

PROYECTO  
**IOMA CFI**

IMPLEMENTACIÓN  
DEL PLAN DE  
TRANSFORMACIÓN  
DIGITAL EN MATERIA  
DE INFRAESTRUCTURA,  
COMUNICACIONES Y  
MICROINFORMÁTICA



# CONTENIDO

<b>1. Reordenar y organizar la gestión de usuarios del Active Directory de la red IOMA</b> (casa central y delegaciones) y Asistencia en la implementación de un servidor de archivos corporativo	4
<b>1.1.</b> Introducción	
<b>1.2.</b> Alcance	
<b>1.3.</b> Plan de trabajo	
<b>1.4.</b> Tareas realizadas	
<b>2. Asegurar todos los dispositivos de la red corporativa de IOMA (Casa Central)</b>	9
<b>2.1.</b> Introducción	
<b>2.2.</b> Plan de trabajo	
<b>2.3.</b> Situación actual	10
<b>2.4.</b> Ejecución del proyecto	
<b>3. Asistir en el proceso de renovación del parque de PCs en casa central</b>	14
<b>3.1.</b> Introducción	19
<b>3.2.</b> Activos IOMA: Parque de PCs	20
<b>3.3.</b> Detalle de entrega de equipamiento	22
<b>4. Asistir en la implementación de un nuevo sistema de email corporativo</b>	30
<b>4.1.</b> Introducción	30
<b>4.2.</b> Alcance	30
<b>4.3.</b> Plan de trabajo	31
<b>4.4.</b> Implementación	31
<b>5. Generar una política organizacional para normalizar los procesos de backup y restore de la información</b>	35
<b>5.1.</b> Introducción	35
<b>5.2.</b> Objetivo	36
<b>5.3.</b> Responsabilidades	36
<b>5.4.</b> Alcance	37
<b>5.5.</b> Desarrollo de la política	37
<b>5.6.</b> Rutinas de seguimiento y control	40
<b>5.7.</b> Posibles pérdidas de datos	40
<b>5.8.</b> Dispositivos	41
<b>6. Actualizar y normalizar los sistemas operativos de los servidores del datacenter IOMA</b>	42
<b>6.1.</b> Introducción	42
<b>6.2.</b> Alcance y requerimientos	44
<b>6.3.</b> Fundamentos del proyecto	45
<b>6.4.</b> Objetivos del proyecto	45
<b>6.5.</b> Plan de trabajo	45
<b>6.6.</b> Relevamiento de la infraestructura	47
<b>7. Asistencia en la implementación de un sistema de monitoreo para el datacenter IOMA</b>	54
<b>7.1.</b> Introducción	54
<b>7.2.</b> Solución implementada	55
<b>8. Generación de pliego técnico para la adquisición de todo el material necesario y las tareas para recablear la red LAN del edificio de casa central y las principales delegaciones IOMA y pliego técnico para la adquisición y configuración de equipamiento para implementar una red Wifi corporativa en el edificio de casa central y principales delegaciones IOMA.</b>	57
<b>8.1.</b> Objetivo	58
<b>8.2.</b> Alcance	58
<b>8.3.</b> Situación actual	58
<b>8.4.</b> Propuesta	58
<b>8.5.</b> Descripción Del Trabajo	59
<b>8.6.</b> Desarrollo Del Trabajo	59
<b>8.7.</b> Topología de la red	62
<b>8.8.</b> Pliego técnico	62

# 1. REORDENAR Y ORGANIZAR LA GESTIÓN DE USUARIOS DEL ACTIVE DIRECTORY DE LA RED IOMA (CASA CENTRAL Y DELEGACIONES) Y ASISTENCIA EN LA IMPLEMENTACIÓN DE UN SERVIDOR DE ARCHIVOS CORPORATIVO

## 1.1 Introducción

El presente documento tiene como fin dar como solución no solo el servidor de archivos sino también la estructura del *Active Directory*.

Un servidor de archivos o *file server* es una computadora responsable de la gestión y almacenamiento centralizado de archivos, de forma tal que cada equipo de la misma red pueda acceder a los documentos almacenados en el servidor. Un servidor de archivos permite compartir documentos en una red entre usuarios. Al tratarse de un equipo centralizado, es posible definir y aplicar políticas para el contenido que los usuarios pueden almacenar, la cantidad de información, etc.

El uso de un único servidor centralizado permite además la ejecución de procesos de backup sobre dicho servidor, asegurando a los usuarios que, ante una eventual pérdida de algún documento, éste es posible que sea recuperado en una versión lo más reciente posible.

**IOMA** en la actualidad no cuenta con un servidor de estas características, lo que resulta en una falla grave en aspectos de gobernanza de TI, impidiendo aplicar políticas de control sobre la información manejada por los usuarios, cuotas de almacenamiento, control efectivo de virus, imposibilidad de realizar respaldos, etc.

## 1.2 Alcance

El proyecto consto en asistir la implementación de la plataforma, relevando el estado actual, analizando las soluciones accesibles para implementar, diseñando a su vez la arquitectura e implementado los entornos listos para su utilización, como así también la organización del *Active Directory* para que tenga completa armonía con el servidor de archivos

## 1.3 Plan de trabajo

Se analizó la estructura del *Active Directory* y se tomó un nuevo estándar para el manejo de usuario como así también para la estructura de un *file server*.

### Las tareas del plan fueron:

1. Relevar el estado actual
2. Diseñar en base al organigrama actual la estructura de carpetas como así también de usuarios.
3. Dimensionar las necesidades de infraestructura.
4. Preparar los recursos necesarios.
5. Estandarizar y crear las estructuras necesarias.
6. Brindar los accesos para que el equipo correspondiente al instituto procesa con la migración de datos y usuarios al nuevo estándar.

## 1.4 Tareas realizadas

### 1.4 .1 Relevamiento

Actualmente no existe un estándar de estructura para los usuarios ni tampoco un único servidor de archivos.

