remitirá al VCHGO el listado de empleados a ser trasladado con el siguiente detalle:
   a. Nombres, apellidos y número de cedula de identidad.
   b. Formación Académica
   c. Antigüedad.
   d. Detalle de puestos ocupados desde su ingreso hasta la actualidad.
   e. Sueldo percibido.
   f. Otras informaciones de interés.
2. El VCHGO informará a las Instituciones Públicas de la existencia del listado de empleados de COPACO a ser trasladados a fin de que las mismas, en caso de estar interesadas, presenten:
   a. Las necesidades de dotación del personal detallando las funciones y los requerimientos técnicos o profesionales del puesto a ser cubierto.
   b. El detalle de disponibilidad presupuestaria del Anexo del Personal. La vacancia deberá corresponder al grupo ocupacional conforme a las necesidades detalladas en el inciso a del presente numeral.
3. Las Entidades interesadas, podrán aplicar evaluaciones durante el proceso de selección y deberán comunicar al VCHGO el listado de empleados a ser trasladados detallando el puesto designado y la categoría salarial a ser otorgada, la cual no podrá ser superior al 20% del salario percibido (OG 111 Sueldo) durante el Ejercicio Fiscal 2024.
4. El VCHGO verificará la correspondencia de la categoría a ser asignada con el grupo ocupacional al que pertenece el empleado a ser trasladado. Se tomará de base el sueldo percibido por el empleado.
5. En caso de parecer favorable, informará a la Institución para que realice los trámites administrativos de nombramiento y posterior alta en el SINARH.
6. En caso de que la Institución cuente con empleados de COPACO prestando servicios en carácter de comisionado, la misma deberá aplicar el traslado conforme a lo establecido en el presente Decreto.

El VCHGO podrá establecer procedimientos y requerimientos adicionales, para dar cumplimiento al traslado.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

2.2 Normas aplicables a la hora de evaluar procedimientos

Algunas de las normas más frecuentemente utilizadas a nivel institución y posteriormente tecnológico son las siguientes:

2.2.1 ISO 9001:2015 Sistema de Gestión de Calidad

Esta se enfoca principalmente en la estandarización de los procesos, descripción de cargos, y posteriores procedimientos, así como la evaluación periódica de la ejecución de estos en la institución

1. **Planificación de la calidad**: La organización debe identificar los procesos necesarios para el SGC y su aplicación en toda la organización. Esto incluye definir objetivos de calidad, políticas, y procedimientos.
2. **Gestión de recursos:** Esto abarca la gestión de los recursos humanos y materiales necesarios para implementar y mantener el SGC, asegurando que el personal esté capacitado y que las infraestructuras y el ambiente de trabajo sean adecuados.
3. **Realización del producto/servicio:** Involucra todas las etapas desde la planificación del producto o servicio hasta su entrega al cliente, incluyendo la identificación de los requisitos del cliente, el diseño y desarrollo, la producción y la prestación del servicio.
4. **Medición, análisis y mejora:** La organización debe realizar actividades de seguimiento y medición para asegurarse de que se cumplen los requisitos del producto o servicio. Esto incluye auditorías internas, medición de la satisfacción del cliente y acciones correctivas y preventivas para mejorar continuamente el SGC.

La ISO 9001 se basa en una serie de principios de gestión de la calidad, incluyendo el enfoque al cliente, el liderazgo, el compromiso del personal, el enfoque basado en procesos, la mejora continua, la toma de decisiones basada en evidencia y la gestión de las relaciones.

2.2.2 ISO 27001:2023 Seguridad de la Información

Esta se enfoca en la protección, confidencialidad y disponibilidad de la información, así como los sistemas de gestión de seguridad de esta.

1. **Evaluación de riesgos**: La organización debe identificar y evaluar los riesgos asociados con la seguridad de la información, determinando cuáles podrían afectar la confidencialidad, integridad y disponibilidad de los datos.
2. **Implementación de controles**: Basado en la evaluación de riesgos, se deben implementar controles adecuados para mitigar los riesgos identificados. Estos controles pueden ser técnicos, organizativos o físicos.
3. **Establecimiento de políticas y procedimientos**: Se deben desarrollar políticas y procedimientos claros para la gestión de la seguridad de la información, asegurando que todos los empleados estén al tanto de sus responsabilidades y sigan las prácticas establecidas.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

4. **Monitoreo y revisión**: La organización debe llevar a cabo un monitoreo continuo y revisiones periódicas del SGSI para asegurar que los controles sean efectivos y que se adapten a los cambios en el entorno de la organización.
5. **Mejora continua**: La norma promueve la mejora continua del SGSI mediante la implementación de acciones correctivas y preventivas basadas en los resultados del monitoreo y las auditorías internas.
6. **Gestión de incidentes**: Se deben establecer procedimientos para gestionar y responder a incidentes de seguridad de la información, minimizando el impacto y recuperando la normalidad lo antes posible.
7. **Capacitación y concienciación**: Es fundamental que todos los empleados reciban formación y estén conscientes de la importancia de la seguridad de la información y de las políticas y procedimientos establecidos.

Estas funciones ayudan a asegurar que la información de una organización esté protegida de manera adecuada y que se cumplan los requisitos legales y reglamentarios.

2.2.3 ISO 22301 Continuidad de Negocios

Los beneficios de la ISO 22301 son mejorar la gestión de los riesgos y de ser posible reducir la probabilidad de interrupciones, evitar pérdidas. Y finalmente mejorar la confianza y la reputación de la institución.

La norma ISO 22301 ayuda a las empresas a:

- Prevenir y anticipar escenarios desfavorables
- Reducir los costes derivados de situaciones adversas
- Mejorar la imagen ante los clientes y otras partes interesadas
- Obtener una ventaja competitiva
- Contribuir a la resiliencia organizacional

Para implementar la norma ISO 22301, las organizaciones deben:

- Identificar los factores de riesgo
- Comprender las necesidades y obligaciones de la organización
- Establecer, aplicar y mantener el sistema de gestión de la continuidad de las actividades
- Medir la capacidad global de la organización para gestionar incidentes

2.2.4 COBIT Marco de la gestión de la tecnología de la información

Nos ayuda a gestionar la tecnología y crear distintos modelos de gestión y control, así como tener una herramienta ágil que aseguran los procesos y recursos de información y tecnología.

1. Alineación de TI con los objetivos empresariales: Asegura que los objetivos de TI se alineen con los objetivos estratégicos de la organización para maximizar el valor y minimizar los riesgos.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

2. Gestión de riesgos: Proporciona un marco para identificar, evaluar y gestionar los riesgos asociados con el uso de la tecnología de la información.

3. Optimización de recursos: Facilita el uso eficiente y eficaz de los recursos de TI, incluyendo personal, infraestructura, aplicaciones y datos.

4. Entrega de valor: Asegura que la organización obtenga el mayor valor posible de sus inversiones en TI, proporcionando beneficios y gestionando los costos y riesgos relacionados.

5. Medición del desempeño: Proporciona herramientas y técnicas para medir y monitorear el desempeño de los servicios y procesos de TI, ayudando a identificar áreas de mejora y garantizar el cumplimiento de los objetivos.

6. Gobernanza y gestión de TI: Establece roles y responsabilidades claras para la gobernanza y gestión de TI, promoviendo la transparencia y la rendición de cuentas.

2.2.5 ITIL Information Technology Infrastructure Library

Es un marco de referencia para ayudar a las organizaciones a mejorar la calidad de los servicios de TI y alienarlos con las necesidades de la institución

El objetivo final de una operación de infraestructura es ser capaz de proveer la disponibilidad de servicios al más alto grado de disponibilidad, acorde al instituto UPTIME, la infraestructura de data center y los servicios dentro del mismo pueden ser calificados de la siguiente manera>

- **Gestión de la Estrategia de Servicios:** Asegura que los servicios de TI se alineen con las necesidades empresariales y las estrategias organizacionales. Incluye la gestión de la cartera de servicios y la gestión financiera de los servicios de TI.

- **Diseño de Servicios:** Planifica y diseña servicios de TI eficaces y eficientes que cumplan con los requisitos empresariales. Se ocupa de la gestión del catálogo de servicios, la gestión de la capacidad, la gestión de la disponibilidad y la continuidad del servicio.

- **Transición de Servicios:** Gestiona la implementación de servicios nuevos o modificados, garantizando que se introduzcan en el entorno operativo de manera controlada. Incluye la gestión del cambio, la gestión de la configuración y la gestión de la liberación y el despliegue.

- **Operación de Servicios:** Gestiona las actividades y procesos necesarios para entregar y gestionar servicios de TI en funcionamiento. Incluye la gestión de incidentes, la gestión de problemas, la gestión de eventos y la gestión de accesos.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

- **Mejora Continua del Servicio:** Identifica y realiza mejoras en los servicios y procesos de TI para aumentar la eficiencia y la efectividad. Se centra en el análisis y revisión de los resultados de desempeño y el desarrollo de planes de mejora.

- **Gestión de la Demanda:** Ayuda a comprender y anticipar las necesidades de los clientes y gestionarlas eficazmente, asegurando que los recursos estén disponibles para satisfacer estas demandas.

- **Gestión de Nivel de Servicio:** Monitorea y gestiona los niveles de servicio acordados con los clientes, garantizando que se cumplan las expectativas y se mantenga una alta calidad del servicio.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

3 Objetivos Operativos Deseados

3.1 Disponibilidad

Los estándares de niveles del Uptime Institute agrupan los centros de datos en cuatro niveles según su disponibilidad:

Nivel I: 99,671 % de disponibilidad o 28,8 horas de inactividad al año

Nivel II: 99,749 % de disponibilidad o 22,7 horas de inactividad al año

Nivel III: 99,982 % de disponibilidad o 1,6 horas de inactividad al año

Nivel IV: 99,995 % de disponibilidad o 25 minutos de inactividad al año

El tiempo de inactividad puede deberse a muchas cosas, incluidas fallas de hardware, desastres naturales, ciberataques, mantenimiento de rutina y errores humanos.

El tiempo de inactividad puede deberse a muchas cosas, incluidas fallas de hardware, desastres naturales, ciberataques, mantenimiento de rutina y errores humanos.

La gestión eficaz de la infraestructura de TI tiene como objetivo lograr estos objetivos clave:

- Maximizar el tiempo de disponibilidad o UPTIME y minimizar las interrupciones
- Asegurarse de que los servicios estén disponibles de manera constante y sean confiables
- Optimizar la utilización de recursos
- Eficientemente asignar capacidad recursos y almacenamiento para satisfacer las necesidades de la institución
- Implementar medidas de seguridad sólidas para proteger datos confidenciales y evitar el acceso no autorizado

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

3.2 Documentación esperada

La gestión de la operación nos requiere que resolvamos en orden cada paso de ejecución de cada tarea. Esto nos obliga a diseñar políticas y procedimientos que cubran las siguientes áreas.

Cada actividad que deseemos realizar para cubrir la operativa requiere lo siguiente:

¿Quién va a realizar la actividad?

Esto debe ser establecido mediante la descripción de cargo y dentro del procedimiento.

¿Qué procedimientos se deben seguir?

Este procedimiento debe indicar el responsable, los pasos a seguir y los plazos.

¿Cómo hacer el seguimiento?

La tarea en proceso debe quedar registrada en algún sistema para su seguimiento

¿Qué registros deben quedar?

Una vez concluido el trabajo, cuáles son los entregables y que registros deben quedar.

¿Cómo se audita?

Cuál es el procedimiento que debe seguir el personal para verificar que el trabajo fue realizado.

¿Qué pasa si no se realizó la acción?

Cada actividad no realizada debe tener un plan de acción para evaluar las alternativas.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

3.3 Áreas de las cuales estamos esperando procedimientos

Una vez que hemos definido que estamos esperando para cada uno de los procedimientos debemos definir de qué áreas requerimos las mismas.

- Descripción de cargos
- Gestión de incidentes
- Gestión de activos de TI
- Gestión de solicitudes de servicio / Tickets
- Gestión del conocimiento
- Gestión de Proyectos
- Gestión de puesta en producción

Adicionalmente deberíamos tener una clara definición entre los servicios de producción, así como operación relacionados a las siguientes áreas del DATACENTER y tecnología en general

Gestión de energía: Procedimientos para garantizar un suministro eléctrico ininterrumpido, incluyendo redundancia de sistemas de alimentación y monitoreo constante.

Gestión de refrigeración: Procedimientos para mantener temperaturas óptimas y asegurar la eficiencia de los sistemas de enfriamiento.

Gestión de la infraestructura física: Procedimientos para el mantenimiento y la seguridad del espacio físico del datacenter, incluyendo la gestión de cables, racks y otros equipos.

Seguridad y acceso: Procedimientos para controlar el acceso al datacenter, incluyendo autenticación, monitoreo de accesos y medidas de seguridad física.

Gestión de red: Procedimientos para asegurar la conectividad y el rendimiento de la red, incluyendo monitoreo de la red y resolución de problemas de conectividad.

Gestión de desastres y recuperación: Procedimientos para planificar y responder a desastres, incluyendo copias de seguridad, replicación de datos y planes de recuperación ante desastres.

Mantenimiento y actualizaciones: Procedimientos para el mantenimiento regular de equipos y la implementación de actualizaciones de software y hardware.

Monitoreo y análisis: Procedimientos para el monitoreo continuo del datacenter y el análisis de datos para identificar y resolver problemas de manera proactiva.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

4 Herramientas utilizadas

Una vez que determinamos cuales son las áreas para cubrir y la información requerida procedemos a la evaluación de las herramientas existentes y como estas son utilizadas para obtener y/o registrar los datos anteriormente citados para que estos puedan ser evaluados en su gestión, así como ser utilizados como referencia y posteriormente sacar los indicadores para cada uno de ellos de así ser solicitado.

4.1 Zabbix (Network Monitor)

Zabbix es una herramienta de monitoreo de código abierto que se utiliza para supervisar la salud y el rendimiento de redes, servidores, componentes de TI, servicios en la nube y máquinas virtuales. Es una solución de monitoreo distribuida que permite a los usuarios recopilar métricas y detectar problemas en tiempo real.

Algunas de las funcionalidades clave de Zabbix incluyen:

Recopilación de Métricas: Zabbix puede recopilar datos de diversas fuentes, como dispositivos de red, servicios en la nube, contenedores, máquinas virtuales, archivos de registro, bases de datos y aplicaciones.

Detección de Problemas: Detecta automáticamente problemas en tiempo real utilizando umbrales inteligentes y predicciones de tendencias.

Visualización de Datos: Proporciona gráficos, mapas de infraestructura y dashboards personalizables para visualizar los datos recopilados.

Notificaciones y Respuesta: Permite configurar alertas personalizadas y notificaciones a través de varios canales, como correo electrónico, SMS y plataformas de comunicación.

Cumplimiento y Seguridad: Ayuda a las organizaciones a cumplir con normativas de seguridad y proporciona capacidades de autenticación segura.

API y Extensibilidad: Ofrece una API para la integración con otros sistemas y herramientas de terceros

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

SOLARWINDS
Pingdom

4.2 Pingdom (Disponibilidad)

Pingdom es una herramienta del paquete de Solarwinds para visualización rápida de la disponibilidad de equipos así como mediciones en tiempo real similares a PRTG, es usada para una rápida respuesta al comportamiento de los servicios más críticos, uptime, network traffic, que nos permiten responder en tiempo real, las otras herramientas poseen lecturas similares, pero con visualización grafica y en tiempo real.

Synthetic Monitoring

Simulate visitor interaction with your website or web app to know if and when critical pages or flows stop working correctly. Synthetic monitoring features:

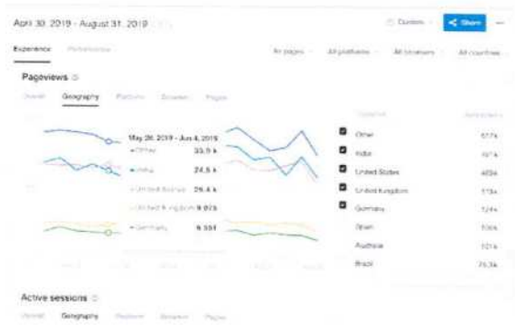
- Uptime monitoring: monitor site availability from over 100+ locations worldwide.
- Page speed analysis: know when and why your website is slow to help you troubleshoot fast and provide the best service to customers.
- Transaction monitoring: test simple or highly complex transactions, such as: new user registrations, user login, search, shopping cart checkout, URL hijacking, and more.

Real User Monitoring

Gain visibility into how actual end users are interacting with and experiencing your website with scalable and easy-to-use Real User Monitoring (RUM). With Pingdom RUM you can:

- Know how your site or web app is performing with real user insights in real time.
- Understand how your visitors experience your site based on browser, device, and geographic location.
- Compare usage metrics over time to see if your website is performing better than last month? Last quarter? Last year?
- Make sure you hit critical KPIs and SLAs by setting your own or using our defaults

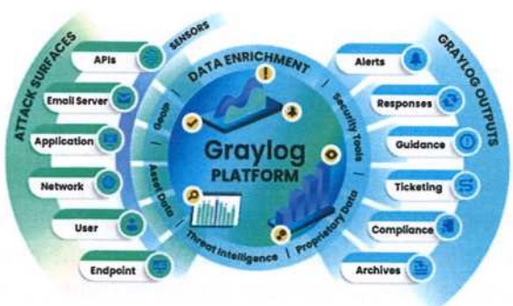
Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030



4.3 Graylog (SIEM)

El componente crítico para operaciones de seguridad efectivas

Las soluciones de gestión de eventos e información de seguridad (SIEM) siguen siendo fundamentales para las operaciones de seguridad modernas. Las organizaciones de todos los tamaños confían en su SIEM para proporcionar la visibilidad integral necesaria para detectar amenazas de forma temprana, responder rápidamente y mantenerse a la vanguardia de los ataques. Sin el SIEM adecuado, los equipos de seguridad pueden tener problemas con la sobrecarga de datos y el logro de sus objetivos de detección, investigación y respuesta ante amenazas (TDIR). Ya sea que esté evaluando su primer SIEM o esté buscando reemplazar uno que ya no le sirve, invertir en Graylog Security es el primer paso para equipar a su equipo de seguridad para el éxito.



Algunas de las funcionalidades clave de Graylog incluyen:

Agregación de Datos: Captura datos de diversas fuentes y los centraliza para su análisis.

Análisis de Datos de Seguridad: Genera informes y dashboards para analizar datos de seguridad.

Correlación y Monitoreo de Eventos de Seguridad: Detecta y monitorea eventos de seguridad para identificar amenazas.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

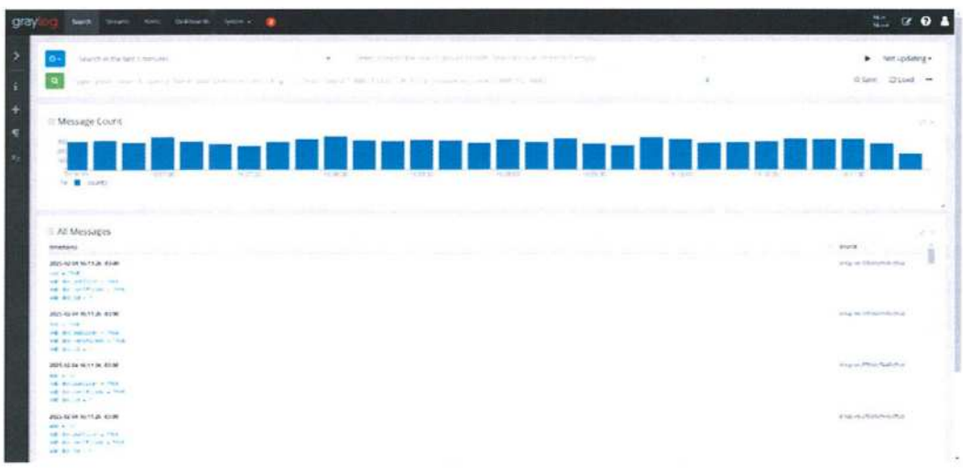
Análisis Forense: Facilita la investigación de incidentes de seguridad.

Detección e Incidencia de Respuesta: Proporciona alertas en tiempo real y capacidades de respuesta a incidentes.

Inteligencia de Amenazas: Utiliza inteligencia de amenazas para mejorar la detección de actividades maliciosas.

Análisis de Comportamiento de Usuario y Entidad (UEBA): Monitorea el comportamiento de usuarios y entidades para detectar actividades sospechosas.

Gestión del Cumplimiento IT: Ayuda a las organizaciones a cumplir con normativas y estándares de seguridad.

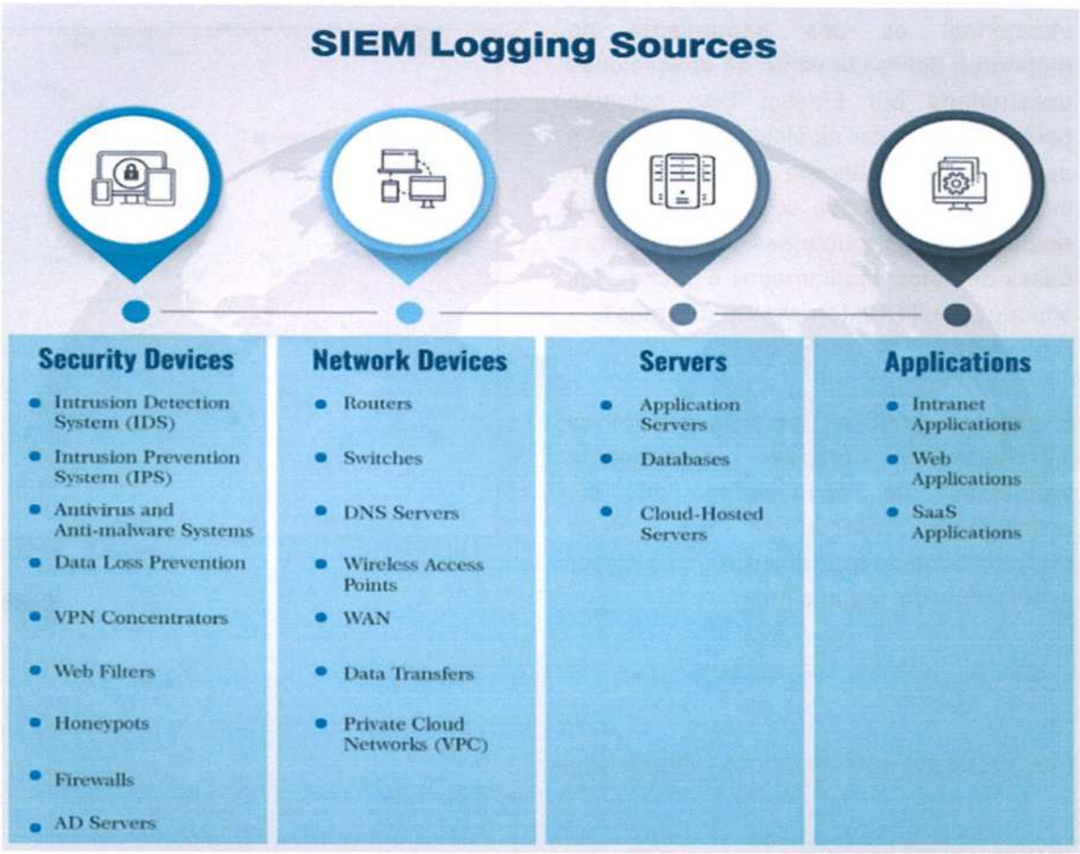


Observación: Graylog es una herramienta adecuada para su uso actual enfocado a infraestructura, pero es importante tener en cuenta que posiblemente se requiera coordinación con otras herramientas utilizadas, principalmente el Wazuh, que posee ambas funcionalidades XDR + SIEM, hoy en día Graylog tiene un enfoque más orientado a infraestructura y fue diseñado por este equipo y su funcionamiento es correcto, a la par que Seguridad Informativa vaya integrando todas las plataformas a un punto de control y monitoreo. El equipo de Infraestructura y Seguridad deberán coordinar cual será la herramienta final que pueda colaborar a ambas áreas y sus necesidades.

No es conveniente segmentar tanto las herramientas de SIEM, ya que posteriormente el análisis de los eventos se vuelve más complejo, ambos en tiempos y cantidad de recursos que conozcan todas las plataformas y estas se deben sincronizar vía o NTP para poder resolver eventos que puedan suceder a futuro.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

¿Que debe centralizarse en un SIEM?



Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

4.4 Elastic APM : (Observabilidad)

Elastic APM (Application Performance Monitoring) es una herramienta de monitoreo del rendimiento de aplicaciones desarrollada por Elastic. Esta solución permite supervisar servicios de software y aplicaciones en tiempo real, recopilando información detallada sobre el tiempo de respuesta de las solicitudes, las consultas a bases de datos, las llamadas a cachés, las solicitudes HTTP externas y mucho más1.

El objetivo principal de Elastic APM es identificar y resolver rápidamente problemas de rendimiento en las aplicaciones, asegurando una mejor disponibilidad de los activos IT y una mayor satisfacción del usuario final.

Figure 1: Magic Quadrant for Observability Platforms

Gartner

Algunas de sus características clave incluyen:

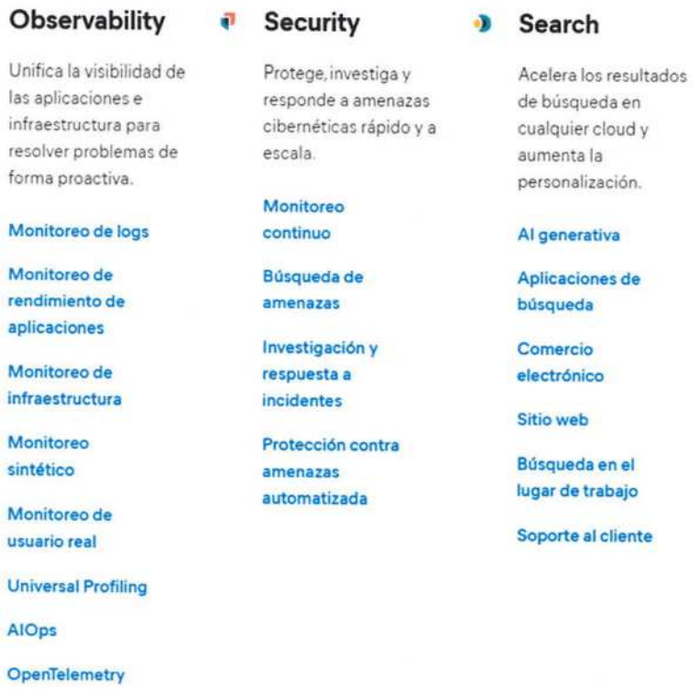
Visibilidad completa: Permite rastrear y analizar el rendimiento de aplicaciones desde la perspectiva del usuario final hasta la infraestructura subyacente.

Detección de problemas: Ayuda a detectar y resolver problemas de rendimiento y errores de manera eficaz.

Rastreo de transacciones: Proporciona información detallada sobre cómo se comporta cada solicitud a medida que navega a través de la aplicación.

Personalización: Los usuarios pueden configurar alertas personalizadas para recibir notificaciones inmediatas sobre eventos críticos.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

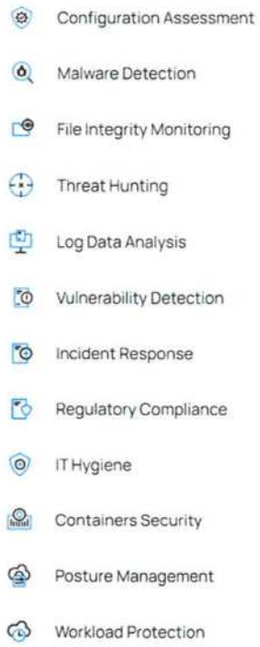


Con referencia a la herramienta podemos considerar que está entre las mejores del mercado mundial, el cuadrante Gartner la sitúa dentro de los lideres como herramientas de observabilidad permite costo eficiencia y mucho código abierto disponible, posteriormente a futuro cuando se requiera integrar con herramientas AI/ML otras herramientas en la actualidad poseen mejor integración, pero a considerable mayor costo.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

4.5 Wazuh (XDR + SIEM)

Wazuh es una plataforma de seguridad de código abierto que ofrece capacidades de Gestión de Información y Eventos de Seguridad (SIEM) y Detección y Respuesta Extendida (XDR). Esta herramienta está siendo utilizada principalmente por el equipo de seguridad informática de la DNCP. Su principal objetivo es ayudar a las organizaciones a proteger sus activos de TI mediante el monitoreo integral de seguridad y la detección de amenazas.



Acorde a datos obtenidos de diversas fuentes Wazuh tiene las siguientes funcionalidades clave que incluyen:

Seguridad en Endpoints: Protege los endpoints contra malware, accesos no autorizados y otras amenazas.

Evaluación de Configuraciones: Monitorea y evalúa las configuraciones de sistemas y aplicaciones para asegurar el cumplimiento de políticas y estándares de seguridad.

Monitoreo de Integridad de Archivos (FIM): Detecta cambios en archivos, permisos, propiedad y atributos para identificar posibles brechas de seguridad.

Detección de Amenazas: Utiliza reglas e inteligencia de amenazas para detectar actividades maliciosas e indicadores de compromiso.

Análisis de Datos de Logs: Recopila y analiza logs de sistemas operativos y aplicaciones para identificar incidentes de seguridad.

Detección de Vulnerabilidades: Identifica vulnerabilidades conocidas en el software y proporciona recomendaciones para su remediación.

Respuesta a Incidentes: Ofrece herramientas y capacidades para responder eficazmente a incidentes de seguridad.

Cumplimiento Normativo: Ayuda a las organizaciones a cumplir con requisitos de normativas como PCI DSS, HIPAA y NIST.

Seguridad en la Nube: Monitorea máquinas virtuales y entornos en la nube, proporcionando seguridad para entornos cloud.

Seguridad en Contenedores: Protege entornos de contenedores mediante la integración con las APIs de Docker y Kubernetes.

Wazuh está diseñado para ser flexible y escalable, lo que lo hace adecuado para diversos casos de uso y entornos. Es una herramienta poderosa para mejorar la postura de ciberseguridad de una organización.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Herramientas similares a Wazuh debemos buscar en dos rubros, end point protection XDR y Security Information and Event Management y si bien esta herramienta no figura en el cuadrante Gartner, es importante tener en cuenta cuales podrían ser sus competidores naturales, así como tener en consideración que al ser una herramienta de uso libre, es apta para el momento y tiempo en el que se encuentra el departamento de seguridad, donde está arrancando sus operaciones y empezando a implementar distintos tipos de herramientas que de otra manera presupuestalmente sería prohibitivo.

Otras alternativas a la par que va progresando el departamento pueden ser encontradas en

https://www.g2.com/products/wazuh-the-open-source-security-platform/competitors/alternatives

Wazuh es considerada una de las líderes en su segmento comparables a Crowdstrike así que no consideramos que sea necesaria otra opción por el momento.

Un punto si importante a tener en cuenta es que Elastic, en su versión Elastic SIEM, una solución ya utilizada por la DNCP contiene funcionalidades de SIEM que se solapan con el Wazuh si es que se desea unificar a futuro la solución y reducir el número de plataformas.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

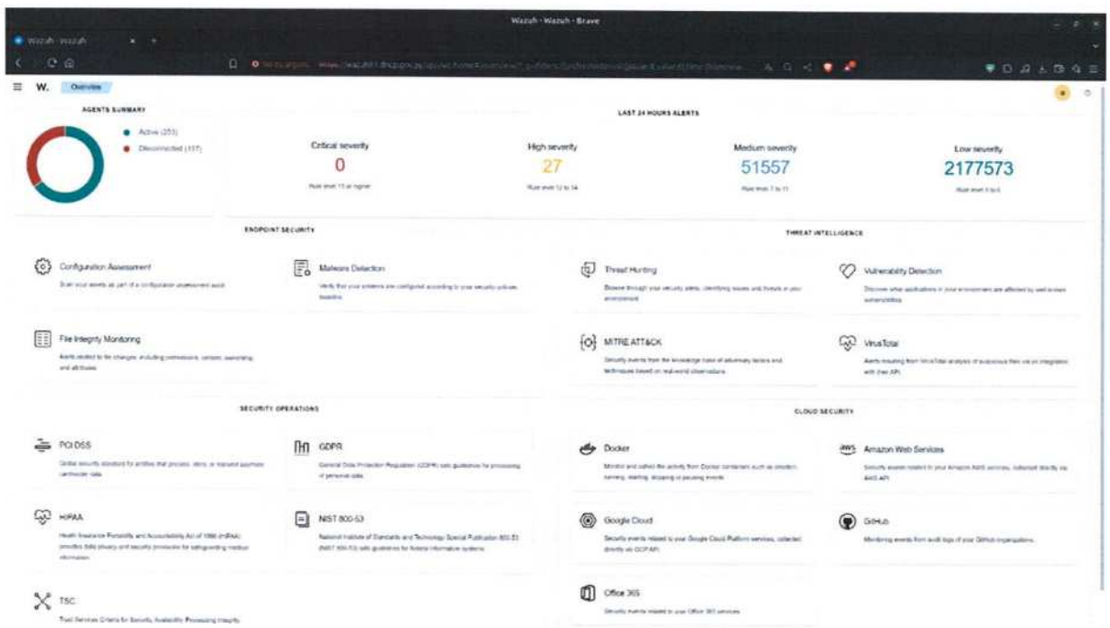
Figure 1: Magic Quadrant for Endpoint Protection Platforms

Gartner

Figure 1: Magic Quadrant for Security Information and Event Management

Gartner

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030



La plataforma Wazuh se encuentra en funcionamiento y es operativa, a la par que se vayan ajustando las mecánicas de solución, estas deberían ir generando tickets de solución de eventos de seguridad que deben ser comunicadas a las áreas afectadas.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

4.6 GLPI (Mesa de Ayuda)

GLPI (Gestionnaire Libre de Parc Informatique) es una herramienta de gestión de servicios de TI de código abierto que ofrece varias características que se ajustan a la norma ITIL para la gestión de eventos, inventario, cambios y proyectos. Provee una herramienta adecuada para que el equipo de soporte pueda gestionar sus tickets.

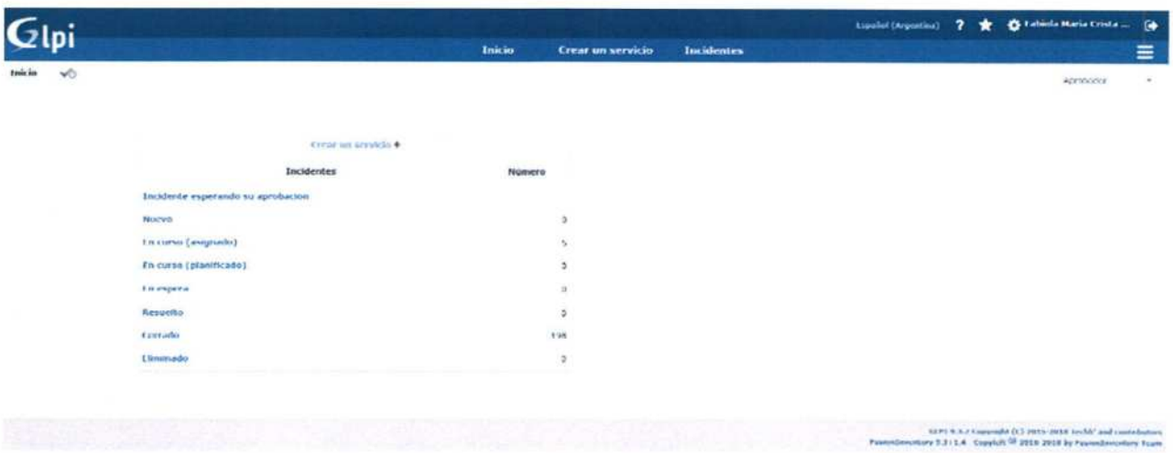
Gestión de inventario: Permite administrar y mantener un inventario completo de hardware, software y centros de datos.

Gestión de Tickets: Facilita la creación, seguimiento y resolución de tickets de soporte técnico.

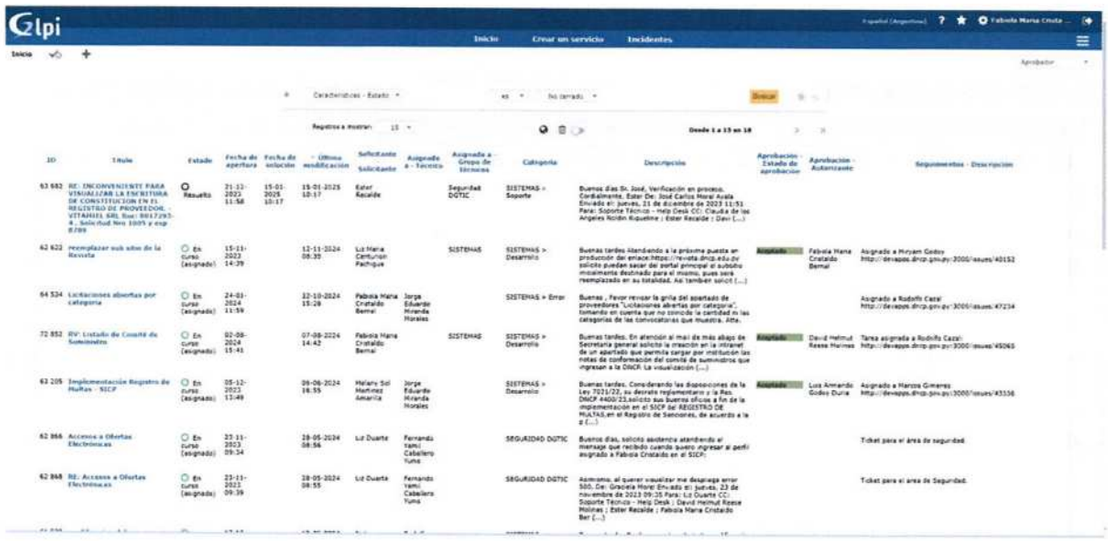
Gestión de problemas y cambios: Ayuda a gestionar y resolver problemas técnicos, así como a implementar cambios en la infraestructura de TI.

Compatibilidad con ITIL: Cumple con los estándares ITIL, lo que garantiza una gestión de servicios de TI eficiente y estructurada.

Gestión de proyectos: Permite gestionar proyectos de TI y asignar recursos de manera eficiente.



Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

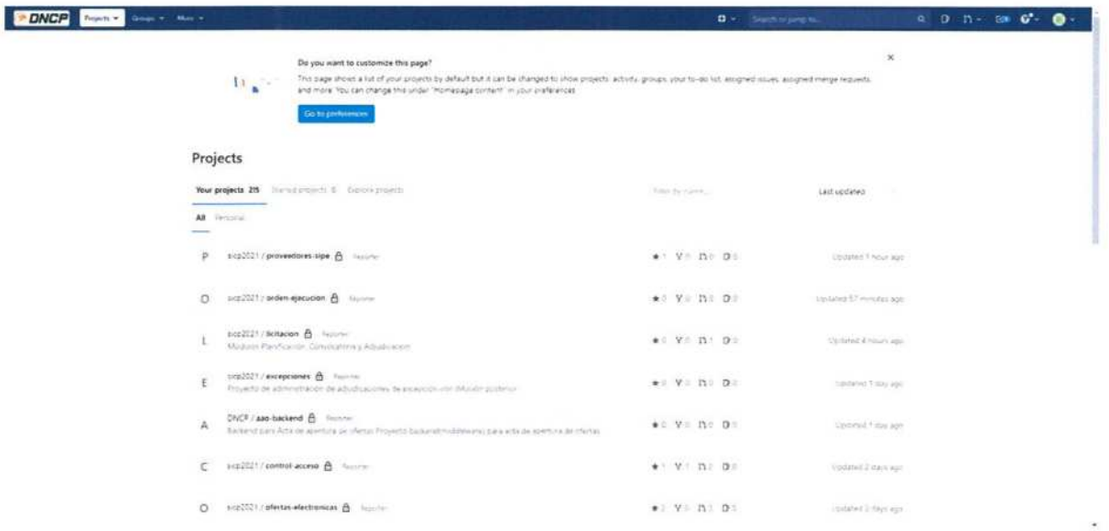


El software en si es adecuado para la operativa y de uso gratuito, los datos cargados permiten tener funcionalidad básica de KNOWLEDBASE, conocido como base de datos de conocimiento que permitiría a futuros técnicos tener un historial de incidentes y la mecánica de solución de estos si así se desea.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

5 GITHUB (Desarrollo)

Si bien el alcance de esta consultoría está enfocado a infraestructura, cabe resaltar que la solución de desarrollo está funcionando sobre la plataforma de GitHub la cual permite controlar el ciclo completo de desarrollo desde su análisis, diseño, desarrollo, test y puesta en producción. Dentro de la plataforma en si se encuentran los manuales operativos que pueden servir de base para la creación de los procedimientos que se ajusten a las etapas anteriormente mencionadas.