A continuación, se detalla la estructura existente:

Los usuarios, no se encuentran catalogados dentro de unidades organizativas correspondiente al sector, esto dificulta el

Usuarios y equipos de Active Directory [AC2012R2-1]	Nombre	Tipo	Descripción
Consultas guardadas	BAHI01GL	Usuario	Region Bahia Blanca - Subdeleg. Villa Iris
ioma.central	BAHI01JO	Usuario	Region Bahia Blanca - Deleg. Tres Arroyos
JOMA	BAHI02FC	Usuario	Region Bahia Blanca
Aplicaciones	BAHI03NB	Usuario	Region Bahia Blanca
DGA	BAHI04VB	Usuario	Region Bahia Blanca - Deleg. Bahia Blanca
Equipos	BAHI05AC	Usuario	Region Bahia Blanca - Deleg. Daniel Cerri (del)
Grupos	BAHI06DF	Usuario	Region Bahia Blanca
Recursos Compartidos	BAHI07DM	Usuario	Region Bahia Blanca - Deleg. Orense (del)
Usuarios	BAHI08SK	Usuario	Region Bahia Blanca
Central	BAHI09MM	Usuario	Region Bahia Blanca - Deleg. Coronel Suarez (del)
Delegaciones	BAHI10SR	Usuario	Region Bahia Blanca - Deleg. Bahia Blanca
Especiales	BAHI11MS	Usuario	Region Bahia Blanca - Deleg. Coronel Suarez
Estadística	BAHI12MS	Usuario	Region Bahia Blanca - Deleg. Coronel Suarez
Externos	BAHI13MV	Usuario	Region Bahia Blanca - Deleg. Bahia Blanca
Grabacion	BAHI14JV	Usuario	Region Bahia Blanca - Deleg. Ingeniero White (del)
PMO	BAHI15DC	Usuario	Region Bahia Blanca - Deleg. Tres Arroyos
Produccion	BAHI16PR	Usuario	Region Bahia Blanca
Sistemas	BAHI17AB	Usuario	Region Bahia Blanca - Deleg. Carmen De Patagones (del)
Soporte			

manejo de políticas de seguridad según al sector jerárquico que se encuentran, los usuarios solo se encuentran catalogados por su descripción.

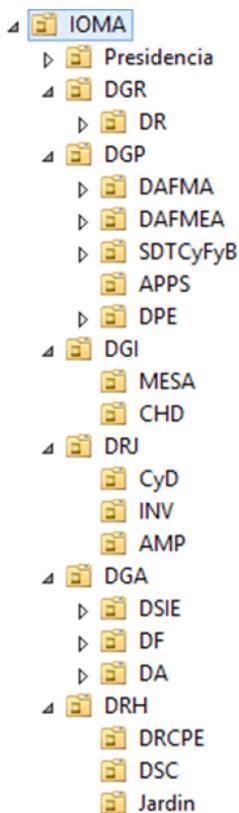
A nivel servidor de archivos, ocurre que cada usuario guarda la información de forma local, pudiendo causar pérdida de información crítica de la organización, como así también fuga de la misma ya que no hay un manejo de la seguridad de la información.

**1.4 .2. Acciones tomadas**

**1.4 .2. 1. A nivel Active Directory**

En post de la estandarización y la mejora de la seguridad se implementó una estructura de organigrama tanto a nivel de servidor de archivos como de estructura organizativa en el *Active Directory*.

A continuación, se muestran los cambios realizados:



Cada unidad organizativa cuenta con su descripción:

	<b>Presidencia</b>	Unidad organizativa	
	<b>DGR</b>	Unidad organizativa	Dirección General de Regionalización
	<b>DGP</b>	Unidad organizativa	Dirección General de Prestaciones
	<b>DGI</b>	Unidad organizativa	Dirección Gestion Institucional
	<b>DRJ</b>	Unidad organizativa	Dirección Relaciones Jurídicas
	<b>DGA</b>	Unidad organizativa	Dirección General de Administracion
	<b>DRH</b>	Unidad organizativa	Dirección Recursos Humanos

Dentro de cada uno de estas, se encuentra la estructura jerárquica la cual permite poder administrar de una manera más transparente las políticas de seguridad que se necesiten implementar.

#### 1.4.2.2.A nivel de file server

Como se puede observar en la imagen anterior, se replicó la misma estructura del Active directory en el file server, de esta



manera se puede manejar una jerarquía no solo en los usuarios sino también en el resguardo de la información.

Datos de la unidad asignada:

**Recurso compartido \\SRVFS03:**

• Ruta de acceso a la carpeta: D:\IOMA

**Nombre del recurso compartido: IOMA**

Ruta de acceso al recurso compartido: \\SRVFS03\IOMA

#### 1.4.3 Jerarquía creada

**1. Presidencia**

1.1. AyP Asesores y Privada

**2. DGR-Dirección General de Regionalización**

**2.1.** DR - Dirección De Regiones

- 2.1.1.** 01-RBB - Región 01 Bahía Blanca
- 2.1.2.** 02-RPJ - Región 02 Rehuajo
- 2.1.3.** 03-RJN - Región 03 Junin
- 2.1.4.** 04-RPE - Región 04 Pergamino
- 2.1.5.** 05-RSI - Región 05 San Isidro
- 2.1.6.** 06-RLZ - Región 06 Lomas de Zamora
- 2.1.7.** 07-RMR - Región 07 Moron
- 2.1.8.** 08-RGP - Región 08 General Pueyrredon
- 2.1.9.** 09-ROL - Región 09 Olvarria
- 2.1.10.** 10-RSA - Región 10 Saladillo
- 2.1.11.** 11-RLP - Región 11 La Plata
- 2.1.12.** 12-RLM - Región 12 La Matanza
- 2.1.13.** 13-RCB - Región 13 CABA
- 2.1.14.** 14-RDL - Región 14 Dolores

**3. DGP - Dirección General de Prestaciones**

**3.1. DAFMA - Dirección Auditoría y Fiscalización Médico Ambulatoria**

- 3.1.1.** AUFO - Auditoría y Fiscalización Odontológica
- 3.1.2.** AUFMA - Auditoría y Fiscalización Médico Ambulatoria

**3.2. DAFMEA - Dirección Auditoría y Fiscalización Médica de Establecimientos Asistenciales**

- 3.2.1.** DepAFMEA Depto. Auditoría y Fiscalización Médica de Establecimientos Asistenciales
  - 3.2.1.1.** AUINT - Auditoría de Internaciones
- 3.2.2.** SDTCyFyB - Subdirección Técnico Científica y de Farmacia y Bioquímica
  - 3.2.2.1.** AUFFyB - Auditoría y Fiscalización Farmacia y Bioquímica
  - 3.2.2.2.** DTC - Departamento Técnico Científico
  - 3.2.2.3.** APPS - Area unidad de prevención y promoción de la salud
  - 3.2.2.4.** DPE - Dirección Programas Específicos
  - 3.2.2.5.** DVGM - Departamento Veteranos de Guerra de Malvinas
  - 3.2.2.6.** DSoc - Departamento Sociales
  - 3.2.2.7.** DDR - Departamento Discapacidad y Rehabilitación

**3.3. DGI - Dirección Gestión Institucional**

- 3.3.1.** MESA - Mesa de entradas, salidas y archivo
- 3.3.2.** CHD - Coordinación Honorable Directorio

**4. DRJ - Dirección Relaciones Jurídicas**

- 4.1.** CyD - Convenios y Dictámenes
- 4.2.** INV - Investigaciones
- 4.3.** AMP - Amparos

**5. DGA - Dirección General de Administración**

**5.1.** DF - Dirección Finanzas

- 5.1.1.** DR - Departamento Rendiciones
- 5.1.2.** SDT - Subdirección Tesorería
  - 5.1.2.1.** DRECAU - Departamento Recaudaciones
  - 5.1.2.2.** DP - Departamento Pagos
- 5.1.3.** SDCS - Subdirección Compras y Suministros
- 5.1.4.** SDC - Subdirección Contable
  - 5.1.4.1.** DRECUR - Departamento Recursos
  - 5.1.4.2.** DLIQ - Departamento Liquidaciones

**5.2 DA - Dirección Afiliaciones**



### 1.4 .5. Consideraciones

Dichas tareas fueron ejecutadas en los ambientes del Instituto, no se ejecutaron migraciones de usuario, ni ejecutaron políticas de seguridad, por posibles impactos en los usuarios finales, recomendamos que el encausar cada usuario en su nueva unidad organizativa y mapear la unidad de disco del file server tiene que ser realizada por personal del instituto.

## 2. ASEGURAR TODOS LOS DISPOSITIVOS DE LA RED CORPORATIVA DE IOMA (CASA CENTRAL)

### 2.1. Introducción

La seguridad en los dispositivos de red es extremadamente importante para la seguridad informática de cualquier organización, y en IOMA no es la excepción.

El edificio de Casa Central tiene una estructura edilicia de grandes proporciones, lo que implica necesariamente una gran cantidad de hardware de red instalado en cada piso para poder brindar todos los servicios ofrecidos por la Dirección de Sistemas.

Cada dispositivo de la red (*routers, switches, firewalls, etc.*) es administrable en forma remota, accediendo a este mediante un usuario y contraseña.

El proyecto actual trabajó sobre esta vulnerabilidad, realizando tareas específicas en pos de asegurar los dispositivos de red relevados en Casa Central.

Descripción del problema

#### 2.1.1. Los passwords por defecto en dispositivos de red

Los passwords por defecto existen en casi cada sistema operativo, sistema, dispositivo y aplicación. Un requerimiento estándar de la política de seguridad informática de IOMA debería contemplar el cambio inmediato de la contraseña de administrador de cualquier dispositivo, en el mismo momento en que se trabaja sobre su configuración, pero esto no sucede así.

Cada dispositivo de infraestructura de red es entregado por parte del proveedor con una contraseña “de fábrica” (estas contraseñas son muy triviales, tales como “password”, “0000”, “admin”, etc.). Si esta contraseña no es cambiada de manera inmediata, el dispositivo en cuestión queda vulnerable a ser accedido por cualquier externo que busque ganar acceso al dispositivo y, por ende, a la red. Si bien IOMA cuenta con un firewall que impide el acceso de cualquier usuario externo a la red local, un usuario accediendo desde la misma red tiene la facilidad de actuar sobre un dispositivo (tal como un router) y modificar aspectos de su configuración.

Esto puede ser causado por atacantes, hackers, empleados o terceros disconformes por algún motivo. Si los dispositivos de red presentan servicios administrativos abiertos sin un control, es muy fácil para un atacante acceder a los equipos y escalar en privilegios en la red interna, afectando la integridad de las configuraciones. Los equipos de red con servicios activos no necesarios y puertos abiertos son oportunidades para que atacantes pueda tomar control del equipo de red.

Y para cada dispositivo al cual se conectó se utilizó una herramienta

### 2.2. Plan de trabajo

Se propuso llevar adelante un relevamiento detallado de cada dispositivo de la red IOMA que fueses susceptible a este tipo de ataques. Se realizó un análisis piso por piso de Casa Central, accediendo al dispositivo, verificando la contraseña utilizada y cambiando esta siguiendo los lineamientos planteados en este documento.

#### 2.2.1. Lineamientos para contraseñas seguras

Una política de contraseñas seguras define un conjunto de reglas creadas pura y exclusivamente para que cada contraseña en una Organización (dispositivos, computadoras, aplicaciones, sistemas, etc.) se haga siguiendo lineamientos específicos que apunten a minimizar los riesgos de que dichas contraseñas sean comprometidas.

##### 2.2.1.1. Forzar el uso de contraseñas seguras

Las contraseñas son la primera línea de protección contra cualquier acceso no autorizado a un dispositivo. Cuánto más robusta sea la contraseña utilizada, más alto el nivel de seguridad con que el dispositivo cuenta contra ataques.

#### Características de las contraseñas utilizadas para el proyecto:

- Mínimo 8 caracteres de largo
- Contiene al menos un número, un símbolo, una letra mayúscula y una letra minúscula.
- No contiene ninguna palabra completa dentro del mismo.

#### 2.2.2. Test de puertos abiertos

Cuando una aplicación se conecta a Internet hace uso de un puerto para poder establecer la conexión. Un router

1. <https://proprivacy.com/guides/default-router-login-details>

cuenta con 65,535 puertos, o caminos, diferentes a través de los cuales se envían datos al exterior o bien se reciben datos desde un cliente o servidor externo. Para que estas conexiones puedan establecerse es necesario que estos puertos estén “abiertos”, es decir, que el tráfico de datos esté permitido a través de ellos.

### 2.2.2.1. Análisis de puertos

Para los dispositivos analizados en la red IOMA, se realizó un análisis de puertos. Los 65535 puertos diferentes son posibles de clasificar en 3 grupos:

- **Del puerto 1 al 1023** – Están reservados para el sistema operativo y los protocolos estándar.
- **Del puerto 1024 al 49151** – Son comúnmente utilizados por la mayoría de las aplicaciones.
- **Del puerto 49152 al 65535** – Están reservados para las aplicaciones que necesitan conectarse a un servidor.

Por lo general, los routers por defecto mantienen abiertos los puertos críticos (como el 80, necesario para las conexiones HTTP o el 443 utilizado en las conexiones HTTPS) y, a medida que se necesitan, se deberán manualmente. Para el análisis de puertos se trabajó con un equipo portátil, con la aplicación *SoftPerfect Network Scanner*<sup>2</sup>, lo que permitió realizar un análisis detallado de cada puerto en cada dispositivo.

## 2.3. Situación actual

Actualmente, el Instituto de Obra Médico Asistencial (IOMA) cuenta con un rack de piso en cada una de las plantas del edificio. A su vez, cada rack contiene, además del switch de fibra, uno o más switches de gestión de distintos fabricantes (Alcatel – 3Com – D Link – Cisco – TP Link).

## 2.4. Ejecución del proyecto

Para esta tarea, se relevó cada rack de piso a fin de conocer la cantidad de switches que dispone IOMA. Con esta información se estableció cuáles deben ser los estándares que se deben cumplir teniendo presente los aspectos definidos de Política de Seguridad de este documento y las políticas de contraseñas definidas por IOMA a fin de llevar adelante una regularización respecto a las contraseñas de gestión de los equipos.