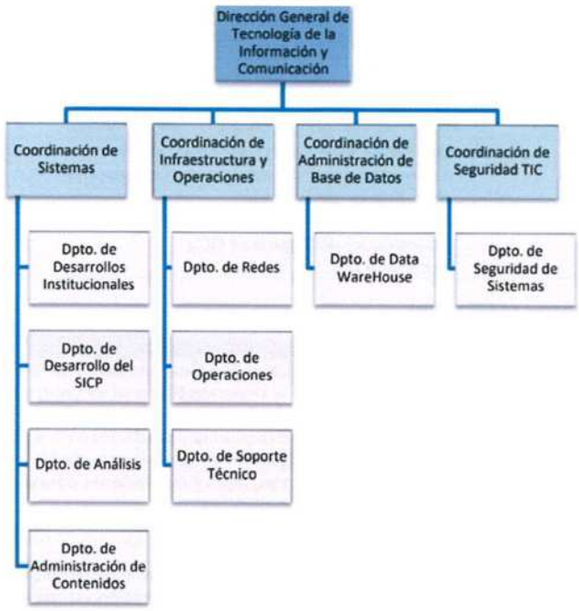


Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

6 Organigrama actual

El equipo humano está organizado de forma tradicional en cuatro áreas principales, esto está acorde a cómo van evolucionando las estructuras operativas de tecnologías en distintas instituciones, vemos que el equipo de tecnología se divide en cuatro grupos principales.

1. Desarrollo
2. Infraestructura
3. Base de Datos
4. Seguridad



Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

7 Descripciones de cargos

7.1 Dirección General de Tecnología de la Información y Comunicación: David Reese

DESCRIPCIÓN DE CARGO
Director General de Tecnología de Información
DC-DGTI-01 Rev.: 09 Vigencia: 28/11/2024 Hoja: 1 / 2

Revisado por: **Coordinadora de Gestión de Sistemas de Desarrollo Institucional**	Aprobado por: **Director General de Tecnología de Información**

1. DATOS GENERALES	
a) ÁREA:	Dirección General de Tecnología de la Información
b) REPORTA A:	Director Nacional de Contrataciones Públicas
c) SUPERVISA A:	– Coordinador de Infraestructura y Operaciones – Coordinador de Sistemas – Coordinador de Administración de Base de Datos – Coordinador de Seguridad TIC´s – Secretaría DTI

2. RESPONSABILIDADES ESPECÍFICAS	
Nº	**Responsabilidades**
1.	Apoyo, asistencia y entrenamiento a usuarios internos y externos según los niveles y calidad requeridos, en el uso de herramientas y sistemas proveídos por la Dirección Nacional de Contrataciones Públicas (DNCP).
2.	Aseguramiento de que las adquisiciones, arrendamientos, licencias, préstamos y contratos o acuerdos en general vinculados al servicio sean de la calidad requerida y se efectúen en tiempo y forma, coordinando con el área administrativa e implementando un Esquema de Adquisiciones de TI.
3.	Verificación del cumplimiento de códigos, normas, leyes y regulaciones para el área tecnológica vigentes en el país, así como las resoluciones de organismos superiores.
4.	Aseguramiento de la innovación tecnológica y evitar la obsolescencia prematura mediante la recomendación de cambios pertinentes.
5.	Establecimiento de un conjunto de responsabilidades y prácticas para dirigir, evaluar y supervisar las Tecnologías de la Información y Comunicación, proveyendo dirección estratégica, garantizando la concreción de los objetivos, estableciendo mecanismos de gestión de riesgos y verificando que los recursos sean utilizados responsablemente, satisfaciendo las demandas actuales y futuras de la organización.
6.	Establecimiento de procesos para garantizar que la adquisición de las TIC sea basada en un análisis apropiado que asegure el correcto dimensionamiento tanto de la capacidad como el desempeño y asegure niveles de servicio comprometidos con el Negocio (SLA).
7.	Gestión de los recursos tecnológicos, humanos y financieros necesarios para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información.
8.	Gestión de los recursos tecnológicos, humanos y financieros necesarios para establecer, implementar, mantener y mejorar los planes de acción en caso de contingencia.
9.	Establecimiento de principios y directrices para la gestión integral de los riesgos, alineado a la estrategia y la operativa de la Dirección Nacional de Contrataciones Públicas.
10.	Establecimiento, monitoreo y revisión del cumplimiento de los niveles de servicios comprometidos con el Negocio (SLA).
11.	Cumplimiento y exigencia de cumplimiento de las leyes, políticas, normas, procedimientos, códigos y regulaciones vigentes para el área a su cargo y para la institución en su conjunto, gestionando oportunamente los recursos necesarios para el efecto y alertando las dificultades que puedan presentarse para el logro de sus fines.
12.	Establecimiento de las políticas y procedimientos aplicables a la gestión de las TIC.
13.	Establecimiento de principios y directrices para la gestión integral de la calidad de los servicios.
14.	Manejo y Administración de los sistemas informáticos especializados que correspondan a su área, pertenecientes a la DNCP u otra institución u organismo oficial del Estado y que contengan información oficial, financiera o patrimonial de carácter confidencial de personas físicas o jurídicas, directamente relacionados con la función misional de la Entidad.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

7.2 Coordinación de Sistemas: Nimia Garcia

DESCRIPCIÓN DE CARGO Coordinador de Sistemas			
DC - DGTI - 02	Rev.: 11	Vigencia:28 /11/2024	Hoja: 1 / 2

Descripción de las modificaciones:
Se ajustan normas de cargos y áreas conforme nuevo Organigrama

Revisado por: **Coordinador/a de Sistemas**	Aprobado por: **Director General de Tecnología de Información**

1. DATOS GENERALES	
a) ÁREA:	Coordinación de Sistemas
b) REPORTA A:	Director General de Tecnología de Información
c) SUPERVISA A:	– Jefe de Departamento de Desarrollos Institucionales – Jefe de Departamento de Desarrollo del SICP. – Jefe de Departamento de Análisis. – Jefe de Departamento de Administración de Contenidos

2. RESPONSABILIDADES ESPECÍFICAS	
Nº	**Responsabilidades**
1.	Cumplimiento de las etapas del ciclo de vida de desarrollo de software en tiempo y forma acordados con los usuarios.
2.	Incorporación de medidas de seguridad en el desarrollo.
3.	Presentación de propuestas de mejoras en las aplicaciones y procesos tanto desde el punto de vista técnico como funcional.
4.	Análisis y diseño de los sistemas o programas usando los mejores criterios técnicos.
5.	Aseguramiento de que los desarrollos de sistemas o programas cumplan con los estándares definidos.
6.	Verificación de que la implementación incluya todos los aspectos necesarios para que el usuario aproveche la aplicación o el sistema lo mejor posible.
7.	Autorización de la puesta en producción de los sistemas o programas en el horario estándar.
8.	Actualización del Cronograma de los proyectos de la DNCP.
9.	Mantenimiento de la documentación de los programas asignados actualizados.
10.	Provisión de documentos e informes en tiempo y forma, de acuerdo a lo requerido por las demás áreas de la DNCP u otras Instituciones del Estado.
11.	Manejo y Administración de los sistemas informáticos especializados que correspondan a su área, pertenecientes a la DNCP u otra institución u organismo oficial del Estado y que contengan información oficial, financiera o patrimonial de carácter confidencial de personas físicas o jurídicas, directamente relacionados con la función misional de la Entidad.
12.	Elaboración de especificaciones técnicas, solicitud y análisis de precios referenciales para la adquisición de bienes y servicios. Administrar los contratos de bienes y servicios del área de su competencia.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

7.2.1 Dpto. de Desarrollos Institucionales: Jonathan Márquez

DESCRIPCIÓN DE CARGO Jefe de Desarrollos Institucionales			
DC-DGTI-22	Rev.: 06	Vigencia: 28/11/2024	Hoja: 1 / 1

Descripción de las modificaciones:
Se ajustan los nombres de cargos y áreas conforme nuevo Organigrama

Revisado por: **Coordinador/a de Sistemas**	Aprobado por: **Director General de Tecnología de la Información**

1. DATOS GENERALES	
a) ÁREA:	Departamento de Desarrollos Institucionales
b) REPORTA A:	Coordinador de Sistemas
c) SUPERVISA A:	No Aplica

2. RESPONSABILIDADES ESPECÍFICAS	
Nº	**Responsabilidades**
1.	Supervisión de los desarrollos realizados sobre los sistemas que afecten al SICP.
2.	Cumplimiento de las etapas del ciclo de vida de desarrollo de software en tiempo y forma acordados con los usuarios.
3.	Incorporación en el desarrollo las medidas de seguridad necesarias para preservar la información.
4.	Logro de que las aplicaciones y sistemas pasen las pruebas.
5.	Proposición de mejoras en las aplicaciones y procesos tanto desde el punto de vista técnico como funcional.
6.	Análisis necesario en el inicio y seguimiento del desarrollo.
7.	Provisión de documentos e informes en tiempo y forma, de acuerdo a lo requerido por las demás áreas de la DNCP u otras Instituciones del Estado, siempre que lo solicitado esté dentro de las áreas de competencia del Departamento.
8.	Manejo y Administración de los sistemas informáticos especializados que correspondan a su área, pertenecientes a la DNCP u otra institución u organismo oficial del Estado y que contengan información oficial, financiera o patrimonial de carácter confidencial de personas físicas o jurídicas, directamente relacionados con la función misional de la Entidad.
9.	Elaboración de especificaciones técnicas, solicitud y análisis de precios referenciales para la adquisición de bienes y servicios. Administrar los contratos de bienes y servicios del área de su competencia.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

7.2.2 Dpto. de Desarrollo del SICP: Jorge Miranda

DESCRIPCIÓN DE CARGO Jefe de Desarrollo del SICP			
DC-DGTI-26	Rev.: 04	Vigencia: 28/11/2024	Hoja: 1 / 1

Descripción de las modificaciones:
Se ajustan los nombres de cargos y áreas conforme nuevo Organigrama

Revisado por: **Coordinadora de Sistemas**	Aprobado por: **Director General de Tecnología de la Información**

1. DATOS GENERALES	
a) ÁREA:	Departamento de Desarrollo del SICP
b) REPORTA A:	Coordinador de Sistemas
c) SUPERVISA A:	- Tester

2. RESPONSABILIDADES ESPECÍFICAS	
Nº	**Responsabilidades**
1.	Cumplimiento de las etapas del ciclo de vida de desarrollo de software en tiempo y forma acordados con los usuarios, lo que incluye en términos generales: • Establecer las especificaciones con el usuario. • Analizar y diseñar el sistema o programa usando los mejores criterios técnicos.
2.	Desarrollo del sistema o programa en tiempo y forma: • Enviar los cambios de los programas al servidor de versiones generando una nueva versión del mismo. • Verificar que la implementación incluya todos los aspectos necesarios para que el usuario aproveche la aplicación o el sistema lo mejor posible.
3.	Incorporación en el desarrollo las medidas de seguridad necesarias para preservar la información.
4.	Logro de que las aplicaciones y sistemas pasen las pruebas.
5.	Proposición de mejoras en las aplicaciones y procesos tanto desde el punto de vista técnico como funcional.
6.	Solicitud de pruebas de funcionamiento al Tester en los casos de desarrollo que aplique.
7.	Realización del análisis necesario en el inicio y seguimiento del desarrollo.
8.	~~Coordinación~~ Gestionar y supervisarán los trabajos de desarrollo del SICP (Sistema de Información de las Contrataciones Públicas).
9.	Manejo y Administración de los sistemas informáticos especializados que correspondan a su área, pertenecientes a la DNCP u otra institución u organismo oficial del Estado y que contengan información oficial, financiera o patrimonial de carácter confidencial de personas físicas o jurídicas, directamente relacionados con la función misional de la Entidad.
10.	Elaboración de especificaciones técnicas, solicitud y análisis de precios referenciales para la adquisición de bienes y servicios. Administrar los contratos de bienes y servicios del área de su competencia.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

7.2.3 Dpto. de Análisis: Ruth Maciel

DESCRIPCIÓN DE CARGO Jefe de Análisis			
DC-DGTI-18	Rev.: 07	Vigencia: 28/11/2024	Hoja: 1 / 1

Descripción de las modificaciones:
Se ajustan nombres de cargo y áreas conforme nuevo Organigrama

Revisado por: **Coordinador de Sistemas**	Aprobado por: **Director General de Tecnología de la Información**

1. DATOS GENERALES		
a)	**ÁREA:**	Departamento de Análisis
b)	**REPORTA A:**	Coordinadora de Sistemas
c)	**SUPERVISA A:**	No Aplica

2. RESPONSABILIDADES ESPECÍFICAS	
Nº	**Responsabilidades**
1.	Seguimiento permanente y mantenimiento del cronograma de los proyectos.
2.	~~Coordinación~~ Gestionar y acompañar~~miento~~ de los trabajos de desarrollo, ya sea con los Departamentos de Desarrollo (Institucionales y del SICP) o con equipos de desarrollo externos (contratos de consultoría para desarrollo)
3.	Actualización de la documentación de los programas asignados.
4.	Establecimiento de las especificaciones con el usuario acerca de las necesidades expresadas por el mismo.
5.	Análisis y diseño del sistema o programa usando los mejores criterios técnicos.
6.	Análisis necesario en el inicio y seguimiento del desarrollo.
7.	Verificación que la implementación incluya todos los aspectos necesarios para que el usuario aproveche la aplicación o el sistema lo mejor posible.
8.	Proposición de mejoras en las aplicaciones y procesos tanto desde el punto de vista técnico como funcional.
9.	Análisis e Investigación de nuevas tecnologías.
10.	Manejo y Administración de los sistemas informáticos especializados que correspondan a su área, pertenecientes a la DNCP u otra institución u organismo oficial del Estado y que contengan información oficial, financiera o patrimonial de carácter confidencial de personas físicas o jurídicas, directamente relacionados con la función misional de la Entidad.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

7.2.4 Dpto. de Administración de Contenidos: Roldolfo Cazal

DESCRIPCIÓN DE CARGO Jefe de Administración de Contenidos				DNCP mecip 2015
DC-DGTI-23	Rev.: 07	Vigencia: 28/11/2024	Hoja: 1 / 1	

Descripción de las modificaciones:
Se ajustan los nombres de cargos y áreas conforme nuevo Organigrama Se modifica el cargo a quien reporta

Revisado por: **Coordinador/a de Sistemas**	Aprobado por: **Director de Tecnología de la Información**

1. DATOS GENERALES		
a)	**ÁREA:**	Departamento de Administración de Contenido
b)	**REPORTA A:**	Coordinador de Sistemas
c)	**SUPERVISA A:**	No Aplica

2. RESPONSABILIDADES ESPECÍFICAS	
Nº	**Responsabilidades**
1.	Investigación, instalación, configuración, administración y mantenimiento de los gestores de contenido (CMS) definidos para ser utilizados por la institución
2.	Aseguramiento de la revisión periódica de las versiones de los gestores de contenidos, asegurando que los mismos estén actualizados a las últimas versiones disponibles.
3.	Apoyo a las diferentes áreas en el manejo de las herramientas.
4.	Apoyo a los usuarios en la preparación de reclamos o pedidos, y atención en el seguimiento de los mismos.
5.	Presentación de propuestas de temas de capacitación según reclamos o usuarios frecuentes.
6.	Provisión de documentos e informes en tiempo y forma, de acuerdo a lo requerido por las demás áreas de la DNCP u otras Instituciones del Estado.
7.	Manejo y Administración de los sistemas informáticos especializados que correspondan a su área, pertenecientes a la DNCP u otra institución u organismo oficial del Estado y que contengan información oficial, financiera o patrimonial de carácter confidencial de personas físicas o jurídicas, directamente relacionados con la función misional de la Entidad.
8.	Velar por el correcto funcionamiento de los gestores de contenido (CMS) utilizados en la institución, así como el aseguramiento de sus copias de seguridad con pruebas periódicas para comprobar el correcto funcionamiento.
9.	Acompañamiento a las diversas áreas de la institución para apoyar en la investigación y toma de decisiones con relación a gestores de contenido (CMS) que puedan ser utilizados por la institución.
10.	Mantener la documentación sobre las configuraciones y cambios realizados en las distintas plataformas de gestión de contenidos (CMS) utilizadas por la institución

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

7.3 Coordinación de Infraestructura y Operaciones: Hugo Araujo

DESCRIPCIÓN DE CARGO Coordinador de Infraestructura y Operaciones				DNCP mecip 2015
DC-DGTI-11	Rev.: 08	Vigencia: 28/11/2024	Hoja: 1 / 2	

Descripción de las modificaciones:
Modificación de los puntos 1.a, 1.b, 1.c, 2.9

Revisado por: **Coordinador de Infraestructura y Operaciones**	Aprobado por: **Director General de Tecnología de Información**

1. DATOS GENERALES	
a) ÁREA:	Coordinación de Infraestructura y Operaciones
b) REPORTA A:	Director General de Tecnología de Información
c) SUPERVISA A:	– Jefe de Redes – Jefe de Operaciones – Jefe de Soporte Técnico –

2. RESPONSABILIDADES ESPECIFICAS	
Nº	**Responsabilidades**
1.	Administración del uso de recursos tales como: red, Internet, acceso a servidores, telefonia IP, video vigilancia, Servidor de correo de la Dirección de Tecnología de la Información.
2.	Mantenimiento de los Sistemas Operativos, los equipos y las instalaciones informáticas en general.
3.	Garantía de la operación adecuada de los sistemas mediante la verificación de la documentación técnica de los mismos y solicitar modificaciones si fueran necesarias.
4.	Control del inventario de los recursos de informática bajo su responsabilidad.
5.	Evaluación del software y/o hardware a ser adquiridos por la institución.
6.	Asistencia a la dirección en la formulación, gestión y evaluación de planes y proyectos en el área de su competencia.
7.	Proposición del uso de herramientas tecnológicas en el ambiente de trabajo de los usuarios.
8.	Coordinación de la atención y resolución de problemas y requerimientos.
9.	Administración de las diferentes redes de la Dirección General de Tecnología de la Información
10.	Control del cumplimiento de los requisitos funcionales de los equipos (humedad, temperatura, protección contra incendios, aislamiento, etc.).
11.	Elaboración de especificaciones técnicas, solicitud y análisis de precios referenciales para la adquisición de bienes y servicios. Administrar los contratos de bienes y servicios del área de su competencia.
12.	Provisión de documentos e informes en tiempo y forma, de acuerdo a lo requerido por las demás áreas de la DNCP u otras Instituciones del Estado.
13.	Supervisión y control del desarrollo de aplicaciones por parte del personal a su cargo, buscando la efectividad en las asignaciones y el cumplimiento de los plazos acordados.
14.	Implementación de todos los controles y procedimientos necesarios y realizar todas las operaciones diarias establecidas en la documentación del SGSI aplicadas al desarrollo de sistemas.
15.	Contribución para el logro de los objetivos de los planes de contingencia tecnológica en el área de su competencia.
16.	Contribución en la gestión integral de los riesgos en el área de su competencia.
17.	Implementación, operación, mantenimiento y mejoramiento continuo de los procesos de gestión de la configuración, gestión de cambios, gestión de entrega y despliegue de sistemas.
18.	Cumplimiento y hacer cumplir las leyes, políticas, normas, procedimientos, códigos y regulaciones vigentes para el área a su cargo y para la institución en su conjunto, gestionando oportunamente los recursos necesarios para el efecto y alertando las dificultades que puedan presentarse para el logro de sus fines.
19.	Establecimiento de políticas y procedimientos aplicables a su gestión.
20.	Gestión de la calidad del software mediante la especificación de requisitos y la evaluación de características de calidad.
21.	Manejo y Administración de los sistemas informáticos especializados que correspondan a su área, pertenecientes a la DNCP u otra institución u organismo oficial del Estado y que contengan información oficial, financiera o patrimonial de carácter confidencial de personas físicas o jurídicas, directamente relacionados con la función misional de la Entidad.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

7.3.1 Dpto. de Redes: Christian Garay

DESCRIPCIÓN DE CARGO Jefe de Redes				DNCP	mecip 2015
DC-DGTI-10	Rev.: 08	Vigencia: 28/11/2024	Hoja: 1 / 1		

Descripción de las modificaciones:
Se modifican los puntos 2.2, 2.5, 2.13 Se elimina los puntos repetidos, 2.11 y 2.12 Se ajustan nombres de cargos y áreas conforme nuevo Organigrama

Revisado por: **Coordinador de Infraestructura y Operaciones**	Aprobado por: **Director General de Tecnología de Información**

1. DATOS GENERALES	
a) ÁREA:	Departamento de Redes
b) REPORTA A:	Coordinador de Infraestructura y Operaciones
c) SUPERVISA A:	- Auxiliar de Redes

2. RESPONSABILIDADES ESPECIFICAS	
Nº	**Responsabilidades**
1.	Administración, creación y mantenimiento de redes de área local.
2.	Administración y mantenimiento de servidores de Telefonía.
3.	Creación de reportes de llamadas.
4.	Administración y mantenimiento de configuraciones de Switches de Acceso, Switches de Core, Routers de Borde, Firewalls de Borde, Firewalls de Core, Balanceadores de Carga, Gateway de telefonía.
5.	Elaboración de especificaciones técnicas de equipos informáticos
6.	Apoyo en la instalación o desinstalación de equipos, aplicaciones o software en general, a fin de asegurar que el usuario tenga las condiciones aptas para emplear el servicio.
7.	Brindar servicios de soporte de conectividad.
8.	Revisión de especificaciones técnicas de pliego de bases y condiciones para adquisición de equipos informáticos y software.
9.	Provisión de documentos e informes en tiempo y forma, de acuerdo a lo requerido por las demás áreas de la DNCP u otras Instituciones del Estado.
10.	Elaboración de reportes de consumo de ancho de banda de internet.
11.	
12.	
13.	Verificación y seguimiento de Backups de Configuraciones de Servidores de Telefonía y Equipos de Redes.
14.	
15.	Manejo y Administración de los sistemas informáticos especializados que correspondan a su área, pertenecientes a la DNCP u otra institución u organismo oficial del Estado y que contengan información oficial, financiera o patrimonial de carácter confidencial de personas físicas o jurídicas, directamente relacionados con la función misional de la Entidad.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

7.3.2 Dpto. de Operaciones: Jorge Javier

DESCRIPCIÓN DE CARGO Jefe de Operaciones				DNCP mecip 2015
DC-DGTI-14	Rev.: 08	Vigencia: 28/11/2024	Hoja: 1 / 1	

Descripción de las modificaciones:
Se actualiza el punto 1.b Se agrega responsabilidades especificas. En los puntos 9 y 13 Punto 2.10, Se actualiza en responsabilidades especificas el nombre de un área,

Revisado por: **Coordinador de Infraestructura y Operaciones**	Aprobado por: **Director General de Tecnología de la Información**

1. DATOS GENERALES		
a)	**ÁREA:**	Departamento de Operaciones
b)	**REPORTA A:**	Coordinador de Infraestructura y Operaciones
c)	**SUPERVISA A:**	- Operador R4

2. RESPONSABILIDADES ESPECÍFICAS	
Nº	**Responsabilidades**
1.	Creación y mantenimiento de cuentas de correo interno y correo externo, usuarios de dominio, usuarios de SICP para funcionarios de la DNCP.
2.	Monitoreo del estado de los servidores, equipos informáticos del Data Center.
3.	Control del acceso al Data Center.
4.	Realización de la atención y el seguimiento de fallas de equipos de Data Center.
5.	Control del cumplimiento de los requisitos funcionales de los equipos (humedad, temperatura, protección contra incendios, aislamiento, etc.).
6.	Administración de los servicios de, Back Up de datos, Video Vigilancia y Acceso de Proximidad, Software Antivirus.
7.	Revisión de especificaciones técnicas de pliego de bases y condiciones para adquisición de equipos informáticos y software.
8.	Ejecución de la puesta a producción de las actualizaciones del SICP y otros sistemas (DEPLOY).
9.	Despliegue de aplicaciones en plataforma de contenedores
10.	Apoyo en tareas de testing de aplicaciones a la Coordinación de Sistemas cuando se requiera.
11.	Actualización de la Bitácora de Eventos.
12.	Provisión de documentos e informes en tiempo y forma, de acuerdo a lo requerido por las demás áreas de la DNCP u otras Instituciones del Estado.
13.	Elaboración de especificaciones técnicas de equipos informáticos.
14.	Manejo y Administración de los sistemas informáticos especializados que correspondan a su área, pertenecientes a la DNCP u otra institución u organismo oficial del Estado y que contengan información oficial, financiera o patrimonial de carácter confidencial de personas físicas o jurídicas, directamente relacionados con la función misional de la Entidad.
15.	Elaboración de especificaciones técnicas, solicitud y análisis de precios referenciales para la adquisición de bienes y servicios. Administrar los contratos de bienes y servicios del área de su competencia.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

7.3.3 Dpto. de Soporte Técnico: Martha Caceres

DESCRIPCIÓN DE CARGO Jefe de Soporte Técnico			
DC - DGTI - 08	Rev.: 15	Vigencia: 28 / 11/2024	Hoja: 1 / 2

Descripción de las modificaciones:

Revisado por: **Coordinador de Infraestructura y Operaciones**	Aprobado por: **Director General de Tecnología de Información**

1. DATOS GENERALES	
a) ÁREA:	Departamento de Soporte Técnico
b) REPORTA A:	Coordinador de Infraestructura y Operaciones
c) SUPERVISA A:	Auxiliar de Soporte Técnico
d) OBSERVACIÓN:	

2. RESPONSABILIDADES ESPECÍFICAS	
Nº	Responsabilidades
1.	Brindar asistencia, a los usuarios internos, respecto a los sistemas y herramientas disponibles
2.	Apoyo a los usuarios internos en la preparación de reclamos o pedidos, y atención en el seguimiento de los mismos.
3.	Apoyo en la instalación o desinstalación de equipos, aplicaciones o software en general asegurando que el usuario tiene las condiciones aptas para emplear el servicio.
4.	Presentación de propuestas de temas de capacitación según reclamos o usuarios frecuentes.
5.	Administración, Verificación y Control del Sistema de Gestión de Reclamos.
6.	Realización del control de Sistemas.
7.	Control del inventario de los recursos de informática bajo su responsabilidad.
8.	Atención al usuario interno en consultas sobre el Portal de Contrataciones.
9.	Provisión de documentos e informes en tiempo y forma, de acuerdo a lo requerido por las demás áreas de la DNCP u otras Instituciones del Estado.
10.	Manejo y Administración de los sistemas informáticos especializados que correspondan a su área, pertenecientes a la DNCP u otra institución u organismo oficial del Estado y que contengan información oficial, financiera o patrimonial de carácter confidencial de personas físicas o jurídicas, directamente relacionados con la función misional de la Entidad.
11.	Elaboración de especificaciones técnicas, solicitud y análisis de precios referenciales para la adquisición de bienes y servicios. Administrar los contratos de bienes y servicios del área de su competencia.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

7.4 Coordinación de Administración de Base de Datos: Diego Ayala

DESCRIPCIÓN DE CARGO Coordinador de Administración de Base de Datos			
DC-DGTI-09	Rev.: 08	Vigencia: 28/11/2024	Hoja: 1 / 1

Descripción de las modificaciones:
Se ajustan nombres de cargos y áreas conforme nuevo Organigrama

Revisado por: **Coordinador de Administración de Base de Datos**	Aprobado por: **Director General de Tecnología de Información**

1. DATOS GENERALES	
a) ÁREA:	Coordinación de Administración de Base de Datos
b) REPORTA A:	Director de Tecnología de Información
c) SUPERVISA A:	– Jefe de Departamento de Data Warehouse – Auxiliar de Administración de Base de Datos

2. RESPONSABILIDADES ESPECÍFICAS	
Nº	**Responsabilidades**
1.	Administración y optimización de todos los sistemas de Base de Datos del SICP.
2.	Administración y optimización de todos los sistemas de Base de Datos de Desarrollo y Capacitación del SICP.
3.	Coordinación de la realización de pruebas de Restore de las distintas Bases de Datos.
4.	Desarrollo de funcionalidades para ejecución de controles y diversas operaciones en el sistema.
5.	Diagnósticos con base a archivos de bitácora.
6.	Garantía de la seguridad de acceso al SGBD.
7.	Desarrollo de diversas soluciones para elaboración de estadísticas sobre los diferentes procesos llevados a cabo en la Dirección.
8.	Investigaciones sobre nuevas herramientas y comandos para el uso de la base de datos PostgreSQL.
9.	Actualización de las documentaciones referentes a la estructura de la base de datos, registros o evidencias de todas las operaciones efectuadas.
10.	Autorización de la puesta en producción de objetos de base de datos en horario estándar
11.	Garantía del funcionamiento del sistema de Datawarehouse.
12.	Provisión de documentos e informes en tiempo y forma, de acuerdo a lo requerido por las demás áreas de la DNCP u otras Instituciones del Estado.
13.	Manejo y Administración de los sistemas informáticos especializados que correspondan a su área, pertenecientes a la DNCP u otra institución u organismo oficial del Estado y que contengan información oficial, financiera o patrimonial de carácter confidencial de personas físicas o jurídicas, directamente relacionados con la función misional de la Entidad.
14.	Elaboración de especificaciones técnicas, solicitud y analisis de precios referenciales para la adquisición de bienes y servicios. Administrar los contratos de bienes y servicios del área de su competencia.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

7.4.1 Dpto. de Data Warehouse: Daniel Delgado

DESCRIPCIÓN DE CARGO Jefe de Datawarehouse				DNCP mecip 2015
DC-DGTI-21	Rev.: 08	Vigencia: 28/11/2024	Hoja: 1 / 2	

Descripción de las modificaciones:
Se agrega la responsabilidad específica número 15 Se ajustan nombres de cargos y áreas conforme nuevo organigrama

Revisado por: **Coordinador de Administración de Base de Datos**	Aprobado por: **Director General de Tecnología de Información**

1. DATOS GENERALES		
a)	**ÁREA:**	Departamento de Datawarehouse
b)	**REPORTA A:**	Coordinador de Administración de Base de Datos
c)	**SUPERVISA A:**	No Aplica

2. RESPONSABILIDADES ESPECÍFICAS	
Nº	**Responsabilidades**
1.	Administración y optimización del Sistema de Información Estadística (S.I.E.)
2.	Actualización mensual de la base de datos del S.I.E.
3.	Actualización de la Documentación del sistema S.I.E.
4.	Elaboración de consultas para la extracción de datos para su envío a las Direcciones o Personas autorizadas solicitantes.
5.	~~Coordinación~~ Gestionar con el Departamento Técnico Estadístico la provisión de información solicitada.
6.	Investigaciones de nuevas herramientas o tecnologías para eventuales implementaciones en Datawarehouse ya sea para el portal público o internamente.
7.	Provisión de documentos, informes o archivos en tiempo y forma previamente registrados y aprobados en la herramienta de seguimiento de solicitudes, de acuerdo a lo requerido por las demás áreas de la DNCP u otras Instituciones del Estado.
8.	Evaluación y creación de estructuras de base de datos para almacenar información relevante según necesidad de la organización.
9.	Manejo y Administración de los sistemas informáticos especializados que correspondan a su área, pertenecientes a la DNCP u otra institución u organismo oficial del Estado y que contengan información oficial, financiera o patrimonial de carácter confidencial de personas físicas o jurídicas, directamente relacionados con la función misional de la Entidad.
10.	Desarrollo de Triggers y funciones para ejecución de controles y diversas operaciones en el sistema.
11.	Pruebas de Restore de los Backups realizados.
12.	Mantener actualizada la estructura de datos del servidor de Capacitación.
13.	Apoyo para optimización de queries.
14.	Monitoreo del funcionamiento del servidor de Base de Datos.
15.	Realizar las tareas relacionadas al área asignadas por el Coordinador de Administración de Base de datos
16.	Elaboración de especificaciones técnicas, solicitud y análisis de precios referenciales para la adquisición de bienes y servicios. Administrar los contratos de bienes y servicios del área de su competencia.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

7.5 Coordinación de Seguridad TIC: Lourdes Angelino

DESCRIPCIÓN DE CARGO Coordinador de Seguridad TIC				DNCP mecip 2015
DC-DGTI-12	Rev.: 11	Vigencia:28/11/2024	Hoja: 1 / 2	

Descripción de las modificaciones:
Se ajustan nombres de cargos y áreas conforme nuevo Organigrama Se modifica responsabilidad especifica número 5

Revisado por: **Coordinadora de Seguridad TIC.**	Aprobado por: **Director General de Tecnología de la Información y Comunicación.**

1. DATOS GENERALES	
a) ÁREA:	Coordinación de Seguridad TIC
b) REPORTA A:	Director General de Tecnología de Información
c) SUPERVISA A:	– Jefe de Dpto. de Seguridad de Sistemas – Técnico en Ciberseguridad
d) OBSERVACIÓN:	

2. RESPONSABILIDADES ESPECÍFICAS	
Nº	**Responsabilidades**
1.	Implementación, gestión y mantenimiento de procesos relacionados a pruebas de seguridad en las aplicaciones dentro del ciclo completo del desarrollo.
2.	Gerenciamiento de los servicios de test de seguridad (Hacking Etico).
3.	Investigación sobre arquitecturas y desarrollo seguro de aplicaciones
4.	Acompañamiento en la implementación de los controles y sub-controles de la norma ISO 27001 referidos a procesos operativos de sistemas e infraestructura tecnológica.
5.	Manejo y Administración de los sistemas informáticos especializados que correspondan a su área, pertenecientes a la DNCP que contengan información oficial, financiera o patrimonial de carácter confidencial de personas físicas o jurídicas, directamente relacionados con la función misional de la Entidad.
6.	Identificar y evaluar los riesgos y las brechas que afectan a los activos de información de la institución y proponer planes y controles para gestionarlos.
7.	Elaborar y velar por la implementación de un plan o estrategia de seguridad de la información en la Institución.
8.	Elaborar, proponer y velar por el cumplimiento de las políticas de seguridad de la información de la Institución.
9.	Proponer los planes de continuidad de negocio y recuperación de desastres en el ámbito de las tecnologías de la información, así como la prueba periódica del mismo.
10.	Supervisar la administración del control de acceso a la información.
11.	Supervisar el cumplimiento normativo de la seguridad de la información, incluido aquellas directrices y lineamientos dispuestas por el Ministerio de Tecnologías de la Información y Comunicación (MITIC) en su carácter de autoridad de prevención, gestión y control en materia de ciberseguridad en resguardo del ecosistema digital nacional.
12.	Velar por la seguridad de todos los activos de Información de la institución en cuanto a su confidencialidad, integridad y disponibilidad.
13.	Proponer políticas de copias de seguridad (backup) y sus respectivos procedimientos.
14.	En el ámbito de la Seguridad TIC: Elaboración de especificaciones técnicas, Administración de contratos, Evaluación de ofertas técnicas.
15.	Elaboración de especificaciones técnicas, solicitud y analisis de precios referenciales para la adquisición de bienes y servicios. Administrar los contratos de bienes y servicios del área de su competencia.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

7.5.1 Dpto. de Seguridad de Sistemas: Victor Ferloni

DESCRIPCIÓN DE CARGO Jefe de Seguridad de Sistemas				DNCP	mecip 2015
DC-DGTI-29	Rev.: 01	Vigencia: 28/11/2024	Hoja: 1 / 1		

Descripción de las modificaciones:
Se modifican nombres de cargos y áreas conforme nuevo organigrama

Revisado por: **Coordinadora de Seguridad TIC.**	Aprobado por: **Director General de Tecnología de la Información**

1. DATOS GENERALES	
a) **ÁREA:**	Departamento de Seguridad de Sistemas
b) **REPORTA A:**	Coordinador de Seguridad TIC
c) **SUPERVISA A:**	No Aplica

2. RESPONSABILIDADES ESPECÍFICAS	
Nº	**Responsabilidades**
1.	Implementación, gestión y mantenimiento de procesos relacionados a pruebas de seguridad en las aplicaciones dentro del ciclo completo del desarrollo.
2.	Gerenciamiento de los servicios de test de seguridad (Hacking Ético).
3.	Investigación sobre arquitecturas y desarrollo seguro de aplicaciones
4.	Acompañamiento en la implementación de los controles y sub-controles de la norma ISO 27001 referidos a procesos operativos de sistemas e infraestructura tecnológica.
5.	Manejo y Administración de los sistemas informáticos especializados que correspondan a su área, pertenecientes a la DNCP que contengan información oficial, financiera o patrimonial de carácter confidencial de personas físicas o jurídicas, directamente relacionados con la función misional de la Entidad.
6.	Supervisar la administración del control de acceso a la información.
7.	Apoyo en la elaboración de especificaciones técnicas, para la adquisición de bienes y servicios para el área de su competencia. Administrar los contratos de bienes y servicios del área de su competencia.
8.	Apoyo en el monitoreo, control y administración de la gestión de identidades de las diferentes aplicaciones de la DNCP.
9.	Apoyo en los mecanismos que permitan monitorear vulnerabilidades en la red y las aplicaciones de la DNCP.
10.	Apoyo en las diferentes tareas relacionadas a capacitación y concienciación llevadas a cabo por la Coordinación de Seguridad TIC
11.	Revisar las solicitudes de verificación de especificaciones técnicas, cuando existan productos o servicios de ciberseguridad
12.	Administración y monitoreo de las herramientas operativas del área.
13.	Elaboración de especificaciones técnicas, solicitud y analisis de precios referenciales para la adquisición de bienes y servicios. Administrar los contratos de bienes y servicios del área de su competencia.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

8 Gestión de incidentes

El equipo de informática tiene como Formularios declarados para dos tipos de eventos, adicionalmente para que estos puedan ser completados correctamente debemos definir los procedimientos asociados para el llenado de dicho incidente, quienes son los responsables y luego finalmente que formularios utilizar, para el correcto llenado de un incidente estos son los parámetros normalmente esperados según la norma ITIL. Estos a su vez algunos son documentados como tareas o no en el GLPI, para que un incidente sea manejado y escalado correctamente, este debe ser detectado por el departamento de operaciones o solicitado a mesa de ayuda y se debe crear un ticket, ser resuelto si es posible por la misma área o escalado a otras, ya sea mesa de ayuda, redes, sistemas, seguridad y otro.

Los datos esperados son:

Identificación y registro del incidente: El primer paso es detectar el incidente y registrar todos los detalles relevantes, como la hora, el lugar y la naturaleza del problema.

Clasificación y análisis del incidente: Una vez registrado, el incidente se clasifica según su gravedad y tipo. Esto ayuda a determinar la prioridad y el equipo responsable de su resolución.

Investigación y diagnóstico: En esta etapa, se investiga la causa del incidente y se realiza un diagnóstico para identificar la solución adecuada.

Resolución del incidente: Se implementa la solución identificada y se verifica que el problema se haya resuelto correctamente.

Cierre del incidente: Una vez resuelto, se cierra el incidente y se documenta todo el proceso para futuras referencias.

Revisión y mejora continua: Finalmente, se revisan los incidentes para identificar posibles mejoras en el proceso y evitar futuros problemas similares

8.1 Procedimiento

Si bien la carga de los eventos es implícita en la plataforma de GLPI se debe elaborar los mismos y que se ajusten a la herramienta, en la actualidad se cuentan se cuentan con dos formas declaradas.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

8.2 FOR-DGTIC-16 Informe de Monitoreo y Análisis de Eventos tipo I

DNCP	Informe de Monitoreo y Análisis de Eventos tipo I				FOR-DTI-16 Rev.:01 Vigencia: 04/11/2020
Fecha:					
Muestra N°:					
Rango de tiempo:					
Parámetros:	Nivel de criticidad Nivel de acción Tipo de firma		Origen Destino Otro		
Observaciones y detalles	1. 2.				
Analisis	1. 2.				
Recomendación	1. 2.				
Datos Adjuntos		Obs.			
Comunicación	Externa	Obs.			
Responsables	Realizado por.		Validado por.		

8.3 FOR-DGTIC-06 Informe de Monitoreo y análisis de Eventos tipo II

DNCP	MONITOREO Y ANALISIS DE EVENTOS TIPO II	FOR-DTI-06 Rev .00 Vigencia: 21/12/22

Fecha: _____ **Informe No:** _____

Muestra No: _____ **Hora:** _____ **Tipo de evento:** _____

Responsable: _____

Observaciones:

a.

Acciones:

1.

Revisando por:

Muestra No: _____ **Hora:** _____ **Tipo de evento:** _____

Responsable: _____

Observaciones:

a.

Acciones:

1.

Revisando por:

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9 Gestión de activos de TI

9.1 Procedimiento

La gestión de activos puede ser registrada en la plataforma GLPI se requiere definir los procedimientos acordes. Hoy en día adicionalmente trabajo con el equipo de Infra para registrar la lista completa de los activos la cual será dejada a cargo de TI, esta lista es la que contiene así mismo un mapeo similar a los que se está usando en los racks, de manera que el equipo de TI pueda tener acceso a ambas herramientas, una grafica y una en planilla.

Esto nos permitirá ir cargando dichos inventarios a la lista de equipos que usemos, sobre esta plataforma se deben ir registrando los mismos.