Esta estandarización de contraseñas se pudo realizar sobre los equipos de marca Alcatel 6224 y 6602, equipos marca 3Com 3C16471 y equipo marca Cisco 3945.

### 2.4.1 Detalle del trabajo realizado

#### 2.4.1.1. Resumen de dispositivos

TIPO DE DISPOSITIVO	MARCA	UBICACIÓN	CANTIDAD
Switch	3Com	Piso 3	1
		Piso 4	1
		Piso 6	2
		Piso 7	1
		Piso 10	1
		Piso 11	1
		<b>Total 3Com</b>	<b>8</b>
	Alcatel	PB	2
		Piso 1	2
		Piso 2	1
		Piso 6	1
		Piso 7	1
Piso 8		2	
	<b>Total Alcatel</b>	<b>10</b>	
Cisco	Piso 8	1	
	<b>Total Cisco</b>	<b>1</b>	
D-Link	Piso 3	1	
	Piso 5	1	
	Piso 8	2	
	Piso 9	2	
	Piso 11	1	
	Piso 12	1	
	Piso 13	1	
	<b>Total D-Link</b>	<b>9</b>	
TP Link	Piso 3	1	
	Piso 7	1	
	<b>Total TP Link</b>	<b>2</b>	
Transition	Piso 8	1	
	<b>Total Transition</b>	<b>1</b>	
	<b>Total Switch</b>	<b>31</b>	
	<b>Total general</b>	<b>31</b>	

2. <https://www.softperfect.com/products/networkscanner/>

### 2.4.1.2. Tareas generales

Luego de haber reasignado posiciones de red en equipos que se encontraban sin actividad a equipos con puertos sin patchear se consiguió liberar switches que se encuentran ociosos. Esta tarea se realizó de forma parcial debido a la constante actividad de la Obra Social. Los equipos liberados deberán reasignarse a aquellos racks que cuentan con switches de marca D-Link y TP-Link con el propósito de unificar de forma uniforme todos los racks. Realizar esta tarea aporta como beneficio una mejor gestión de los equipos.

### 2.4.1.3. Trabajo realizado por cada dispositivo

UBICACIÓN	TIPO DE DISPOSITIVO	MARCA	MODELO	PROBLEMA DETECTADO	TAREAS REALIZADAS
PB	Switch	Alcatel	6224	<ul style="list-style-type: none"> <li>• Password por defecto</li> <li>• Puertos abiertos inseguros</li> </ul>	<ul style="list-style-type: none"> <li>• Se asignó password robusta</li> <li>• Se configuraron los puertos en relación con el uso del equipo</li> </ul>
PB	Switch	Alcatel	6602	<ul style="list-style-type: none"> <li>• No cumplía política de contraseña segura</li> <li>• Puertos abiertos inseguros</li> </ul>	<ul style="list-style-type: none"> <li>• Se asignó password robusta</li> <li>• Se configuraron los puertos en relación con el uso del equipo</li> </ul>
Piso 1	Switch	Alcatel	6224	<ul style="list-style-type: none"> <li>• Con password por defecto</li> </ul>	<ul style="list-style-type: none"> <li>• Se asignó password robusta</li> </ul>
Piso 1	Switch	Alcatel	6602	<ul style="list-style-type: none"> <li>• Con password defecto</li> <li>• Puertos abiertos inseguros</li> </ul>	<ul style="list-style-type: none"> <li>• Se asignó password robusta</li> <li>• Se configuraron los puertos en relación con el uso del equipo</li> </ul>
Piso 2	Switch	Alcatel	6224	<ul style="list-style-type: none"> <li>• Con password defecto</li> <li>• Puertos abiertos inseguros</li> </ul>	<ul style="list-style-type: none"> <li>• Se asignó password robusta</li> <li>• Se configuraron puertos en relación con el uso del equipo</li> </ul>
Piso 3	Switch	TP Link	TLSG1016	<ul style="list-style-type: none"> <li>• Sin password asignado</li> </ul>	<ul style="list-style-type: none"> <li>• Se asignó password robusta</li> </ul>
Piso 3	Switch	D-Link	DES 3852	<ul style="list-style-type: none"> <li>• Sin password asignado</li> <li>• Puertos abiertos inseguros</li> </ul>	<ul style="list-style-type: none"> <li>• Se asignó password robusta</li> <li>• Se configuraron los puertos en relación con el uso del equipo</li> </ul>
Piso 3	Switch	3Com	C17300A	<ul style="list-style-type: none"> <li>• No cumplía política de contraseña segura</li> <li>• Puertos abiertos inseguros</li> </ul>	<ul style="list-style-type: none"> <li>• Se asignó password robusta</li> <li>• Se configuraron los puertos en relación con el uso del equipo</li> </ul>
Piso 4	Switch	3Com	3C16471	<ul style="list-style-type: none"> <li>• No cumplía política de contraseña segura</li> <li>• Puertos abiertos inseguros</li> </ul>	<ul style="list-style-type: none"> <li>• Se asignó password robusta</li> <li>• Se configuraron los puertos en relación con el uso del equipo</li> </ul>
Piso 5	Switch	D-Link	DGS1210-52	<ul style="list-style-type: none"> <li>• Password en blanco</li> <li>• Puertos abiertos inseguros</li> </ul>	<ul style="list-style-type: none"> <li>• Se asignó password robusta</li> <li>• Se configuraron los puertos en relación con el uso del equipo</li> </ul>

UBICACIÓN	TIPO DE DISPOSITIVO	MARCA	MODELO	PROBLEMA DETECTADO	TAREAS REALIZADAS
Piso 6	Switch	3Com	3C16471	<ul style="list-style-type: none"> <li>• No cumplía política de contraseña segura</li> <li>• Puertos abiertos inseguros con el uso del equipo</li> </ul>	<ul style="list-style-type: none"> <li>• Se asignó password robusta</li> <li>• Se configuraron los puertos en relación</li> </ul>
Piso 6	Switch	Alcatel	6602 por defecto	<ul style="list-style-type: none"> <li>• Con password robusta</li> </ul>	<ul style="list-style-type: none"> <li>• Se asignó password robusta</li> </ul>
Piso 6	Switch	3Com	3C16471 BS	<ul style="list-style-type: none"> <li>• No cumplía política de contraseña segura</li> <li>• Puertos abiertos inseguros</li> </ul>	<ul style="list-style-type: none"> <li>• Se asignó password robusta</li> <li>• Se configuraron los puertos en relación con el uso del equipo</li> </ul>
Piso 7	Switch	TP Link	TLSG1016	<ul style="list-style-type: none"> <li>• Password en blanco</li> <li>• Puertos abiertos inseguros</li> </ul>	<ul style="list-style-type: none"> <li>• Se asignó password robusta</li> <li>• Se configuraron los puertos en relación con el uso del equipo</li> </ul>
Piso 7	Switch	Alcatel	6602	<ul style="list-style-type: none"> <li>• Con password por defecto</li> </ul>	<ul style="list-style-type: none"> <li>• Se asignó password robusta</li> </ul>
Piso 7	Switch	3Com	3C16471	<ul style="list-style-type: none"> <li>• Con password por defecto</li> <li>• Puertos abiertos inseguros</li> </ul>	<ul style="list-style-type: none"> <li>• Se asignó password robusta</li> <li>• Se configuraron los puertos en relación con el uso del equipo</li> </ul>
Piso 8	Switch	D-Link	DGS3100	<ul style="list-style-type: none"> <li>• Password en blanco</li> <li>• Puertos abiertos inseguros</li> </ul>	<ul style="list-style-type: none"> <li>• Se asignó password robusta</li> <li>• Se configuraron los puertos en relación con el uso del equipo</li> </ul>
Piso 8	Switch	D-Link	Star 3120	<ul style="list-style-type: none"> <li>• Password en blanco</li> </ul>	<ul style="list-style-type: none"> <li>• Se asignó password robusta</li> </ul>
Piso 8	Switch	Alcatel	6602	<ul style="list-style-type: none"> <li>• No cumplía política de contraseña segura</li> <li>• Puertos abiertos inseguros</li> </ul>	<ul style="list-style-type: none"> <li>• Se asignó password robusta</li> <li>• Se configuraron los puertos en relación con el uso del equipo</li> </ul>
Piso 8	Switch	Alcatel	6602	<ul style="list-style-type: none"> <li>• Con password por defecto</li> <li>• Puertos abiertos inseguros</li> </ul>	<ul style="list-style-type: none"> <li>• Se asignó password robusta</li> <li>• Se configuraron los puertos en relación con el uso del equipo</li> </ul>
Piso 8	Switch	Cisco	3945	<ul style="list-style-type: none"> <li>• No cumplía política de contraseña segura</li> <li>• Puertos abiertos inseguros</li> </ul>	<ul style="list-style-type: none"> <li>• Se asignó password robusta</li> <li>• Se configuraron los puertos en relación con el uso del equipo</li> </ul>

UBICACIÓN	TIPO DE DISPOSITIVO	MARCA	MODELO	PROBLEMA DETECTADO	TAREAS REALIZADAS
Piso 8	Switch	Transition	SM4T4DPA	<ul style="list-style-type: none"> <li>• Password por defecto</li> </ul>	<ul style="list-style-type: none"> <li>• Se asignó password robusta</li> </ul>
Piso 9	Switch	D-Link	3052	<ul style="list-style-type: none"> <li>• Password en blanco</li> <li>• Puertos abiertos inseguros</li> </ul>	<ul style="list-style-type: none"> <li>• Se asignó password robusta</li> <li>• Se configuraron los puertos en relación con el uso del equipo</li> </ul>
Piso 9	Switch	D-Link	DES 1252	<ul style="list-style-type: none"> <li>• Password en blanco</li> <li>• Puertos abiertos inseguros</li> </ul>	<ul style="list-style-type: none"> <li>• Se asignó password</li> <li>• Se configuraron los puertos en relación con el uso del equipo</li> </ul>
Piso 10	Switch	3Com	2024	<ul style="list-style-type: none"> <li>• No cumplía política de contraseña segura</li> <li>• Puertos abiertos inseguros</li> </ul>	<ul style="list-style-type: none"> <li>• Se actualizó password</li> <li>• Se configuraron los puertos en relación con el uso del equipo</li> </ul>
Piso 10	Switch	Alcatel	6602	<ul style="list-style-type: none"> <li>• No cumplía política de contraseña segura</li> <li>• Puertos abiertos inseguros</li> </ul>	<ul style="list-style-type: none"> <li>• Se asignó password robusta</li> <li>• Se configuraron los puertos en relación con el uso del equipo</li> </ul>
Piso 11	Switch	D-Link	DES1210	<ul style="list-style-type: none"> <li>• Password en blanco</li> <li>• Puertos abiertos inseguros</li> </ul>	<ul style="list-style-type: none"> <li>• Se asignó password</li> <li>• Se configuraron los puertos en relación con el uso del equipo</li> </ul>
Piso 11	Switch	3Com	3C16471	<ul style="list-style-type: none"> <li>• Password en blanco</li> <li>• Puertos abiertos inseguros</li> </ul>	<ul style="list-style-type: none"> <li>• Se asignó password</li> <li>• Se configuraron los puertos en relación con el uso del equipo</li> </ul>
Piso 12	Switch	D-Link	DES 1252	<ul style="list-style-type: none"> <li>• No cumplía política de contraseña segura</li> </ul>	<ul style="list-style-type: none"> <li>• Se asignó password robusta</li> </ul>
Piso 12	Switch	3Com	3C16471	<ul style="list-style-type: none"> <li>• No cumplía política de contraseña segura</li> <li>• Puertos abiertos inseguros</li> </ul>	<ul style="list-style-type: none"> <li>• Se asignó password robusta</li> <li>• Se configuraron los puertos en relación con el uso del equipo</li> </ul>
Piso 13	Switch	D-Link	DES 1252	<ul style="list-style-type: none"> <li>• No cumplía política de contraseña segura</li> </ul>	<ul style="list-style-type: none"> <li>• Se actualizó password</li> </ul>

### 3. ASISTIR EN EL PROCESO DE RENOVACIÓN DEL PARQUE DE PCS EN CASA CENTRAL

#### 3.1 Introducción

La gestión de activos de TI es un conjunto de prácticas comerciales que unen funciones financieras, contractuales y de inventario para respaldar la gestión del ciclo de vida y la toma de decisiones estratégicas para el entorno de TI<sup>3</sup>. La administración de los activos de TI le permite obtener el máximo valor del uso de los activos, el inventario de TI y optimizar las decisiones y estrategias de compra de inventario. La gestión de activos de TI proporciona los medios para lograr una visibilidad completa de su inventario de infraestructura de TI, ayudándole a obtener una comprensión profunda de:

- ¿Qué sistemas y equipos existen?
- Dónde residen los componentes
- Cómo se usan
- Lo que cuestan
- ¿Cuándo se agregaron al inventario?
- Si tienen una fecha de vencimiento
- Cómo impactan los servicios de

Este nivel de visibilidad de los detalles de los activos ayudará a la organización a mejorar la eficiencia y el rendimiento de la infraestructura y minimizar los gastos generales relacionados. Todas las organizaciones, de una forma u otra, deben realizar una "Gestión de Activos de IT (ITAM – IT Asset Management)". Es importante implementar las prácticas de ITAM de manera inteligente, para lograr la eficiencia operativa de TI.