9.2 FOR-DTI-03 Orden de Retiro de Equipo

DNCP	ORDEN DE RETIRO DE EQUIPO	FOR-DTI-03 Rev.: 01

Institución: DIRECCIÓN NACIONAL DE CONTRATACIONES PÚBLICA	Lugar: ASUNCIÓN	Orden de Retiro N°_____
Empresa:	Fecha:	

Referencia:

ITEM	DESCRIPCIÓN	CANTIDAD	CÓDIGO	N° DE SERIE

Plazo de Entrega:	Lugar de Retiro: Dirección Nacional de Contrataciones Públicas
Obs.:	

RETIRO DE EQUIPO	
ENTREGADO POR	ENCARGADO DE PATRIMONIO
Nombre:	Nombre:
Firma:	Firma:

EMPRESA	Obs.: El campo **EMPRESA** se completar en caso de no contar con documento de retiro.
Nombre:	
Firma:	

DEVOLUCIÓN DE EQUIPO	
RECEPCIONADO POR	Obs.:
Nombre:	
Firma:	
Fecha:	

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9.3 DATACENTER 1

9.3.1 RACK 1

Rack						
Item	Etiqueta	patrimonio	Marca	Modelo	Serial	Tipo
45	Patch panel -01/ rack 01	N/A		24p	N/A	PATCH PANEL
44	ORDENADOR		SIN MARCA		N/A	ORDENADOR
43	Patch panel -02/ rack 01	N/A		24p	N/A	PATCH PANEL
42	LIBRE					LIBRE
41	Dio d.a trayecto a avda fdo de la mora		FURUKAWA	24		DIO
40	Dio d.a trayecto b Teodoro s mongelos		FURUKAWA	24		DIO
39	SIN ETIQUETA		SIN MARCA	12		DIO
38	LIBRE					LIBRE
37	SIN ETIQUETA		SIN MARCA	6 slots		DIO
36	LIBRE					LIBRE
35	E1		Digitel	Metrofiber	(01)07892275400864 6(21)91	MODEM
34	LIBRE					LIBRE
33	Rasp nodo set		SIN MARCA	12 slots		DIO
32	LIBRE					LIBRE
31	INTERNET USUARIO		Fiber Media Conv	TRX/1000-Internet Usuario	HC1807B8334102B	TRANSCEIVER
31	IPTV		Media Converter	TRX100/100-IPTV	-	TRANSCEIVER
31	E1 snmp		Digitel	Modulo snmp e1	(01)07892754811093(21)987	MODEM
30	Copaco		SIN MARCA	12 slots		DIO
29	LIBRE					LIBRE
28	SIN ETIQUETA		FURUKAWA			DIO
27	PATRIMONIO MITIC	112021-52-95-018(mi	CISCO	catalyst9300x 12y		SWITCH
26	odf teisa uffinet		SIN MARCA	12 puertos		DIO
25	ORDENADOR		SIN MARCA		N/A	ORDENADOR
24	LIBRE					LIBRE
23	SW DISTRIBUCION B	23.19.04.01.8551	HUAWEI	S6730-h48x6c	102296316791	SWITCH
22	SW DISTRIBUCION A	23.19.04.01.8553	HUAWEI	S6730-h48x6c	102296316714	SWITCH
21	ORDENADOR		SIN MARCA		N/A	ORDENADOR
20	SIN ETIQUETA		Geist	Gsro		SENSOR
19	SIN ETIQUETA		Geist	Grsex16		SENSOR
18	LIBRE					LIBRE
17	Caja de empalme					CAJA DE EMPALME
16	SIN ETIQUETA		Rle	Ld310		Sensor
15	LIBRE					LIBRE
14	LIBRE					LIBRE
13	SIN ETIQUETA	23.19.04.06.8021	COMET	MS6D	21060077	Monitor
12	Bandeja					BANDEJA
11	LIBRE					LIBRE
10	LIBRE					LIBRE
9	SIN ETIQUETA CONTROL DE AIRES		Vertiv	Rdu-a g2 irm-host 2		SWITCH
8	LIBRE					LIBRE
7	LIBRE					LIBRE
6	LIBRE					LIBRE
5	LIBRE					LIBRE
4	LIBRE					LIBRE
3	LIBRE					LIBRE
2	LIBRE					LIBRE
1	LIBRE					LIBRE

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9.3.2 Rack 2

Rack						
Item	Etiqueta	Codigo	Marca	Modelo	SERIAL	Tipo
45	LIBRE					
44	Patch panel -01/rack -01	N/A	Furukawa	24 p		Patch panel
43	ORDENADOR					
42	Patch panel -01/rack -04	N/A	Furukawa	24 p		Patch panel
41	ORDENADOR					
40	Patch panel -01/rack -05	N/A	Furukawa	24 p		Patch panel
39	ORDENADOR					
38	Patch panel -01/rack -06	N/A	Furukawa	24 p		Patch panel
37	ORDENADOR					
36	Patch panel -01/rack -07	N/A	Furukawa	24 p		Patch panel
35	ORDENADOR					
34	Patch panel -01/rack -08	N/A	Furukawa	24 p		Patch panel
33	ORDENADOR					
32	Patch panel -01/rack -09	N/A	Furukawa	24 p		Patch panel
31	ORDENADOR					
30	Patch panel -01/rack -10	N/A	Furukawa	24 p		Patch panel
29	ORDENADOR					
28	LIBRE					
27	CENTRAL TELEFONICA	23.19.04.02.6591	CISCO	ISR4431	FJC2207D09U	CENTRAL IP
26	CENTRAL TELEFONICA	23.19.04.02.6590	CISCO	ISR4431	FJC2207D09T	CENTRAL IP
25	LIBRE					LIBRE
24	LIBRE					LIBRE
23	LIBRE					LIBRE
22	LIBRE					LIBRE
21	LIBRE					LIBRE
20	FIREWALL BORDE01(JAGU	23.19.04.02.7437	FORTIGATE	501E	FG5H1E5819904125	FIREWALL
19	LIBRE					LIBRE
18	BALANCEADOR 1	23.19.04.02.7784	F5 NETWORKS	big-ip i 2000	F5-HZKG-UXEJ	BALANCEADOR
17	ORDENADOR		SIN MARCA		N/A	ORDENADOR
16	LIBRE					LIBRE
15	LIBRE					LIBRE
14	ROUTER BORDE 1	23.19.04.02.6588	CISCO	ASR1001-x	FSX2141Q309	Router
13	ORDENADOR		SIN MARCA		N/A	ORDENADOR
12	LIBRE					LIBRE
11	LIBRE					LIBRE
10	LIBRE					LIBRE
9	LIBRE					LIBRE
8	LIBRE					LIBRE
7	ORDENADOR		SIN MARCA		N/A	ORDENADOR
6	LIBRE					LIBRE
5	LIBRE					LIBRE
4	LIBRE					LIBRE
3	LIBRE					LIBRE
2	LIBRE					LIBRE
1	LIBRE					LIBRE

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9.3.3 RACK 3

Rack						
Item	Etiqueta	Patrimonio	Marca	Modelo	Serial	Tipo
45	LIBRE					
44	Patch panel -02/rack -01		Furukawa	24 p		Patch panel
43	ORDENADOR					
42	Patch panel -02/rack -04		Furukawa	24 p		Patch panel
41	ORDENADOR					
40	Patch panel -02/rack -05		Furukawa	24 p		Patch panel
39	ORDENADOR					
38	Patch panel -02/rack -06		Furukawa	24 p		Patch panel
37	ORDENADOR					
36	Patch panel -02/rack -07		Furukawa	24 p		Patch panel
35	ORDENADOR					
34	Patch panel -02/rack -08		Furukawa	24 p		Patch panel
33	ORDENADOR					
32	Patch panel -02/rack -09		Furukawa	24 p		Patch panel
31	ORDENADOR					
30	Patch panel -02/rack -10		Furukawa	24 p		Patch panel
29	ORDENADOR					
28						
27	SWITCH CORE DC1-0	23.19.04.01.7829	HUAWEI	S6730-H48X6C	1020B0174667	SWITCH
26	SWITCH CORE DC1-1	23.19.04.01.7831	HUAWEI	S6730-H48X6C	1020B0174734	SWITCH
25	ORDENADOR		SIN MARCA		N/A	ORDENADOR
24	LIBRE					LIBRE
23						
22						
21						
20						
19						
18						
17						
16						
15						
14						
13						
12						
11						
10						
9						
8						
7						
6						
5						
4						
3						
2						
1						

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9.3.4 RACK 4

Rack						
Item	Etiqueta	Patrimonio	Marca	Modelo	Serial	Tipo
Arriba			Emerson	Irm-s02th		Sensor
45	LIBRE					
44	Patch panel -02/rack -01		Furukawa	24 p		Patch panel
43	Ordenador					ordenador
42	Patch panel -02/rack -04		Furukawa	24 p		Patch panel
41	LIBRE					
40	LIBRE					
39	LIBRE					
38	LIBRE					
37	LIBRE					
36	LIBRE					
35	LIBRE					
34	LIBRE					
33	SERVIDOR	23.19.04.06.3774	IBM	XSERIE 235	KPCMB22	SERVIDOR
32						
31						
30						
29						
28	BANDEJA					
27	FIREWALL CORE 1	23.19.04.01.7787	SOPHOS	XG 450	C4307BF3CM2R41A	FIREWALL
26	LIBRE					
25	LIBRE					
24	ORDENADOR					
23	LIBRE					
22	LIBRE					
21	pc					
20	BANDEJA					
19	LIBRE					
18	LIBRE					
17	LIBRE					
16	LIBRE					
15	LIBRE					
14	LIBRE					
13	LIBRE					
12	LIBRE					
11	LIBRE					
10	LIBRE					
9	LIBRE					
8	LIBRE					
7	SIN ETIQUETA	23.19.04.06.3777	HP	HP COMPAQ DX2000MT		PC
6						
5						
4						
3						
2						
1						

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9.3.5 RACK 5

Item	Etiqueta	Patrimonio	Marca	Modelo	Serial	Tipo
42	LIBRE					
41	LIBRE					
40	LIBRE					
39	LIBRE					
38	LIBRE					
37	LIBRE					
36	LIBRE					
35	LIBRE					
34	LIBRE					
33	LIBRE					
32	ORDENADOR					
31	LIBRE					
30	LIBRE					
29	LIBRE					
28	LIBRE					
27	LIBRE					
26	LIBRE					
25	5035	23.19.04.06.5035	IBM	KVM FLAT PANEL IBM	23DH484	KVM
24	LIBRE					
23	LIBRE					
22	FANALYZER	23.19.04.01.7745	DELL	DELL EMC R440	35N5H13	SERVIDOR
21		23.19.04.14.6467	IBM	STORAGE IBM v3700 2072L2C	78A2069	STORAGE
20						
19	NAS01	23.19.04.01.8081	HP STOREEASY 1660	STOREEASY 1660	2M22020109	STORAGE
18						
17	CENTRAL TELEFONICA	23.19.04.02.8540	CISCO	BE 6000 H	WMP2637004P	SERVIDOR
16	RHEVM	23.19.04.01.7743	DellEMC	DELL EMC R440	35N7H13	SERVIDOR
15	WAZUH 1		HP	PROLIANT DL360P GEN10 PLUS	Mxq236105v	SERVIDOR
14		23.19.06.13.8924	LENOVO	THINKYSTEM SR630 V35415X2	J1054T4W	SERVIDOR
13		23.19.06.13.8923	LENOVO	THINKYSTEM SR630 V35415X2	J1054T4V	SERVIDOR
12		23.19.06.13.8925	LENOVO	THINKYSTEM SR630 V35415X2	J1054T4X	SERVIDOR
11		23.19.06.13.8922	LENOVO	THINKYSTEM SR630 V35415X2	J10544DA	SERVIDOR
10	NAS NEW	23.19.06.13.9076	LENOVO	THINKSYSTEM SR655 V3	J10591X0	SERVIDOR
9						
8			DELL	R6625	G66vz44	SERVIDOR
7						
6	Libreria de cintas		IBM	TS4300	78-02bw3	SERVIDOR
5						
4	LIBRE					
3	LIBRE					
2	LIBRE					
1	LIBRE					

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9.3.6 RACK 6

Rack						
Item	Etiqueta	patrimonio	Marca	Modelo	Serial	Tipo
42	LIBRE					
41	LIBRE					
40	LIBRE					
39	LIBRE					
38	LIBRE					
37	LIBRE					
36	LIBRE					
35	LIBRE					
34	LIBRE					
33	LIBRE					
32	Syslogelek		HP	Proliant dl160 gen 9	2M2542009G	SERVIDOR
31						
30	Mono1	23.19.04.14.6470	HP	Proliant DL380 gen 9	USE54811JL	SERVIDOR
29						
28	ADDC01	23.19.04.14.6471	HP	Proliant DL380 gen 9	USE54811JM	SERVIDOR
27						
26	Ovirt de prueba		LENOVO	System x 3650 m5	E2btf71	SERVIDOR
25	SIN ETIQUETA	23.19.04.03.6099	HP	Proliant DL360p gen 8	0vp	SERVIDOR
24	SIN ETIQUETA	23.19.04.03.6098	HP	Proliant DL360p gen 8	0vn	SERVIDOR
23	virtualizacion	8088	DellEMC	Power edge R6525	Fctjnk3	SERVIDOR
22	virtualizacion	8082	DellEMC	Power edge R6525	7ctjnk3	SERVIDOR
21	virtualizacion	8083	DellEMC	Power edge R6525	8ctjnk3	SERVIDOR
20	virtualizacion	8089	DellEMC	Power edge R6525	Gctjnk3	SERVIDOR
19						
18	Virtualizacion	8080	DellEMC	Power edge R7515	89qp2l3	SERVIDOR
17						
16	Virtualizacion	8081	DellEMC	Power edge R7515	99qp2l3	SERVIDOR
15	LIBRE					
14		23.19.04.01.7741	DellEMC	R640	Fsl4613	SERVIDOR
13	SIN ETIQUETA	23.19.04.01.7739	DellEMC	R640	Fsl2613	SERVIDOR
12						
11	Backup exec	23.19.04.03.6929	LENOVO	Sr550	J1009XC5	SERVIDOR
10						
9	FOREMAN	23.19.04.06.4990	DELL	Power edge r710	7QBR7S1	SERVIDOR
8	SIN ETIQUETA		DellEMC	R640	Db9tbm2	SERVIDOR
7	SIN ETIQUETA		DellEMC	R640	Db8zbm2	SERVIDOR
6	SIN ETIQUETA		DellEMC	R640	Db9xbm2	SERVIDOR
5	LIBRE					
4	LIBRE					
3	LIBRE					
2	LIBRE					
1	LIBRE					

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9.3.7 RACK 7

Rack	v storage system gen 3					
Item	Etiqueta	Patrimonio	Marca	Modelo	Serial	Tipo
45						
44						
43						
42						
41						
40						
39						
38						
37						
36						
35						
34						
33						
32						
31						
30	OPENSHIFT 413	23.19.06.13.8920	LENOVO	Sr630 V3 7d73	J10544d8	SERVIDOR
29	OPENSHIFT 413	23.19.06.13.8930	LENOVO	Sr630 V3 7d73	J1054T53	SERVIDOR
28	OPENSHIFT 413	23.19.06.13.8929	LENOVO	Sr630 V3 7d73	J1054T52	SERVIDOR
27	OPENSHIFT 413	23.19.06.13.8931	LENOVO	Sr630 V3 7d73	J1054T51	SERVIDOR
26						
25						
24						
23						
22						
21						
20						
19						
18						
17						
16						
15						
14						
13						
12						
11						
10						
9						
8			Ibm	IBM xiv storage system gen 3		Ups
7						
6						
5			Ibm	IBM xiv storage system gen 3		Ups
4						
3						
2			Ibm	IBM xiv storage system gen 3		Ups
1						

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9.3.8 RACK 8

A						
Item	Etiqueta	Patrimonio	Marca	Modelo	Serial	Tipo
45	LIBRE					
44	LIBRE					
43	LIBRE					
42	LIBRE					
41	LIBRE					
40	LIBRE					
39	LIBRE					
38	LIBRE					
37	LIBRE					
36	LIBRE					
35	LIBRE					
34	LIBRE					
33	LIBRE					
32	LIBRE					
31	LIBRE					
30	LIBRE					
29	LIBRE					
28	LIBRE					
27	LIBRE					
26	LIBRE					
25	LIBRE					
24	LIBRE					
23	LIBRE					
22	LIBRE					
21	LIBRE					
20	LIBRE					
19	LIBRE					
18	LIBRE					
17	LIBRE					
16	LIBRE					
15	LIBRE					
14	LIBRE					
13	LIBRE					
12	LIBRE					
11	LIBRE					
10	LIBRE					
9	LIBRE					
8	LIBRE					
7	LIBRE					
6	LIBRE					
5	LIBRE					
4	LIBRE					
3	LIBRE					
2	LIBRE					
1	LIBRE					

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9.3.9 RACK 9

RACK						
Item	Etiqueta	Patrimonio	Marca	Modelo	Serial	Tipo
42	LIBRE					
41	LIBRE					
40	LIBRE					
39	LIBRE					
38	LIBRE					
37	LIBRE					
36	LIBRE					
35	LIBRE					
34	LIBRE					
33	LIBRE					
32	LIBRE					
31	LIBRE					
30	LIBRE					
29	LIBRE					
28	LIBRE					
27	LIBRE					
26	LIBRE					
25	LIBRE					
24	3760	23.19.04.06.3760	IBM	1723-hc1	23X0585	KVM
23	LIBRE					
22	LIBRE					
21		006.13.20.0660/3759	Hp	Storage works msl4048 tape library	MXA8091C1B	Storage
20						
19						
18						
17	LIBRE					
16	LIBRE					
15	LIBRE					
14	LIBRE					
13	LIBRE					
12	LIBRE					
11	LIBRE					
10	LIBRE					
9						
8			IBM	Storwize v5100	78E05AB	STORAGE
7	LIBRE					
6	LIBRE					
5	LIBRE					
4	LIBRE					
3	LIBRE					
2	LIBRE					
1	LIBRE					

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9.3.10 RACK 10

Rack Item	Etiqueta	Patrimonio	Marca	Modelo	Serial	Tipo
42						
41	1		Ibm	IBM HS-1235T		STORAGE
40						
39	4		Ibm	IBM HS-1235T		STORAGE
38						
37	3		Ibm	IBM HS-1235T		STORAGE
36						
35	6		Ibm	IBM HS-1235T		STORAGE
34						
33	5		Ibm	IBM HS-1235T		STORAGE
32						
31	3		Ibm	IBM HS-1235T		STORAGE
30						
29	2		Ibm	IBM HS-1235T		STORAGE
28	LIBRE					
27	LIBRE					
26	LIBRE					
25	LIBRE					
24	LIBRE					
23	LIBRE					
22	LIBRE					
21	LIBRE					
20	LIBRE					
19	LIBRE					
18	LIBRE					
17	LIBRE					
16	LIBRE					
15	LIBRE					
14	LIBRE					
13	LIBRE					
12	LIBRE					
11	LIBRE					
10	LIBRE					
9	LIBRE					
8	LIBRE					
7	LIBRE					
6	LIBRE					
5	LIBRE					
4	LIBRE					
3	LIBRE					
2	LIBRE					
1	LIBRE					

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9.4 DATACENTER 2

9.4.1 RACK 1

Rack 1 MITIC						
Item	Etiqueta	Patrimonio	Marca	Modelo	Tipo	SERIAL
42						
41			Furukawa	3 slots de 6		Dio
40	ORDENADOR					ORDENADOR
39						
38	Mitic	112021-52-95-002	CISCO	C9300x-12y	Fjc27091ck8	SWITCH
37						
36	Mitic	12001-52-1-2900	JUNIPER	SRX550-645ap	Al4814ak0044	Router
35						
34						
33						
32	Mitic	12001-52-1-2902	JUNIPER	EX4300-48p	Pd3714460026	SWITCH giga
31	Mitic	12001-52-1-2901	JUNIPER	SRX550-645ap	Al4814ak0047	Router
30						
29						
28						
27	Mitic	112021-52-1-2453	Dell	Sonic wall NSA660/ 1R2K7-0A5	Coeae490fbe2	Utm/firewall
26						
25	Mitic	112021-52-1-2455	Dell	Sonic wall NSA660/ 1R2K7-0A5	Coeae4911d7c	Utm/firewall
24						
23	Mitic	12001-22-1-458	CISCO	CATALYST 4506		SWITCH
22					Fox11240ud8	
21					Ipu2aladaa	
20					Ipu2aladaa	
19					Coucadhcaa	
18					Cnuqacaaa	
17					Ipupabnaab	
16					Ipupabnaab	
15						
14						
13						
12						
11						
10						
9						
8						
7						
6						
5						
4						
3						
2						
1						

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9.4.2 RACK 2

Rack 2 CONACYT						
Item	Etiqueta	Patrimonio	Marca	Modelo	Tipo	SERIAL
42						
41						
40						
39						
38						
37						
36						
35	SRV-171	12001-38-03-2436	LENOVO	SR570/7Y03	J1009t0k	SERVIDOR
34	SRV-172		LENOVO	SR570/7Y03	J1009t0h	SERVIDOR
33	SRV-173		LENOVO	SR570/7Y03	J1009w5g	SERVIDOR
32	NAS-176	12001-38-03-2441	QNAT	TS-469U-RP		STORAGE
31						
30	V5000-175		IBM	REWISE V5000/207	781en74	STORAGE
29						
28						
27						
26						
25						
24						
23						
22						
21						
20						
19						
18						
17						
16						
15						
14						
13						
12						
11						
10						
9						
8						
7						
6						
5						
4		12001.38.02.2292	Mousehp			Mouse
3			Hp	Lp1965		Monitor
2		12001.38.02.2293	Hp			Teclado
1						Bandeja

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9.4.3 RACK 3

Rack Item	Etiqueta	Patrimonio	Marca	Modelo
42	LIBRE			
41	LIBRE			
40	LIBRE			
39	LIBRE			
38	LIBRE			
37	LIBRE			
36	LIBRE			
35	LIBRE			
34	LIBRE			
33	LIBRE			
32	LIBRE			
31	OPENSHIFT 413	231.906.138.921	LENOVO	SR630 V3/7D73
30	OPENSHIFT 413	231.906.138.927	LENOVO	SR630 V3/7D73
29	OPENSHIFT 413	231.906.138.928	LENOVO	SR630 V3/7D73
28	OPENSHIFT 413	231.906.138.926	LENOVO	SR630 V3/7D73
27	HOST- VIRTUALIZACION	8087	DELL EMC	R6525 POWEREDGE
26		23.19.04.01.7742	DELL EMC	R640
25	HOST- VIRTUALIZACION	8086	DELL EMC	R6525 POWEREDGE
24	OCP410	23.19.04.01.7740	DELL EMC	R640
23	HOST- VIRTUALIZACION	8085	DELL EMC	R6525 POWEREDGE
22	OCP410		DELL EMC	R640
21	HOST- VIRTUALIZACION	8084	DELL EMC	R6525 POWEREDGE
20			DELL EMC	R640
19	HOST- VIRTUALIZACION	8078	DELL EMC	R7515 POWEREDGE
18			DELL EMC	R6625
17	HOST- VIRTUALIZACION	8079	DELL EMC	R7515 POWEREDGE
16			HP	PROLIANT DL 360 GEN10
15	2x3.84TB/WAZUH 02		DELL EMC	R640
14	HOST- VIRTUALIZACION	23.19.04.03.6580	HP	PROLIANT DL 380 GEN9
13	HP DL380 MON02	23.10.04.14.6468	Huawei	5288v5
12				
11	BACKUP			
10				
9				
8				
7	LIBRE			
6	SERVIDOR para host de virtualizacion	23.10.04.14.6469	Hp	PROLIANT DL 380 GEN9
5				
4	LIBRE			
3	LIBRE			
2	LIBRE			
1				

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9.4.4 RACK 4

Rack					
Item	Etiqueta	Patrimonio	Marca	Modelo	Serial
42	LIBRE				
41	LIBRE				
40	LIBRE				
39	LIBRE				
38	LIBRE				
37	LIBRE				
36	LIBRE				
35	LIBRE				
34	LIBRE				
33	LIBRE				
32	LIBRE				
31	LIBRE				
30	LIBRE				
29	LIBRE				
28	LIBRE				
27	LIBRE				
26	LIBRE				
25	LIBRE				
24	LIBRE				
23	LIBRE				
22	LIBRE				
21	LIBRE				
20	LIBRE				
19	LIBRE				
18	LIBRE				
17	LIBRE				
16	LIBRE				
15	LIBRE				
14	LIBRE				
13	LIBRE				
12	LIBRE				
11	TELEFONIA	23.19.04.01.8541	cisco	BE6H-M5-K9	WMP26370051
10	LIBRE				
9	LIBRE				
8	LIBRE				
7	LIBRE				
6	LIBRE				
5	LIBRE				
4	LIBRE				
3	LIBRE				
2	LIBRE				
1	LIBRE				

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9.4.5 RACK 5

Rack Item	Etiqueta	Patrimonio	Marca	Modelo	Serial	Tipo
42	LIBRE					
41	AG07-F41		Furukawa	3 slots de 6		Dio
40	ORDENADOR					ORDENADOR
39	AG07-F39		Furukawa	3 slots de 6		Dio
38	AG07-F38		Furukawa	3 slots de 6		Dio
37	ORDENADOR					ORDENADOR
36	AG07-F36		FURUKAWA	24p		Patch panel
35	LIBRE					
34	LIBRE					
33	LIBRE					
32	LIBRE					
31	SW-CORE-SITE B	23.19.04.01.7835	Huawei	S6730-h48x6c	1020b0174737	SWITCH
30	LIBRE					
29	SW-CORE-SITE B(stac	23.19.04.01.7830	Huawei	S6730-h48x6c	1020b0174689	SWITCH
28	LIBRE					
27	LIBRE					
26	LIBRE					
25	SIN ETIQUETA	23.19.04.03.5579	CISCO	N5K-C5548UP	Ssi15310hx0	SWITCH
24	LIBRE					
23	LIBRE					
22	FIREWALL BORDE 02		FORTIGATE	501E	Fg5h1e5819904270	FIREWALL
21	LIBRE					
20	LIBRE					
19	LIBRE					
18	BALANCEADOR 02	23.19.04.01.7785	F5	BIG-IP I2600	F5-wmdt-yaxq	Balanceador
17	LIBRE					
16	LIBRE					
15	LIBRE					
14	LIBRE					
13	LIBRE					
12	LIBRE					
11	LIBRE					
10	LIBRE					
9	LIBRE					
8	LIBRE					
7	LIBRE					
6	LIBRE					
5	LIBRE					
4	LIBRE					
3	LIBRE					
2	LIBRE					
1	LIBRE					

9.4.6 RACK 6

Rack 6 MITIC						
Item	Etiqueta	Patrimonio	Marca	Modelo	Serial	Tipo
42						
41						
40						
39						
38						
37						
36						
35						
34						
33						
32						
31						
30						
29						
28						
27						
26						
25						
24						
23						
22						
21						
20			CISCO	NEXUS 1110-S		SWITCH
19	UCSC220-1		CISCO	NEXUS 1110-S		SWITCH
18	UCSC220-1					
17						
16						
15						
14						
13						
12						
11		12001-52-1-1866	Cisco	Ucs 5108		SERVIDOR
10						
9						
8						
7						
6						
5		12001-52-1-1866	Cisco	Ucs 5108		SERVIDOR
4						
3						
2						
1						

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9.4.7 RACK 7

Rack 7 MITIC					
Item	Etiqueta	Patrimonio	Marca	Modelo	Serial
42					
41					
40			HITACHI	SERVICE PROCESOR 2	
39					
38					
37					
36					
35					
34					
33					
32					
31	MITIC Canasta de extension con discos HITACHI	12021-52-1-647	HITACHI	4u	
30					
29					
28					
27	CONTROLLER		HITACHI	VIRTUAL STORAGE PLATFORM G350	
26					
25	DB09-MITIC-CANASTA DE EXTENSION DE DISCOS		HITACHI	HUS 110	
24					
23	DB08-MITIC-CANASTA DE EXTENSION DE DISCOS		HITACHI	HUS 110	
22					
21	DB07-MITIC-CANASTA DE EXTENSION DE DISCOS		HITACHI	HUS 110	
20					
19	DB06-MITIC-CANASTA DE EXTENSION DE DISCOS		HITACHI	HUS 110	
18					
17	DB05-MITIC-CANASTA DE EXTENSION DE DISCOS		HITACHI	HUS 110	
16					
15	DB04-MITIC-CANASTA DE EXTENSION DE DISCOS		HITACHI	HUS 110	
14					
13	DB03-MITIC-CANASTA DE EXTENSION DE DISCOS		HITACHI	HUS 110	
12					
11	DB02-MITIC-CANASTA DE EXTENSION DE DISCOS		HITACHI	HUS 110	
10					
9	DB01-MITIC-CANASTA DE EXTENSION DE DISCOS		HITACHI	HUS 110	
8					
7	DB00-MITIC-CANASTA DE EXTENSION DE DISCOS		HITACHI	HUS 110	
6					
5	Controller		HITACHI	Unified storage VM	
4					
3					
2					
1					

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9.4.8 RACK 8

Rack Item	Etiqueta	Patrimonio	Marca	Modelo	Serial	Tipo
42	LIBRE					
41	LIBRE					
40	LIBRE					
39	LIBRE					
38	LIBRE					
37	LIBRE					
36	LIBRE					
35	LIBRE					
34	LIBRE					
33	LIBRE					
32			LENOVO	System X 3650m5/5462-AC1	E2btf68	SERVIDOR
31		23.19.04.03.6101	HP	PROLIANT DL360P GEN8	Mxq50100vl	SERVIDOR
30						
29	LIBRE	23.19.04.03.6100	HP	PROLIANT DL360P GEN8	Mxq50100vm	SERVIDOR
28						
27	LIBRE					
26	LIBRE					
25	GRABACION CCTV	23.19.04.01.8090	HPE	STORE EASY 1660	2m22020108	STORAGE
24						
23						
22		23.19.04.14.6474	IBM	POWER S824L/8247 42L	213f0fa	STORAGE
21						
20						
19	STORAGE PARA PRODUCCION		IBM	STOREWISE V5100/2078-AF4	78e05ad	STORAGE
18						
17	LIBRE					
16	LIBRE					
15	LIBRE					
14	LIBRE					
13	LIBRE					
12	LIBRE					
11	LIBRE					
10	LIBRE					
9	LIBRE					
8	LIBRE					
7	LIBRE					
6	LIBRE					
5	LIBRE					
4	LIBRE					
3	LIBRE					
2	LIBRE					
1	LIBRE					

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9.4.9 RACK 9

Rack						
Item	Etiqueta	Patrimonio	Marca	Modelo	Serial	Tipo
42	LIBRE					
41	LIBRE					
40	LIBRE					
39	LIBRE					
38	LIBRE					
37	LIBRE					
36	LIBRE					
35	LIBRE					
34	LIBRE					
33	LIBRE					
32	LIBRE					
31	LIBRE					
30	LIBRE					
29	LIBRE					
28	LIBRE					
27	LIBRE					
26		23.19.04.06.5000	IBM	KVM/1723-HC1	1723hc123dh984	KVM
25	LIBRE					
24	LIBRE					
23	LIBRE					
22	LIBRE					
21	LIBRE					
20	LIBRE					
19	LIBRE					
18	ADDC02	23.19.04.01.7744	DELL EMC	R440	35n8h13	SERVIDOR
17	LIBRE					
16	LIBRE					
15	LIBRE					
14	LIBRE					
13	LIBRE					
12	LIBRE					
11	LIBRE					
10	LIBRE					
9	LIBRE					
8	LIBRE					
7	LIBRE					
6	LIBRE					
5	LIBRE					
4	LIBRE					
3	LIBRE					
2	LIBRE					
1	LIBRE					

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9.4.10 RACK 10

Rack Item	Etiqueta	Patrimonio	Marca	Modelo	Serial	Tipo
42	LIBRE					
41	AD07-F41		FURUKAWA	3 de 6 slots		DIO
40	SIN ETIQUETA					ORDENADOR
39	AD07-F39		FURUKAWA	3 de 6 slots		DIO
38	AD07-F38		FURUKAWA	3 de 6 slots		DIO
37	SIN ETIQUETA					ORDENADOR
36	AD07-F36		FURUKAWA	12/24		PATCH PANEL
35	LIBRE					
34	LIBRE					
33	LIBRE					
32	LIBRE					
31	LIBRE					
30	FIREWALL CORE 02	23.19.04.01.7785	SOPHOS	XG 450	C4307B94DX6	FIREWALL
29	LIBRE					
28	LIBRE					
27	LIBRE					
26	LIBRE					
25	LIBRE					
24	N5k2-b	23.19.04.03.5578	CISCO	N5K-C5548UP	Ss/16410lw2	SWITCH
23	LIBRE					
22	LIBRE					
21	LIBRE					
20	LIBRE					
19	LIBRE					
18	LIBRE					
17	LIBRE					
16	LIBRE					
15	LIBRE					
14	LIBRE					
13	LIBRE					
12	LIBRE					
11	LIBRE					
10	LIBRE					
9	ROUTER BORDE 02	23.19.04.02.6589	CISCO	ASR1001X v03	Cmmw400ara	ROUTER
8	LIBRE					
7	LIBRE					
6	LIBRE					
5	LIBRE					
4	LIBRE					
3	LIBRE					
2	LIBRE					
1	LIBRE					

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9.4.11 RACK 11

Rack Item	Etiqueta	Patrimonio	Marca	Modelo	Serial
36	LIBRE				
35	LIBRE				
34	LIBRE				
33	LIBRE				
32	LIBRE				
31	LIBRE				
30	LIBRE				
29	LIBRE				
28	LIBRE				
27	LIBRE				
26	LIBRE				
25	LIBRE				
24	LIBRE				
23	LIBRE				
22	LIBRE				
21	LIBRE				
20	LIBRE				
19	LIBRE				
18	LIBRE				
17	VTL	23.19.04.13.6309	EMC2	STORAGE DATA DOMAIN EMC DD2500	FCNSD152700504 / CKM00154100669
16					
15					
14					
13					
12					
11					
10					
9	LIBRE				
8	LIBRE				
7	LIBRE				
6	LIBRE				
5	LIBRE				
4	LIBRE				
3	LIBRE				
2	LIBRE				
1	LIBRE				

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9.4.12 RACK 12

Rack Item	Etiqueta	Patrimonio	Marca	Modelo	Serial	Tipo
42						
41						
40						
39						
38						
37						
36						
35						
34						
33						
32						
31						
30						
29						
28						
27						
26						
25						
24						
23						SERVIDOR
22	XIV STORAGE SYSTEM GEN3	23.19.04.03.5864	IBM	System X 3250		
21						
20						
19						
18						
17						
16						
15	XIV STORAGE SYSTEM GEN3	12X2TB	IBM	XIV STORAGE SYSTEM GEN3		STORAGE
14						
13	XIV STORAGE SYSTEM GEN3	12X2TB	IBM	XIV STORAGE SYSTEM GEN3		STORAGE
12						
11	XIV STORAGE SYSTEM GEN3	12X2TB	IBM	XIV STORAGE SYSTEM GEN3		STORAGE
10						
9						
8	XIV STORAGE SYSTEM GEN3		Ibm	IBM xiv storage system gen 3		UPS
7						
6						
5	XIV STORAGE SYSTEM GEN3		Ibm	IBM xiv storage system gen 3		UPS
4						
3						
2	XIV STORAGE SYSTEM GEN3		Ibm	IBM xiv storage system gen 3		UPS
1						

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9.4.13 RACK 13

Rack						
Item	Etiqueta	PATRIMONIO	Marca	Modelo	Serial	Tipo
45	LIBRE					
44	LIBRE					
43	LIBRE					
42	infocenter	006.13.10.0666	cisco	CATALYST 3750G-12s-e	FDO1137Z66J	SWITCH
41	LIBRE					
40	LIBRE					
39	LIBRE					
38	LIBRE					
37	LIBRE					
36	LIBRE					
35	E03AP-PB01	23.19.04.02.6652	Cisco	Cisco Meraki MR33	Q2PD-TRSL-A4KS	ACCESS POINT
34	LIBRE					
33	Va a dinapi/32	TEISA	O net	AN-UMG150-AS-20		TRANSCEIVER
31	Dncp complejo santos	TEISA	O net	AN-UMG150-AS-20		TRANSCEIVER
30	SIN ETIQUETA		Dio furukawa	24p		
30	LIBRE					
29	Teisa		Dio	12 slots		
28	LIBRE					
27	LIBRE					
26	LIBRE					
25	TEISA		JUNIPER	SRX300	Cv4717af0712	FIREWALL
25	SIN ETIQUETA	12001-52-1-2463	Sopto	Spm-1T253-N20S		TRANSCEIVER
25	DNCP-MITIC	12001-52-10-00204	MEDIA CONVERTER			TRANSCEIVER
25	SIN ETIQUETA	12001-52-10-00165	PLANET	FT806A20V4	AA30194200807(000)	TRANSCEIVER
24	SIN ETIQUETA		DIO	12 SLOTS		
23	LIBRE					
22	SIN ETIQUETA		Huawei	Smartax MA5626		SWITCH
21	LIBRE					
20	LIBRE					
19	LIBRE					
18	LIBRE					
17	LIBRE					
16	LIBRE					
15	LIBRE					
14	LIBRE					
13	LIBRE					
12	LIBRE					
11	LIBRE					
10	LIBRE					
9	LIBRE					
8	LIBRE					
7	LIBRE					
6	LIBRE					
5	LIBRE					
4	LIBRE					
3	LIBRE					
2	LIBRE					
1	LIBRE					

9.4.14 RACK 14

Rack						
Item	Etiqueta	Patrimonio	Marca	Modelo	Serial	Tipo
42			Furukawa	3 de 6		Dio
41	sin etiqueta		Furukawa			ORDENADOR
40			Furukawa	24p		Patch Panel
39	LIBRE					
38	LIBRE					
37	LIBRE					
36	LIBRE					
35	LIBRE					
34	LIBRE					
33		23.19.04.02.6602	Cisco	Ms120-24p	Q2ex-gyrn-sdkk	SWITCH
32	LIBRE					
31	LIBRE					
30	Tramo avda fdo de la mora		Furukawa	24p		
29	LIBRE					
28	LIBRE					
27	LIBRE					
26	LIBRE					
25	LIBRE					
24	LIBRE					
23	LIBRE					
22	LIBRE					
21	LIBRE					
20	LIBRE					
19	LIBRE					
18	LIBRE					
17	LIBRE					
16	LIBRE					
15	LIBRE					
14	LIBRE					
13	LIBRE					
12	LIBRE					
11	LIBRE					
10	LIBRE					
9	LIBRE					
8	LIBRE					
7	LIBRE					
6	LIBRE					
5	LIBRE					
4	LIBRE					
3	LIBRE					
2	LIBRE					
1	LIBRE					

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

10 Gestión de servicios Externos

10.1 Procedimientos

Estos servicios externos hoy en día se manejan vía solicitudes de servicio, y posteriormente estos son ejecutados, si bien no está documentado es una mecánica establecida mediante las licitaciones para prestación de servicios preventivos y correctivos.

10.2 FOR-DTI-04 Informe de Servicio Externo

DNCP Dirección Nacional de Contrataciones Públicas	**INFORME DE SERVICIO EXTERNO**	FOR-DTI-04 Rev.: 01

Nombre de Proveedor:	Fecha:	Informe N°_____
Tipo de Equipo:	N° de Serie:	

Motivo (problema detectado/tarea solicitada):

Tarea realizada:	
Obs.:	
Entregado por:	Firma:

RECEPCIÓN DEL EQUIPO

Conforme: SI ☐ NO ☐	
Obs.:	
Recibido por:	Firma:

Fecha de Emisión: 02/05/2018

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

11 Gestión de solicitudes de servicio internos / Tickets

11.1 Procedimiento

Los tickets internos son registrados en la actualidad en la plataforma GLPI, se debe generar los procedimientos acordes a la mecánica actualmente utilizada. Vemos que la cantidad de tickets cargados no refleja la cantidad de trabajos realizado por el equipo que ampliamente supera ese número, es importante que el equipo humano registre correctamente dichos tickets para poder dimensionar correctamente la cantidad de trabajo realizado. De no ser así, normalmente se subestima la cantidad de personal que se necesita.

12 Gestión de usuarios, accesos, permisos, ABM

12.1 Procedimiento

Se requiere un procedimiento de ABM que utilice dicha forma, y así mismo que indique que dicha actividad fue ejecutada mediante el sistema de Tickets.