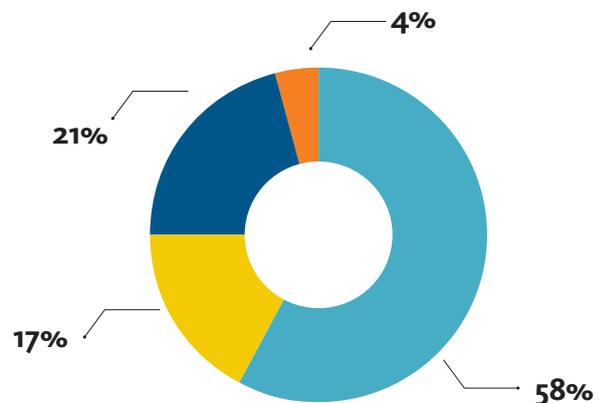
#### 3.2. Activos IOMA: Parque de PCs

##### 3.2.1. Situación actual<sup>4</sup>

El parque de PCs actual no cumple con las necesidades de la Organización. Considerando el sistema operativo de cada equipo actualmente en uso en IOMA (casa central) es posible determinar la viabilidad y capacidad de cada computadora, y el resumen se presenta a continuación:

Sistema Operativo PC	Cantidad
Windows 10 Pro	121
Windows 2000 Professional	1
Windows 7 Enterprise	148
Windows 7 Ultimate	3
Windows 8.1 Enterprise	26
Windows XP Professional	415
<b>Total general</b>	<b>714</b>

- Windows 10 Pro
- Windows 7 Ultimate= o
- Windows 2000 Professional= o
- Windows 8.1. Enterprise
- Windows 7 Enterprise
- Windows XP Professional



3. [https://es.wikipedia.org/wiki/Gesti%C3%B3n\\_de\\_activos\\_de\\_software](https://es.wikipedia.org/wiki/Gesti%C3%B3n_de_activos_de_software)  
 4. Información relevada en la etapa I de la consultoría, que a la fecha de generación del presente informe se determinó que la situación no había cambiado.

En la actualidad, Microsoft Windows XP se encuentra fuera de soporte por parte del proveedor, porque es considerado obsoleto. En el gráfico anterior surge a las claras que el 58% de equipos de PC de Casa Central tienen ese sistema operativo, y por las características técnicas de las computadoras.

En relación con los equipos ubicados fuera de casa central, de las entrevistas sostenidas surge una cantidad aproximada de 700 computadoras adicionales (sobre este equipamiento no fue posible obtener las características técnicas detalladas de cada uno). Respetando la proporción anterior, este equipo de trabajo infiere que un mínimo de 415 equipos no cumple con las características mínimas requeridas para el uso actual.

De lo anterior surge un total de equipos de PC disponibles de alrededor de 1400, con al menos 800 obsoletos y que requieren ser cambiados por nuevos.

Sumado a esto, hay que considerar que la cantidad de empleados de IOMA en la actualidad es de aproximadamente 2.500, la cual excede sustancialmente la cantidad de equipos disponibles.

En resumen:

#### Resumen parque de PCs

PCs Casa Central	714
PCs Delegaciones (*)	700
<b>Total PCs</b>	<b>1414</b>
Equipos obsoletos (*)	848
Equipos disponibles (*)	566
Empleados IOMA (*)	2500
<b>Déficit equipos/empleados (*)</b>	<b>1934</b>

### 3.2.2 Proyecto de asistencia

El objetivo del presente proyecto consistió en brindar asistencia a la Dirección de Sistemas IOMA en la ejecución de un plan de renovación del parque de PCs actual, a fin de lograr contar con equipamiento con:

- Soporte técnico actualizado
- Capacidades de procesamiento adecuadas
- Capacidades de almacenamiento adecuadas
- Con capacidad suficiente para la correcta ejecución de los sistemas de IOMA

A los fines de la renovación, la Dirección de Sistemas coordinó la adquisición de un total de 965 PCs para reemplazar los equipos más viejos de la Organización, de los cuales:

#### • 821 equipos de escritorio, marca EXO, con las siguientes características de hardware:

- **Modelo:** H7X-V5448
- **Procesador:** Intel® Core™ i5-7400
- **Memoria RAM:** 4Gb
- **Disco rígido:** 1Tb
- **Sistema Operativo:** Microsoft Windows Pro

#### • 144 notebooks marca Dell, con las siguientes características:

- **Modelo:** Vostro 14 3000 Series 3468
- **Procesador:** Intel® Core™ i5-7200U
- **Memoria RAM:** 8Gb
- **Disco rígido:** 1Tb
- **Pantalla:** 14 pulgadas
- **Sistema Operativo:** Microsoft Windows 10 Pro

(\*) Números aproximados, el valor exacto no fue posible de determinar a partir de los relevamientos realizados.

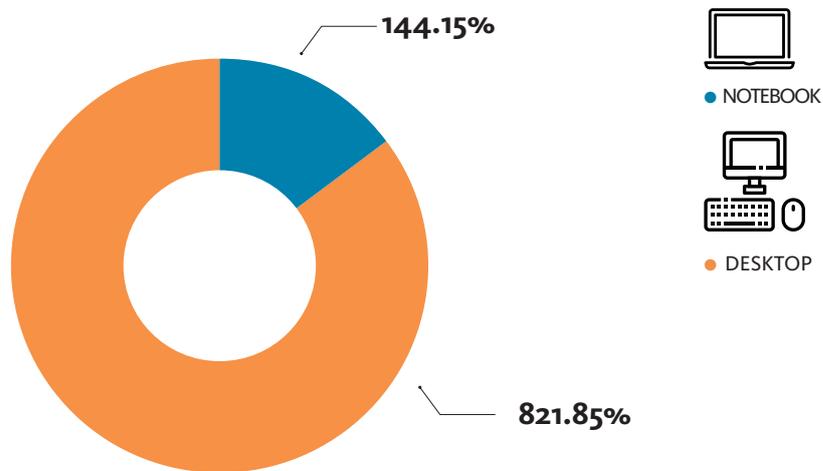
### 3.2.3. Plan de renovación

Si bien no existe un plan formalizado de entrega del equipamiento adquirido, las entregas e instalaciones de los equipos se realizó de forma sistematizada, generalmente siguiendo pedidos específicos de cada una de las áreas. Se cuenta con un sistema de gestión de activos que responde satisfactoriamente a las necesidades de la organización, y le permite a la Dirección contar con un seguimiento detallado de cada uno de los equipos entregados y en stock.

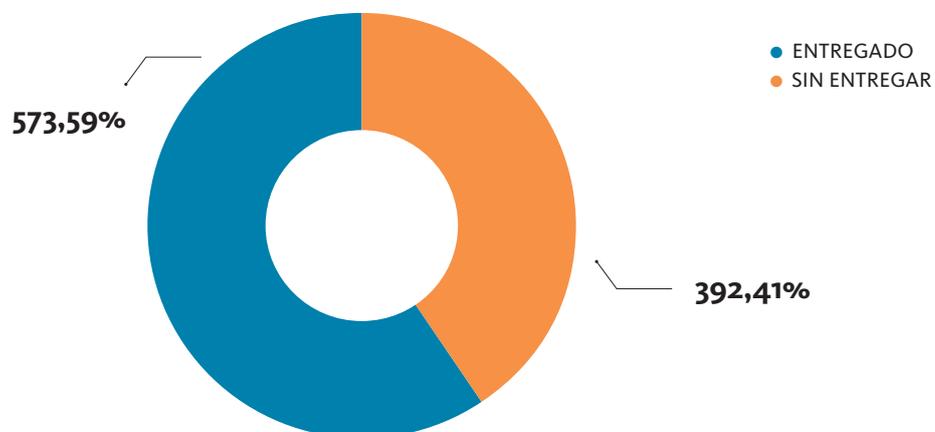
## 3.3. Detalle de entrega de equipamiento

A continuación, se presenta el detalle del estado de entrega del equipamiento adquirido:

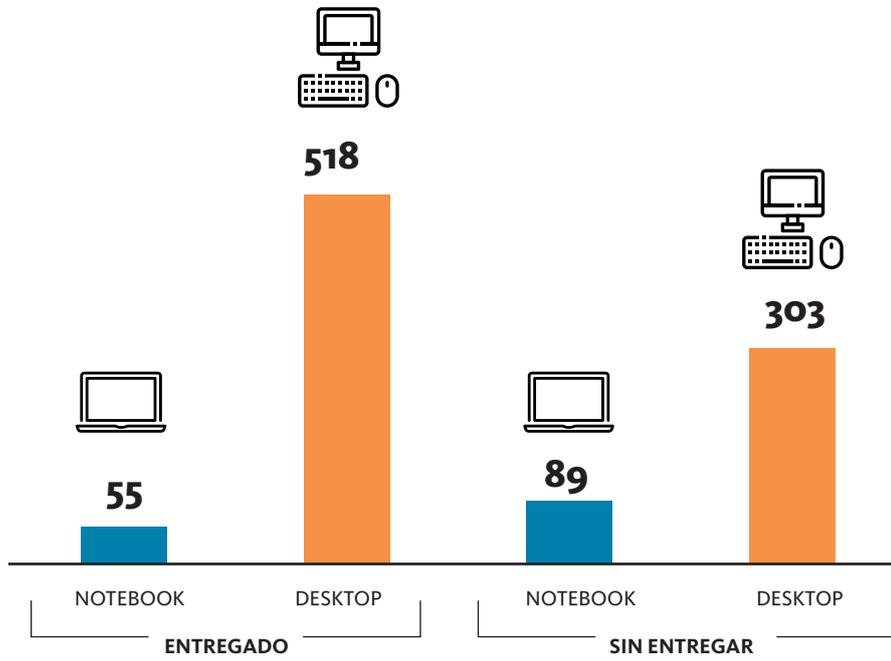
### 3.3.1. Total de equipamiento adquirido



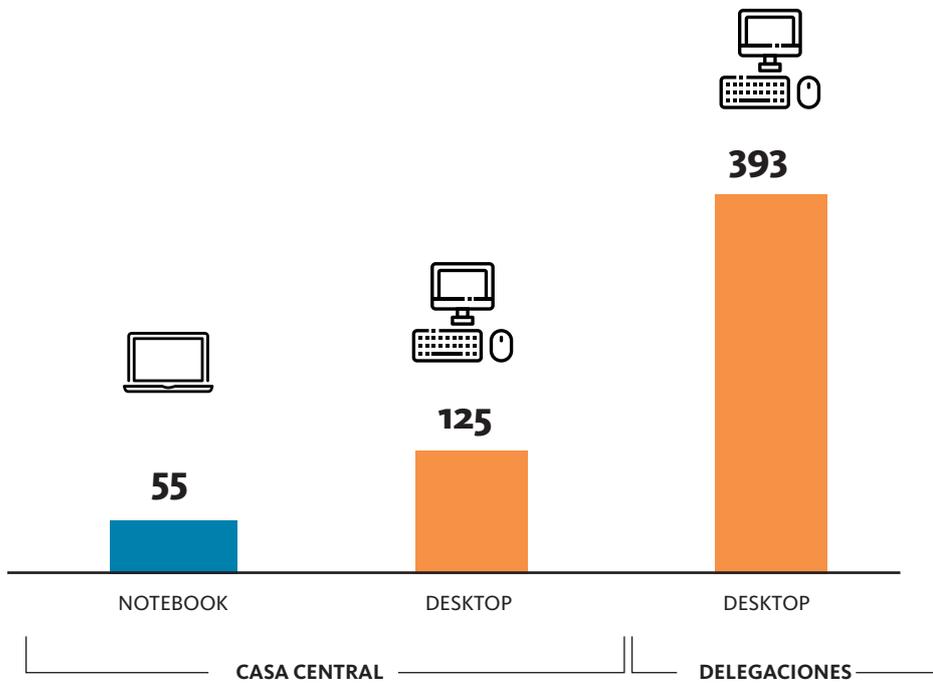
### 3.3.2. Total estado de instalación de equipamiento



3.3.3. Total estado de instalación de equipamiento por tipo de PC



3.3.4. Total instalado por delegación y tipo de PC



**3.3.5. Detalle de equipamiento instalado**

**3.3.5.1. Total Casa Central**

<b>PISO</b>	<b>SECTOR</b>	<b>TIPO</b>	<b>CANTIDAD</b>
Po0	ANEXO - REND.CUENTAS (DCCION. DE FINANZAS) Po0	Desktop	1
	COMISION DE PRESTACIONES Po0	Desktop	3
	DIRECTORIO (DIR. GESTION INSTITUCIONAL) Po0	Desktop	13
	MESA DE ENTRADAS (DIR. GEST. INSTITUCIONAL) Po0	Desktop	9
	DCCION. GRAL. DE REGIONALIZACION Po1	Notebook	2
Po1	VOCALIA Po1	Desktop	7
		Notebook	1
Po2		Desktop	1
	ASUNTOS PUBLICOS Po1	Desktop	1
	PRESIDENCIA Po1	Desktop	2
	REGIONES Po1	Desktop	2
	DCCION. DE GESTION INSTITUCIONAL. Po2	Notebook	1
		Desktop	1
	DCCION. RELACIONES JURIDICAS Po2	Desktop	2
	SECTOR AMPAROS (JURIDICAS) Po2	Desktop	3
	SECTOR REG. Y COMUNICACIONES (DIR. GEST. INST) Po2	Desktop	9
	Po3	SUBD. FARMACIA Po3	Notebook
		Desktop	2
DEPTO. AUDIT. Y FISC. FARMACIA Y BIOQ. (SUB, FARM) Po3		Desktop	1
SECTOR AMPAROS (SUBDIR. FARMACIA) Po3		Desktop	3
Po4	DEPTO. RECURSOS (SUBDIR. CONTABLE) Po4	Notebook	1
	DEPTO. LIQUIDACIONES (SUBDIR. CONTABLE) Po4	Desktop	4
Po5	RECAUDACIONES (DIR. DE FINANZAS) Po5	Desktop	5
Po6	DEPTO. AFIL. VOLUNTARIOS Y CONVESPEC.(DIR. AFIL) Po6	Desktop	5
	DEPTO. AFILIADOS OBLIGATORIOS (DIR. AFILIACIONES) Po6	Desktop	2
	SECTOR AFILIADOS VOLUNTARIOS (DIR. AFILIACIONES) Po6	Desktop	1
Po7	ASESORIA PRESIDENCIA Po7	Notebook	1
	DCCION. DE FINANZAS (REINTEGROS) Po7	Notebook	2
		Desktop	1
	DCCION. GRAL. DE ADMINISTRACION Po7	Notebook	1
		Desktop	1
	SUELDOS (DIR. DE FINANZAS) Po7	Notebook	2
	Desktop	2	