12.2 FOR-DTI-08 R05 - Habilitacion y Deshabilitacion de Accesos

DNCP DIRECCIÓN NACIONAL DE CONTRATACIONES PÚBLICAS	HABILITACION Y DESHABILITACION DE ACCESOS	FOR-DTI-08 Rev.: 05

Solicitante:	(Nombre de Quien Solicita)
Para:	(Nombre del Funcionario por quien se solicita)
Cargo:	(Cargo de Dicho Funcionario)
Area:	(Area de Dicho Funcionario)
Coordinación:	(Coordinación de Dicho Funcionario)
Dirección:	(Dirección de Dicho Funcionario)
Superior Inmediato:	(Nombre del encargado de derivarle llamados, pacs, adjudicaciones, etc..)
Fecha:	(Fecha de la Solicitud)
Funcionario Nuevo:	(Nuevo en la Institución (Si / No))
Ticket N°	(Numero de Ticket de solicitud de Servicio)

N°	ACCESOS DEL USUARIO	HAB. (√)	DESHAB. (√)
1	ACCESO A DNCP AD (Dominio Active Directory)	☐	☐
2	ACCESO A Skype for Business (Chat)	☐	☐
Usuario AD:			
Contraseña AD:			
OBS.: El campo Usuario y Contraseña es completado por el personal técnico de la DTI			

N°	SICP	HAB. (√)	DESHAB. (√)
1	ACCESO AL SICP	☐	☐
2	ACCESO AL SISTEMA DE RRHH	☐	☐
3	ACCESO AL SISTEMA DE DENUNCIAS	☐	☐
4	ACCESO AL SISTEMA DE INVENTARIO	☐	☐
Usuario SICP:			
Contraseña SICP:			
OBS.: El campo Usuario y Contraseña es completado por el personal técnico de la DTI, el sistema de Inventario comparte datos con el del SICP.			
Usuario RRHH:			
Contraseña RRHH:			
OBS.: El campo Usuario y Contraseña es completado por el personal técnico de la DTI			
Usuario DENUNCIAS:			
Contraseña DENUNCIAS:			
OBS.: El campo Usuario y Contraseña es completado por el personal técnico de la DTI			

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

13 Gestión eventos de recuperación

13.1 Procedimiento PG-DGTI-01 R09 Backup y Recuperación de Datos

PROCEDIMIENTO Backup y Recuperación de Datos				DNCP mecip 2015
PG - DGTI - 01	Rev.: 09	Vigencia: 28/11/2024	Hoja: 1 / 4	

MACROPROCESO: Gestión Tecnológica	PROCESO: Mantenimiento de plataforma tecnológica	DUEÑO DEL PROCESO: Jefe de Dpto. Operaciones

Descripción de las modificaciones:
Se actualizan definiciones de abreviaturas y nombres de áreas responsables, en los puntos 1.b, 1.c, 2.1, 2.2, 2, 2.2.3, 2.2.4, 2.2.5, 2.2.6, 2.3.1, 2.3.2, 2.3.3

Revisado por: **Coordinador de Infraestructura y Operaciones**	Aprobado por: **Director General de Tecnología de Información**

1. DETALLES DEL PROCEDIMIENTO		
a) **OBJETO:**	Definir el procedimiento para la realización de backup y recuperación de Datos de la Dirección Nacional de Contrataciones Públicas.	
b) **ALCANCE:**	**Desde:** La configuración del proceso de Backup.	**Hasta:** El cierre del proceso de backup o recuperación en el SIGR.
	Áreas a las que se aplica: Coordinación de Infraestructura y Operaciones de la Dirección Nacional de Contrataciones Públicas.	
c) **DEFINICIONES / ABREVIATURAS:**	**DNCP:** Dirección Nacional de Contrataciones Públicas. **DTI:** Dirección General de Tecnología de la Información y Comunicaciones. **SIGR:** Sistema Informático de Gestión de Reclamos.	

CONSIDERACIONES GENERALES

Criticidad de la Información:
Todos los datos existentes, así como la información generada a partir de ellos, deberán ser considerados como un activo crítico. El origen y función de los mismos, determinaran su grado de criticidad, siendo los de mayor sensitividad aquellos que estén íntimamente relacionados con las estrategias de la DNCP.
Se clasifica la información según su grado de criticidad en tres niveles:

- **Alto:** Informaciones del Sistema de la DNCP y Datos del Directorio.
- **Medio:** Datos de las Jefaturas.
- **Bajo:** Datos del personal Operativo.

En caso de que existan datos específicos de niveles inferiores al Alto, y sean considerados críticos por el Director del Área correspondiente; el mismo podrá solicitar mediante notificación al Director General de Tecnología de la Información, la adición al Nivel consiguiente, justificando debidamente.

2. RESPONSABILIDADES Y PROCEDIMIENTOS **2.1 Secuencia de actividades: Backup de datos.**		
Paso	**Responsable**	**Actividad**
1. Configuración de Backup	Coordinador de Infraestructura y Operaciones / Coordinador de Seguridad TICs / Jefe de Dpto. Operaciones / Operador / Personal Tercerizado	• Configura en el Servidor de Backup, el programa para que se ejecute el proceso de Backup según el detalle establecido en el Anexo 1. **Nota:** Es una tarea no rutinaria, se realiza una sola vez y se modifica según la necesidad.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

PROCEDIMIENTO Backup y Recuperación de Datos				DNCP mecip 2015
PG - DGTI - 01	Rev.: 09	Vigencia: 28/11/2024	Hoja: 1 / 4	

MACROPROCESO: Gestión Tecnológica	PROCESO: Mantenimiento de plataforma tecnológica	DUEÑO DEL PROCESO: Jefe de Dpto. Operaciones

Descripción de las modificaciones:
Se actualizan definiciones de abreviaturas y nombres de áreas responsables, en los puntos 1.b, 1.c, 2.1, 2.2, 2, 2.2.3, 2.2.4, 2.2.5, 2.2.6, 2.3.1, 2.3.2, 2.3.3

Revisado por: **Coordinador de Infraestructura y Operaciones**	Aprobado por: **Director General de Tecnología de Información**

1. DETALLES DEL PROCEDIMIENTO		
a) **OBJETO:**	Definir el procedimiento para la realización de backup y recuperación de Datos de la Dirección Nacional de Contrataciones Públicas.	
b) **ALCANCE:**	**Desde:** La configuración del proceso de Backup.	**Hasta:** El cierre del proceso de backup o recuperación en el SIGR.
	Áreas a las que se aplica: Coordinación de Infraestructura y Operaciones de la Dirección Nacional de Contrataciones Públicas.	
c) **DEFINICIONES / ABREVIATURAS:**	**DNCP:** Dirección Nacional de Contrataciones Públicas. **DTI:** Dirección General de Tecnología de la Información y Comunicaciones. **SIGR:** Sistema Informático de Gestión de Reclamos.	

:ONSIDERACIONES GENERALES

:riticidad de la Información:

'odos los datos existentes, así como la información generada a partir de ellos, deberán ser considerados como un activo :rítico. El origen y función de los mismos, determinaran su grado de criticidad, siendo los de mayor sensitividad aquellos que :stén íntimamente relacionados con las estrategias de la DNCP.

:e clasifica la información según su grado de criticidad en tres niveles:

- **Alto:** Informaciones del Sistema de la DNCP y Datos del Directorio.
- **Medio:** Datos de las Jefaturas.
- **Bajo:** Datos del personal Operativo.

:n caso de que existan datos específicos de niveles inferiores al Alto, y sean considerados críticos por el Director del Área :orrespondiente; el mismo podrá solicitar mediante notificación al Director General de Tecnología de la Información, la ıdición al Nivel consiguiente, justificando debidamente.

2. RESPONSABILIDADES Y PROCEDIMIENTOS **2.1 Secuencia de actividades: Backup de datos.**		
Paso	**Responsable**	**Actividad**
1. Configuración de Backup	Coordinador de Infraestructura y Operaciones / Coordinador de Seguridad TICs / Jefe de Dpto. Operaciones / Operador / Personal Tercerizado	• Configura en el Servidor de Backup, el programa para que se ejecute el proceso de Backup según el detalle establecido en el Anexo 1. **Nota:** Es una tarea no rutinaria, se realiza una sola vez y se modifica según la necesidad.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

2. Verificación del Backup diario del Servidor de Base de Datos	Coordinador de Administración Base de Datos	**Nota:** Este paso sólo es válido para el Servidor de Base de Datos, previo al proceso automático que diariamente realiza el Servidor de Backup, debido a que este activo requiere de la ejecución de un script previo. • Verifica el log de cumplimiento del Script de Backup de la Base de Datos, que se realiza en forma automática.
3. Verificación del Backup diario al sistema de respaldo	Coordinador de Infraestructura y Operaciones / Coordinador de Seguridad TICs / Jefe de Operaciones / Operador	**Nota:** El Servidor de Backup realiza automáticamente Backup de datos de los Servidores de la DNCP al Sistema de Respaldo de la DNCP conforme a lo establecido en el Anexo 1. • Verifica el reporte del Backup efectuado el día anterior emitido por la herramienta de Backup. • Archiva el Reporte en el File Server por Año, Mes y Día.

2.2 Secuencia de actividades: Recuperación de Datos.

Nota: esta secuencia de actividades aplica a recuperación de datos por solicitud, o por muestreo, a fin de verificar la copia de datos. Para el segundo caso, se procede a partir del paso 3 de esta secuencia de actividades.

Paso	Responsable	Actividad
1. Solicitud de Recuperación	Solicitante	• Detecta la pérdida o necesidad de restauración de datos. • Solicita a través del Sistema de Gestión de Reclamos la recuperación de los datos.
2. Recepción de la solicitud	Jefe de Dpto. Soporte Técnico /Auxiliar de Soporte Técnico	• Recibe la solicitud de recuperación de datos. • Deriva por el mismo medio al Departamento de Operaciones / Coordinación de Infraestructura y Operaciones / Coordinación de Seguridad TICs.
3. Ejecución de Prueba de Recuperación de Datos	Jefe de Operaciones / Operador / Coordinador de Administración de Base de Datos / Coordinación de Infraestructura y Operaciones / Coordinación de Seguridad TICs / Partes interesadas	**Nota 1:** Omite este paso ante la existencia de una solicitud de Recuperación y continua en el paso 4. • Selecciona en el Sistema, segun tabla de pruebas de restauración, procede a ejecutarlos. **Nota 2:** El objetivo de este paso es verificar que la copia de datos esté siendo realizada adecuadamente. El Jefe de Dpto. Operaciones / Coordinación de Infraestructura y operaciones / Coordinación de Seguridad TICsdebe realizarlo según tabla de pruebas de restauración, solo en caso de que no se presenten solicitudes de Recuperación en este periodo de Tiempo. • Al finalizar el proceso, completa el Formulario Registro de Recuperación de Datos (FOR-DTI-02). • Si detecta fallas en el proceso de recuperación, registra los problemas en el Formulario Registro de Recuperación de Datos (FOR-DTI-02), sugiriendo ideas y aportando soluciones.
4. Recuperación de Datos por Solicitud	Jefe de Dpto. Operaciones / Operador / Coordinador de Administración de Base de Datos / Coordinación de Infraestructura y Operaciones /	• Realiza la recuperación del dato, al lugar de origen o según la ubicación acordada entre las partes. • Verifica con el Solicitante la calidad del dato recuperado (que se encuentre completo y fiel al dato original). • Al finalizar exitosamente el proceso, completa el Formulario Registro de Recuperación de Datos (FOR-DTI-02) y el solicitante manifiesta su conformidad mediante el Sistema de Gestión de Reclamos.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

	Coordinación de Seguridad TICs	• Si detecta fallas en el proceso de recuperación, registra los problemas en el Formulario Registro de Recuperación de Datos (FOR-DTI-02), sugiriendo ideas y aportando soluciones.
5. Solución del problema	Coordinador de Infraestructura y Operaciones / Jefe de Dpto. Operaciones / Operador	**Nota:** Aplicable únicamente si se detectaron fallas en el proceso. • Verifica el Formulario Registro de Recuperación de Datos (FOR-DTI-02) y define acciones al respecto.
6. Finalización de Proceso	Coordinacion de Infraestructura y Operaciones / Coordinacion de Seguridad TICs Jefe de Dpto. Operaciones / Operador	• Da por finalizada la tarea en el Sistema de Gestión de Reclamos.

2.3 Secuencia de actividades: Recuperación en caso de desastres.

Paso	Responsable	Actividad
1. Detección de desastre	Coordinador de Infraestructura y Operaciones/ Director General de Tecnología de la Información y Comunicaciones	• Se informa del caso y comunica a él/los afectado(s).
2. Dimensión del desastre	Jefe de Operaciones / Coordinador de Infraestructura y Operaciones	• Analizan la situación, las acciones que correspondan e identifican las copias de backup a ser recuperadas.
3. Recuperación de backup	Coordinacion de Infraestructura y Operaciones / Jefe de Operaciones / Operador	• Procede a recuperar la copia del backup. Va al paso 4 de la secuencia 2.2.

ANEXO 1: DETALLE DEL BACKUP.

Tipo de Backup	Frecuencia mínima
Base de Datos.	Diaria
Datos del Usuario (Directorio, Jefatura, Operativo) en ambiente de producción según su grado de criticidad.	Diaria
Sistemas relacionados al Sistema de Información de Contrataciones Públicas (SICP): Mesa de Entrada Digital (MED), Denuncias, Sistema de Proveedores del Estado (SIPE), Subasta a la Baja Electrónica, etc.	Fecha de Puesta en Producción y al fin del día de cada modificación
Parametrizaciones de Seguridad.	Diaria

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

3. REGISTRO APLICABLE						
Nombre del registro	**Código**	**Identificación**	**Área archivo**	**Forma de archivo**	**Tiempo de retención**	**Obs.**
Informe de la Herramienta de Backup	N/A	Por Día	Servidor de la Dirección de Tecnología de la Información	Por Día	3 años	En archivo informático
Registro de Recuperación de Datos	FOR-DTI-02	Por Mes	Servidor de la Dirección de Tecnología de la Información	Por Mes	3 años	En archivo informático

13.2 FOR-DTI-02 RV 03 Registro de Recuperación de Datos

DNCP	REGISTRO DE RECUPERACION DE DATOS										FOR-DTI-02 Rev.: 03 Vigencia: 08/11/2021 Hoja 1
Fecha	Activo	Categoria Activo	Descripción	Alcance	Tipo de Validación:	Se recuperó correctamente (SI/NO)	Problemas Encontrados	Solución caso Problema Encontrado SI/NO Comentarios (Opcional)	Responsables		OBS.
									Restaurado por	Validado por	

14 Gestión de Seguridad

14.1 Procedimientos

A la fecha se llevan todos los registros de los accesos al departamento de TI de personas terceras a la institución, es recomendado que esta mecánica sea documentada, la forma asociada a la misma y de ser posible registrar en una plataforma online.

Así mismo la mecánica de acceso al DC también tiene un comportamiento similar, pero requiere procedimientos escritos y digitalización.

14.2 FOR-DGTIC-12 Planilla de Control de Acceso a la DTI

DNCP DIRECCIÓN NACIONAL DE CONTRATACIONES PÚBLICAS	PLANILLA DE CONTROL DE ACCESO A LA DTI							FOR-DTI-12 Rev.: 00	
REGISTRO DE INGRESO			Fecha: ____/____/____				Folio N°		
	DATOS DEL INGRESANTE						Autorización del Funcionario de la DTI		
								Ambiente Tecnológico Restringido	
N°	Hora de Entrada	Nombre y Apellido	Empresa	Area	Motivo de Visita	Firma	Firma y Aclaración	Data Center/NOC/ S. UPS	C.I. del Visitante

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

15 Procedimientos adicionales que requieren definirse

Si bien la DNCP está llevando adelante muchas áreas operativas con personal propio y tercerizado entrenado para el efecto, los mismos realizan las tareas operativas acordes a protocolos definidos y acordados internamente, pero sobre los cuales se deben plasmar los procedimientos acordados en documentos que quedará para el persona y posterior verificación de la realización de estos.

Estos son los puntos adicionales que deberán definirse:

15.1 Gestión de energía

Actualmente dependiente de la dirección de mantenimiento y se cuenta con contrato, se deben tener registros de mantenimiento preventivo, correctivo, así como algún método de reposición de combustible designado, tarjeta flota, tanques de reserva y/u otros.

Como ejemplo damos un indicativo de como sería un procedimiento completo para el grupo de electrógenos, en este caso si bien estamos enfocado a la infraestructura tecnológica, finalmente este procedimiento debe ir para la dirección de mantenimiento y el control de estas acciones, específicamente para el generador del datacenter debe recaer en el equipo de operaciones de infraestructura.

Acorde a la ISO 9001, una descripción de manejo de generadores debería contener lo siguiente:

1. Objetivo: Definir el procedimiento para el control y mantenimiento de los generadores, asegurando su funcionamiento eficiente y seguro.
2. Alcance: Este procedimiento aplica a todos los generadores utilizados en la organización.
3. Responsabilidades:

• **Responsable de Mantenimiento:** Realizar el mantenimiento preventivo y correctivo.
• **Supervisor de Operaciones:** Monitorear el rendimiento del generador y coordinar las inspecciones.
• **Operadores de Generador:** Operar el generador de acuerdo con las instrucciones y reportar cualquier anomalía.

4. Procedimientos:
4.1 Inspección Inicial:

• Verificar el estado general del generador antes de su uso.
• Revisar niveles de aceite y combustible.
• Inspeccionar conexiones eléctricas y mecánicas.

4.2 Operación del Generador:

• Iniciar el generador siguiendo el manual del fabricante.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

- Monitorear constantemente los indicadores de funcionamiento (voltaje, corriente, temperatura, etc.).
- Registrar todos los parámetros de funcionamiento en un registro diario.

4.3 Mantenimiento Preventivo:

- Seguir un calendario de mantenimiento basado en horas de operación y recomendaciones del fabricante.
- Realizar cambios de aceite y filtros según las especificaciones del fabricante.
- Inspeccionar y limpiar componentes críticos como radiadores y sistemas de escape.

4.4 Mantenimiento Correctivo:

- Identificar y diagnosticar fallas o problemas en el generador.
- Realizar reparaciones necesarias o coordinar con un proveedor especializado.
- Documentar todas las acciones correctivas realizadas y actualizar el historial de mantenimiento del generador.

5. Documentación:

- Mantener registros detallados de todas las inspecciones, mantenimientos y reparaciones.
- Archivar los registros en un sistema de gestión de la calidad accesible para el personal autorizado.

6. Indicadores de Desempeño:

- Tasa de fallos del generador.
- Tiempo medio entre fallos (MTBF).
- Tiempo de inactividad del generador.
- Cumplimiento del calendario de mantenimiento.

7. Revisión del Procedimiento:

- Revisar y actualizar el procedimiento anualmente o cuando haya cambios significativos en el equipo o en los requisitos normativos.

- **Ejemplo de Registro de Mantenimiento**

Fecha	Actividad Realizada	Responsable	Observaciones
01/02/2025	Cambio de aceite y filtros	Juan Pérez	Todo en orden
15/02/2025	Inspección de conexiones	María González	Se detectaron conexiones sueltas, ajustadas

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

15.2 Gestión de refrigeración

Se cuenta con contrato de mantenimiento, se deben definir los procedimientos a realizarse, y posteriormente registrar los eventos preventivos y correctivos.

15.3 Gestión de la infraestructura física

Mantener el cableado ordenado y etiquetado requiere mantenimiento periódico, hoy no se cuenta con personal asignado para eventos de interrupción de servicio, mudanzas ni tampoco nuevos puestos

15.4 Gestión de red

A la fecha se cuenta con contratos de garantía y soporte de equipos, no se cuentan con procedimientos específicos para el área de redes, pero se siguen la mecánica del área de desarrollo, donde los cortes de servicio se ejecutan de forma inmediata, en la primera ventana de uso bajo de plataforma o a la medianoche.

15.5 Mantenimiento y actualizaciones

Las actualizaciones son llevadas por el área de operaciones en general pero no se cuentan con procedimientos para el mantenimiento regular de equipos y la implementación de actualizaciones de software y hardware.

16 Gestión del conocimiento

En conversaciones con el equipo este proceso está siendo evaluado para ir generando una base de datos de conocimientos de eventos y sus respectivas soluciones, estas pueden ser cargadas en la plataforma de eventos, usar el SharePoint, o crear una plataforma aparte. Como punto de partida inicial lo ideal sería utilizar el sistema de eventos. GLPI

Esta plataforma va más allá de infraestructura, pero es una herramienta fundamental para toda la organización.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Enfoque: Mejorar procesos, eliminar desperdicios y aumentar la eficiencia.

Ideal Para: Proyectos industriales y manufactura, aunque adaptable a otros contextos.

7. Six Sigma

Descripción: Metodología centrada en la mejora de procesos y reducción de defectos.

Enfoque: Uso de datos y análisis estadístico para mejorar la calidad.

Ideal Para: Proyectos donde la calidad y precisión son críticas.

8. Waterfall

Descripción: Metodología secuencial donde cada fase del proyecto debe completarse antes de pasar a la siguiente.

Enfoque: Enfoque lineal y estructurado con fases claramente definidas.

Ideal Para: Proyectos con requisitos bien definidos y poco susceptibles a cambios.

17.1 Algunas de las herramientas candidatas son:

Trello: Utiliza tableros, listas y tarjetas para organizar tareas y proyectos de manera visual y colaborativa.

Asana: Ideal para gestionar equipos multitarea, permite crear tareas, asignar responsabilidades y seguir el progreso del proyecto1.

Monday.com: Ofrece herramientas integrales de organización para usuarios individuales o equipos, con múltiples formas de visualizar proyectos.

Jira Software: Popular entre equipos de desarrollo, especialmente aquellos que utilizan metodologías ágiles.

Smartsheet: Combina las características de una hoja de cálculo con las de una plataforma de gestión de proyectos, ideal para proyectos que requieren planificación detallada.

Microsoft Project: Una herramienta robusta para la planificación y gestión de proyectos, con capacidades avanzadas de programación y seguimiento.

Podio Proyectos: Facilita la colaboración y la gestión de proyectos con una interfaz intuitiva y funcionalidades integradas.

Redbooth: Ofrece herramientas para la gestión de proyectos y la colaboración en equipo, con vistas Kanban y Gantt.

Evernote Teams: Permite a los equipos organizar notas, tareas y proyectos en un solo lugar.

Aqua Project & Services: Una solución avanzada para la automatización de empresas, con funcionalidades como planificación de hitos, control presupuestario y análisis en tiempo real.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

- **KPI:** Número de incidentes de seguridad por mes/trimestre.

7. Eficiencia del Equipo de Soporte:

- **Definición:** Evaluación del rendimiento del equipo de soporte en términos de resolución de problemas y satisfacción del usuario.
- **Objetivo:** Mejorar la eficiencia y la capacidad de respuesta del equipo de soporte.
- **KPI:** Tiempo medio de resolución de tickets, tasa de satisfacción del usuario.

8. Capacidad de la Infraestructura:

- **Definición:** Monitoreo de la capacidad disponible y proyectada de la infraestructura.
- **Objetivo:** Asegurar que la infraestructura pueda soportar la demanda actual y futura.
- **KPI:** Porcentaje de capacidad utilizada, tasa de crecimiento de la demanda.

9. Costos Operativos:

- **Definición:** Medición de los costos asociados a la operación y mantenimiento de la infraestructura.
- **Objetivo:** Controlar y optimizar los costos operativos.
- **KPI:** Costos operativos totales, costo por unidad de servicio.

10. Tasa de Cumplimiento de Proyectos:

- **Definición:** Evaluación de la capacidad del departamento para completar proyectos dentro del plazo y presupuesto.
- **Objetivo:** Mejorar la gestión de proyectos y la entrega de resultados.
- **KPI:** Porcentaje de proyectos completados a tiempo y dentro del presupuesto.

Estas métricas te proporcionarán una visión integral del rendimiento y la eficacia del departamento de infraestructura de TI. ¿Te gustaría profundizar en alguna métrica en particular o necesitas alguna adicional?

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

DGIPED: Dirección General de Innovación Productiva y Economía Digital
DHCP: Dynamic Host Configuration Protocol (Protocolo de Configuración Dinámica de Host)
DIMM: Dual In-Line Memory Module (Módulo de Memoria de Línea Doble)
DINAPI Dirección Nacional de Propiedad Intelectual
DNP: Departamento Nacional de Planeación de Colombia
DNS: Domain Name System (Sistema de Nombres de Dominio)
DR: Disaster Recovery (Recuperación ante Desastres)
DRAM: Dynamic Random-Access Memory (Memoria de Acceso Aleatorio Dinámica)
DSL: Digital Subscriber Line (Línea de Suscriptor Digital)
DWDM: Dense Wavelength Division Multiplexing (Multiplexación por División en Longitudes de Onda Densas)
EAI: Enterprise Application Integration (Integración de Aplicaciones Empresariales)
EAP: Extensible Authentication Protocol (Protocolo de Autenticación Extensible)
EBD Emprendimiento de Base Digital
ECC: Error-Correcting Code (Código de Corrección de Errores)
ECI Entidad consumidora de la información
EDR: Endpoint Detection and Response (Detección y Respuesta de Puntos de Extremo)
EIGRP: Enhanced Interior Gateway Routing Protocol (Protocolo de Enrutamiento de Puerta de Enlace Interior Mejorad
ENCONEC: Estrategia Nacional de Conectividad
EOL: End of Life (Fin de Vida Útil)
EPI: Entidad productora de la información
ERP: Enterprise Resource Planning (Planificación de Recursos Empresariales)
ESXi: Elastic Sky X Integrated (Versión de VMware de su Hipervisor)
FCoE: Fibre Channel over Ethernet (Canal de Fibra sobre Ethernet)
FEEI Fondo para la Excelencia de la Educación y la Investigación
FO: Fibra Óptica
FONTED: Fondo Nacional de Tecnologías en la Educación
FONTIC: Fondo Nacional de Tecnologías de la Información
FTP: File Transfer Protocol (Protocolo de Transferencia de Archivos)
Gbps: Gigabits Per Second (Gigabits Por Segundo)
GDL: Gestor de Documentos en Línea
GPU: Graphics Processing Unit (Unidad de Procesamiento Gráfico)
HBA: Host Bus Adapter (Adaptador de Bus de Host)
HIS: Sistema de Información en Salud
HTTP: HyperText Transfer Protocol (Protocolo de Transferencia de Hipertexto)
HTTPS: HyperText Transfer Protocol Secure (Protocolo Seguro de Transferencia de Hipertexto)
HVAC: Heating, Ventilation, and Air Conditioning (Calefacción, Ventilación y Aire Acondicionado)
I+D+i: Investigación, Innovación y Desarrollo
IA: Inteligencia Artificial
IaaS: Infrastructure as a Service (Infraestructura como Servicio)
IAEE: Instituto de Altos Estudios Estratégicos
ICMP: Internet Control Message Protocol (Protocolo de Mensajes de Control de Internet)
ICT: Information and Communication Technology (Tecnología de la Información y Comunicación)
IDS: Intrusion Detection System (Sistema de Detección de Intrusos)
IDU: Impuesto a los Dividendos y a las Utilidades

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

NVMe: Non-Volatile Memory Express (Interfaz de Memoria No Volátil)
OAuth: Open Authorization (Autorización Abierta)
ODS: Objetivos de Desarrollo Sostenible
ONG: Organización No Gubernamental
OPEX: Operating Expense
OPEX: Operational Expenditure (Gasto Operativo)
OS: Operating System (Sistema Operativo)
OSI: Open Systems Interconnection (Interconexión de Sistemas Abiertos)
OTP: One-Time Password (Contraseña de Un Solo Uso)
PaaS: Platform as a Service (Plataforma como Servicio)
PBX: Private Branch Exchange (Central Telefónica Privada)
PCI: Peripheral Component Interconnect (Interconexión de Componentes Periféricos)
PCI-DSS: Payment Card Industry Data Security Standard (Estándar de Seguridad de Datos de la Industria de Tarjetas d
PDU: Power Distribution Unit (Unidad de Distribución de Energía)
PDU: Protocol Data Unit (Unidad de Datos de Protocolo)
PIB: Producto Interno Bruto
PNC: Plan Nacional de Ciberseguridad
PND: Plan Nacional de Desarrollo
PNT: Plan Nacional de Telecomunicaciones
PNTE: Plan Nacional de Transformación Educativa 2030
PNTIC: Plan Nacional de Tecnologías de la Información y la Comunicación
PROINNOVA: Programa de Innovación en Empresas Paraguayas
QA: Quality Assurance
QoS: Quality of Service (Calidad de Servicio)
RAID: Redundant Array of Independent Disks (Matriz Redundante de Discos Independientes)
RDP: Remote Desktop Protocol (Protocolo de Escritorio Remoto)
RFID: Radio-Frequency Identification (Identificación por Radiofrecuencia)
RIPC: Red Integrada de Infraestructura Pública de Conectividad
RMM: Remote Monitoring and Management (Monitoreo y Gestión Remotos)
RMSP Red Metropolitana del Sector Público
ROE Reglamento Operativo Específico
ROM: Read-Only Memory (Memoria de Solo Lectura)
RPM: Revolutions Per Minute (Revoluciones Por Minuto)
RTC: Real-Time Clock (Reloj en Tiempo Real)
RTO: Recovery Time Objective (Objetivo de Tiempo de Recuperación)
RUE Registro Único del Estudiante
SaaS: Software as a Service (Software como Servicio)
SAN: Storage Area Network (Red de Área de Almacenamiento)
SAS: Serial Attached SCSI (SCSI Conectado en Serie)
SATA: Serial Advanced Technology Attachment (Interfaz de Tecnología Avanzada en Serie)
SDN: Software-Defined Networking (Redes Definidas por Software)
SENAC: Secretaría Nacional Anticorrupción
SENATIC: Secretaría Nacional de Tecnologías de la Información y Comunicación
SET: Subsecretaría de Estado de Tributación

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Contrato Nro 21/2024

Proyecto de Mejoramiento de las Finanzas Públicas para el Desarrollo Sostenible del Paraguay

Contrato de Préstamo N° 4671/OC-PR

"Definición del Plan de Infraestructura Tecnológica"

OBP N° P230707.

Recomendación de procedimientos

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

1 Contenido

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

2 Objetivos de las recomendaciones de procedimientos.

Una vez que hemos evaluado los procedimientos vigentes de la institución, así como los realizados por el personal, así como los adicionales requeridos para poder llevar la operación de una manera eficiente acorde a las necesidades de la institución se procede a realizar una presentación de una lista de procedimientos recomendados que posteriormente deban ser evaluados por el equipo actual y posteriormente aprobados por la institución.

Toda función misional de la institución que requiere conocimiento especifico y crítico tenemos que asegurarnos que sea realizado por el personal propio, y que adicionalmente estos tengan personas de respaldo para que la institución pueda proyectarse en el tiempo y sus recursos tener un balance trabajo/vida que les permita capacitarse, tomarse permisos, vacaciones y estar respaldados por sus compañeros.

Para el efecto debemos diseñar procedimientos para el equipo humano propio y para el externo, y las actividades y registro de dichos procedimientos deberán ser guardadas en una plataforma compartida por las distintas áreas de la institución.

Para lo cual nos centraremos en el GLPI como plataforma globalizadora de los procesos el cual ya está siendo utilizado para las tareas de mesa de ayuda, pero puede expandirse ampliamente a toda la gestión del equipo de infraestructura, e ir creando una base de conocimiento a ser utilizado por los distintos grupos de trabajo.

Si bien la tipografía actualmente utilizada por la institución para sus procedimientos actuales varía entre "Arial ,11pt" y "Calibri, 11", sugerimos que esto sea estandarizado como institución, está fuera del alcance de este documento.

El formato base que estaremos utilizando es standard utilizado por la DNCP, con el siguiente encabezado de página:

3 Formato de los procedimientos

3.1 Encabezado

PROCEDIMIENTO Backup y Recuperación de Datos				DNCP DIRECCIÓN NACIONAL DE CONTRATACIONES PÚBLICAS / mecip 2015
PG - DGTI - 01	Rev.: 09	Vigencia: 28/11/2024	Hoja: 4 / 48	

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

MACROPROCESO: Gestión Tecnológica	PROCESO: Mantenimiento de plataforma tecnológica	DUEÑO DEL PROCESO: Jefe de Dpto. Operaciones

A este encabezado recomendamos agregar los datos referentes a la elaboración de dicho documento:

Descripción de las modificaciones:
Se modifica dueño del proceso por Jefe de Dpto. de Operaciones. Se modifica el paso uno, en la nota 2 de las secuencias de actividades 2.1 y 2.2, Tramitación de Alta de Usuarios Internos y Tramitación de Modificación de Usuarios Internos respectivamente, aclarando que por cada alta o modificación debera emitirse un formulario FOR-DTI-08. Se actualiza abreviaciones y nombres de área responsable.

Revisado por: Coordinador de Infraestructura y Operaciones	Aprobado por: Director General de Tecnología de Información

3.2 Detalle

Una vez definido el encabezado estándar procederemos a definir el cuerpo estándar el cual debe explicar la finalidad de este, los alcances en tareas y quienes son los responsables de las tareas, estos pueden ser personal interno como externo, también pueden darse equipos propios o de terceros relacionados con un servicio subcontratado por la entidad.

Detalles del procedimiento:

Objetivo: El objetivo del procedimiento en sí.

Alcance: A que se aplica y quienes son los responsables

Definiciones/Abreviaturas: En caso de que se requiera aclarar las mismas

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Ejemplo:

1. DETALLES DEL PROCEDIMIENTO		
OBJETO:	Definir el procedimiento a utilizar para las altas, modificaciones, bajas y otorgamiento de acceso lógico y físico de los usuarios internos de la Dirección Nacional de Contrataciones.	
ALCANCE:	**Desde:** La solicitud de alta, baja o modificaciones.	**Hasta:** El registro de la finalización del proceso.
	Áreas a las que se aplica: Coordinación de Infraestructura y Operaciones de la Dirección General de Tecnología de la Información.	
DEFINICIONES / ABREVIATURAS:	**DNCP:** Dirección Nacional de Contrataciones Públicas. **DGTI:** Dirección General de Tecnología de la Información. **SICP:** Sistema de Información de Contrataciones Públicas. **AD:** Directorio Activo. **RRHH:** Recursos Humanos **GLPI:** Sistema Informático de Gestión de Reclamos	

3.3 Procedimentos

Responsabilidades y procedimientos: Los cuales deben contener los pasos, los responsables y las actividades de cada uno de los mismos, desde el inicio y/o solicitud hasta el fin del trabajo, así como las tareas de registro se deben realizar para documentar la acción, debe hacer referencia a los formularios aplicables en cada procedimiento y/u otras plataformas donde deben realizarse o registrarse las actividades.

2. RESPONSABILIDADES Y PROCEDIMIENTOS 2.1 Secuencia de actividades: Tramitación de Alta de Usuarios Internos.		
Paso	**Responsable**	**Actividad**
Solicitud de Alta de Usuario	Solicitante	Completa el Formulario Habilitación y Deshabilitación de Accesos (FOR-DTI-08), y lo remite a través del Sistema Informático de Gestión de Reclamos.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

		Nota 1: En cualquiera de los pasos el FOR-DTI-08 puede ser creado o modificado por personal técnico de la Dirección de Tecnología de la Información o por el solicitante. **Nota 2:** Por cada pedido realizado se emitirá un Formulario FOR-DGTIC-08 conteniendo los cambios solicitados en dicho pedido.

3.4 Registros

Y por último debemos indicar cuales son los registros aplicables, ya sean en formulario impreso o digital.

3. REGISTRO APLICABLE						
Nombre del registro	Código	Identificación	Área archivo	Forma de archivo	Tiempo de retención	Obs.
Habilitación y Deshabilitación de Accesos	FOR-DTI-08	Por fecha	Servidor de la Dirección de Tecnología de la Información	En medio informático	3 años	En archivo informático
Solicitud de Alta / Modificación / Baja de Usuarios Internos	N/A	Por fecha	Servidor de la Dirección de Tecnología de la Información	En medio informático	3 años	En archivo informático

4 Trabajo preparatorio

4.1 Selección de herramienta

Para el efecto de documentar y registrar todos los datos de la gestión debemos seleccionar y utilizar una herramienta que nos permita documentar las ubicaciones, el inventario, las acciones y los formularios. Esto es fundamental para la gestión de la tecnología a largo plazo ya que la utilización de papeles obliga a tener un archivo extenso de los registros así como luego es imposible gestionar y sacar métricas y/o estadísticas de todo lo realizado.

He ahí que conjunto al equipo vemos la necesidad de actualizar el sistema de GLPI a la última versión, así como empezar a utilizar las funcionalidades más avanzadas de la herramienta.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Adicionalmente, todos y cada uno de los procedimientos, así como sus documentaciones nos obligan a registrar los datos en algún tipo de sistema preferiblemente digital esto siguiendo la norma ISO 9001.

Estos son los motivos por los cuales queremos hacer uso de la herramienta GLPI por que nos brida las siguientes funcionalidades:

GLPI es un software de código abierto que ayuda a gestionar los activos informáticos de una organización. Entre sus funciones se encuentran:

- Administrar inventarios de equipos de red, periféricos, software y computadores
- Seguimiento de incidencias
- Servicio de asistencia
- Optimizar los procesos de gestión de servicios informáticos
- Crear un banco de datos de recursos técnicos
- Gestionar y hacer un historial de acciones de mantenimiento
- Declarar incidentes o solicitudes

GLPI está escrito en PHP y se distribuye bajo la Licencia Pública General GNU. Esto significa que cualquier persona puede ejecutar, modificar o desarrollar el código.

GLPI es una herramienta integral para gestionar los recursos informáticos de una organización, incluyendo:

- Equipos
- Servidores
- Periféricos
- Licencias de software
- Topología de red
- Recursos compartidos

Todo procedimiento requiere documentar conceptos básicos asociados a los siguientes puntos, y que posteriormente nos sirvan de información para generar una base de conocimientos y métricas de eficiencia.

¿Cuál es el origen del requerimiento?

¿Dónde debe realizarse?

¿Qué equipos están involucrados?

¿Qué personas están involucradas?

¿Cuándo empezó, cuando terminó?

Estos datos son los que finalmente formaran parte de las gestiones de asistencia que conforman los tickets, casos, incidentes, problemas, planificación y finalmente estadísticas.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

En este documento nos enfocaremos en tres tipos de asistencia:

- Tickets/Casos
- Problemas
- Cambios.

4.2 Identificación de las ubicaciones

4.2.1 Ubicaciones

Ubicaciones Físicas: Puedes definir ubicaciones específicas como oficinas, salas de servidores, almacenes o cualquier espacio físico donde se encuentren los activos.

Inicio / Configuración / Menús desplegables / Ubicaciones

Un ejemplo sería:

DNCP, Dirección EE.UU. 961 c/ Tte. Fariña

Ubicaciones Geográficas: Con el uso de plugins como el de geolocalización, puedes asignar coordenadas geográficas a los activos para ubicarlos en un mapa.

Ubicaciones Jerárquicas: GLPI permite crear una estructura jerárquica de ubicaciones, como "Edificio > Piso > Sala", para mayor precisión.

Un ejemplo sería:

DNCP, Dirección EE.UU. 961 c/ Tte. Fariña
Datacenter Primario

4.2.2 Contenedores

Racks y Gabinetes: En el caso de equipos de red o servidores, puedes asignarlos a racks o gabinetes específicos dentro de un centro de datos.

Inicio / Activos / Bastidores

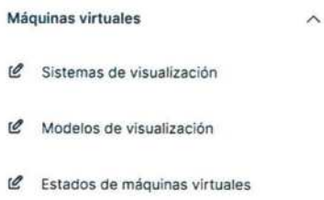
Un ejemplo sería:

DNCP, Dirección EE.UU. 961 c/ Tte. Fariña
Datacenter Primario
Rack DC1R1

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Almacenes: Los activos pueden estar asignados a almacenes o áreas de stock mientras no estén en uso.

Contenedores Virtuales: Puedes agrupar activos lógicamente, como en el caso de máquinas virtuales asignadas a un host físico.



4.3 Carga de Activos

Determinar los ACTIVOS compuestos por sedes, data centers, racks, equipos (hardware y software), sistemas de información, y servicios asociados necesarios para las operaciones del datacenter. Acorde a la norma ITIL, todo proceso de datacenter arranca con la identificación de la infraestructura a la cual vamos a asistir o dar soporte, ya que las tareas y trabajos son realizados sobre dicha infraestructura, la misma puede ser categorizada en una de las siguientes

- Generadores
- Aires Acondicionados
- Equipos de extinción y prevención de incendios.
- Equipos de UPS y bancos de baterías
- Racks
- Servidores
- Ruteadores
- Switches
- Firewalls
- Balanceadores GLSB
- Otros dispositivos

Estos equipos fueron identificados en el plan de relevamiento de infraestructura y documentados mediante los siguientes medios:

- Diagrama de Infraestructura de redes
- Planillas de equipos por rack de los Datacenter 1 y Datacenter 2.
- Diagramas de equipos por rack en los datacenter 1 y datacenter 2.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

4.3.1 Procedimiento: Carga de activos en GLPI

Antes de poder realizar cualquier procedimiento necesitamos cargar los activos, existen dos formas, la carga automática o la carga manual.

GLPI Agent es el sucesor de FusionInventory Agent , ya que se basa en el mismo código y se puede utilizar fácilmente en lugar de cualquier agente FusionInventory.

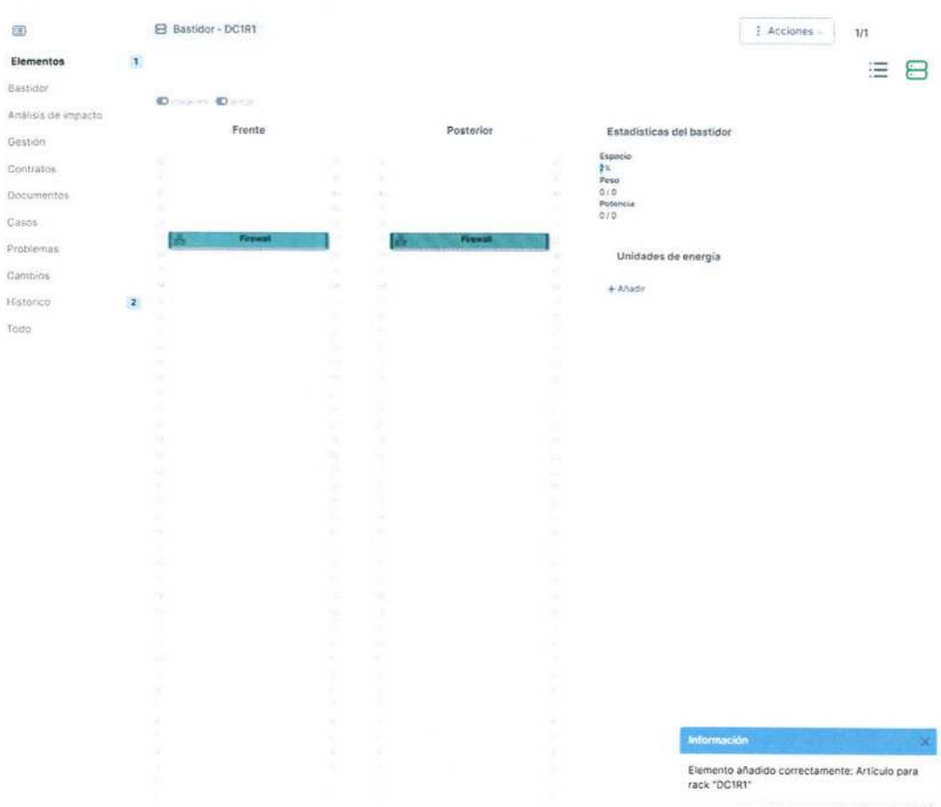
- Se utiliza para ejecutar el inventario automático y funciona con la herramienta de software GLPI ITSM .
- También admite la ejecución de algunas otras tareas, como implementación de paquetes, recopilación de información, descubrimiento e inventario de dispositivos de red e inventario remoto de ESX.
- También admite inventario sin agente a través de su tarea de inventario remoto.
- Fue desarrollado para permitirle ejecutar automáticamente tareas que actualmente solo se pueden ejecutar manualmente o usando el complemento glpi-inventory.
- Del lado del servidor, solo depende de GLPI a partir de la versión GLPI 10.

Para el proceso de carga manual de activos, recomendamos los siguientes procedimientos:

Paso	Responsable	Actividad
1	Administrador de Inventario	Recopilar información de los activos: nombre, número de serie, ubicación, y datos relevantes.
2	Administrador de GLPI	Configurar categorías y campos personalizados necesarios en el sistema GLPI.
3	Administrador de Inventario	Verificar que los datos recopilados estén completos y correctamente documentados.
4	Operador de GLPI	Acceder al módulo de "Activos" y crear los registros, completando los campos requeridos. Adjuntar documentos relevantes como facturas o garantías al registro del activo.
5	Supervisor del Proceso	Revisar los registros creados para asegurar exactitud y cumplimiento.
6	Auditor Interno	Realizar auditorías regulares para validar la calidad y actualización de los registros.
7	Administrador de GLPI	Generar informes periódicos para asegurar la trazabilidad y cumplimiento del proceso.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

2 – Poblar los equipos en cada rack con los datos recabados en el relevamiento, así como nuevas adquisiciones.



Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

5 Tipos de servicios realizados

Gestión de Tickets/Casos

- Son peticiones formales de los usuarios para que se les proporcione algo
- Pueden ser solicitudes de información, asesoramiento, o acceso a un servicio
- Pueden ser solicitudes para obtener un nuevo dispositivo o cambiar una contraseña
- Se pueden automatizar para responder a consultas de soporte rutinario.
- Los tickets con soluciones comunes dan origen a los casos.

Gestión de Problemas

- Son causas o posibles causas de uno o más incidentes, tickets o casos.
- Se originan cuando hay incidentes recurrentes que tienen problemáticas comunes
- Se deben investigar para identificar la raíz de los incidentes y tratar de que no vuelvan a ocurrir
- Son eventos que interrumpen o reducen la calidad de un servicio de TI
- Son fallas de componentes de un servicio que aún no han afectado al servicio
- Se deben resolver lo antes posible para que las operaciones puedan continuar

Gestión de Cambios

- Un cambio es una modificación de la infraestructura del sistema de información.
- Permite planificar y documentar cambios en la infraestructura IT derivados de incidentes o problemas.
- Incluye análisis de impacto y evaluación de riesgos.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

6 Procedimiento de Operación, mantenimiento preventivo, correctivo

- Crear un plan anual que detalle las operaciones de mantenimiento preventivo y correctivo para garantizar la funcionalidad y disponibilidad de los equipos e instalaciones.

6.1 Generadores

En el caso de los generadores debido a que estos son del tipo stand-by, y no están siendo utilizados en forma permanente, estos deben ser arrancados periódicamente, lo ideal es que esto sea semanal o máximo quincenal, ya que algunos componentes como las baterías pueden deteriorarse prematuramente si no están en uso, el tiempo de vida de estas depende mucho de su uso, así mismo las cañerías de combustible y aceite requieren que su uso sea periódico para lubricar el sistema y evitar oxidación en el mismo.

Periodicidad recomendada de mantenimiento:

Mantenimiento Semanal:

- Inspección visual del generador.
- Verificación de niveles de aceite, refrigerante y combustible.
- Pruebas de arranque en vacío para asegurar que el generador funcione correctamente.

Mantenimiento Anual:

- Limpieza de filtros de aire y combustible.
- Inspección de conexiones eléctricas y sistemas de escape.
- Pruebas de carga para evaluar el rendimiento bajo condiciones reales.
- Revisión completa del sistema de refrigeración.
- Inspección y ajuste de correas y mangueras.
- Pruebas de transferencia de carga entre el generador y la red eléctrica.
- Cambio de aceite y filtros.
- Inspección detallada de todos los componentes mecánicos y eléctricos.
- Pruebas exhaustivas de rendimiento y eficiencia.
- Revisión de baterías.

Observación: Debido a la poca cantidad de trabajo de este tipo de servicio, se recomienda tercerizar estos servicios y agregar los procedimientos a las tareas que deben cumplir las empresas contratadas, con un personal interno que haga el seguimiento y la emisión de las ordenes de servicio.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

6.1.1 Procedimiento: Operación y mantenimiento preventivo de generador

Número y Nombre del Paso	Responsable	Actividad
1. Creación del Ticket en GLPI	Operador del Sistema GLPI	Crear un ticket en GLPI especificando "Mantenimiento Preventivo de Generador", incluyendo la ubicación, fecha y hora programada.
2. Inspección Visual Inicial	Técnico de Mantenimiento	Revisar visualmente el estado general del generador: estructura, conexiones eléctricas y mangueras. Registrar observaciones iniciales en el ticket.
3. Verificación de Niveles de Fluidos	Técnico de Mantenimiento	Inspeccionar niveles de aceite, refrigerante y combustible, y recargar si es necesario. Documentar los resultados en el ticket.
4. Revisión de Filtros	Técnico de Mantenimiento	Inspeccionar y limpiar o reemplazar filtros de aire, combustible y aceite. Registrar la acción tomada en el ticket.
5. Comprobación del Sistema Eléctrico	Técnico de Mantenimiento	Verificar el estado de las conexiones eléctricas, baterías y el sistema de arranque. Documentar cualquier ajuste o anomalía en el ticket.
6. Inspección de Conductos de Escape	Técnico de Mantenimiento	Revisar el sistema de escape para asegurarse de que no haya bloqueos o fugas. Registrar esta actividad en el ticket.
7. Pruebas de Arranque y Funcionamiento	Técnico de Mantenimiento	Encender el generador y realizar pruebas para evaluar parámetros como voltaje, frecuencia y estabilidad. Incluir los resultados en el ticket.
8. Limpieza del Generador	Técnico de Mantenimiento	Limpiar la superficie del generador para eliminar polvo y residuos. Registrar esta actividad en el ticket.
9. Registro Final y Observaciones	Supervisor de Mantenimiento	Revisar que todas las actividades se hayan completado y documentar las observaciones finales en GLPI. Cerrar el ticket.
10. Análisis de Resultados	Responsable de Infraestructura	Analizar los resultados registrados para identificar mejoras en el proceso de mantenimiento preventivo.

6.1.2 Procedimiento: Mantenimiento correctivo de generador

Periodicidad recomendada: Acorde a las fallas ocurridas, detectadas.

SLA: Este es un elemento CRITICO NO REDUNDANTE, requiere un tiempo de respuesta prácticamente inmediato, respuesta en menos de 30 minutos, equipo de repuesto o reparación en menos de 3 horas.

Número y Nombre del Paso	Responsable	Actividad
1. Creación del Ticket en GLPI	Operador del Sistema GLPI	Crear un ticket en GLPI detallando el problema reportado, ubicación del generador y prioridad de atención.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Número y Nombre del Paso	Responsable	Actividad
2. Identificación del Problema	Operador del Datacenter	Detectar y describir la falla observada (por ejemplo, ruido inusual, falta de arranque, caída de voltaje). Registrar detalles en el ticket.
3. Asignación del Caso	Supervisor de Mantenimiento	Asignar el ticket al técnico especializado en generadores y registrar esta acción en el sistema GLPI.
4. Inspección y Diagnóstico Inicial	Técnico de Mantenimiento	Realizar una inspección física y funcional del generador para identificar la causa del problema. Documentar el diagnóstico detallado en el ticket.
5. Aislamiento del Generador	Técnico de Mantenimiento	Desconectar el generador afectado para evitar riesgos a otros sistemas. Registrar esta actividad en el ticket.
6. Reparación o Reemplazo de Componentes	Técnico de Mantenimiento	Reparar o reemplazar las piezas dañadas (baterías, filtros, sistemas de inyección de combustible, etc.). Detallar los componentes utilizados en el ticket.
7. Pruebas Post-Reparación	Técnico de Mantenimiento	Realizar pruebas de funcionamiento del generador para verificar que opere dentro de los parámetros normales. Registrar los resultados en GLPI.
8. Validación Final	Supervisor de Mantenimiento	Revisar las actividades realizadas y validar la reparación. Adjuntar reportes o documentos relevantes al ticket antes de cerrar.
9. Análisis de Causa Raíz	Responsable de Infraestructura	Analizar la causa del problema y documentar medidas preventivas para evitar su recurrencia. Registrar las conclusiones en el ticket.

6.2 Aire acondicionado

Los aires acondicionados del tipo industrial que normalmente son utilizados en los datacenters funcionan en un esquema 12/12 horas de régimen contino, esto significar que su funcionamiento es de fácil validación, lo que si es importante tener en cuenta es que si bien están diseñados para un uso continuo ininterrumpido su uso es permanente, así que se recomienda las verificaciones y los mantenimientos que se realicen con una periodicidad semestral por lo menos y luego los mantenimientos anuales.

Periodicidad recomendada:

Mantenimiento Semestral:

- Inspección visual del equipo.
- Limpieza de filtros de aire y revisión de serpentines.
- Verificación de parámetros básicos como flujo de aire y temperatura.
- Limpieza más profunda de serpentines y ventiladores.
- Revisión de conexiones eléctricas y drenajes.
- Comprobación de niveles de refrigerante y ajustes si es necesario.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Mantenimiento Anual:

- Revisión exhaustiva de todos los componentes mecánicos y eléctricos.
- Cambio de piezas desgastadas, como filtros o correas.
- Pruebas de eficiencia energética y optimización del sistema.
- Inspección completa del sistema de refrigeración.
- Verificación de sensores y controles.
- Pruebas de rendimiento bajo carga.

Observación: Debido a la poca cantidad de trabajo de este tipo de servicio, se recomienda tercerizar estos servicios y agregar los procedimientos a las tareas que deben cumplir las empresas contratadas, con un personal interno que haga el seguimiento y la emisión de las ordenes de servicio.

6.2.1 Procedimiento: Operación y mantenimiento preventivo de aire acondicionado

Paso	Responsable	Actividad
1. Creación del Ticket en GLPI	Operador del Sistema GLPI	Crear un ticket en GLPI para registrar las tareas del mantenimiento preventivo. Incluir detalles como el equipo a revisar, ubicación y fecha programada.
2. Planificación del Mantenimiento	Supervisor de Mantenimiento	Programar las actividades de mantenimiento preventivo en coordinación con los técnicos y registrar esta planificación en el ticket.
3. Inspección Inicial	Técnico de Mantenimiento	Revisar visualmente el estado general del aire acondicionado (conexiones eléctricas, estado físico, etc.). Registrar observaciones iniciales en el ticket.
4. Limpieza de Componentes	Técnico de Mantenimiento	Limpiar filtros, serpentinas, ventiladores y rejillas. Registrar estas actividades en el ticket con fotos (si aplica).
5. Inspección de Niveles de Refrigerante	Técnico de Mantenimiento	Verificar los niveles de refrigerante y, si es necesario, realizar ajustes. Registrar los resultados y acciones tomadas en el ticket.
6. Revisión de Sensores y Controles	Técnico de Mantenimiento	Verificar termostatos, sensores de temperatura y sistemas de control, asegurando su correcto funcionamiento. Registrar el estado de los sensores en el ticket.
7. Inspección y Limpieza de Drenajes	Técnico de Mantenimiento	Revisar y limpiar los sistemas de drenaje para evitar bloqueos o acumulación de agua. Registrar esta actividad y su resultado en el ticket.
8. Pruebas de Operación	Técnico de Mantenimiento	Encender el aire acondicionado y realizar pruebas de rendimiento, revisando parámetros como presión, flujo de aire y temperatura. Incluir resultados de las pruebas en el ticket.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9. Registro y Cierre del Ticket	Supervisor de Mantenimiento	Revisar toda la información registrada en el ticket, adjuntar reportes finales y cerrar el ticket una vez completadas todas las actividades.

6.2.2 Procedimiento: Mantenimiento correctivo de aire acondicionado

Periodicidad recomendada: Acorde a las fallas ocurridas, detectadas.

SLA: Si bien este es un elemento redundante, se debe definir un tiempo de respuesta razonable, 48 horas.

Paso	Responsable	Actividad
1. Creación del Ticket en GLPI	Operador del Sistema GLPI	Crear un ticket en GLPI especificando el problema reportado, ubicación del equipo y prioridad de atención.
2. Identificación del Problema	Operador del Datacenter	Reportar anomalías detectadas, como ruidos, fallas en la temperatura o alarmas, y registrar estos detalles en el ticket.
3. Asignación del Caso	Supervisor de Mantenimiento	Asignar el ticket al técnico adecuado y registrar esta acción en GLPI.
4. Diagnóstico del Problema	Técnico de Mantenimiento	Inspeccionar el aire acondicionado para identificar la causa raíz del problema. Registrar el diagnóstico detallado en el ticket.
5. Aislamiento del Equipo	Técnico de Mantenimiento	Desconectar el equipo afectado y asegurarlo para evitar daños adicionales. Documentar esta actividad en el ticket.
6. Reparación del Componente	Técnico de Mantenimiento	Reemplazar o reparar los componentes dañados (ventiladores, compresores, sensores, etc.). Detallar las piezas usadas y las acciones realizadas en el ticket.
7. Pruebas Post-Reparación	Técnico de Mantenimiento	Encender el equipo y realizar pruebas para confirmar su correcto funcionamiento. Registrar los resultados en GLPI.
8. Monitoreo y Validación	Supervisor de Mantenimiento	Verificar que el equipo funciona dentro de los parámetros establecidos. Cerrar la incidencia en GLPI con un informe final.
9. Análisis de Causa Raíz	Responsable de Infraestructura	Revisar el problema y documentar medidas preventivas en el sistema para evitar recurrencias similares.

6.3 Extinción de incendios

Los sistemas de extinción se rigen por varias normas, el Datacenter debe cubrir la norma asociada a los niveles de disponibilidad del tipo TIER, de TIA-942, ya sea UPTIME INSITUTE o similar y la norma de PCI del Municipio donde se encuentre, hoy en día los Municipios aceptan que el Datacenter en si puede guiarse por normas ajenas a PCI ya que en teoría no se encuentra personal operativo dentro. Lo que si es importante tener en cuenta son las fechas de vencimiento de los agentes extintores, para un datacenter se utiliza un extintor del tipo ABC, que es un polvo químico seco diseñado para combatir incendios de clase A (materiales sólidos), B (líquidos inflamables) y C (gases inflamables o aparatos eléctricos).

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Si bien estos agentes tienen un tiempo de duración acorde a la lista siguiente, es importante la revisión periódica de la presión del mismo, ya que pueden existir fallas en el sistema que eviten su capacidad de uso cuando el tiempo sea necesario.

El tiempo de vida útil por agentes es el siguiente:

FM-200 (Heptafluoropropano): Este gas se usa ampliamente en datacenters. Tiene un tiempo de almacenamiento prolongado, normalmente entre 10 y 15 años, siempre y cuando el sistema reciba mantenimiento adecuado.

CO_2 (Dióxido de Carbono): Aunque no es tan común en datacenters modernos debido a preocupaciones de seguridad, su duración puede superar los 10 años con el cuidado adecuado.

Inergen (mezcla de gases inertes): Este sistema suele durar más, porque es una mezcla de gases naturales (nitrógeno, argón y dióxido de carbono). Generalmente no tiene una fecha de vencimiento, pero los cilindros deben revisarse periódicamente.

Novec 1230 (Ketona fluorado): Es considerado muy eficiente y ecológico. Su duración suele ser de 20 a 30 años con un buen mantenimiento, y algunos fabricantes ofrecen garantías extendidas.

El más utilizado para data centers últimamente es el NOVEC 1230.

Periodicidad de mantenimiento y tareas recomendadas:

Mensual:

Inspección visual del sistema, incluyendo cilindros, válvulas, boquillas y tuberías.

Verificación de la accesibilidad y señalización de los equipos.

Trimestral:

Comprobación de la presión de los cilindros de agentes limpios.

Pruebas funcionales de detectores de humo y calor.

Revisión de alarmas audibles y visuales.

Anual:

Pruebas completas del sistema, incluyendo simulaciones controladas de activación (sin descarga del agente).

Inspección detallada de todos los componentes mecánicos y eléctricos.

Revisión de la documentación y actualización de registros.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Observación: Debido a la poca cantidad de trabajo de este tipo de servicio, se recomienda tercerizar estos servicios y agregar los procedimientos a las tareas que deben cumplir las empresas contratadas, con un personal interno que haga el seguimiento y la emisión de las ordenes de servicio.

6.3.1 Procedimiento: Mantenimiento preventivo de extinción de incendios

Número y Nombre del Paso	Responsable	Actividad
1. Creación del Ticket en GLPI	Operador del Sistema GLPI	Registrar un ticket detallado para el mantenimiento preventivo, especificando ubicación y alcance.
2. Inspección Visual Inicial	Técnico de Mantenimiento	Verificar condiciones físicas del sistema, como cilindros, válvulas, boquillas y tuberías. Registrar hallazgos en el ticket.
3. Verificación de Niveles y Presión	Técnico de Mantenimiento	Revisar la presión de los cilindros de agentes limpios y verificar niveles según especificaciones del fabricante. Registrar resultados en GLPI.
4. Comprobación de Detectores	Técnico Especializado en Seguridad	Revisar y probar los detectores de humo y calor. Registrar pruebas realizadas en el ticket.
5. Inspección del Sistema de Alarmas	Técnico de Mantenimiento	Verificar que las alarmas audibles y visuales funcionen correctamente. Documentar esta actividad en GLPI.
6. Prueba del Sistema de Activación	Técnico de Mantenimiento	Realizar una prueba controlada de activación del sistema (sin descargar el agente). Registrar los resultados de la prueba.
7. Limpieza General del Sistema	Técnico de Mantenimiento	Limpiar boquillas, detectores y paneles de control. Registrar la actividad en el ticket.
8. Registro y Cierre del Ticket	Supervisor de Mantenimiento	Revisar el trabajo realizado, documentar el estado final del sistema y cerrar el ticket en GLPI.

6.3.2 Procedimiento: Mantenimiento correctivo de extinción de incendios

Periodicidad recomendada: Acorde a las fallas ocurridas, detectadas.

Paso	Responsable	Actividad
1. Creación del Ticket en GLPI	Operador del Sistema GLPI	Registrar el problema detectado en un ticket, indicando ubicación, descripción del fallo y prioridad.
2. Diagnóstico del Problema	Técnico Especializado en Seguridad	Inspeccionar el sistema para determinar la causa del fallo. Documentar el diagnóstico en el ticket.
3. Aislamiento del Sistema	Técnico de Mantenimiento	Asegurar que el sistema esté desconectado para evitar descargas accidentales. Registrar esta actividad en GLPI.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

4. Reparación o Reemplazo de Componentes	Técnico de Mantenimiento	Reemplazar o reparar componentes defectuosos (detectores, válvulas, cilindros, etc.). Documentar las piezas utilizadas y las acciones tomadas en el ticket.
5. Pruebas Post-Reparación	Técnico de Mantenimiento	Realizar pruebas para garantizar que el sistema funcione correctamente. Registrar resultados en GLPI.
6. Validación del Sistema	Supervisor de Mantenimiento	Confirmar que el sistema cumple con las normativas y estándares. Documentar observaciones finales en el ticket y cerrarlo.
7. Análisis de Causa Raíz	Responsable de Infraestructura	Analizar el motivo del fallo y proponer medidas preventivas para evitar futuros problemas. Registrar conclusiones en el ticket.

6.4 Cableado estructurado

En el caso del cableado estructurado es importante tener personal interno capacitado en la norma TIA-568 básica, que nos permita resolver rápidamente cualquier evento simple, y así mismo cuando el cableado, las herramientas y los materiales excedan al equipo humano.

En este caso no existe una periodicidad sino un contrato abierto de servicio y unos tiempos de respuesta.

En el caso de enlace de fibra óptica al sitio redundante, si es que este no es un servicio contratado debe tener un SLA con 30 minutos de respuesta, y reparación en menos de 6 horas.

Observación: Debido al que el cableado estructurado es muy frecuentemente utilizado, el equipo interno debe contar con todas las herramientas, materiales y repuestos para resolver todo tipo de problema de terminación de cableado UTP, así como repuestos de cables de PATCH para UTP y FO de por lo menos 3m para resolver problemas de corta distancia en el Datacenter. Para trabajos externos o de larga distancia se recomienda tercerizar estos servicios y agregar los procedimientos a las tareas que deben cumplir las empresas contratadas, con un personal interno que haga el seguimiento y la emisión de las ordenes de servicio.

6.4.1 Procedimiento: Reparación de Cableado Estructurado

Paso	Responsable	Actividad
1. Reporte del problema	Usuario / Técnico de TI	Crear un ticket en el sistema GLPI describiendo el problema detectado en el cableado estructurado.
2. Revisión inicial del ticket	Técnico de TI	Analizar el ticket y priorizar el caso según la criticidad y el impacto en las operaciones.
3. Inspección del área afectada	Técnico de TI	Realizar una inspección visual y técnica en el lugar para identificar la causa del problema.
4. Determinación de solución	Técnico de TI	Establecer las acciones necesarias para reparar el daño (reemplazo de cables, conectores, etc.).

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Paso	Responsable	Actividad
5. Ejecución de la reparación	Técnico de TI	Llevar a cabo la reparación según lo planificado, utilizando herramientas y materiales adecuados.
6. Verificación de funcionamiento	Técnico de TI	Realizar pruebas para garantizar el correcto funcionamiento del cableado después de la reparación.
7. Actualización y cierre del ticket	Técnico de TI / Supervisor	Registrar en GLPI los detalles de la reparación y cerrar el ticket si el problema ha sido resuelto.

6.4.2 Procedimiento: Instalación de Nuevos Puestos de Cableado Estructurado

En el caso de puestos nuevos se define un SLA razonable, 24 – 48 horas posterior a la emisión de la orden de servicio.

Paso	Responsable	Actividad
1. Solicitud de instalación	Usuario / Técnico de TI	Crear un ticket en GLPI solicitando la instalación de un nuevo puesto de cableado estructurado.
2. Evaluación técnica	Técnico de TI	Inspeccionar el área para determinar la viabilidad técnica y los requerimientos del nuevo puesto.
3. Planificación de la instalación	Técnico de TI / Supervisor	Definir ubicación, herramientas, materiales necesarios y cronograma para la instalación.
4. Instalación del cableado	Técnico de TI	Realizar la instalación física del cableado, conectores, canalizaciones y etiquetas según normas de calidad.
5. Pruebas de rendimiento	Técnico de TI	Realizar pruebas de continuidad y desempeño para validar el correcto funcionamiento del puesto instalado.
6. Documentación en GLPI	Técnico de TI / Supervisor	Registrar en GLPI los detalles de la instalación y los resultados de las pruebas realizadas.
7. Cierre del ticket	Técnico de TI / Supervisor	Validar que la instalación se haya completado según los requerimientos y cerrar el ticket en GLPI.

6.5 UPS y Baterias

En el caso de las UPS tienen la gran ventaja que deben ser diseñadas en configuración 2N que alimenten el lado A y el lado B del datacenter, si bien es un componente crítico del mismo es un componente redundante.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

En el caso de las baterías se recomienda realizar una prueba por separado de las baterías, ya sea mediante un elemento de descarga individual por baterías, o directamente un banco de carga con el cual se mida el tiempo de autonomías de estas.

El tiempo de vida útil de las baterías en la actualidad es el siguiente:

Baterías VRLA (Ácido-Plomo Reguladas por Válvula):

- Vida útil típica: **3 a 5 años**.
- Factores que afectan: Temperatura, ciclos de carga/descarga y mantenimiento adecuado2.

Baterías de Plomo-Ácido Abiertas:

- Vida útil típica: **10 a 15 años**.
- Requieren mantenimiento regular, como la reposición de agua destilada y monitoreo constante.

Baterías de Iones de Litio:

- Vida útil típica: **8 a 10 años**.
- Ventajas: Mayor densidad energética, menor mantenimiento y mejor tolerancia a temperaturas altas.

Baterías de Níquel-Cadmio (NiCd):

- Vida útil típica: **15 a 20 años**.
- Usadas en aplicaciones críticas debido a su alta durabilidad y resistencia a temperaturas extremas.

Periodicidad recomendada: Anual

Observación: Debido a la poca cantidad de trabajo de este tipo de servicio, se recomienda tercerizar estos servicios y agregar los procedimientos a las tareas que deben cumplir las empresas contratadas, con un personal interno que haga el seguimiento y la emisión de las ordenes de servicio. Pueden tenerse en cuenta stocks de repuestos. Para los bancos de poder y baterías.

6.5.1 Procedimiento: Mantenimiento Preventivo de UPS y Baterías

Paso	Responsable	Actividad
1. Creación del ticket	Usuario solicitante	Registrar la solicitud en GLPI especificando la necesidad de mantenimiento preventivo.
2. Validación y asignación del ticket	Administrador GLPI	Validar la solicitud y asignar el ticket al técnico responsable.
3. Inspección inicial	Técnico asignado	Realizar una revisión visual del estado del UPS y las baterías, documentando observaciones en GLPI.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Paso	Responsable	Actividad
4. Limpieza y verificación general	Técnico asignado	Limpiar componentes externos e inspeccionar conexiones, ventiladores y terminales de las baterías.
5. Comprobación de carga	Técnico asignado	Verificar el estado de carga de las baterías y realizar pruebas funcionales al sistema UPS.
6. Documentación del mantenimiento	Técnico asignado	Registrar en GLPI las actividades realizadas, resultados de las pruebas y cualquier observación relevante.
7. Cierre del ticket	Técnico asignado	Actualizar el ticket como resuelto y notificar al usuario solicitante.

6.5.2 Procedimiento de Mantenimiento Correctivo de UPS y Baterías

Paso	Responsable	Actividad
1. Creación del ticket	Usuario solicitante	Reportar la incidencia en GLPI describiendo el problema presentado.
2. Validación y asignación del ticket	Administrador GLPI	Validar la información inicial y asignar el ticket al técnico responsable.
3. Diagnóstico del problema	Técnico asignado	Identificar la causa del fallo en el UPS o las baterías, documentando el análisis en GLPI.
4. Reparación del sistema	Técnico asignado	Reparar o sustituir los componentes dañados del UPS o las baterías.
5. Pruebas de funcionamiento	Técnico asignado	Realizar pruebas bajo condiciones normales de carga para asegurar que el sistema funcione correctamente.
6. Documentación final	Técnico asignado	Registrar en GLPI las actividades realizadas, piezas sustituidas y resultados de pruebas.
7. Cierre del ticket	Técnico asignado	Marcar el ticket como resuelto en GLPI y notificar al usuario solicitante.

A la par que vayamos creciendo en los servicios y la disponibilidad de estos, así como la documentación pertinente para permitir una continuidad de negocios debemos empezar a focalizarnos en la planificación de como estas tareas deben ser resueltas por personal propio o tercerizado.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

7 Procedimientos Operativos

7.1 Gestión de incidentes/tickets/casos

Una vez ya con el trabajo preparatorio para GLPI realizados, la creación de los tickets y asociación a localidades, equipos y usuarios empieza a convertirse en una tarea operativa, esto ya está ocurriendo en la actualidad en la DNCP, así que generar el procedimiento es meramente a base de documentación.

7.1.1 Procedimiento: Creación de Tickets y Gestión de la Resolución en GLPI

Paso	Responsable	Actividad
1. Recepción de la solicitud	Usuario solicitante o Mesa de ayuda	Recibir la solicitud de servicio a través de correo, llamada telefónica o entrada directa al sistema GLPI.
2. Creación del ticket en GLPI	Mesa de ayuda	Registrar el ticket en GLPI, incluyendo detalles del incidente o solicitud proporcionados por el usuario.
3. Categorización y priorización	Mesa de ayuda	Asignar una categoría al ticket, determinar su prioridad y añadir cualquier información relevante.
4. Asignación del ticket	Administrador GLPI	Asignar el ticket al técnico o grupo responsable de la resolución del incidente.
5. Gestión de la solicitud	Técnico asignado	Revisar el ticket, realizar las acciones necesarias para atender la solicitud o solucionar el problema. Documentar cada actividad realizada en el ticket.
6. Resolución del problema	Técnico asignado	Resolver el problema reportado, confirmar con el usuario final y documentar la solución en el ticket de GLPI.
7. Carga en la base de conocimiento	Técnico asignado o Equipo de documentación	Extraer la resolución del ticket y registrar los detalles relevantes en la base de conocimiento para referencia futura.
8. Cierre del ticket	Técnico asignado	Marcar el ticket como resuelto en GLPI, incluir la referencia a la entrada en la base de conocimiento (si aplica) y notificar al usuario final.

Es importante tener en cuenta que para cada evento existe un ticket UNICO, no así la resolución u origen del problema que tiene relación, estos tienen una relación N:1.

Ticket N : 1 Problema

La idea es que a futuro, una vez que el equipo vaya resolviendo los tickes simplemente vayan asociando a problemas frecuentes, y esto sirva como base de conocimiento para resolver los tickets a futuro, lo cual permitiría la rotación de personal sin perder el conocimiento operativo

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

que nace del día a día en la gestión de problemas similares debido a la infraestructura que suele ser homologada en las compras, computadoras, impresoras, dispositivos similares llevan drivers y/o soluciones similares.

A esto se suma uno de los procesos más detallados del área de informática

7.1.2 Procedimiento: Asistencia al usuario interno:

2. RESPONSABILIDADES Y PROCEDIMIENTOS 2.1 Secuencia de actividades: Asistencia a Usuarios Internos.		
Paso	**Responsable**	**Actividad**
1. Solicitud de Asistencia.	Usuario Interno	Identifica la necesidad de asistencia y la comunica a través del Sistema Informático de Gestión de Reclamos, proporcionando una descripción detallada del apoyo específico requerido, así como una explicación del motivo de la solicitud. Las solicitudes de ABM (alta/incorporación, baja/desvinculación o modificaciones) de accesos físicos o lógicos para usuarios internos de la DNCP será realizada por la DGGDP. Las solicitudes o comunicaciones de traslados de un área a otra serán realizada por la DGGDP.
2. Recepción de solicitud.	Jefe de Dpto. Soporte Técnico / Técnico de Soporte Técnico	1. Recibe la solicitud e identifica si el mismo requiere aprobación. 1.1. Si la solicitud requiere de aprobación: Deriva a través del mismo mecanismo al responsable de aprobar (director/coordinador/jefe) según lo establecido en la Tabla de plazos para la ejecución de servicios de la DGTI, solicitando la aprobación y continúa en el paso 3 de esta secuencia de actividades. 1.2. Aquellas solicitudes que hagan referencia a procesos cuyos dueños sean de otra área del solicitante, deberán ser aprobadas primeramente por el director del solicitante, y luego por el dueño del proceso. 1.2. Si no requiere: Asigna a través del Sistema Informático de Gestión de Reclamos a un responsable de la DGTIC para realizar la tarea y según sea el acaso, continúa en el paso 5 de esta secuencia de actividades. Nota 1: si la clasificación asignada a la solicitud otorga al solicitante la autoridad para aprobarla, se omite el paso de solicitar aprobación. . Pasa al paso 4. Nota 2: en casos excepcionales el director de DGTIC podrá autorizar o dar su aval para la realización de solicitudes, dejando constancia por medio de nota en el GLPI, el motivo por el cual autorizó. 2. Si la solicitud requiere alguna aclaración del pedido o algún documento, se solicita por medio del GLPI. Esta acción puede ser realizada por cualquier técnico de la DGTIC asignado a la tarea (ticket) 2.1. Una vez recibida la respuesta de aclaración, pasa al siguiente paso, que pueden ser: 1.1. solicitar aprobación, 1.2. Si no requiere aprobación, asignar a un técnico.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

		3. Solicitud de ABM funcionarios, para casos de ALTA, el ticket se asigna a Operaciones, una vez que se haya creado el usuario de dominio, Operaciones, crea 4 tickets hijos y asigna a: Seguridad TIC, Redes, Soporte, Administración de contenidos. Para Baja y Modificaciones, soporte técnico asigna el ticket a Operaciones y crea 4 tickets hijos y asigna a: Seguridad TIC, Redes, Soporte, Administración de contenidos 4. Solicitud de traslado de funcionarios comunicado por RRHH el ticket se asigna a Operaciones, se crean tickets hijos para: Seguridad TIC, Redes, Soporte, Administración de contenidos. Solicitud de traslado de funcionarios dentro de la misma área/dirección se analiza la viabilidad de lo solicitado según circular DAF-DTI N° 01/2019, si es viable, se agendará para viernes según disponibilidad. 6. Verificación de EETT que deben ser realizadas por más de un área, el Jefe de Dpto. de Soporte Técnico / Tecnico de Soporte Tecnico, asigna el ticket a las áreas correspondientes, El primer departamento en terminar de verificar carga una nota de seguimiento en el ticket con su verificación. El segundo departamento se encarga de "resolver" el ticket, escribiendo en la solución su observación y copiando todo lo escrito en la nota de seguimiento por el otro departamento, de modo que el último en verificar cargue una solución completa en el ticket. 7. Solicitud de VPN para equipos institucionales: Se verifica si cuenta con periodo de inicio/fin, sin este dato se rechaza el pedido. El departamento de Soporte Técnico verifica el equipo de acuerdo a los requisitos establecidos por la coordinación de Seguridad TIC y remite informe para su aprobación vía correo electrónico, una vez aprobado reenvía dicha aprobación al GLPI y asigna el ticket al área de operaciones para la habilitación del perfil correspondiente, operaciones finaliza el ticket . |Solicitud de VPN para equipos no institucionales: Se verifica si cuenta con periodo de inicio/fin, sin este dato se rechaza el pedido Se solicita aprobación del director, si aprueba pasa al siguiente paso, de lo contrario se finaliza el ticket comunicando al solicitante que su director no aprobó la solicitud. Las solicitudes que no son aprobadas en 15 días calendario desde su creación serán finalizadas por falta de aprobación. El departamento de Soporte Técnico remite por correo al solicitante los requisitos que serán verificados, coordina con el usuario fecha y hora para la verificación y realización de informe de seguridad, deja constancia de lo acordado en una nota de seguimiento y cambio a estado "en espera" el ticket.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

		campos de "DEVOLUCION DE EQUIPOS". Caso no conforme, devuelve el mismo al proveedor para su corrección. 1.3. Verifica que acompañe al equipo el informe del servicio realizado. Si no acompaña completa el Formulario Informe de Servicio Externo (FOR-DTI-04). Nota 2: En ausencia del Jefe de Dpto. de Soporte Técnico / Técnico de Soporte Técnico, la recepción del equipo puede ser realizada por un funcionario de la DGTIC .
12. Realización de Asistencia al Usuario.	Responsable o grupo asignado de la DGTIC	1. Este paso aplica caso la asistencia sea asignada a un responsable o grupo interno (responsable de la DGTIC).1.1. Realiza el servicio in situ, vía on line o correo interno acorde a la necesidad. 1.2. De ser necesaria la derivación de algunas de las tareas a otras áreas de la DGTIC, lo realiza a través del Sistema Informático de Gestión de Reclamos. 2. En caso de una asignación errónea, el responsable asignado debe cargar en el GLPI una nota de seguimiento o nota de aclaración donde informa claramente que no le corresponde realizar la tarea, debe asignar al área de soporte técnico o al grupo de técnicos) correspondiente
13. Solución de lo solicitado.	Responsable o grupo asignado de la DGTIC Usuario Interno	1. El responsable de la DGTIC asignado para realizar la tarea, carga la solución en el GLPI, y este de forma automática remite al solicitante una notificación en la cual informa que su solicitud se encuentra Resuelta: detallando de forma breve y concisa la tarea que realizó.
14. Finalización y Cierre de Proceso.	Usuario Interno	1. Si la asistencia solicitada finalizó correctamente, el solicitante da su conformidad a través del GLPI. Caso contrario rechaza la solución, aclarando el motivo y la solicitud sigue en proceso. 1.1. Si el solicitante simplemente rechaza la solución sin justificar, la solicitud se cierra y el solicitante deberá realizar una solicitud nueva. 2. En caso de no obtener una respuesta por parte del solicitante luego de 48 horas de haber recibido la notificación de finalización de su solicitud, se toma como realizada con éxito, y el GLPI lo cierra automáticamente.
15. Solicitudes con estado EN ESPERA	Jefe de Dpto. de Soporte Técnico / Técnico de Soporte Técnico / Responsable o grupo asignado de la DGTIC a realizar una tarea	Pone en espera la solicitud cuando la misma necesita aprobación. Si una solicitud se encuentra en espera por 15 días corridos sin ser aprobada, se cancela la misma, por falta de aprobación Se pone en espera una solicitud cuando la misma necesita una aclaración por parte del solicitante. Si una solicitud se encuentra en espera por 30 días corridos sin ser aclarada, se cancela la misma, por falta de aclaración por parte del solicitante. Se pone en espera aquellas solicitudes que tengan una justificación que impida continuar con lo solicitado. Semanalmente se realiza control de todas las solicitudes con estado "en espera", completando los datos de la "Tabla Verificación de solicitudes en espera - GLPI", que se encuentra almacenada en la intranet, en el

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

	Comunicación/ Jefe de Dpto. de Operaciones	
Alta de Usuario	Responsable de la DGTIC	Crea el Usuario en el Sistema Informático (SI), asignando adecuadamente que éste acceda sólo a los programas autorizados. Establece una Contraseña Inicial. De ser necesaria la derivación de algunas de las tareas, lo realiza a través del Sistema Informático de Gestión de Reclamos, correo electrónico o telefónicamente.
Modificación de Contraseña	Usuario	Define e implementa una Contraseña Personal para su acceso. Nota: Este paso solo aplica para acceso al SICP, AD y el Sistema de RRHH. El Usuario deberá modificar su contraseña de acceso cada tres meses.
Aprobación del Servicio	Usuario Solicitante	Si la asistencia finalizó correctamente, da su conformidad a través del Sistema Informático de Gestión de Reclamos. Caso contrario, contacta con el responsable asignado hasta solucionar el problema.
Finalización del Proceso	Responsable de la DTI	Da por finalizada la tarea en el Sistema Informático de Gestión de Reclamos. Nota: En caso de no obtener una respuesta por parte del solicitante luego de 48 horas de haber recibido la notificación de finalización de su solicitud, se toma como realizada con éxito, y el SIGR lo cierra automáticamente.
2.2 Secuencia de actividades: Tramitación de Modificación de Usuarios Internos.		
Paso	Responsable	Actividad
Solicitud de Modificación de Usuario	Solicitante	Completa el Formulario Habilitación y Deshabilitación de Accesos (FOR-DTI-08), y lo remite a través del Sistema Informático de Gestión de Reclamos. Nota 1: En cualquiera de los pasos el FOR-DTI-08 puede ser creado o modificado por personal técnico de la Dirección de Tecnología de la Información o por el solicitante. Nota 2: Por cada pedido realizado se emitira un FOR-DTI-08 conteniendo los cambios solicitados en dicho pedido.
Recepción de la Solicitud	Jefe de Dpto. Soporte / Auxiliar de Soporte	Recibe la solicitud aprobada por el Director / Coordinador de Área / Jefe de Departamento. Si lo anterior es correcto, deriva la solicitud al Coordinador de Infraestructura y Operaciones / Director General de Tecnología de la Información y Comunicacion / Jefe de Dpto. de Operaciones. Si no es correcto, devuelve la solicitud al Solicitante para su adecuación. Nota 1: No se requiere de aprobación en el caso que el pedido fuese realizado por el mismo Director / Coordinador de Área / Jefe de Departamento. Nota 2: En casos excepcionales el Director de DTI / Coordinador de Infraestructura y Comunicacion/ Jefe de Dpto. Operaciones podrá autorizar o dar su aval para la realización de solicitudes con alguna observación.
Autorización de Modificación de Usuario	Coordinador de Infraestructura y Operaciones /	Analiza la solicitud. Si corresponde, autoriza las modificaciones pertinentes. Si no, comunica al Solicitante explicando el motivo.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

		De ser necesaria la derivación de algunas de las tareas (configuración), lo realiza a través del Sistema Informático de Gestión de Reclamos, correo electrónico o telefónicamente. Completa el Formulario Habilitación y Des habilitación de Accesos (FOR-DTI-08).

7.1.4 FOR-DTI-08 R05 - Habilitacion y Deshabilitacion de Accesos

DNCP Dirección Nacional de Contrataciones Públicas	HABILITACION Y DESHABILITACION DE ACCESOS	FOR-DTI-08 Rev.: 05

Solicitante:	(Nombre de Quien Solicita)
Para:	(Nombre del Funcionario por quien se solicita)
Cargo:	(Cargo de Dicho Funcionario)
Area:	(Area de Dicho Funcionario)
Coordinación:	(Coordinación de Dicho Funcionario)
Dirección:	(Dirección de Dicho Funcionario)
Superior Inmediato:	(Nombre del encargado de derivarle llamados, pacs, adjudicaciones, etc..)
Fecha:	(Fecha de la Solicitud)
Funcionario Nuevo:	(Nuevo en la Institución (Si / No))
Ticket N°	(Numero de Ticket de solicitud de Servicio)

N°	**ACCESOS DEL USUARIO**	**HAB. (√)**	**DESHAB. (√)**
1	ACCESO A DNCP AD (Dominio Active Directory)	☐	☐
2	ACCESO A Skype for Business (Chat)	☐	☐
Usuario AD:			
Contraseña AD:			
OBS.: El campo Usuario y Contraseña es completado por el personal técnico de la DTI			

N°	**SICP**	**HAB. (√)**	**DESHAB. (√)**
1	ACCESO AL SICP	☐	☐
2	ACCESO AL SISTEMA DE RRHH	☐	☐
3	ACCESO AL SISTEMA DE DENUNCIAS	☐	☐
4	ACCESO AL SISTEMA DE INVENTARIO	☐	☐
Usuario SICP:			
Contraseña SICP:			
OBS.: El campo Usuario y Contraseña es completado por el personal técnico de la DTI, el sistema de Inventario comparte datos con el del SICP.			
Usuario RRHH:			
Contraseña RRHH:			
OBS.: El campo Usuario y Contraseña es completado por el personal técnico de la DTI			
Usuario DENUNCIAS:			
Contraseña DENUNCIAS:			
OBS.: El campo Usuario y Contraseña es completado por el personal técnico de la DTI			

7.2 Gestión eventos de recuperación

7.2.1 Procedimiento: Backup y Recuperación de Datos

El proceso de backup y recuperación de datos está definido in extenso, este no requiere modificación alguna, a futuro se debe tener en cuenta la plataforma de TAPE backup que se encuentra en proceso de implementación.

2. RESPONSABILIDADES Y PROCEDIMIENTOS 2.1 Secuencia de actividades: Backup de datos.		
Paso	Responsable	Actividad

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

	Administración de Base de Datos / Coordinación de Infraestructura y Operaciones / Coordinación de Seguridad TICs	Al finalizar exitosamente el proceso, completa el Formulario Registro de Recuperación de Datos (FOR-DTI-02) y el solicitante manifiesta su conformidad mediante el Sistema de Gestión de Reclamos. Si detecta fallas en el proceso de recuperación, registra los problemas en el Formulario Registro de Recuperación de Datos (FOR-DTI-02), sugiriendo ideas y aportando soluciones.
Solución del problema	Coordinador de Infraestructura y Operaciones / Jefe de Dpto. Operaciones / Operador	Nota: Aplicable únicamente si se detectaron fallas en el proceso. Verifica el Formulario Registro de Recuperación de Datos (FOR-DTI-02) y define acciones al respecto.
Finalización de Proceso	Coordinación de Infraestructura y Operaciones / Coordinación de Seguridad TICs Jefe de Dpto. Operaciones / Operador	Da por finalizada la tarea en el Sistema de Gestión de Reclamos.

2.3 Secuencia de actividades: Recuperación en caso de desastres.

Paso	Responsable	Actividad
Detección de desastre	Coordinador de Infraestructura y Operaciones/ Director General de Tecnología de la Información y Comunicaciones	Se informa del caso y comunica a él/los afectado(s).
Dimensión del desastre	Jefe de Operaciones / Coordinador de Infraestructura y Operaciones	Analizan la situación, las acciones que correspondan e identifican las copias de backup a ser recuperadas.
Recuperación de backup	Coordinacion de Infraestructura y Operaciones / Jefe de Operaciones / Operador	Procede a recuperar la copia del backup. Va al paso 4 de la secuencia 2.2.

7.2.2 FOR-DTI-02 RV 03 Registro de Recuperación de Datos

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Paso	Responsable	Actividad
7. Cierre del ticket	Técnico asignado	Actualizar el ticket como resuelto y notificar al usuario.

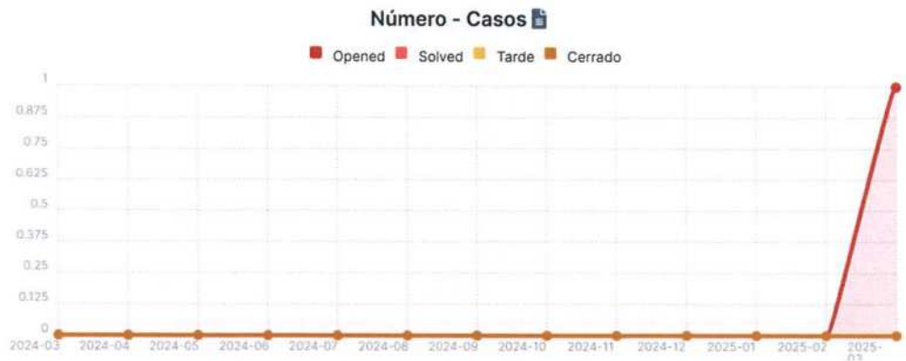
7.3.2 Procedimiento: Modificación de Equipos Activos de Red

Paso	Responsable	Actividad
1. Creación del ticket	Usuario solicitante	Registrar en GLPI una solicitud describiendo las modificaciones requeridas.
2. Validación de la solicitud	Administrador GLPI	Revisar la solicitud y asignar al técnico correspondiente.
3. Implementación de cambios	Técnico asignado	Realizar las modificaciones solicitadas en la configuración del equipo.
4. Pruebas posteriores a los cambios	Técnico asignado	Verificar que los cambios realizados funcionen correctamente.
5. Backup de configuración actualizada	Técnico asignado	Crear y almacenar un respaldo de la nueva configuración del equipo.
6. Documentación y base de conocimiento	Técnico asignado	Registrar en GLPI los detalles de los cambios realizados y documentar en la base de conocimiento.
7. Cierre del ticket	Técnico asignado	Marcar el ticket como resuelto y notificar al usuario.

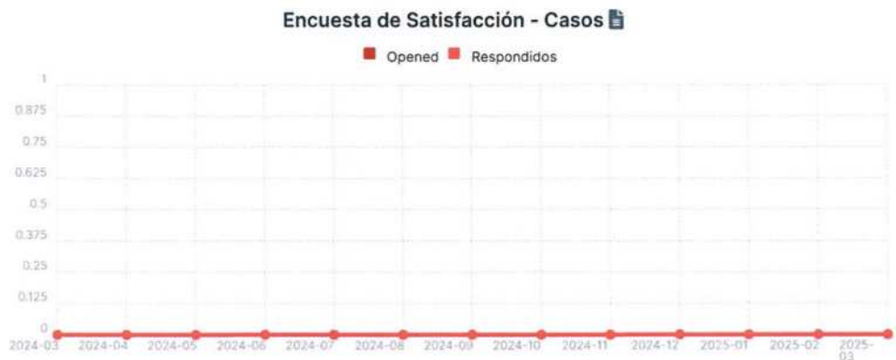
7.3.3 Procedimiento: Soporte de Equipos Activos de Red

Paso	Responsable	Actividad
1. Creación del ticket	Usuario solicitante	Reportar el problema o solicitud en GLPI con una descripción detallada.
2. Diagnóstico inicial	Técnico asignado	Revisar el equipo afectado y determinar la causa del problema.
3. Resolución del problema	Técnico asignado	Aplicar la solución adecuada (configuración, reparación o ajuste).
4. Pruebas de funcionalidad	Técnico asignado	Verificar que el problema haya sido resuelto exitosamente.
5. Backup de configuración actualizada (si aplica)	Técnico asignado	Realizar un respaldo de la configuración si se realizaron ajustes importantes.
6. Documentación y base de conocimiento	Técnico asignado	Registrar en GLPI las acciones realizadas y documentar la resolución en la base de conocimiento.
7. Cierre del ticket	Técnico asignado	Actualizar el estado del ticket como resuelto y notificar al usuario afectado.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030



En el caso de mesa de ayuda se puede contemplar la utilización de la encuesta, así como el nivel de satisfacción, pero esto requiere que los usuarios tengan acceso a la plataforma de GLPI.



Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

8 Bibliografía

TIA 942, Telecommunications Industry Association, Estándar que rige la certificación de datacenters
URL= https://tiaonline.org/products-and-services/tia942certification/ansi-tia-942-standard/
URL= https://en.wikipedia.org/wiki/TIA-942
URL= https://tiaonline.org/942-datacenters/

UPTIME INSTITUTE, Entidad privada que certifica data centers acorde a la TIA-942 y otras practicas propias de la institución.
URL= https://uptimeinstitute.com/

TIA-568
URL= https://en.wikipedia.org/wiki/ANSI/TIA-568

ISO 9001
URL= https://es.wikipedia.org/wiki/ISO_9001
URL= https://www.iso.org/obp/ui/#iso:std:iso:9001:ed-5:v1:es:fn:1

ISO 14001
URL= https://es.wikipedia.org/wiki/ISO_14000
URL= https://www.iso.org/obp/ui#iso:std:iso:14001:ed-3:v1:es

ISO 22301
URL= https://en.wikipedia.org/wiki/ISO_22301
URL= https://www.iso.org/standard/75106.html

COBIT
URL=https://es.wikipedia.org/wiki/Objetivos_de_control_para_la_informaci%C3%B3n_y_tecnolog%C3%ADas_relacionadas
URL= https://www.freshworks.com/es/explore-it/que-es-cobit-definicion-ventajas-y-funciones/

ITIL
URL= https://www.globalsuitesolutions.com/es/que-es-itil-y-para-que-sirve/
URL= https://es.wikipedia.org/wiki/Information_Technology_Infrastructure_Library

GLPI
URL= https://glpi-project.org/es/
URL= https://glpi-user-documentation.readthedocs.io/fr/latest/

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

DGIPED: Dirección General de Innovación Productiva y Economía Digital
DHCP: Dynamic Host Configuration Protocol (Protocolo de Configuración Dinámica de Host)
DIMM: Dual In-Line Memory Module (Módulo de Memoria de Línea Doble)
DINAPI Dirección Nacional de Propiedad Intelectual
DNP: Departamento Nacional de Planeación de Colombia
DNS: Domain Name System (Sistema de Nombres de Dominio)
DR: Disaster Recovery (Recuperación ante Desastres)
DRAM: Dynamic Random-Access Memory (Memoria de Acceso Aleatorio Dinámica)
DSL: Digital Subscriber Line (Línea de Suscriptor Digital)
DWDM: Dense Wavelength Division Multiplexing (Multiplexación por División en Longitudes de Onda Densas)
EAI: Enterprise Application Integration (Integración de Aplicaciones Empresariales)
EAP: Extensible Authentication Protocol (Protocolo de Autenticación Extensible)
EBD Emprendimiento de Base Digital
ECC: Error-Correcting Code (Código de Corrección de Errores)
ECI Entidad consumidora de la información
EDR: Endpoint Detection and Response (Detección y Respuesta de Puntos de Extremo)
EIGRP: Enhanced Interior Gateway Routing Protocol (Protocolo de Enrutamiento de Puerta de Enlace Interior Mejorad
ENCONEC: Estrategia Nacional de Conectividad
EOL: End of Life (Fin de Vida Útil)
EPI: Entidad productora de la información
ERP: Enterprise Resource Planning (Planificación de Recursos Empresariales)
ESXi: Elastic Sky X Integrated (Versión de VMware de su Hipervisor)
FCoE: Fibre Channel over Ethernet (Canal de Fibra sobre Ethernet)
FEEI Fondo para la Excelencia de la Educación y la Investigación
FO: Fibra Óptica
FONTED: Fondo Nacional de Tecnologías en la Educación
FONTIC: Fondo Nacional de Tecnologías de la Información
FTP: File Transfer Protocol (Protocolo de Transferencia de Archivos)
Gbps: Gigabits Per Second (Gigabits Por Segundo)
GDL: Gestor de Documentos en Línea
GPU: Graphics Processing Unit (Unidad de Procesamiento Gráfico)
HBA: Host Bus Adapter (Adaptador de Bus de Host)
HIS: Sistema de Información en Salud
HTTP: HyperText Transfer Protocol (Protocolo de Transferencia de Hipertexto)
HTTPS: HyperText Transfer Protocol Secure (Protocolo Seguro de Transferencia de Hipertexto)
HVAC: Heating, Ventilation, and Air Conditioning (Calefacción, Ventilación y Aire Acondicionado)
I+D+i: Investigación, Innovación y Desarrollo
IA: Inteligencia Artificial
IaaS: Infrastructure as a Service (Infraestructura como Servicio)
IAEE: Instituto de Altos Estudios Estratégicos
ICMP: Internet Control Message Protocol (Protocolo de Mensajes de Control de Internet)
ICT: Information and Communication Technology (Tecnología de la Información y Comunicación)
IDS: Intrusion Detection System (Sistema de Detección de Intrusos)
IDU: Impuesto a los Dividendos y a las Utilidades

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

NVMe: Non-Volatile Memory Express (Interfaz de Memoria No Volátil)
OAuth: Open Authorization (Autorización Abierta)
ODS: Objetivos de Desarrollo Sostenible
ONG: Organización No Gubernamental
OPEX: Operating Expense
OPEX: Operational Expenditure (Gasto Operativo)
OS: Operating System (Sistema Operativo)
OSI: Open Systems Interconnection (Interconexión de Sistemas Abiertos)
OTP: One-Time Password (Contraseña de Un Solo Uso)
PaaS: Platform as a Service (Plataforma como Servicio)
PBX: Private Branch Exchange (Central Telefónica Privada)
PCI: Peripheral Component Interconnect (Interconexión de Componentes Periféricos)
PCI-DSS: Payment Card Industry Data Security Standard (Estándar de Seguridad de Datos de la Industria de Tarjetas d
PDU: Power Distribution Unit (Unidad de Distribución de Energía)
PDU: Protocol Data Unit (Unidad de Datos de Protocolo)
PIB: Producto Interno Bruto
PNC: Plan Nacional de Ciberseguridad
PND: Plan Nacional de Desarrollo
PNT: Plan Nacional de Telecomunicaciones
PNTE: Plan Nacional de Transformación Educativa 2030
PNTIC: Plan Nacional de Tecnologías de la Información y la Comunicación
PROINNOVA: Programa de Innovación en Empresas Paraguayas
QA: Quality Assurance
QoS: Quality of Service (Calidad de Servicio)
RAID: Redundant Array of Independent Disks (Matriz Redundante de Discos Independientes)
RDP: Remote Desktop Protocol (Protocolo de Escritorio Remoto)
RFID: Radio-Frequency Identification (Identificación por Radiofrecuencia)
RIPC: Red Integrada de Infraestructura Pública de Conectividad
RMM: Remote Monitoring and Management (Monitoreo y Gestión Remotos)
RMSP Red Metropolitana del Sector Público
ROE Reglamento Operativo Específico
ROM: Read-Only Memory (Memoria de Solo Lectura)
RPM: Revolutions Per Minute (Revoluciones Por Minuto)
RTC: Real-Time Clock (Reloj en Tiempo Real)
RTO: Recovery Time Objective (Objetivo de Tiempo de Recuperación)
RUE Registro Único del Estudiante
SaaS: Software as a Service (Software como Servicio)
SAN: Storage Area Network (Red de Área de Almacenamiento)
SAS: Serial Attached SCSI (SCSI Conectado en Serie)
SATA: Serial Advanced Technology Attachment (Interfaz de Tecnología Avanzada en Serie)
SDN: Software-Defined Networking (Redes Definidas por Software)
SENAC: Secretaría Nacional Anticorrupción
SENATIC: Secretaría Nacional de Tecnologías de la Información y Comunicación
SET: Subsecretaría de Estado de Tributación

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Contrato Nro 21/2024

Proyecto de Mejoramiento de las Finanzas Públicas para el Desarrollo Sostenible del Paraguay

Contrato de Préstamo N° 4671/OC-PR

"Definición del Plan de Infraestructura Tecnológica"

OBP N° P230707

Plan de infraestructura tecnológica

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

1 Contenido

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

2 Objetivos

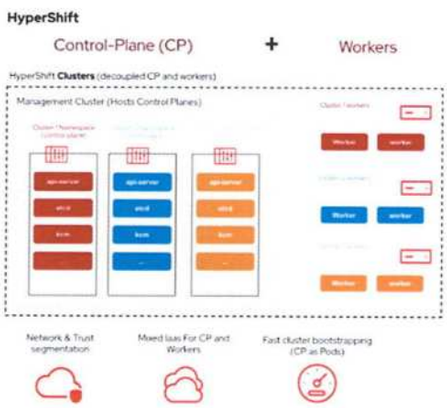
Plan de infraestructura tecnológica, conteniendo recomendaciones mínimas para tener en cuenta para la adquisición de nuevas tecnologías o equipos, y el inventario del Portafolio de Proyectos necesarios para dar continuidad a la transformación del Modelo Tecnológico de la Institución.

Para poder identificar la estructuración del presupuesto debemos tipificar los distintos rubros aplicados a tecnología y como estos impactan dentro del departamento, este presupuesto podemos partirlos hoy en día en las distintas coordinaciones ejecutoras del presupuesto.

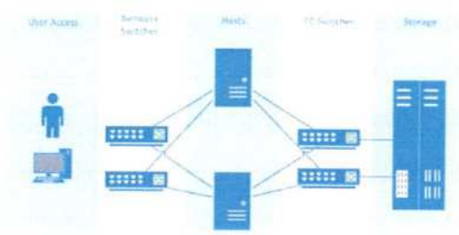
En el caso de este proyecto, la coordinación sobre la cual vamos a poner foco es la de Coordinación de Infraestructura, que hoy en día incluyen redes, operaciones y soporte técnico.

El objetivo de la eficiencia de ejecución del presupuesto es maximizar la ejecución de este minimizando los gastos en cada área, encontrando la mejor propuesta costo económica del mismo.

Tomando los objetivos principales de la DNCP y la herramienta principal que provee todo el servicio del SICP es la infraestructura de RedHat Open Swift



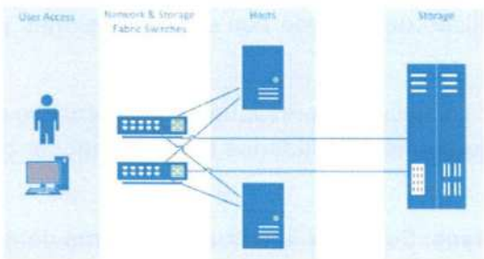
La estructura de red que estamos utilizando en esta etapa es la estructura tradicional donde las capas de red están separadas de las capas de storage, esto fácilmente puede ser observado en la estructura dividida Ethernet de un lado, y Fibre Channel del otro lado, donde cada infraestructura tiene sus respetivos equipos como lo muestra la figura siguiente.



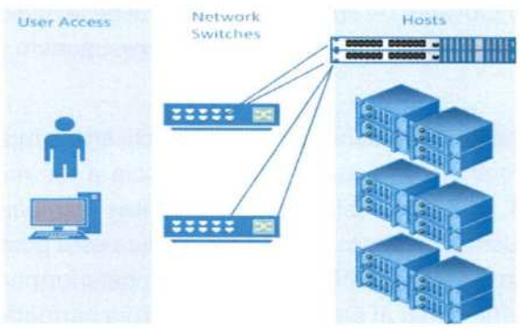
Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Sobre este modelo de arquitectura luego se construyen la arquitectura redundante de switches FC, los equipos redundantes de storage, switches, así como la doble capa de seguridad de firewalls de core y de borde.

Esto nos diferencia de las siguientes estructuras que podríamos estar utilizando, la convergente que la que implementa una capa de Ethernet y FCoE, esta estructura será evaluada a futuro cuando la DNCP empiece a utilizar Centros de datos compartidos públicos o privados donde ya no pueda montar una estructura doble, principalmente los switches FC dedicados.



Y la hiper convergente que es donde hosts/storage se fusionan en una solución hyper escalar, esta ultima solución ya es recomendada en ambientes de gran cantidad de servidores y storages con funcionalidades distintas a una escala de hyper datacenters. En este caso ya todos los servidores potencialmente son contratados como servicio, y la DNCP posee un tenant en dicha infraestructura, el modelado acá es fundamental, ya que permite que la DNCP transparentemente pueda migrarse a cualquier tipo de nube.



Una vez que arrancamos con la estructura tecnológica prácticamente todos los equipos diseñados y seleccionados irán acompañando dicha estructura.

Acorde al Ministerio de Economía y Finanzas y mediante Decreto 3310 se aprobó la vigencia del Plan Financiero 2025, estableciendo las normas y procedimientos para la ejecución del Presupuesto General de la Nación (PGN), aprobado mediante la Ley N° 7408/2024. Este instrumento, elaborado por el Ministerio de Economía y Finanzas (MEF), es esencial para la planificación mensual, distribución y control de los recursos públicos.

El objetivo principal de la ejecución presupuestaria del gobierno de Paraguay es asegurar que los recursos asignados en el Presupuesto General de la Nación (PGN) se utilicen de manera eficiente y efectiva para alcanzar las metas y objetivos establecidos en el plan de desarrollo del

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

país. En otras palabras, se busca optimizar la utilización de los recursos públicos para lograr los resultados esperados.

Plan Financiero: El Poder Ejecutivo aprueba un plan financiero anual para la ejecución del PGN, estableciendo los límites de gasto y asegurando que cada entidad tenga los fondos necesarios para operar de manera eficiente.

Asignación de Recursos: La ejecución presupuestaria implica asignar, comprometer, devengar y pagar el dinero destinado a financiar las actividades y proyectos del sector público.

Control y Seguimiento: Se implementan mecanismos de control y seguimiento para verificar que los recursos se utilicen de acuerdo con las asignaciones y que se logren los objetivos propuestos.

Rendición de Cuentas: La ejecución presupuestaria contribuye a la transparencia y rendición de cuentas, permitiendo que los ciudadanos puedan conocer cómo se utilizan los recursos públicos.

Optimización de Recursos: Se busca la utilización óptima del talento humano, los recursos materiales y financieros asignados en el presupuesto para obtener los bienes, servicios y obras previstos.

3 Proceso de presupuesto compra de suministros

El MEF establece los lineamientos generales para los procesos de programación, formulación y presentación de los anteproyectos de presupuestos institucionales como marco de referencia para la elaboración del proyecto de presupuesto general de la nación (PGN) correspondiente al ejercicio fiscal siguiente y para la programación del presupuesto plurianual de los siguientes tres años.

Para lo cual el equipo de la DNCP tiene vasta experiencia en los mismos, así mismo agregamos los mismos como referencia ya que se hará referencia a los mismos a la hora de evaluar distintos proveedores privados, así como fabricantes nacionales e internacionales. Es importante tener en cuenta los pasos y procesos, ya que esto posteriormente nos afectará en los tiempos requeridos para planificar, diseñar y posteriormente ejecutar los proyectos necesarios para hacer funcionar el área de infraestructura correctamente.

3.1 Procesos del Presupuesto General de la Nación

3.1.1 Lineamientos Generales:

Se establecen las directrices para la programación, formulación y presentación de los anteproyectos de presupuestos institucionales. Esto sirve como marco de referencia para la elaboración del PGN.

3.1.2 Programación y Formulación:

- Se realiza la estimación de ingresos y gastos.
- Se fundamentan los programas y proyectos a incluir en el presupuesto.
- Se justifican los montos programados con base en necesidades institucionales.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

3.1.3 Presentación de Anteproyectos:

- Las instituciones públicas deben presentar sus anteproyectos de presupuesto al Ministerio de Economía y Finanzas.
- Se utilizan formularios específicos, como el Anexo B, que incluye previsiones presupuestarias, planificación de actividades y fundamentación de ingresos.

3.1.4 Evaluación y Ajustes:

- El Ministerio de Economía y Finanzas revisa los anteproyectos y realiza ajustes según las prioridades nacionales y disponibilidad de recursos.

3.1.5 Aprobación Legislativa:

- El PGN es enviado al Congreso Nacional para su discusión y aprobación.
- Se pueden realizar modificaciones antes de su aprobación final.

3.1.6 Publicación y Ejecución:

- Una vez aprobado, el presupuesto se publica y las instituciones comienzan su ejecución conforme a lo establecido.

4 Proceso de licitación pública en Paraguay

Si bien el equipo de la DNCP es experto en el proceso de contrataciones públicas colocamos los pasos para que podamos dimensionar como estos pasos posteriormente se alinean al ciclo de vida de los productos y como deberíamos realizar los llamados y cuáles son las restricciones que tenemos especialmente en el área de la tecnología aplicada a infraestructura, así mismo también entender los ciclos de las distintas áreas y la vida útil de las mismas.

Mientras que el cableado estructurado nos puede durar en exceso de 15 años con poca o ninguna modificación, un antivirus o un XDR o similar nos dura un año y debe ser actualizado periódicamente, todos estos datos deben ser evaluados.

4.1.1 Planificación y Convocatoria:

La entidad pública planifica la necesidad de adquirir bienes o servicios y elabora los términos de referencia o pliegos de bases y condiciones.

Se realiza la convocatoria a licitación pública, anunciando la contratación a través de los medios oficiales y electrónicos designados por la Dirección Nacional de Contrataciones Públicas (DNCP).

4.1.2 Presentación de Propuestas:

Los oferentes interesados presentan sus propuestas técnicas y económicas dentro del plazo establecido.

La presentación de propuestas se realiza de forma electrónica a través de la plataforma de la DNCP.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

4.1.3 Evaluación de Propuestas:

Un comité de evaluación designado por la entidad pública evalúa las propuestas recibidas, verificando el cumplimiento de los requisitos técnicos y económicos.

Se elabora un acta de evaluación con los resultados de la evaluación.

4.1.4 Adjudicación:

La entidad contratante aprueba el procedimiento de evaluación y adjudica el contrato al oferente que haya presentado la mejor oferta.

Se emite un certificado de adjudicación o acto administrativo que formaliza la adjudicación.

4.1.5 Firma del Contrato:

Se procede a la firma del contrato entre la entidad pública y el adjudicatario.

Se puede emitir una orden de compra o servicio, según corresponda.

6. Publicación de la Adjudicación:

La adjudicación del contrato se publica en los mismos medios en los que se anunció la licitación.

Acorde a la normativa vigente de la SET según la LEY 6380/2019 se fijan los tiempos de amortización de los activos fijos, si bien esto es algo más bien contable, es importante tenerlos en cuenta ya que normalmente los bienes se rigen por periodos similares y nos sirven de referencia adicional cual es el uso normal que se le da a estos.

5 Costo total de propiedad (TCO)

El costo total de propiedad, conocido en inglés como TCO (Total Cost of Ownership) el gasto total que una institución realiza en algún tipo de inversión separado en distintos rubros, eso significa que, si una institución desea realizar una inversión, una compra o adquisición de un nuevo bien, la sostenibilidad del mismo debe estar también incluida en el presupuesto, así como el soporte y/o repuestos y en el caso que su ausencia, daño o impacto a terceros pueda generar un riesgo financiero, las garantías y/o seguros correspondientes.

Esto de manera a maximizar el valor y utilización de este a lo largo del tiempo.

Total Cost of Ownership

5.1 Componentes del TCO

El TCO incluye tanto costos directos como indirectos, entre ellos:

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

- **Precio de adquisición:** El costo inicial de compra del activo.

- **Mantenimiento y soporte:** Gastos recurrentes para mantener el activo en funcionamiento.

- **Capacitación:** Costos asociados a la formación del personal para el uso del activo.

- **Consumo de recursos:** Energía, insumos y otros costos operativos.

- **Depreciación:** Pérdida de valor del activo con el tiempo.

- **Costos de actualización o reemplazo:** Inversiones necesarias para mantener la funcionalidad del activo.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Para evaluar el portafolio de proyectos debemos tener en cuenta los siguientes factores:

- Recursos humanos
- Trabajos y capacidad interna
- Servicios
- Subscripciones
- Soporte
- Software
- Hardware

El equipo de la Coordinación de Infraestructura está dividido en tres equipos, el departamento de redes, el departamento de operaciones y el departamento de soporte técnico.

De esos dos, los departamentos que pertenecen a la estructura tradicional son los dos primeros, mientras que el departamento de soporte técnico debería ser la puerta de entrada a todas las otras áreas.

Una vez que hemos determinado los bienes o servicios que deseamos adquirir es importante que tengamos en dos factores principalmente, uno de estos es el proceso general de un llamado a licitación y el segundo es el ciclo de vida del producto que deseamos adquirir.

El equipo humano es reducido pero muy capaz, el gran desafío que tiene la DNCP es preparar la operativa para un servicio 24/7 ya que, así como muchos otros OEE mucho del servicio cae sobre los hombros de personas que sacrifican tardes, noches y fines de semana cubriendo la operación. Así como vamos hacía un Gobierno Digital, también debemos dar a nuestros recursos las herramientas para poder tener continuidad operativa sin que esto afecte gravemente las vidas de nuestros recursos críticos.

Un tentativo de lo que podría ser un escalafón para el área de tecnología es el siguiente.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Nivel	Nombre del rol	Perfil típico	Responsabilidades generales
N1	*Técnico Junior / Help Desk / Operador NOC*	Formación básica, atención de 1er nivel, turnos rotativos	Atención de tickets simples, monitoreo básico, escalamiento de incidentes
N2	*Técnico Senior / Analista / Soporte Especializado*	Certificaciones técnicas, experiencia operativa	Resolución de incidentes complejos, scripting, análisis de causa raíz, configuración avanzada
N3	*Ingeniero / Administrador de Plataforma / DBA / NetOps*	Expertise en área (redes, sistemas, DB, seguridad), análisis de diseño	Gestión avanzada, automatización, tuning de performance, documentación de procedimientos
N4	*Arquitecto / Líder Técnico / Coordinador de área*	Visión cross-tecnológica, diseño y gobernanza	Planificación de capacidades, arquitectura, estandarización, revisión de SLA y procesos
N5	*Gerente de Producción / Jefe de Operaciones / CTO Adjunto*	Liderazgo, compliance, estrategia IT	Gestión de equipos, análisis TCO, continuidad operativa, cumplimiento de ISO 27001/9001

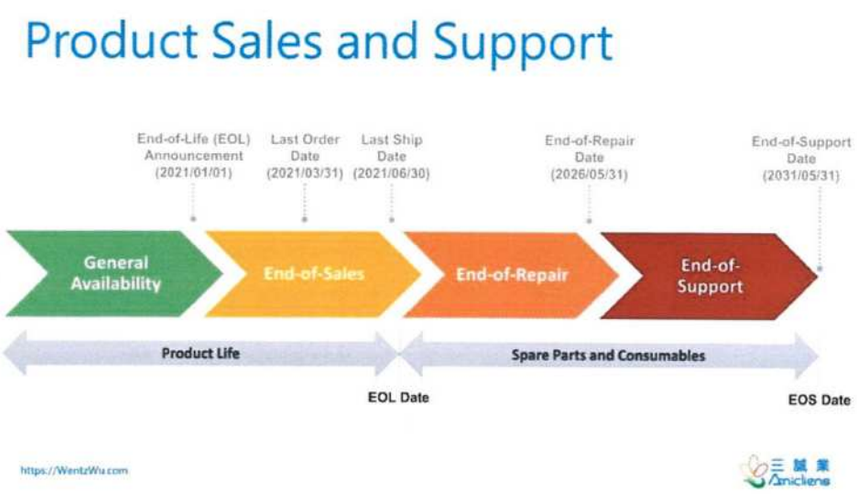
Los turnos que debería tener el proveedor:

Turno	Horario	Duración	Características clave
Turno A	06:00 – 14:00	8 h	Inicio de operaciones, mantenimiento, coordinación con áreas administrativas
Turno B	14:00 – 22:00	8 h	Cierre del día, tareas técnicas, soporte vespertino, preparación de respaldos
Turno C	22:00 – 06:00 (+1)	8 h	Turno nocturno, foco en monitoreo, alertas, contingencias y eventos automatizados

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

6 Ciclo de vida de los productos

Para entender la mecánica de los bienes y servicios asociados a la operativa debemos comprender como se comportan dichos bienes y entender el ciclo de vida de estos, estos nos ayudan a determinar los tiempos de cada llamado para la compra muchos de estos llamados pueden o no estar alineados con los ciclos contables establecidos por la SET. Pero mayormente nos sirven de referencia para entender como algo en el mercado tiene su equivalencia en la contabilidad. Si bien el estado se enfoca más en la operación y la gestión, estos conceptos de depreciación nos ayudan a entender la vida útil de cada bien. Adjuntamos un cuadro de revaluo a manera de referencia explicación de dichos procesos. ANEXO I



Cada fabricante y tipo de producto maneja una terminología acorde al lenguaje y la región, estas son las más comúnmente utilizadas y elaboraremos sobre las mismas para entender como nos afecta en la planificación del presupuesto que estamos diseñando para la entidad.

Estos ciclos son muy importantes a la hora de definir o decidir sobre la compra de un producto dentro de un proceso de licitación, así como cuando vayamos a definir los plazos requeridos para que dichos equipos puedan brindar un correcto servicio para lo que fue adquirido/contratado.

6.1 EOL (End-of-life) Fin de vida,

Indica que el producto ha llegado al final de su ciclo de vida y ya no se fabricará ni venderá. Puede seguir recibiendo soporte limitado, como parches de seguridad, pero no nuevas características.

El tiempo de vida o EOL incluye los siguientes tiempos adentro

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

1- El tiempo general de vida del producto.
2- El tiempo hasta cuándo se puede realizar el **ULTIMO PEDIDO DE COMPRA**
3- El tiempo donde se realiza el **ULTIMO EMBARQUE**

En términos licitatorios es fundamental que las especificaciones técnicas que estamos diseñando estén alineadas con los productos en el mercado y sus ciclos de vida, más presentamos ejemplos para que se entienda como esto nos puede afectar en una licitación. Es fundamental desde que se diseñan las EETT.

Los escenarios que nos pueden pasar si sobrepasamos los tiempos de compra son los siguientes:

6.2 EoS (End of Sale) fin de compra.

Este escenario el producto sigue vigente, con soporte, servicios, contratos y actualizaciones, pero ya no se puede comprar, y se marca el último embarque para los pedidos que fueron cargados con anterioridad, los cuales serán fabricados hasta momentos antes de la última fecha de embarque.

El tiempo de End of Sale incluye los siguientes tiempos.

1- Plazo para colocar la última orden de compra.
2- Periodo durante que la marca va seguir teniendo abierta una línea de producción para el equipo marca y modelo que estamos buscando.
3- Periodo donde los repuestos se encuentran en alta disponibilidad.
4- Se acerca la fecha del último embarque, que ocurre posteriormente a la última fabricación.
5- Las líneas de proveedores, componentes y partes de dichos equipos están cerrándose.
6- Fabrica o producto podría estar cambiando, mudándose de lugar, o dejando de existir.

6.3 EOS (End-of-support) Fin Soporte

El siguiente escenario que nos encontramos en el tiempo de vida de un producto es fin del soporte de este, marca el punto en el que el producto deja de estar disponible para la compra. Sin embargo, los clientes existentes pueden seguir recibiendo soporte según la política del fabricante.

Dentro del End-of-support entran varios tiempos

1- End of Repair, fin del periodo de reparaciones
2- End-of-RMA fin del retorno de mercaderías (Return Merchandise Authorization)
3- End-of-NSS fin de nuevas actualizaciones de software.
4- EoSCR fin del contrato de soporte y/o garantías

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

6.4 EoRMA (End-of-RMA) Fin RMA

Indica que el fabricante ya no aceptará devoluciones ni reemplazos del producto bajo garantía. Este plazo es conocido como "Periodo de envío y/o devolución por defectos de fabrica" . El RMA es la herramienta que usa el representante local para realizar las devoluciones o envíos a fabrica debido a defectos o para reparación de estos. En la mayoría de los casos el equipo es reemplazado en su totalidad si se trata de plataformas enteras, en caso de que solo sean componentes o módulos fallidos, estos podrían ser remplazados y el equipo completo retornado al cliente. Los plazos están asociados directamente a la ubicación del proveedor y pueden demorarse meses. Existe gastos adicionales en el RMA tales como logística, así como importación que deben tenerse en cuenta.

6.5 EoNSS (End of New Software support) Fin actualizaciones software

Se refiere al momento en que el producto deja de recibir nuevas versiones de software, aunque aún pueda recibir soporte técnico. En algunas plataformas este periodo puede ser extenso, por ejemplo actualizaciones de Windows XP que duraron prácticamente 12 años, o más corto en el caso de un Firewall, este periodo es fundamental tener en cuenta por que además del EOL, extiende el tiempo de vida de uso hardware y de software dándole mayor provecho a los mismos. Si bien un software puede que ya no se venda más, pero puede que todavía cumpla con los requisitos técnicos para los cuales ha sido adquirido, si sigue actualizándose y vigente con compatibilidad a nuevas herramientas, o las que estamos utilizando, puede que sirva

6.6 EoSCR (End of Support Contract Renewal) Fin renovación de soporte

Marca el punto en el que los clientes ya no pueden renovar contratos de soporte para el producto, esto es importante tener en cuenta ya que por sobre ese limite la Marca ya no garantiza la asistencia o servicio a un producto, y dentro de su plan estratégico los recursos y capacitaciones están siendo asignados a nuevas plataformas. Detrás del contrato de soporte caen varios elementos.

- RMA
- Actualizaciones
- Creación de Tickets
- Garantías
- Repuestos
- Parches

6.7 EoTS (End of Technical Support) Fin de soporte

Señala el fin de cualquier tipo de asistencia técnica para el producto, este es el punto crítico para un representante donde ha descontinuado completamente el producto y ya no lo consideran parte de su cartera, no se hará ningún esfuerzo en mantenerlo de ninguna manera y más allá de este límite solo dependemos de lo que tengamos en stock.

La alternativa para hardware critico en esta situación es la compra de equipos de repuestos o

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

La alternativa para software critico en esta situación es contratación de desarrolladores propios expertos asignados a la operación y mantenimiento. Y adicionalmente la adquisición del código fuente si es posible.

7 Escenarios

7.1 Se supera el EOL

Realizamos con las EETT de un proyecto o proceso anterior o de equipos que anteriormente funcionaban perfectamente para las necesidades de la entidad, el equipo que especificamos estaba en sus últimos tiempos de EOL, los bienes solicitados han sido reemplazados con nuevos modelos o ya no se fabrican. Ningún proveedor cumple, o tiene equipos equivalentes dentro del pack, o debe ofrecer soluciones sobredimensionadas. O peor aún, presentan ofertas con equipos EOL que posiblemente no cumplan con las garantías ni soporte adicional requerido.
Solución: Ese escenario requiere reescribir por completo las EETT.

7.2 Se supera el EoS

Se termina el proceso licitatorio con adjudicación, pero la emisión de orden de servicio supera el tiempo del último pedido de compra, la fábrica ya no va a aceptar pedidos y se debe evaluar alternativas.
Solución: Se debe emitir una nota de fuerza mayor y llegar a un acuerdo de nuevas especificaciones si el pliego lo permite.

7.3 EOL, EoS vigente, pero proyecto de larga duración

Se adjudica, pero la orden de servicio depende de obras civiles y/u otros proyectos que deben ser terminados con anterioridad, se ha cargado la propuesta, pero la orden de servicio se emite posterior al último embarque. La acción preventiva ante esta situación es lastimosamente elegir el equipo más nuevo, que permita esperar todo el periodo de la obra civil o proyecto a ejecutarse.
Solución: Se debe emitir una nota de fuerza mayor y llegar a un acuerdo de nuevas especificaciones si el pliego lo permite.

7.4 EOL, EoS vigente, durante licitación, pero se supera el EOS

El proyecto está vigente y corriendo con EOL y EoS vigentes, pero es posible que la duración del proyecto mismo nos lleve a que el soporte deje de estar vigente en el transcurso de este, lo más probable es que no se pueda tener RMA (reemplazos vía garantía) y/o a veces, actualizaciones de software si es que el EoNSS (actualización de software) es superado
Solución: Este escenario nos lleva a evaluar que tipo de equipo es el propuesto, si son equipos de SEGURIDAD, los mismos deben ser reemplazamos lo antes posible, si son equipos OPERATIVOS, switches, almacenamiento, servidores, que no estén expuestos

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

al exterior o con bugs o defectos conocidos, estos pueden continuar operando siempre y cuando se tengan sistemas de redundancia ante fallos.

7.5 EoNSS expirado, se desea ampliar soporte

En caso que el caso que haya sobrepasado el límite de las actualizaciones de software lo primero que se debe evaluar es si la versión actual es "estable" lo cual nos indica que es una versión ya verificada y sin fallas, en el caso de hardware tradicional esto es posible, switches, ruteadores, almacenamiento, FC Fabrics, CCTV todas pueden llegar a un nivel donde no se requiere modificación alguna en su funcionalidad, así que las actualizaciones son irrelevantes, ahí estaremos ya jugándonos contra el MTBF natural del hardware que ocurren ya por desgaste en la electrónica o problemas físicos externos, calor, humedad, polvo, etc.

Solución: Si el equito es hardware estable y no está en una ubicación crítica (CORE) se lo deja funcionando y se prevee los equipos de repuestos en caso de falla.

Si el equipo se encuentra en una ubicación critica, se lo migra a una no critica para seguir haciendo uso del mismo, y se reemplaza por un equipo más nuevo para mitigar el impacto de fallas.

Si el equipo es de seguridad o está expuesto a terceros (interne, proveedores, etc) el mismo debe ser sacado de producción lo antes posible.

Si el equipo es de uso personal, pero asistido o protegido por otras plataformas de seguridad XDR, Crowdstrike, PaloAlto, etc, entonces se asegurar que el equipo esté en una zona segura, o se lo blinda completamente por ejempo si son controladores viejos.

O si pertenecen a plataformas que no se pueden actualizar directamente debido a herramientas legacy, jboss, tomcat, bases de datos con código a la medida, versiones de Windows user o server anteriores, Linux o sus variantes, se ve que se pueda construir un front end de protección que lo blinde de acceso directo.

7.6 Ejemplo 1: EETT Equipo Wifi

En este caso presentamos las EETT potenciales para una licitación de equipos para una solución wifi de baja escala.

Tipo: Router.
Router Tipo de conectividad: Ethernet.
Velocidad de transmisión inalámbrica: 300Mbps.
Velocidad del puerto Ethernet: 10 / 100Mbps.
Protocolos de red: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g.
Estándar inalámbrico: Inalámbrico AC.
Seguridad inalámbrica: WPA-PSK, WPA2-PSK.
WiFi Distancia: 10 metros.
LAN Puertas: 2 puertas.
Máx. Velocidad de datos de LAN: 300 Mbps.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Observación: A simple vista este equipo puede proveer un servicio más que suficiente para una oficina pequeña, pero este escenario va presentar los siguientes desafíos.

- Puertos 10/1000Mbps ya en desuso, los switches ya no vienen para esas velocidades.
- Seguridad WPA que no tenga AES de fácil quiebre.
- IEEE 802.11a, IEEE 802.11b, IEEE 802.11g. corresponden a WIFI 4, limites de frecuencia y velocidad aplican.

7.7 Ejemplo : EETT Equipo Firewall

GE RJ-45/SFP=	2
GE RJ45 internals	6
IPS Throughput=	1.4 Gbps
NGFW Throughput=,	1 Gbps
Threat Protection Throughput=	900 Mbps
System Performance	
Firewall Throughput (1518 / 512 / 64 byte UDP packets)=	10/10/7 Gbps
Firewall Latency (64 byte UDP packets)=	3.23 µs
Firewall Throughput (Packets Per Second)=	10.5 Mpps
Concurrent Sessions (TCP)=	1.5 Million
New Sessions/Second (TCP)=	45,000
Firewall Policies=	5,000
IPsec VPN Throughput (512 byte)=	6.5 Gbps
Gateway-to-Gateway IPsec VPN Tunnels=	200
Client-to-Gateway IPsec VPN Tunnels=,	500
SSL-VPN Throughput=	950 Mbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)=	200
SSL Inspection Throughput (IPS, avg. HTTPS)=	715 Mbps
SSL Inspection CPS (IPS, avg. HTTPS)=	3 700
SSL Inspection Concurrent Session (IPS, avg. HTTPS) =	100,000
Application Control Throughput (HTTP 64K)=	1.8 Gbps
CAPWAP Throughput (HTTP 64K)=	9 Gbps
Virtual Domains (Default / Maximum)=	10 / 10
Maximum Number of FortiSwitches Supported=	16
Maximum Number of FortiAPs (Total / Tunnel Mode)=	96 / 48
Maximum Number of FortiTokens=	500
High Availability Configurations=	Active / Active, Active / Passive,
Clustering	

Observación: Este es un caso más complejo de evaluar ya que si bien las EETT son razonables, estas corresponden a un equipo **FORTIGATE 80F** el cual es en si un equipo muy bueno, pero si buscamos la matriz de productos de Fortinate ,ANEXO II vemos que un equipo más pequeño, pero de nueva generación el **FORTIGATE 70G** tiene mejores especificaciones técnicas, además de ser más nuevo, EOL y EOS más extenos, esto suele ser normal en los fabricantes donde los mismos tienen familias de equipos y generaciones de equipos, y cada nueva generación es mucho más potente que la anterior. Las generaciones se miden con letras o números, en el caso de FORTIGATE se miden con letras A, B, C, D, E, F, G y las familias se miden con números, 30, 40, 50, 60, 70, 100, 200, 400 etc. Colocamos debajo el cuadro comparativo donde ampliamente un 70G supera a un 80F, excepto en algunas limitaciones tales como IP SEC tunnels, que difícilmente estemos montando 2500 de ellas, pero igualmente debe ser evaluado.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

	FG/FWF-70G	FG/FWF-80F
Firewall Throughput (1518/512/64 byte UDP)	10 / 10 / 10 Gbps	10 / 10 / 7 Gbps
IPsec VPN Throughput (512 byte) [1]	7.1 Gbps	6.5 Gbps
IPS Throughput (Enterprise Mix) [2]	2.5 Gbps	1.4 Gbps
NGFW Throughput (Enterprise Mix) [2,4]	1.5 Gbps	1 Gbps
Threat Protection Throughput (Ent. Mix) [2,5]	1.3 Gbps	900 Mbps
Firewall Latency	2.46 µs	3.23 µs
Concurrent Sessions	1.4 Million	1.5 Million
New Sessions/Sec	100 000	45 000
Firewall Policies	5 000	5 000
Max G/W to G/W IPSEC Tunnels	200	200
Max Client to G/W IPSEC Tunnels	500	2,500
SSL VPN Throughput	—	950 Mbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	—	200
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	1.4 Gbps	715 Mbps
Application Control Throughput (HTTP 64K) [2]	3.6 Gbps	1.8 Gbps
Max FortiAPs (Total / Tunnel)	96 / 48	96 / 48
Max FortiSwitches	24	24
Max FortiTokens	500	500
Virtual Domains (Default/Max)	10 / 10	10 / 10
Interfaces	10x GE RJ45	8x GE RJ45, 2x Shared Port Pairs
Local Storage	64 GB (71G)	128 GB (81F)
Power Supplies	Single AC PS	Single AC PS, dual inputs
Form Factor	Desktop	Desktop
Variants	WiFi, POE	WiFi, 3G4G, DSL, Bypass, Storage

7.8 Ejemplo : EETT Storage Fibre Channel

Compra de switch Fibre Channel con sus distintas tecnologías, en este caso el propio fabricante indica que el equipo está activo en su ciclo de vida

Lifecycle Active
Access Gateway Supports
Bandwidth 2 Tb/s
Certified Maximum 6,000 active nodes; 56 switches, 19 hops in Brocade Fabric OS® fabrics; larger fabrics certified as required
Fibre Channel Performance Fibre Channel: 4.25Gb/s line speed, full duplex; 8.5Gb/s line speed, full duplex; 10.53Gb/s line speed, full duplex; 14.025Gb/s line speed, full duplex; 28.05Gb/s line speed, full duplex; auto-sensing of 4/8/10/16/32G port speeds; 10 Gb/s optionally programmable to fixed port speed. Auto-sensing of 4×32/4×16/4×8/4×4G speeds on the QSFP ports with Brocade FOS v8.2.0
FICON Support Supports
Frame Based ISL Trunking 256Gb/s frame-based trunk (optional)
Power Text 205W, dual hot-swappable power supplies
Size (mm) 440(W) x 43.9(H) x 355.6(D)
Total Line Rate Ports 24 to 64 @ 32G

Observación: En el caso de equipos con tecnologías retrocompatibles como lo es FC, lo único que tenemos que asegurarnos que es el equipo nuevo tenga igual o mayor velocidad que los equipos actualmente utilizados. Eso si, la transferencia siempre será limitada a la del equipo más lento en la cadena FC y sus tecnologías de storage.

Por ejemplo, un DISCO duro HDD no supera los 200 MB/s, que son equivalentes a un 1800Mb/s, o sea funciona tranquilamente con un FC 4Gbps, así mismo si compramos un SSD a 3000MB/s que son equivalentes a 24000Mb/s requiere por lo menos un FC a 32Gbps para poder sacarle

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

beneficio correctamente, y eso sin tener en cuenta las configuraciones RAID que crean bundles para mayor almacenamiento o mayor velocidad.

8 Observaciones de CAPEX y OPEX

Para el efecto y poder evaluar correctamente lo que nos pide el MEF debemos tener en cuenta dos conceptos principales, el CAPEX o inversiones en sistemas e infraestructura, así como el OPEX, los gastos necesarios para sostener exitosamente nuestra operación, si bien una institución pública no se maneja directamente con estos dos conceptos, es importante entender que uno representa gastos puntuales o asignados a algo nuevo, y el otro representa el gasto operativo recurrente posterior a la inversión.

8.1 CAPEX (Capital Expenditures):

Son los gastos de capital destinados a la adquisición, mejora o mantenimiento de activos a largo plazo. En una institución pública, esto puede incluir la construcción de edificios gubernamentales, la compra de equipos tecnológicos, la implementación de infraestructura de transporte o la inversión en sistemas de seguridad. Estos gastos suelen requerir aprobación presupuestaria y tienen un impacto en el patrimonio de la entidad.

8.2 OPEX (Operational Expenditures):

Son los gastos operativos recurrentes necesarios para el funcionamiento diario de la institución. Esto abarca costos como salarios de empleados públicos, mantenimiento de instalaciones, servicios públicos, suministros administrativos y contratos de servicios externos. A diferencia del CAPEX, estos gastos se reflejan directamente en el presupuesto anual y no generan activos a largo plazo.

Para el efecto de análisis de presupuesto realizamos la evaluación por cortes.

Servicios: Contratos de prestación de servicios para realizar la operación, mantenimiento de servicios recurrentes los cuales no son misionales para la institución y no tienen un riesgo de ser delegados a terceros siempre y cuando cumplan con los requisitos de seguridad y operación delineados por la institución.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9 Inventario del portafolio de proyectos

9.1 Servicios: Operación y Mantenimiento

Dentro de este lote incluimos aquellos proyectos asociados a mantener la funcionalidad de las plataformas, las

9.1.1 Mantenimiento de aires de precisión del datacenter principal y el alternativo

El ultimo aire comprado data de la Licitación 446121 - ADQUISICION DE AIRES DE PRECISION Y UPS PARA EL DATACENTER ALTERNATIVO POR SBE - SEGUNDO LLAMADO, adjudicado 22/12/2023 con una duración de 12 meses (VENCIDO) pero por el momento manejado mediante otro contrato.

Todo este proceso debe ser subcontratado ya que no es misional para la DNCP.

Unidad Interior

a. Revisión y lubricación de turbinas y rodamientos.
b. Revisión y limpieza de filtros de aire, y cambio de los mismos mínimamente 2 veces durante el periodo del contrato.
c. Verificación de sistema de cañerías.
d. Limpieza de partes.
e. Reapriete de borneras de conexión.
f. Verificación y limpieza de las cañerías de desagüe.
g. Limpieza de la bandeja del humidificador.
h. Lectura de parámetros y reseteo de alarmas si los hubiere

Unidad exterior.

a. Verificación, limpieza y lubricación de rulemanes
b. Revisión de motores de ventiladores.
c. Limpieza de serpentinas
d. Reapriete de borneras de conexión
e. Limpieza de partes
f. Revisión de recorrido de cañerías y su correcta fijación.
g. Reposición de la aislación de rubatex si fuera necesario
h. Verificación de presión de Gas: ALTA y BAJA.
i. Reposición de gas refrigerante si fuera necesario
j. Verificación de funcionamiento del regulador de velocidad de cada condensador.

Servicio de Mantenimiento general para cada equipo.

a. Verificación de funcionamiento de unidades.
b. Chequeo del funcionamiento Secuencial de las Unidades.
c. Pruebas de funcionamiento de cada unidad.
d. Verificación y medición de temperatura de aire en los equipos, tanto inyección de aire de cada unidad como retorno de estos.

9.1.2 Mant. UPS DC principal, alternativo y UPS de puestos de trabajo

Este contrato se está llevando por la 445958 - Mantenimiento de UPS Datacenter Principal, la cual incluye las tareas y los elementos a ser operados, tiene una vigencia de 14 meses a partir de la adjudicación el 20-08-2024, y estarán cubiertos todo el

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

2025, este llamado debería empezar Q3 2025 para poder tener un proveedor listo para el 2026.

Este mantenimiento cubre las dos UPS principales

Marca	Modelo	Número de Serie
Liebert Vertiv	EXS	2101201915219A010009
Liebert Vertiv	EXS	2101201915219B050002

Los bienes y servicios incluidos en el mantenimiento son los siguientes

ÍTEM DESCRIPCIÓN DEL BIEN/SERVICIO
1. Asistencia técnica in-situ a pedido de la contratante
2. Módulo de potencia de 30kW
3. Mano de obra por cambio de módulo de potencia
4. Módulo de Control
5. Mano de obra por cambio de módulo de Control
6. Baterías homologadas CSB de 12V-9Ah (96unid)
7. Mano de obra por cambio de baterías de la UPS
8. Filtro de aire
9. Mano de obra por cambio de filtro
10. Llave termomagnética 3x100A
11. Mano de obra por cambio de llave 3x100A
12. Contactor de 65A
13. Mano de obra por cambio Contactor de 65A
14. Llave termomagnética 3x50A
15. Mano de obra por cambio de llave 3x50A
16. Protector de sobretensión DPs 20KA
17. Mano de obra por cambio de protector de sobretensión DPs 20KA
18. Llave termomagnética 3x125A
19. Mano de obra por cambio de llave termomagnética 3x125A

ITEM DESCRIPCION
Servicio de Mantenimiento Específicos para cada equipo.

- Verificación de estado de la carcasa.
- Lectura de Temperatura a la entrada del equipo.
- Lectura de Humedad Relativa a la entrada del equipo.
- Lectura de Temperatura de la Batería Interna.
- Lectura de Temperatura de la Batería Externa.
- Limpieza de la carcasa.
- Limpieza de las placas.
- Limpieza y lubricación de Coolers.
- Verificación y Ajuste de Bornes de conexión de entrada y salida
- en el equipo.
- Verificación y Ajuste de Bornes de entrada y salida en Tablero
- Eléctrico.
- Limpieza de Bornes de entrada y salida en el equipo.
- Verificación de Cableado Eléctrico de entrada y salida del
- equipo.
- Lectura de valores de Tensión de Entrada.
- Lectura de valores de Corriente de Salida.
- Calibración de Tensión de Salida.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

- Chequeo y calibración de cargador de baterías.
- Verificación de Tiempo de Autonomía.
- Chequeo y calibración de cargador de baterías.
- Medición y control de baterías.
- Verificación de Registros.
- Verificación de Firmware.

Pruebas de funcionamiento

- Funcionamiento Modo En Línea.
- Funcionamiento Modo Batería.
- Funcionamiento Modo Bypass Interno.
- Funcionamiento de Bypass Externo.
- Horario de
- trabajo
- Las tareas de mantenimiento preventivo serán coordinadas con el
- administrador de contrato o área requirente, vía mail o teléfono,
- dentro del horario de lunes a viernes de 08:00 a 16:00 hs, en el Edificio
- Principal de la DNCP.
- Informes

El oferente que resulte adjudicado deberá presentar un informe de los equipos con registros de los valores que arrojen la verificación de cada tarea de mantenimiento solicitado en las especificaciones, además se deberán registrar los números de serie de los mismos, el estado de funcionamiento de cada equipo y también se deberán registrar todos los eventos y actuaciones a las cuales fueron sometidos los equipos durante los trabajos de mantenimiento. Este informe será entregado al administrador de contrato y/o área requirente y tendrá un plazo de 2 días hábiles posterior a cada servicio de mantenimiento preventivo entregado.

9.1.3 Mant. UPS DC principal, alternativo y UPS cambio de batería

Los cambios de batería fueron cubiertos con la Licitación 419637 - CAMBIO DE BATERIAS PARA UPS, en este caso la licitación ordinaria corresponde a las baterías actualmente vigentes, se recomienda una periodicidad de 2 años, previo al llamado se debe realizar un estudio de carga y descarga que se debe incluir dentro del proceso de mantenimiento.

Ítem 1: Mantenimiento de UPS

Desarme del equipo, limpieza interna de partes y componentes
Cambio de las Baterías
Verificación de placas.
Verificación de cargador de baterías.
Pruebas de funcionamiento

Ítem 2: Provisión de 80 Baterías

Características del Equipo y Baterías
Marca UPS: RIELLO
Modelo UPS : MST
Cantidad de Baterías: 80 (ochenta).
Las baterías deben tener una garantía 12 meses posterior a la instalación.
Las baterías que deberán ser provistas deben ser de 12V, entre 33AH y 40AH.
Las baterías deben ser selladas sin mantenimiento.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Los bancos de baterías contienen 4 bandejas cada uno y las dimensiones de las bandejas donde se alojarán las baterías son: ancho 45 cm., largo 67 cm. alto 23 cm. El oferente deberá tener en cuenta estas dimensiones para el alojamiento de las baterías.

9.1.4 Servicio De Helpdesk / soporte, operaciones y redes

Este servicio actualmente está siendo cubierto por el ID 428251 - SERVICIO DE HELPDESK SOPORTE TECNICO, OPERACIONES Y REDES con una vigencia de 18 meses, este estipula la asignación de 4 recursos

Técnico I Soporte Técnico	2	3.500.000
Técnico II – Soporte Técnico	1	5.840.000
Técnico II – Operaciones	2	5.840.000
Técnico I – Redes	1	3.500.000

Este llamado está siendo utilizado por la DNCP, la sugerencia es que preparen los llamados basados en **múltiplos del salario mínimo** que les permita realizar los llamados de forma más rápida utilizando los mismos documentos, ya que sino agrega un retraso innecesario en el proceso, como todas las funciones no son misionales pueden subcontratadas y/o delegadas a terceros.

Observaciones:

- Es importante tener en cuenta que muchos de estas personas son contratados en forma temporal, se puede tener mejor rentabilidad si se extiende a 36 meses, ya que el personal tiene mayor estabilidad.
- Así mismo se pueden contemplar aumentos progresivos acorde a índice de inflación.
- Adicionalmente se debe armar un plan de carrera y/o mejoras salariales de los roles en caso de que se desea tener continuidad y generar un plan de carrera que permita mayor estabilidad operativa.
- Estos roles deben ser cargados en la matriz de descripción de cargos.

9.1.5 Servicio técnico horas hombre para servicio de red

Este servicio fue estudiado y ampliado a que cubra funciones de monitoreo NOC 24x7, esto es fundamental para una operación como la DNCP que recibe solicitudes de todas las OEE y las entidades privadas llevando un proceso licitatorio. Para el efecto hemos evaluado varios pliegos similares de otras entidades con un servicio similar.

En principio se está evaluando el Monitoreo 24/7 y este debe integrarse a todo el ecosistema.

1. Cobertura del monitoreo

- Infraestructura crítica: UPS, generadores, aire acondicionado, sistemas de detección/extinción de incendios.
- Red y conectividad: switches, routers, firewalls, balanceadores de carga.
- Sistemas y aplicaciones: servidores físicos, máquinas virtuales, servicios en la nube.
- Seguridad: eventos de WAF, IDS/IPS, logs de acceso físico/lógico.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

2. Plataforma de monitoreo unificada

- Selecciona herramientas que permitan monitoreo en tiempo real, alertas proactivas y dashboards consolidados. Herramientas como Zabbix, Graylog o Elastic APM pueden integrarse para una vista completa de eventos, rendimiento y logs.

3. Gestión de alertas y correlación de eventos

- Define umbrales y reglas para evitar falsos positivos.
- Implementa correlación de eventos para detectar incidentes complejos y reducir el ruido.
- Considera herramientas tipo SIEM que integren monitoreo con análisis de seguridad.

4. Procedimientos operativos normalizados (SOPs)

- Protocolos para notificación, escalamiento y respuesta ante incidentes.
- Integración con tu plataforma de tickets (como GLPI) para trazabilidad.
- Versionado y control documental alineado con ISO 9001 e ISO 27001.

5. Monitoreo continuo de SLA

- Establece métricas de disponibilidad y tiempo de respuesta.
- Incluye mecanismos de auditoría para cumplimiento de SLA internos y externos.

6. Cobertura humana

- Turnos rotativos o esquema "follow the sun" para presencia continua.
- Capacitación del personal en gestión de incidentes, herramientas de monitoreo y seguridad.

7. Capacidad de resiliencia

- Redundancia geográfica de nodos de monitoreo.
- Almacenamiento de logs fuera del sitio principal.
- Testing periódico de alertas, failovers y planes de contingencia.

8. Reportes y análisis predictivo

- Dashboards históricos y tendencias.
- Análisis de causa raíz (RCA) de fallas e identificación de patrones.

9.1.6 Servicio De Impresión, Fotocopiado Y Help Desk

Este servicio está vigente y corriendo vía Licitación 460196 - SERVICIO DE IMPRESIÓN Y FOTOCOPIADO SEGUNDO LLAMADO – AD REFERENDUM, fecha 10/02/2025, se encuentra vigente

Es importante tener en cuenta que este contrato debe ser sobre cantidad de impresiones mensuales y todas las tareas y controles mensuales para la emisión de las hojas de servicio deben ser cargadas en el GLPI, este contrato no pertenece al área de infraestructura.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

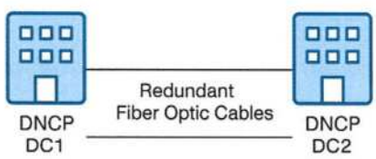
9.1.7 Servicio de internet alternativo para SICP

Este servicio se está cubriendo por la Licitación 438784 - CONTRATACIÓN DE SERVICIO DE INTERNET ALTERNATIVO PARA EL SICP - AD REFERENDUM, adjudicado el en este caso ya se están agregando funcionalidades de protección de ataques volumétricos del tipo DDoS, 80 Mbps y 220 Mbps entregado por 12 meses en interfaces GE y con peer de protocolo BGP. Estos a la larga para optimizar la eficiencia de servicios se debe realizar con múltiples ítems balanceando la carga total y aumentando los enlaces redundantes.

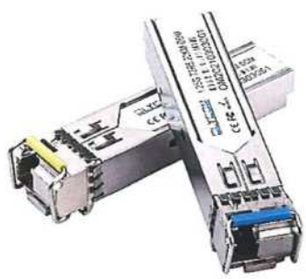
La DNCP debería terminar teniendo dos o tres proveedore más además de COPACO, esto les va a permitir tener mayor disponibilidad y velocidad de respuesta en la red.
Para el llamado 2026 se debe evaluar el consumo y distribuir la carga de 80 y 200 Mbps, verificar si se requiere incremento y distribuirla entre varios proveedores.

9.1.8 Enlaces de Fibra OPTICA entre DC 1 y DC 2

A la par que vamos aumentando los servicios la criticidad y otros la DNCP deberá evaluar el uso de los pelos de fibra de cada camino redundante.



Para equipos Ethernet, lo recomendado siempre es usar interfaces SFP 1G o SFP + 10G o más que soporten el uso de la fibra óptica en forma bidireccional, esto nos ahorra la mitad del servicio.



Una vez que los servicios y conexiones entre datacenters ha superado un número de 4 pelos, automáticamente la institución debería buscar montar soluciones de WDM que reduzcan el número de fibra óptica contratado y haga uso de este como Lambdas, esto nos permitirá contratar solo dos pelos de fibra y proveer unos 8 enlaces coloreados y 1 simple de muy alta velocidad.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9.2 Subscripción:

9.2.1 Suscripción a Microsoft 365

Esto corre con la Licitación 446123 - RENOVACION DE LICENCIAS DE MICROSOFT, adjudicada el 23/11/2024, en este caso el llamado se hace de forma directa, es innegable la dependencia tecnológica de esta herramienta y lo eficiente que es en la operativa.

Hay dos maneras de correr las licencias, vía contrato SELECT o vía adquisición, es posible que se deba realizar una verificación final de las licencias CAL siendo utilizadas. Cambios de la plataforma de gestión requieren esfuerzo a nivel gobierno, que escapa a las responsabilidades de la entidad.

9.2.2 Suscripción Pingdom/Adq software y suscripción varias

Este y otros softwares son de uso corriente, este tipo de subscripción se debe armar un pack anual por ítems, dentro de esta situación se encuentran las herramientas de Pingdom, Glpi, zabbix, Elastic APM.

El pingdom es una solución mucho más costo eficiente que otras plataformas tipo PRTG.

9.2.3 Certificados digitales

Esto es utilizado para tener páginas seguras, la licitación Licitación 462128 - ADQUISICIÓN DE CERTIFICADOS DIGITALES está en proceso y cerrada pendiente para adjudicación. No existen observaciones.

9.2.4 Membresia Lacnic

Corriendo con la licitación Licitación 446059 - ADQUISICION DE SERVICIO DE PAGO DE MEMBRESIA LACNIC - SEGUNDO LLAMADO, no existen observaciones.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9.3 Soporte

9.3.1 Renovación de Soporte Software Redhat

Corriendo con la Licitación 454345 - SERVICIO DE SUSCRIPCION DE SOFTWARE RED HAT - AD REFERENDUM, plataforma crítica para la operación adjudicada el 2/12/2024 vigencia 12 meses, en este contrato se debe evaluar las alternativas de contratación. Vence el 14/12/2025

9.3.2 Soporte Local De Microsoft y Soporte de Datacenter

La licitación adjudicada es la Licitación 461866 - SOPORTE LOCAL MICROSOFT Y SOPORTE DATACENTER, adjudicada el 25/05/25 con vigencia de 24 meses, estos dos contratos son importantes para apoyo y continuidad a la operativa.
Es importante tener en cuenta que el foco de este es Sistemas Operativos y Plataformas, el llamado debe ir enfocándose, así como asegurarse que el personal que da el soporte está debidamente preparado.

Se debería ir considerando agregar como requisito los siguientes certificados acorde a la necesidad, esto de manera a que los proveedores se sigan actualizando y cuando proveedores nuevos se presenten puedan garantizar un nivel similar de soporte, casi contrario un nuevo proveedor puede ganar un contrato con la mejor oferta de precio, pero no estar al nivel de experiencia requerido, es algunos casos como Linux, se pueden solicitar certificados similares, RedHat, Suse, Ubuntu, etc, esto agregará consistencia entre los proveedores.

- Red Hat Certified Specialist in OpenShift Automation and Integration Certification
- Microsoft Windows Server Hybrid Administrator Associate
- Red Hat Certified Professional
- SUSE Certified Administrator
- SCE in SUSE Linux Enterprise
- Microsoft Hyper-V
- Microsoft Power BI Data Analyst Certification
- Certified Git Practitioner

Lote 1. Soporte Técnico para Datacenter

Objetivo: Contar con un soporte técnico externo especializado en mantenimiento de ambientes de procesamiento de datos mediante infraestructura de alta criticidad, de manera a asegurar el funcionamiento óptimo de los equipos para la entrega de servicios con la calidad adecuada.

Red Hat OpenShift AI

Alcance y tipo de servicios sobre los que se deberá prestar soporte:
El proveedor deberá prestar servicios de mantenimiento, mejoramiento, respaldo, contingencia y resolución de problemas sobre la infraestructura de la DNCP.
A continuación, se mencionan algunas de las actividades generales que se deberán realizar en el contexto de este servicio.
Implementar nuevos servicios a nivel de infraestructura informática.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Garantizar y mejorar la continuidad de los servicios informáticos.
Mejorar el tiempo de respuesta a nuevos requerimientos y aumentar los criterios para la toma de decisiones.
Implementar actualizaciones de versiones y nuevas funcionalidades.
Maximizar los servicios de tecnología de manera eficiente, oportuna, segura y confiable.
Minimizar el tiempo de restablecimiento de cualquier servicio informático.
Reuniones de relevamiento y análisis técnico para determinar el contexto y realizar propuestas de solución o implementación.
Instalación, configuración y optimización de servicios de infraestructura basados sobre GNU/Linux. (EJ: JBOSS, DNS, NTP, BIND, APACHE, TOMCAT, ELASTIC STACK, EMAIL, LDAP, SYSLOG, PROXMOX, OSSIM, GRAYLOG, OSSIN, GIT, OPENDCIM, GLUSTER, HAPROXY, GLPI).
Elaboración de guías y documentación para ejecución de pruebas de diagnóstico.
Resolución de problemas con documentación de esta.
Diseños y diagramas de arquitectura.
Actividades específicas.
Sobre entorno para virtualización y contenedores
Instalación, configuración, optimización, despliegue de aplicaciones sobre Openshift Container Platform.
Actualización de versiones, implementación de nuevas funcionalidades.
Elaboración de guías y documentación para ejecución de pruebas de diagnóstico.
Resolución de problemas con documentación de esta.
Diseños y diagramas de arquitectura.
Sobre entorno para repositorio de paquetes para servidores

Instalación, configuración y optimización de Red Hat Satellite para repositorio de paquetes.
Actualización de versiones, implementación de funcionalidades
Elaboración de guías y documentación para ejecución de pruebas de diagnóstico.
Resolución de problemas con documentación de esta.
Diseños de diagramas de arquitectura
Lugar y horario de trabajo:

Lote 2. Soporte Local Microsoft

Objetivo: Contar con el servicio técnico profesional para el soporte, configuración y/o Optimización de soluciones implementadas sobre la plataforma Microsoft por 2 años.

PERSONAL TÉCNICO.

El proveedor deberá prestar los servicios en la oficina central de la Dirección Nacional de Contrataciones Públicas o vía remota mediante plataformas virtuales, con profesionales certificados en Microsoft SQL Server, MS SharePoint, MS PowerBi, System Center Configuration Manager, Windows Server, Active Directory, Exchange Server, Skype for Business Server e Hyper-V. En función a la complejidad de la incidencia presentada deberá proveer la cantidad necesaria de profesionales para el fiel cumplimiento del contrato.

9.3.3 Soporte extensión de garantía para equipos no contemplados

Este apartado es fundamental en el presupuesto, ya que nos permite tener espacio de solucionar problemas inesperados y/o imprevistos.

9.4 Hardware

9.4.1 Adquisición de Switches SAN / implementación y capacitación

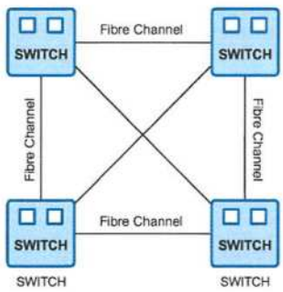
El llamado registrado para este fue la Licitación 337839 - ADQUISICIÓN DE SISTEMA DE BACKUP, SWITCH SAN Y SERVIDORES PARA LA DNCP, este incluyó sistema de backup, switch SAN y Servidores Iniciales IBM, normalmente este tipo de equipos se compra en combo con las soluciones de servidores y/o storage y teniendo en cuenta la capacidad

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

de transmisión de Fibre Channel, el ultimo es la Licitación 446086 - ADQUISICION DE STORAGE, DISCOS Y LIBRERIA - AD REFERENDUM fecha 27/01/2025 cuyo equipos fueron instalados recientemente.

Marca	Especificar
Modelo	Especificar
Numero de Parte	Especificar
Procedencia	Especificar
Cantidad requerida	4 (cuatro)
Numero de Puertos	24 (veinticuatro)
Cantidad de puertos activos y licenciados, con sus respectivos SFPs. Por cada switch	24 (23 SFP de 16 GBPS + 1 SFP 16 GBPS de Largo Alcance > 8KM)
Velocidad de conexión FC	>=16Gbps
Estándares de Fibra Canal soportados mínimamente	FC-PH, FC-PH-2, FC-GS-2
Tipos de Puertos	D_Port (Puerto de Diagnóstico), E_Port, F_Port, M_Port (Puertos Espejo); (U_Port)
Performance	Auto detección de 4, 8 y 16 Gbps
Soporte de Trunk ISL	Requerido
Soporte Agregación de ancho de banda	Requerido
Incluir Licencias para la Extensión de la Fabric	Una por switch
Clase de Servicios	Class 2,Class 3, Class F
Tamaño de marco de paquetes	>= 8000 bytes
Servicios Fabric	SNS, RSCN, NTP, RADIUS, LDAP, Port&Switch Binding, RCS, Zonificación Avanzada, ISL Trucking, Fabric Extendida.
Factor de Forma	>=1U
Fuente de alimentación redundante	220V
Rackeable	REQUERIDO
Gestión	HTTP, SSH
Garantía/Soporte	3 (Tres) años modalidad 8 x 5 NBD, incluyendo mantenimiento sin costo adicional con mano de obra, repuestos y partes en las oficinas del cliente (on site), una vez al año.
Autorización del Fabricante	El oferente deberá estar acreditado por el fabricante o representante local para prestar el servicio solicitado.
Plazo de Entrega	30 (treinta) días calendario.
Fabricación	Todos los equipos deben ser nuevos, de fabricación reciente, encontrarse en comercialización activa.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030



Esta topología debemos diseñarla acorde a un grafico N-Complete, donde cada nodo tiene acceso a cada Nodo, eso a futuro permitirá maximizar el uso de los enlaces sin tener que recurrir a anchos de bandas superiores.
Eso nos va obligar a usar troncales adicionales por cada camino de fibra redundante

En este caso sugerimos que la velocidad de FC sea 32 Gbps o superior, hay que tener en cuenta que en ese entonces se solicitaron servidores de 8 Gbps

Hoy en día la DNCP está usando los siguientes STORAGES

Storwize v5100, este equipo está llegando a su fin de soporte para 2025
Las soluciones Storage huawei Ocean x3000, IBM Xyratex IBM HS-1235T siguen vigentes

Es importante tener en cuenta que si bien las solicitudes son para FC 8 y 16GB/s mínimo, los nuevos equipos ya están saliendo con 16/32 como mínimos, estos en si ya son back compatibles, y teniendo en cuenta que la solicitud solicita SSD en toda la solución de STORAGE NVME a 6,8Gbps Read,, 5,3Gbps Write, antes que nada es importante entender que las velocidades de transferencia de los discos en general sin expresadas en **bytes por segundo** y las tasas de transferencia de los equipos de redes están expresadas en **bits por segundo**.

Acorde a la Licitación 446086, las especificaciones pedidas para los discos NVME son:

Factor de Forma	2,5
Capacidad	7,68 TB
Conector	PCIe 4.0 (NVMe)
Velocidad de Lectura	6,8 Gbps o superior
Velocidad de Escritura	5,3 Gbps o superior

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Technical specifications

The following tables present the technical specifications for the PM1733 Entry NVMe PCIe SED SSDs. Note that the performance data and power consumption is based on whether the drives are connected to a PCIe 4.0 host interface or a PCIe 3.0 host interface.

Table 2. Technical specifications

Feature	3.84 TB drive	7.68 TB drive
Interface	PCIe 4.0 x4*	PCIe 4.0 x4*
Capacity	3.84 TB	7.68 TB
SED encryption	TCG Opal	TCG Opal
Endurance (drive writes per day for 5 years)	1 DWPD	1 DWPD
Endurance (total bytes written)	7008 TB	14,016 TB
Data reliability (UBER)	< 1 in 10^{17} bits read	< 1 in 10^{17} bits read
MTBF	2,000,000 hours	2,000,000 hours
Performance & Power - PCIe 4.0 host interface		
IOPS reads (4 KB blocks)	1,500,000	1,450,000
IOPS writes (4 KB blocks)	135,000	135,000
Sequential read rate (128 KB blocks)	7000 MBps	7000 MBps
Sequential write rate (128 KB blocks)	3500 MBps	3500 MBps
Latency (random R/W)	100 µs / 25 µs	100 µs / 25 µs
Latency (sequential R/W)	220 µs / 80 µs	220 µs / 80 µs
Typical power (R/W)	20 W / 20 W	20 W / 20 W
Performance & Power - PCIe 3.0 host interface		
IOPS reads (4 KB blocks)	800,000	800,000
IOPS writes (4 KB blocks)	135,000	135,000
Sequential read rate (128 KB blocks)	3400 MBps	3400 MBps
Sequential write rate (128 KB blocks)	3200 MBps	3200 MBps
Latency (random R/W)	100 µs / 25 µs	100 µs / 25 µs
Latency (sequential R/W)	250 µs / 100 µs	250 µs / 100 µs
Typical power (R/W)	15 W / 20 W	15 W / 20 W

* Backwards compatible with a PCIe 3.0 x4 host interface

Para aprovechar al máximo un NVMe con velocidad de lectura de 6.8 Gbps, se necesita una conexión Fibre Channel (FC-NVMe) que iguale o supere ese ancho de banda. Considerando que Fibre Channel se mide en Gbps (Gigabits por segundo) y que cada generación tiene una eficiencia variable, aquí está la recomendación:

- 16GFC (~1.6 GBps): Insuficiente para el NVMe.
- 32GFC (~3.2 GBps): Aún sería un cuello de botella.
- 64GFC (~6.4 GBps): Se acerca, pero sigue siendo ligeramente inferior.
- 128GFC (~12.8 GBps): Ideal para garantizar que no haya pérdida de rendimiento.

A corto plazo la DNCP ya esta considerando **FC 32 Gbps** ya que esta avanzando con su infraestructura y los volúmenes de datos están creciendo considerablemente, las consultas de los servidores a los discos debería ser evaluadas en tiempo y procesamiento.

Para máxima eficiencia, 128GFC es la mejor opción para evitar cuellos de botella y permitir futuras expansiones. Sin embargo, 64GFC podría ser suficiente si el tráfico no es constante al máximo rendimiento. También puedes considerar multipathing para distribuir la carga entre múltiples enlaces FC.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Technical Specifications

Model	OceanProtect X3000
	HDD Form
Hardware specifications	
Physical backup bandwidth of the system	Up to 6 TB/hour
Logical backup bandwidth of the system	Up to 10 TB/hour
Recovery bandwidth of the system	Up to 1 TB/hour
Number of controllers	2
Usable capacity per node	16 TB - 60 TB
Data disk types	4TB/8TB/14TB NL-SAS
Front-end port types	8/16/32 Gbit/s FC, 10/25/40/100 GbE
Software specifications	
RAID type	RAID 2.0+
RAID levels	RAID 6 (default), and RAID-TP (optional)
Software functions	Inline deduplication, inline compression, multi-tenancy, quota management, snapshot, remote replication, audit logs, intelligent service quality control, and data erase
System management	Device O&M (DeviceManager), Remote O&M (DME-IQ)
Electrical specifications	
Power supply	200 V to 240 V AC ±10%; 192 V to 288 V DC
Dimensions(H x W x D)	86.1mm×447mm×488mm
Weight	23.3 kg (including the weight of the hard disk unit)
Operating temperature	-60 m to +1800 m altitude: 5°C to 35°C (bay) or 40°C (enclosure); 1800 m to 3000 m altitude: The max. temperature threshold decreases by 1°C for every altitude increase of 220 m
Operating temperature	10% ~ 90%R.H.

Eso quiere decir que en futuros llamados deberíamos ir aumentando la velocidad de los FC para sacarle provecho a los discos, especialmente en consultas pesadas o cuando queramos realizar backup.
Así mismo a nivel capa de red si queremos hacer backup vía Ethernet, 10Gbps ya no es suficiente, deberíamos estar considerando 100Gbps, esto posterior a una evaluación en detalle de cuál es la cantidad de información que deseamos hacer backup, si es completo o si es diferencial.

En caso de falla de un disco el equipo deberá contar con tecnologías para la protección del arreglo o disco spare, se debe incluir la menos un spare por sistema RAID. Este apartado a future requiere una especificación a profundidad

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

RAID Levels	RAID 0	RAID 1	RAID 5	RAID 6	RAID 10	RAID 50	RAID 60
Description	Striping	Mirroring	Striping with Parity	Striping with double parity	Mirroring and striping	Striping and distributed parity	Striping and double parity
Minimum Disks	2	2	3	4	4	6	8
Read Performance	High	High	High	High	High	High	High
Write Performance	High	Medium	High	High	Medium	Medium	Medium
Cost	Low	High	Low	Low	High	Medium	High
Data Protection	No	Yes	Yes	Yes	Yes	Yes	Yes
Capacity Utilization %	1	0.5	67%-94%	50%-80%	0.5	67%-94%	50%-88%
Common Implementation	Live streaming, video editing	OS, database operations	Information warehousing	Financial and accounting applications, database servers	Fast databases, application servers	Large databases, file and application servers	Servers with large capacity requirements

9.4.2 Adquisición de Equipos de red/ balanceador de carga

380745 - ADQUISICIÓN DE BALANCEADOR DE CARGA, adjudicación 09/11/2020 el modelo adjudicado es el F5 BIG-IP 2000, si bien este equipo va a funcionar correctamente es importante tener en cuenta que ha llegado a su tiempo de EoS, pero sigue vigente por los próximos años para soporte y RMA en sus series 2600 y 2800.

Front view of the platform

1. Management 10/100/1000 Ethernet port
2. USB ports
3. Console serial port
4. Serial (hard-wired) failover port
5. 10/100/1000 interfaces
6. 1/10G SFP+ ports
7. Indicator LEDs
8. LCD display
9. LCD control buttons

The back of the platform includes one AC power supply by default. Optionally, you can install a second power supply. You can manually power off the power supply from the back of the platform.

Back view of the platform

1. Power input panel 1 (power switch and power receptacle)
2. Power input panel 2 (power switch and power receptacle)
3. Chassis ground lug

Este tipo de plataformas tiene la ventaja que realiza distribución del tráfico, eso significa que su funcionalidad no se verá afectada. La funcionalidad de este es darnos flexibilidad y redundancia a la hora de brindar el servicio, así que, ante un fallo total, esta capa de red puede ser reemplazada por una configuración dura, pero requiere ingeniero.

Se recomienda renovar garantía acorde a la Licitación 428240 - RENOVACIÓN DE GARANTIA.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

BIG-IP i2000 series

The entry-level BIG-IP i2000 series of high-performance ADC appliances provides small-to-medium sized enterprises with integrated application delivery and security services, delivering up to:

- L7 requests per second: 650K
- L4 connections per second: 250K
- L4 HTTP requests per second: 1M
- Maximum L4 concurrent connections: 14M
- Throughput: 10 Gbps (L4/L7)

Es recomendable evaluar la progresión de sesiones y nuevas sesiones por Segundo, ya que suele ser la mayor limitante de estos equipos.

Con referencia al tráfico de 10Gbps es más que suficiente ya que los enlaces actuales recién se encuentran en los cientos de megas.

9.4.3 Adquisición de Equipos de red/Firewall de borde

Posterior a eso ambos equipos de borde y core son solicitados en la Licitación 460737 - ADQUISICIÓN DE EQUIPOS DE SEGURIDAD Y NETWORKING, este deberá migrar la configuración del equipo FG 501E, en este caso la decisión de reducir y volver redundante al Firewall de borde es la correcta, el FG 501 es un equipo muy potente, y el escalamiento del consumo de borde depende mucho de la plataforma de SICP y el tamaño de los documentos utilizados, hasta el momento el borde se maneja de manera eficiente.

El dimensionamiento principal del nuevo firewall de borde está dictado mayormente por estas tres líneas

Throughput de Firewall de 10Gbps.

Throughput IDS/IPS de 2.5Gbps Exigido

Throughput IPsec VPN de 2.5Gbps- Exigido

2 (Dos) interfaces de fibra de 10Gbps equipados con 2 SFP+ Multimodo

2 interfaz de fibra de 1Gbps equipados con 1 SFP

Monomodo (hasta 10 Km) por cada equipo que componga la solución,

Además, cada equipo debe tener una interfaz de cobre dedicada para administración.

Esto reduce el equipo a un equipo similar a un FG-100F o similar, en este caso podemos observar que el equipo de nueva generación FG-90G tiene mejores rendimientos que el 100F, pero limitaciones en storage y otras funcionalidades esto debe ser tenido en cuenta para futuros llamados.

Esto optimizará bastante el llamado y reducirá el costo recurrente de las licencias de soporte.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

9.4.4 Adquisición de Equipos de red/Firewall de core

El equipo Legacy se renovará vía Licitación 439206 - RENOVACION DE LICENCIAS PARA FIREWALL SOPHOS XG450

ITEM 1. XG 450 Xstream Protection

ITEM 2. XG 450 Webserver Protection

ITEM 3. XG 450 Email Protection

Esta licitación se encuentra en proceso con la Licitación 460737 - ADQUISICIÓN DE EQUIPOS DE SEGURIDAD Y NETWORKING.

Las configuraciones más importantes son:

Procesador 4 núcleos, 2.0Ghz por núcleo

Memoria Ram 8GB

Firewall de capa 7,4,3 y 2

Throughput de Firewall de 15Gbps.

Throughput IDS/IPS de 3 Gbps.

La política de tener una doble capa de seguridad separada en equipos es la correcta, ya que esto permite que fallas en un marca no afecten sistemáticamente toda la solución de seguridad.

9.4.5 Adquisición de switches SAN

Acorde a la última licitación 460737 - ADQUISICIÓN DE EQUIPOS DE SEGURIDAD Y NETWORKING los switches SAN solicitados ya contemplan interfaces FC 32 Gbps, esto acorde a las necesidades de crecimiento. Estos 4 equipos solicitados conformaran una fábrica única, lo cual permitiría tener una red redundante en cada Datacenter. Se debe evaluar tener una red SAN entre datacenters

Acorde a las tablas de distancias de un proveedor de FO, estas son las distancias que ellos certifican en laboratorio, esto a su vez se debe certificar con el fabricante del equipo.

Utilizando fibras normales

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

Table 2.1: Fibre Channel Duplex - Maximum Distance Capability for Systems with Multimode Low Loss/ Single mode Standard loss MTP®/LC Modules (0.5/1.0) dB

Fibre Channel - Duplex - Maximum Distance Capability (All Distances in Meters)									
Fiber Type	Data Rate Protocol	Speed	Number of (MM/SM) Low/Std. Loss MTP/LC Modules (0.5/1.0) dB in the System						
			1	2	3	4	5	6	7	8
OM3	400-M5E-SN-I	4 GFC	540	515	490	470	445	420	400	390
	800-M5E-SN-I	8 GFC	215	215	210	195	185	175	165	155
	1200-M5E-SN-I	10 GFC	325	325	325	325	325	325	325	325
	1600-M5E-SN-I	16 GFC	150	140	135	125	115	105	95	90
	3200-M5E-SN-I	32 GFC	80	80	80	80	80	75	65	60
	6400-M5E-SN-I	64 GFC	75	75	75	75	75	70	70	70
OM4	400-M5F-SN-I	4 GFC	655	625	595	570	540	510	490	470
	800-M5F-SN-I	8 GFC	290	275	260	250	235	220	210	200
	1200-M5F-SN-I	10 GFC	560	555	550	540	530	520	520	515
	1600-M5F-SN-I	16 GFC	205	190	180	170	155	140	130	120
	3200-M5F-SN-I	32 GFC	130	130	125	120	115	110	95	85
	6400-M5F-SN-I	64 GFC	115	115	115	115	110	105	100	95
OS2	800-SM-LC-L	8 GFC	12150	10400	9050	7550	6150	4800	3500	2200
	1600-SM-LC-L	16 GFC	11750	10250	9050	7700	6350	5000	3750	2400
	3200-SM-LC-L	32 GFC	11850	10400	9250	8000	6750	5500	4350	3100

Utilizando fibras de muy baja perdida

Table 2.2: Fibre Channel Duplex - Maximum Distance Capability for Systems with Multimode/Single mode Ultra Low Loss (ULL) MTP/LC Modules (0.35/0.6) dB

Fibre Channel - Duplex - Maximum Distance Capability (All Distances in Meters)									
Fiber Type	Data Rate Protocol	Speed	Number of (MM/SM) Ultra Low Loss (ULL) MTP/LC Modules (0.35/0.6) dB in the System						
			1	2	3	4	5	6	7	8
OM3-ULL	400-M5E-SN-I	4 GFC	550	535	515	495	475	455	430	410
	800-M5E-SN-I	8 GFC	215	215	215	210	200	190	180	170
	1200-M5E-SN-I	10 GFC	325	325	325	325	325	325	325	325
	1600-M5E-SN-I	16 GFC	155	150	145	135	130	120	110	100
	3200-M5E-SN-I	32 GFC	80	80	80	80	80	80	75	65
	6400-M5E-SN-I	64 GFC	75	75	75	75	75	75	70	65
OM4-ULL	400-M5F-SN-I	4 GFC	670	650	625	605	580	550	520	490
	800-M5F-SN-I	8 GFC	295	285	275	265	255	240	225	215
	1200-M5F-SN-I	10 GFC	565	560	555	550	540	535	525	520
	1600-M5F-SN-I	16 GFC	210	200	190	180	170	160	145	135
	3200-M5F-SN-I	32 GFC	130	130	130	125	120	115	110	95
	6400-M5F-SN-I	64 GFC	115	115	115	115	115	115	110	100
OS2-ULL	800-SM-LC-L	8 GFC	13000	11950	11000	10300	9550	8750	8000	7250
	1600-SM-LC-L	16 GFC	12500	11600	10900	10150	9500	8750	8100	7400
	3200-SM-LC-L	32 GFC	12500	11700	11000	10300	9700	9000	8350	7700

Estos nos podrían permitir hacer backup en el sitio redundante vía FC a 32 Gbps

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

CUADRO DE REVALÚO Y DEPRECIACIÓN DE BIENES DEL ACTIVO FIJO

1. IDENTIFICACIÓN DEL CONTRIBUYENTE		2. DATOS DE LA DECLARACIÓN JURADA		3. EJERCICIO FISCAL	
RAZÓN SOCIAL O APELLIDOS/NOMBRES	IDENTIFICADOR RUC	FORMULARIO UTILIZADO	No. ORDEN	DESDE	HASTA

4- IDENTIFICACIÓN DEL REPRESENTANTE LEGAL		5- IDENTIFICACIÓN DEL CONTADOR	
APELLIDOS / NOMBRES	IDENTIFICADOR RUC	APELLIDOS / NOMBRES	IDENTIFICADOR RUC/CI

1. Descripción de los Bienes	2. Valor de Costo o de Adquisición	3. Fecha de Adquisición	4. Coeficiente de Revalúo	VALORES FISCALES							VALORES CONTABLES							
				5. Años de Vida Útil Fiscal	6. Años de Vida Útil Fiscal Restantes	7. Valor Fiscal Neto del Ejercicio Anterior	8. Valor Fiscal Revaluado	9. Cuota Fiscal de Depreciación Anual	10. Depreciación Fiscal Acumulada	11. Valor Fiscal Neto al Cierre	12. Años de Vida Útil Contable	13. Años de Vida Útil Contable Restantes	14. Valor Contable Neto del Ejercicio Anterior	15. Valor Contable Revaluado	16. Cuota Contable de Depreciación Anual	17. Cuota de Depreciación Anual no Deducible	18. Depreciación Contable Acumulada	19.Valor Contable Neto al Cierre

Definiciones de las Columnas

1. Descripción de los Bienes: Consignar detalladamente cada bien o partida, considerando para el efecto la fecha de adquisición y tipo de bien.

2. Valor de Costo o de Adquisición: Consignar el valor de compra en guaraníes de cada bien, conforme a la documentación de respaldo.

3. Fecha de Adquisición: Consignar la fecha que consta en el documento respaldatorio de compra de cada uno de los bienes.

4. Coeficiente de Revalúo: Consignar el coeficiente de Revalúo para cada tipo de Bien conforme a los valores establecidos por Resolución de la Administración Tributaria.

5. Años de Vida Útil Fiscal: Consignar los años de vida útil conforme a los criterios establecidos por la Administración Tributaria para cada tipo de bien.

6. Años de Vida Útil Fiscal Restantes: Consignar los años de vida útil (fiscal), restantes al término del ejercicio fiscal que se liquida.

7. Valor Fiscal Neto del Ejercicio Anterior: Trasladar del ejercicio anterior, los valores consignados en la columna 11(Valor Fiscal Neto al Cierre). En caso que los bienes hayan sido adquiridos en el transcurso del ejercicio, este valor debe coincidir con el de la columna 2 (Valor del Costo o de Adquisición).

8. Valor Fiscal Revaluado: Consignar el valor que resulte de multiplicar el Valor Fiscal Neto del Ejercicio Anterior, por el Coeficiente de Revalúo (valor de columna 7 x valor de columna 4).

9. Cuota Fiscal de Depreciación Anual: Consignar el valor que resulte de dividir el Valor Fiscal Revaluado por el número de años de Vida Útil Fiscal restantes, incluido el que se liquida (valor de la columna 8 / (valor de la columna 6 +1)).

10. Depreciación Fiscal Acumulada: Consignar la suma de las Cuotas de Depreciación Fiscal de cada año, incluyendo el que se liquida (valor de columna 9 + valor de columna 10 del ejercicio anterior).

11. Valor Fiscal Neto al Cierre: Consignar el Valor Revaluado Fiscal deducido el valor de la Cuota Fiscal de Depreciación Anual del ejercicio que se liquida (valor de columna 8 - valor de columna 9).

12. Años de Vida Útil Contable: Consignar los años durante los cuales el bien puede ser utilizado o pueda generar renta a criterio de la empresa.

13. Años de Vida Útil Contable Restantes: Consignar los años de vida útil (contable), restantes al término del ejercicio fiscal que se liquida.

14. Valor Contable Neto del Ejercicio Anterior: Trasladar del ejercicio anterior, los valores consignados en la columna 19 (Valor Contable Neto al Cierre). En caso que los bienes hayan sido adquiridos en el transcurso del ejercicio, este valor debe coincidir con el 2 (Valor del Costo de Adquisición).

15. Valor Contable Revaluado: Consignar el valor que resulte de multiplicar el Valor Contable Neto del Ejercicio Anterior, por el Coeficiente de Revalúo (valor de la columna 14 x valor de la columna 4).

16. Cuota Contable de Depreciación Anual: Consignar el valor que resulte de dividir el Valor Contable Revaluado por el número de años de Vida Útil Contable restantes incluido el que se liquida (valor de la columna 15/ (valor de la columna 13 +1)).

17. Cuota de Depreciación Anual no Deducible: Consignar la diferencia entre la Cuota Fiscal de Depreciación Anual y la Contable; cuando la contable sea mayor que la Fiscal. En caso contrario consignar "0". (valor de la columna 9 - valor de la columna 16).

18. Depreciación Contable Acumulada: Consignar la suma de las Cuotas de Depreciación Contable de cada año, incluyendo el que se liquida (valor de la columna 16 + valor de la columna 18 del ejercicio anterior).

19.Valor Contable Neto al Cierre: Consignar el Valor Contable Revaluado deducido el valor de la Cuota Contable de Depreciación Anual (valor de la columna 15 - valor de la columna 16). La sumatoria o total de esta columna deberá coincidir con los respectivos saldos de las cuentas del Balance General.

COPIA FIEL DEL ORIGINAL

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

11 ANEXO II Fortigate Product Matrix

FORTINET

Product Matrix
June 2025

FortiGate® Network Security Platform - *Top Selling Models Matrix

	FG/FWF-30G	FG/FWF-40F	FG/FWF-50G	FG/FWF-60F	FG-70F
Firewall Throughput (1518/512/64 byte UDP)	4/4/3.9 Gbps	5/5/5 Gbps	5/5/4 Gbps	10/10/6 Gbps	10/10/6 Gbps
IPsec VPN Throughput (512 byte) [1]	3.5 Gbps	4.4 Gbps	4.5 Gbps	6.5 Gbps	6.1 Gbps
IPS Throughput (Enterprise Mix) [2]	800 Mbps	1 Gbps	2.25 Gbps	1.4 Gbps	1.4 Gbps
NGFW Throughput (Enterprise Mix) [2,4]	570 Mbps	800 Mbps	1.25 Gbps	1 Gbps	1 Gbps
Threat Protection Throughput (Ent. Mix) [2,5]	500 Mbps	600 Mbps	1.1 Gbps	700 Mbps	800 Mbps
Firewall Latency	2.87 µs	2.97 µs	2.42 µs	3.3 µs	2.54 µs
Concurrent Sessions	600 000	700 000	720 000	700 000	1.5 Million
New Sessions/Sec	30 000	35 000	85 000	35 000	35 000
Firewall Policies	2 000	2 000	2 000	2 000	5 000
Max G/W to G/W IPSEC Tunnels	200	200	200	200	200
Max Client to G/W IPSEC Tunnels	250	250	250	500	500
SSL VPN Throughput	—	490 Mbps [10]	—	900 Mbps [10]	405 Mbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	—	200 [10]	—	200 [10]	200
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	400 Mbps	310 Mbps	1.3 Gbps	630 Mbps	700 Mbps
Application Control Throughput (HTTP 64K) [2]	830 Mbps	990 Mbps	2.8 Gbps	1.8 Gbps	1.8 Gbps
Max FortiAPs (Total / Tunnel)	16/8	16/8	16/8	64/32	64/32
Max FortiSwitches	8	8	8	24	24
Max FortiTokens	500	500	500	500	500
Virtual Domains (Default/Max)	—	10/10	5/5	10/10	10/10
Interfaces	4x GE RJ45	5x GE RJ45	5x GE RJ45	10x GE RJ45	10x GE RJ45
Local Storage	30 GB (31G)	—	64 GB (51G)	128 GB (61F)	128 GB (71F)
Power Supplies	Single AC PS	Single AC PS	Single AC PS	Single AC PS	Single AC PS
Form Factor	Desktop	Desktop	Desktop	Desktop	Desktop
Variants	WiFi	WiFi, 3G4G	WiFi, DSL, SFP, POE, 5G	WiFi, Storage	—

	FG/FWF-70G	FG/FWF-80F	FG-90G	FG-100F	FG-120G
Firewall Throughput (1518/512/64 byte UDP)	10/10/10 Gbps	10/10/7 Gbps	28/28/27.9 Gbps	20/18/10 Gbps	39/39/28 Gbps
IPsec VPN Throughput (512 byte) [1]	7.1 Gbps	6.5 Gbps	25 Gbps	11.5 Gbps	35 Gbps
IPS Throughput (Enterprise Mix) [2]	2.5 Gbps	1.4 Gbps	4.5 Gbps	2.6 Gbps	5.3 Gbps
NGFW Throughput (Enterprise Mix) [2,4]	1.5 Gbps	1 Gbps	2.5 Gbps	1.6 Gbps	3.1 Gbps
Threat Protection Throughput (Ent. Mix) [2,5]	1.3 Gbps	900 Mbps	2.2 Gbps	1 Gbps	2.8 Gbps
Firewall Latency	2.46 µs	3.23 µs	3.23µs	4.97µs	3.17 µs
Concurrent Sessions	1.4 Million	1.5 Million	3 Million	1.5 Million	3 Million
New Sessions/Sec	100 000	45 000	124 000	56 000	140 000
Firewall Policies	5 000	5 000	5 000	10 000	10 000
Max G/W to G/W IPSEC Tunnels	200	200	200	2 000	2 000
Max Client to G/W IPSEC Tunnels	500	2,500	2 500	16 000	16 000
SSL VPN Throughput	—	950 Mbps	1.4 Gbps [10]	1 Gbps	1.5 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	—	200	200 [10]	500	500
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	1.4 Gbps	715 Mbps	2.6 Gbps	1 Gbps	3 Gbps
Application Control Throughput (HTTP 64K) [2]	3.6 Gbps	1.8 Gbps	6.7 Gbps	2.2 Gbps	6.7 Gbps
Max FortiAPs (Total / Tunnel)	96/48	96/48	128/64	128/64	128/64
Max FortiSwitches	24	24	24	32	48
Max FortiTokens	500	500	500	5 000	5 000
Virtual Domains (Default/Max)	10/10	10/10	10/10	10/10	10/10
Interfaces	10x GE RJ45	8x GE RJ45, 2x Shared Port Pairs	8x GE RJ45, 2x 10GE Shared Port Pairs	2x 10 GE SFP+, 18x GE RJ45, 4x Shared Port Pairs, 8x GE SFP	4x 10 GE SFP+, 18x GE RJ45, 8x GE SFP
Local Storage	64 GB (71G)	128 GB (81F)	120 GB (91G)	480 GB (101F)	480 GB (121G)
Power Supplies	Single AC PS	Single AC PS, dual inputs	Single AC PS, dual inputs	Dual AC PS	Dual AC PS
Form Factor	Desktop	Desktop	Desktop	1 RU	1 RU
Variants	WiFi, POE	WiFi, 3G4G, DSL, Bypass, Storage	—	—	—

1

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

FortiGate® Network Security Platform - *Top Selling Models Matrix

	FG-200F	FG-200G	FG-400F	FG-600F	FG-900G
Firewall Throughput (1518/512/64 byte UDP)	27 / 27 / 11 Gbps	39 / 39 / 26.5 Gbps	79.5 / 78.5 / 70 Gbps	139 / 137.5 / 70 Gbps	164 / 163 / 153 Gbps
IPsec VPN Throughput (512 byte) [1]	13 Gbps	36 Gbps	55 Gbps	55 Gbps	55 Gbps
IPS Throughput (Enterprise Mix) [2]	5 Gbps	9 Gbps	12 Gbps	14 Gbps	42 Gbps
NGFW Throughput (Enterprise Mix) [2,4]	3.5 Gbps	7 Gbps	10 Gbps	11.5 Gbps	31 Gbps
Threat Protection Throughput (Ent. Mix) [2,5]	3 Gbps	6 Gbps	9 Gbps	10.5 Gbps	30 Gbps
Firewall Latency	4.78 µs	4.36 µs	4.19 µs / 2.5 µs [7]	4.12 µs / 2.5 µs [7]	3.78 / 2.5 µs [7]
Concurrent Sessions	3 Million	11 Million	7.8 Million	8 Million	16 Million
New Sessions/Sec	280 000	400 000	500 000	550 000	720 000
Firewall Policies	10 000	10 000	10 000	30 000	50 000
Max G/W to G/W IPSEC Tunnels	2 000	2 000	2 000	2 000	2 000
Max Client to G/W IPSEC Tunnels	16 000	16 000	50 000	50 000	50 000
SSL VPN Throughput	2 Gbps	3 Gbps [8]	3.6 Gbps	4.3 Gbps	10 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	500	500	5000	10 000	10 000
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	4 Gbps	7 Gbps	8 Gbps	9 Gbps	16.7 Gbps
Application Control Throughput (HTTP 64K) [2]	13 Gbps	27.8 Gbps	28 Gbps	32 Gbps	74.8 Gbps
Max FortiAPs (Total, Tunnel)	256 / 128	256 / 128	512 / 256	1 024 / 512	2 048 / 1 024
Max FortiSwitches	64	64	96	128	196
Max FortiTokens	5 000	5 000	5 000	5 000	5 000
Virtual Domains (Default/Max)	10 / 25	10 / 25	10 / 25	10 / 50	10 / 50
Interfaces	4× 10 GE SFP+, 18x GE RJ45, 8x GE SFP	8× 10 GE SFP+, 8× 5GE RJ45, 10x GE RJ45, 4x GE SFP	8× 10GE SFP+ , 8x GE SFP, 18 x GE RJ45	4× 25G SFP28, 4× 10GE SFP+ , 8x GE SFP, 18 x GE RJ45	4× 25 GE SFP28, 4× 10 GE SFP+, 1× 2.5GE RJ45, 8 x GE SFP, 17x GE RJ45
Local Storage	480 GB (201F)	480 GB (201G)	960 GB (401F)	480 GB (601F)	960 GB (901G)
Power Supplies	Dual AC PS	Dual AC PS	Dual AC PS	Dual AC PS	Dual PS
Form Factor	1 RU	1 RU	1 RU	1 RU	1 RU
Variants	—	—	DC	—	DC

	FG-1000F	FG-1800F	FG-2600F	FG-3000F	FG-3200F
Firewall Throughput (1518/512/64 byte UDP)	198 / 196 / 134 Gbps	198 / 197 / 140 Gbps	198 / 196 / 140 Gbps	397 / 389 / 221 Gbps	387 / 385 / 178.5 Gbps
IPsec VPN Throughput (512 byte) [1]	55 Gbps	55 Gbps	55 Gbps	105 Gbps	105 Gbps
IPS Throughput (Enterprise Mix) [2]	19 Gbps	22 Gbps	31 Gbps	36 Gbps	63 Gbps
NGFW Throughput (Enterprise Mix) [2,4]	15 Gbps	17 Gbps	27 Gbps	34 Gbps	47 Gbps
Threat Protection Throughput (Ent. Mix) [2,5]	13 Gbps	15 Gbps	25 Gbps	33 Gbps	45 Gbps
Firewall Latency	3.45 µs	3.22 µs	3.41 µs	3.92 µs	3.42 µs
Concurrent Sessions	7.5 Million	12 Million / 40 Million [6]	24 Million / 40 Million [6]	70 Million / 230 Million [6]	70 Million
New Sessions/Sec	650 000	750 000 / 2 Million [6]	1 Million / 2 Million [6]	870 000 / 3 Million [6]	800 000
Firewall Policies	100 000	100 000	100 000	200 000	200 000
Max G/W to G/W IPSEC Tunnels	20 000	20 000	20 000	40 000	40 000
Max Client to G/W IPSEC Tunnels	100 000	100 000	100 000	200 000	200 000
SSL VPN Throughput	5.3 Gbps	11 Gbps	16 Gbps	11 Gbps	11 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	10 000	10 000	30 000	30 000	30 000
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	10 Gbps	12 Gbps	20 Gbps	29 Gbps	29 Gbps
Application Control Throughput (HTTP 64K) [2]	44 Gbps	34 Gbps	64 Gbps	115 Gbps	109 Gbps
Max FortiAPs (Total, Tunnel)	4 096 / 2 048	4 096 / 2 048	4 096 / 2 048	4 096 / 2 048	4 096 / 2 048
Max FortiSwitches	196	196	196	300	300
Max FortiTokens	20 000	20 000	20 000	20 000	20 000
Virtual Domains (Default/Max)	10 / 250	10 / 250	10 / 500	10 / 500	10 / 500
Interfaces	2× 100 GE QSFP28, 8x 25 GE SFP28, 16×10 GE SFP+, 8× 10GE RJ45, 1x 2.5GE RJ45, 1 GE RJ45	4× 100 GE QSFP28, 12x 25 GE SFP28, 2×10 GE SFP+, 8x GE SFP, 18x GE RJ45 [9]	4× 100GE QSFP28/40GE QSFP+, 16× 25GE SFP28, 16× 10GE RJ45, 2× 10GE SFP+, 2x GE RJ45	6× 100GE QSFP28/40GE QSFP+, 16× 25GE SFP28, 18× 10GE RJ45, 2x GE RJ45	4× 400GE QSFP-DD, 12x 50GE SFP56, 4× 25GE SFP28, 2× 10GE RJ45
Local Storage	960 GB (1001F)	2× 960 GB (1801F)	2× 960 GB (2601F)	2× 960 GB (3001F)	2× 960 GB (3201F)
Power Supplies	Dual PS	Dual PS	Dual PS	Dual PS	Dual PS
Form Factor	2 RU	2 RU	2 RU	2 RU	2 RU
Variants	—	DC	DC	DC	—

* Featured Top selling models, for complete FortiGate offerings please visit www.fortinet.com. FortiGate virtual appliances are also available. All performance values are "up to" and vary depending on system configuration.

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

12 Bibliografía

Lineamientos PGN
https://www.mef.gov.py/dependencias/viceministerio-administracion-financiera/gerencia-gestion-financiera-estado/direccion-general-presupuesto/lineamientos-pgn-2025

IMPUESTO A LA RENTA EMPRESARIAL (IRE)
https://www.bacn.gov.py/archivos/9332/Ley+6380.pdf

POR EL CUAL SE REGLAMENTA EL IMPUESTO A LA RENTA EMPRESARIAL (IRE) ESTABLECIDO EN LA LEY N° 6380/2019, «DE MODERNIZACIÓN Y SIMPLIFICACIÓN DEL SISTEMA TRIBUTARIO NACIONAL»
https://www.bacn.gov.py/archivos/9332/DECRETO+3182+LEY6380.pdf

Fortigate Product Matrix
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/Fortinet_Product_Matrix.pdf

Microsoft Core Cal licensing
https://download.microsoft.com/download/3/d/4/3d42bdc2-6725-4b29-b75a-a5b04179958b/licensing_core_cal_and_enterprise_suite.pdf

Redhat subscription Guide
https://www.redhat.com/en/resources/self-managed-openshift-subscription-guide

F5 BIG-IP i2000
https://my.f5.com/manage/s/article/K000133583

Catalogo de distancias de Fibras
https://www.corning.com/catalog/coc/documents/application-engineering-notes/AEN162.pdf

Fortigate 501E Datasheet
https://www.router-switch.com/pdf2html/pdf/fg-501e-datasheet.pdf

Nutanix convergence models
https://www.unixarena.com/2014/12/nutanix-web-scale-converged-infrastructure.html/#google_vignette

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

13 Glosario

AC: Air Conditioner (Aire Acondicionado)
AC: Alternating Current (Corriente Alterna)
ACL: Access Control List (Lista de Control de Acceso)
AES: Advanced Encryption Standard (Estándar de Encriptación Avanzada)
ANDE: Administración Nacional de Electricidad
ANEAES Agencia Nacional de Evaluación y Acreditación de la Educación Superior
API: Application Programming Interface (Interfaz de Programación de Aplicaciones)
APP Asociación Público Privada
ARP: Address Resolution Protocol (Protocolo de Resolución de Direcciones)
BA: Banda Ancha
BCP: Banco Central de Paraguay
BGP: Border Gateway Protocol (Protocolo de Puerta de Enlace Fronteriza)
BIOS: Basic Input/Output System (Sistema Básico de Entrada/Salida)
BMC: Baseboard Management Controller (Controlador de Gestión de Placa Base)
BPS: Bits Per Second (Bits Por Segundo)
BYOD: Bring Your Own Device (Trae Tu Propio Dispositivo)
CaaS: Container as a Service (Contenedor como Servicio)
CAF: Corporación Andina de Fomento
CAPEX: Capital Expenditure (Gasto de Capital)
CDN: Content Delivery Network (Red de Entrega de Contenidos)
CERT-PY: Centro de Respuestas a Incidentes Cibernético
CIFS: Common Internet File System (Sistema de Archivos Común en Internet)
CISO: Chief information security officer (Oficial de Seguridad de la Información)
CLI: Command Line Interface (Interfaz de Línea de Comandos)
CNAME: Canonical Name (Nombre Canónico)
CONACYT: Compañía Nacional de Ciencia y Tecnología
CONATEL: Comisión Nacional de Telecomunicaciones
CONES: Consejo Nacional de Educación Superior
COPACO: Compañía Paraguaya de Comunicaciones
CPU: Central Processing Unit (Unidad Central de Procesamiento)
CRM: Administración de Relaciones del Ciudadano con el Estado
CRUD: Create, Read, Update, Delete (Crear, Leer, Actualizar, Eliminar)
DAC: Discretionary Access Control (Control de Acceso Discrecional)
DBMS: Database Management System (Sistema de Gestión de Bases de Datos)
DCIM: Data Center Infrastructure Management (Gestión de Infraestructura de Centro de Datos)
DDoS: Distributed Denial of Service (Denegación de Servicio Distribuida)
DFS: Distributed File System (Sistema de Archivos Distribuido)
DGCPI: Dirección General de Ciberseguridad y Protección de la Información
DGGE: Dirección General de Gobierno Electrónico
DGIC: Dirección General de Infraestructura y Conectividad
DGIDTE: Dirección General de Inclusión Digital y TIC en la Educación

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

DGIPED: Dirección General de Innovación Productiva y Economía Digital
DHCP: Dynamic Host Configuration Protocol (Protocolo de Configuración Dinámica de Host)
DIMM: Dual In-Line Memory Module (Módulo de Memoria de Línea Doble)
DINAPI Dirección Nacional de Propiedad Intelectual
DNP: Departamento Nacional de Planeación de Colombia
DNS: Domain Name System (Sistema de Nombres de Dominio)
DR: Disaster Recovery (Recuperación ante Desastres)
DRAM: Dynamic Random-Access Memory (Memoria de Acceso Aleatorio Dinámica)
DSL: Digital Subscriber Line (Línea de Suscriptor Digital)
DWDM: Dense Wavelength Division Multiplexing (Multiplexación por División en Longitudes de Onda Densas)
EAI: Enterprise Application Integration (Integración de Aplicaciones Empresariales)
EAP: Extensible Authentication Protocol (Protocolo de Autenticación Extensible)
EBD Emprendimiento de Base Digital
ECC: Error-Correcting Code (Código de Corrección de Errores)
ECI Entidad consumidora de la información
EDR: Endpoint Detection and Response (Detección y Respuesta de Puntos de Extremo)
EIGRP: Enhanced Interior Gateway Routing Protocol (Protocolo de Enrutamiento de Puerta de Enlace Interior Mejo
ENCONEC: Estrategia Nacional de Conectividad
EOL: End of Life (Fin de Vida Útil)
EPI: Entidad productora de la información
ERP: Enterprise Resource Planning (Planificación de Recursos Empresariales)
ESXi: Elastic Sky X Integrated (Versión de VMware de su Hipervisor)
FCoE: Fibre Channel over Ethernet (Canal de Fibra sobre Ethernet)
FEEI Fondo para la Excelencia de la Educación y la Investigación
FO: Fibra Óptica
FONTED: Fondo Nacional de Tecnologías en la Educación
FONTIC: Fondo Nacional de Tecnologías de la Información
FTP: File Transfer Protocol (Protocolo de Transferencia de Archivos)
Gbps: Gigabits Per Second (Gigabits Por Segundo)
GDL: Gestor de Documentos en Línea
GPU: Graphics Processing Unit (Unidad de Procesamiento Gráfico)
HBA: Host Bus Adapter (Adaptador de Bus de Host)
HIS: Sistema de Información en Salud
HTTP: HyperText Transfer Protocol (Protocolo de Transferencia de Hipertexto)
HTTPS: HyperText Transfer Protocol Secure (Protocolo Seguro de Transferencia de Hipertexto)
HVAC: Heating, Ventilation, and Air Conditioning (Calefacción, Ventilación y Aire Acondicionado)
I+D+i: Investigación, Innovación y Desarrollo
IA: Inteligencia Artificial
IaaS: Infrastructure as a Service (Infraestructura como Servicio)
IAEE: Instituto de Altos Estudios Estratégicos
ICMP: Internet Control Message Protocol (Protocolo de Mensajes de Control de Internet)
ICT: Information and Communication Technology (Tecnología de la Información y Comunicación)
IDS: Intrusion Detection System (Sistema de Detección de Intrusos)
IDU: Impuesto a los Dividendos y a las Utilidades

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

IGEP: Internet Gratuito en Espacios Públicos
INCUNI: La Incubadora de Empresas de la Universidad Nacional de Itapúa
INE: Instituto Nacional de Estadística
INR: Impuesto a la Renta de No Residentes
IoT: Internet de las cosas
IoT: Internet of Things (Internet de las Cosas)
IP: Internet Protocol (Protocolo de Internet)
IPMI: Intelligent Platform Management Interface (Interfaz de Gestión de Plataforma Inteligente)
IPS: Instituto de Previsión Social
IPS: Intrusion Prevention System (Sistema de Prevención de Intrusiones)
IR: Incident Response (Respuesta a Incidentes)
IRE: Impuesto a la Renta Empresarial
IRP: Impuesto a la Renta Personal
ISCSI: Internet Small Computer System Interface (Interfaz de Sistema de Computadora Pequeña por Internet)
ISP: Internet Service Provider (Proveedor de Servicios de Internet)
ITIL: Information Technology Infrastructure Library (Biblioteca de Infraestructura de Tecnología de la Información)
ITU International Telecommunication Union
IXPy Punto de Intercambio de Internet de Paraguay
JSON: JavaScript Object Notation (Notación de Objetos de JavaScript)
KVM: Kernel-based Virtual Machine (Máquina Virtual Basada en Núcleo)
IaaS: Infraestructura como Servicio
LAN: Local Area Network (Red de Área Local)
LDAP: Lightweight Directory Access Protocol (Protocolo Ligero de Acceso a Directorios)
LUN: Logical Unit Number (Número de Unidad Lógica)
MAC: Media Access Control (Control de Acceso al Medio)
MADES: Ministerio del Ambiente y Desarrollo Sostenible
MAG: Ministerio de Agricultura y Ganadería
Mbps: Megabits Per Second (Megabits Por Segundo)
MEC: Ministerio de Educación y Ciencias
MEF: Ministerio de Economía y Finanzas
MH: Ministerio de Hacienda
MIC: Ministerio de Industria y Comercio
MIPYMES: Pequeñas y Medianas Empresas
MITIC: Ministerio de Tecnologías de la Información y Comunicación
MPLS: Multiprotocol Label Switching (Conmutación de Etiquetas Multiprotocolo)
MSPBS Ministerio de Salud Pública y Bienestar Social
MTBF: Mean Time Between Failures (Tiempo Medio Entre Fallos)
MTTR: Mean Time to Repair (Tiempo Medio para Reparar)
MUVH Ministerio de Urbanismo, Vivienda y Hábitat
NAS: Network Attached Storage (Almacenamiento Conectado a la Red)
NAT: Network Address Translation (Traducción de Direcciones de Red)
NOC Centro de Operación y Atención al Cliente
NOC: Network Operations Center (Centro de Operaciones de Red)
Nube Py: Nube del Estado

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

NVMe: Non-Volatile Memory Express (Interfaz de Memoria No Volátil)
OAuth: Open Authorization (Autorización Abierta)
ODS: Objetivos de Desarrollo Sostenible
ONG: Organización No Gubernamental
OPEX: Operating Expense
OPEX: Operational Expenditure (Gasto Operativo)
OS: Operating System (Sistema Operativo)
OSI: Open Systems Interconnection (Interconexión de Sistemas Abiertos)
OTP: One-Time Password (Contraseña de Un Solo Uso)
PaaS: Platform as a Service (Plataforma como Servicio)
PBX: Private Branch Exchange (Central Telefónica Privada)
PCI: Peripheral Component Interconnect (Interconexión de Componentes Periféricos)
PCI-DSS: Payment Card Industry Data Security Standard (Estándar de Seguridad de Datos de la Industria de Tarjetas
PDU: Power Distribution Unit (Unidad de Distribución de Energía)
PDU: Protocol Data Unit (Unidad de Datos de Protocolo)
PIB: Producto Interno Bruto
PNC: Plan Nacional de Ciberseguridad
PND: Plan Nacional de Desarrollo
PNT: Plan Nacional de Telecomunicaciones
PNTE: Plan Nacional de Transformación Educativa 2030
PNTIC: Plan Nacional de Tecnologías de la Información y la Comunicación
PROINNOVA: Programa de Innovación en Empresas Paraguayas
QA: Quality Assurance
QoS: Quality of Service (Calidad de Servicio)
RAID: Redundant Array of Independent Disks (Matriz Redundante de Discos Independientes)
RDP: Remote Desktop Protocol (Protocolo de Escritorio Remoto)
RFID: Radio-Frequency Identification (Identificación por Radiofrecuencia)
RIPC: Red Integrada de Infraestructura Pública de Conectividad
RMM: Remote Monitoring and Management (Monitoreo y Gestión Remotos)
RMSP Red Metropolitana del Sector Público
ROE Reglamento Operativo Específico
ROM: Read-Only Memory (Memoria de Solo Lectura)
RPM: Revolutions Per Minute (Revoluciones Por Minuto)
RTC: Real-Time Clock (Reloj en Tiempo Real)
RTO: Recovery Time Objective (Objetivo de Tiempo de Recuperación)
RUE Registro Único del Estudiante
SaaS: Software as a Service (Software como Servicio)
SAN: Storage Area Network (Red de Área de Almacenamiento)
SAS: Serial Attached SCSI (SCSI Conectado en Serie)
SATA: Serial Advanced Technology Attachment (Interfaz de Tecnología Avanzada en Serie)
SDN: Software-Defined Networking (Redes Definidas por Software)
SENAC: Secretaría Nacional Anticorrupción
SENATIC: Secretaría Nacional de Tecnologías de la Información y Comunicación
SET: Subsecretaría de Estado de Tributación

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030

SFP: Secretaría de la Función Pública
SFTP: Secure File Transfer Protocol (Protocolo Seguro de Transferencia de Archivos)
SICOM: Secretaría de Información y Comunicación para el Desarrollo
SII: Sistema de Intercambio de Información
SIIS: Sistema Integrado de Información Social
SIP: Sistema de Información Policial
SLA: Service Level Agreement (Acuerdo de Nivel de Servicio)
SLB: Server Load Balancing (Equilibrio de Carga de Servidores)
SMTP: Simple Mail Transfer Protocol (Protocolo Simple de transferencias de correos)
SNC: Servicio Nacional de Catastro
SNMP: Simple Network Management Protocol (Protocolo Simple de Gestion de Redes)
SOC: Centro de Operaciones de Seguridad
STEAM: Ciencia, Tecnología, Ingeniería, Arte y Matemáticas
STP: Secretaría Técnica de Planificación del Desarrollo Económico y Social
TA: Tecnologías Adaptativas
TI: Tecnología e Información
TIC: Tecnologías de la Información y las Comunicaciones
UAT: User Acceptance Testing
UGPR: Unidad de Gestión de la Presidencia de la República
UIS: Instituto de Estadística de la UNESCO
UNA: Universidad Nacional de Asunción
USF: Unidades de Salud Familiar
VPN: Virtual Private Network

Victor Morel
1204808
Consultor

Consultor: Victor Hugo Morel Cattebeke
e-mail: cattebeke@gmail.com
Tel: +595 971 102030