Po8	DCCION. SISTEMAS DE INFORMACION ESTAD. Po8	Notebook	3
	DEPTO. SISTEMAS Po8	Notebook	4
	DEPTO. SOPORTE TECNICO - EN USO Po8	Notebook	3
	DEPTO. SOPORTE TECNICO - PARA REPARAR O GARANTIA Po8	Notebook	1
	<hr/>		
Po9	DCCION. DE PROGRAMAS ESPECIFICOS Po9	Notebook	3
<hr/>			
P10	DCCION. AUD. Y FISC. MEDICA DE EST. ASISTENCIALES P10	Notebook	22
<hr/>			
P11	DCCION. AUD. Y FISC. MEDICO AMBULATORIA P11	Notebook	3
		Desktop	26
<hr/>			
P12	DCCION. RECURSOS HUMANOS P12	Desktop	10
	DEPTO. REGISTRO CTROL. PLANTEL Y ESTRUC (DIR RRHH) P12	Desktop	5
<hr/>			
P13	UNIDAD PREVENCION Y PROMOCION DE LA SALUD P13	Notebook	1
		Desktop	1
<hr/>			
P2S	AREA INFRAESTRUCTURA - SECTOR PLANEAMIENTO P13	Desktop	1
	SECTOR AUTOMOTORES P2S	Notebook	2
		Desktop	1
<hr/>			
<b>TOTAL GENERAL</b>			<b>180</b>

### 3.3.5.1. Total Delegaciones

REF.	SECTOR	TIPO	CANTIDAD
RBB	DCCION. REG. BAHIA BLANCA	Desktop	7
	DELEG. ADOLFO ALSINA - CARHUE ( BAHIA BLANCA )	Desktop	2
	DELEG. CARMEN DE PATAGONES ( BAHIA BLANCA )	Desktop	2
	DELEG. CASBAS ( BAHIA BLANCA )	Desktop	2
	DELEG. CERRI -VILLA IRIS ( BAHIA BLANCA )	Desktop	2
	DELEG. CNEL. PRINGLES ( BAHIA BLANCA )	Desktop	2
	DELEG. CNEL.DORREGO ( BAHIA BLANCA )	Desktop	2
	DELEG. CNEL.ROSALES ( BAHIA BLANCA )	Desktop	2
	DELEG. CNEL.SUAREZ ( BAHIA BLANCA )	Desktop	3
	DELEG. GONZALES CHAVEZ ( BAHIA BLANCA )	Desktop	2
	DELEG. GUAMINI ( BAHIA BLANCA )	Desktop	2
	DELEG. HUANGUELEN ( BAHIA BLANCA )	Desktop	1
	DELEG. M.BURATOVICH ( BAHIA BLANCA )	Desktop	2
	DELEG. MONTE HERMOSO ( BAHIA BLANCA )	Desktop	2
	DELEG. ORENSE ( BAHIA BLANCA )	Desktop	1
	DELEG. ORIENTE ( BAHIA BLANCA )	Desktop	2
	DELEG. PEDRO LURO ( BAHIA BLANCA )	Desktop	1
	DELEG. PIGUE ( BAHIA BLANCA )	Desktop	2
	DELEG. PUAN ( BAHIA BLANCA )	Desktop	2
	DELEG. SAAVEDRA ( BAHIA BLANCA )	Desktop	1
	DELEG. SIERRA DE LA VENTANA( BAHIA BLANCA )	Desktop	2
	DELEG. STROEDER ( BAHIA BLANCA )	Desktop	2
	DELEG. TORNQUIST ( BAHIA BLANCA )	Desktop	2
	DELEG. TRES ARROYOS ( BAHIA BLANCA )	Desktop	3
	DELEG. VILLALONGA ( BAHIA BLANCA )	Desktop	1
	DELEG. VILLARINO - MEDANOS ( BAHIA BLANCA )	Desktop	2

RCF	DCCION. REG. CAPITAL FEDERAL (RCF)	Desktop	11
RDO	DCCION. REG. DOLORES	Desktop	4
	DELEG. CASTELLI (DOLORES)	Desktop	2
	DELEG. CHASCOMÚS (DOLORES)	Desktop	2
	DELEG. GRAL. GUIDO (DOLORES)	Desktop	2
	DELEG. GRAL. LAVALLE (DOLORES)	Desktop	2
	DELEG. GRAL. MADARIAGA (DOLORES)	Desktop	3
	DELEG. LEZAMA ( DOLORES )	Desktop	2
	DELEG. MAIPU ( DOLORES )	Desktop	2
	DELEG. MAR DE AJÓ ( DOLORES	Desktop	2
	DELEG. PILA (DOLORES )	Desktop	2
	DELEG. SAN CLEMENTE (DOLORES)	Desktop	2
	DELEG. SANTA TERESITA (DOLORES)	Desktop	2
	DELEG. TORDILLO (DOLORES)	Desktop	2
RGP	DCCION. REG. GRAL PUEYRREDON - MAR DEL PLATA	Desktop	12
	DELEG. AYACUCHO (GENERAL PUEYRREDON)	Desktop	2
	DELEG. BALCARCE (GENERAL PUEYRREDON)	Desktop	2
	DELEG. GRAL.ALVARADO ( MIRAMAR ) (GRAL PUEYRREDON)	Desktop	3
	DELEG. LOBERIA (GENERAL PUEYRREDON)	Desktop	2
	DELEG. NECOCHEA (GENERAL PUEYRREDON)	Desktop	3
	DELEG. PINAMAR (GENERAL PUEYRREDON )	Desktop	1
	DELEG. QUEQUÉN (GENERAL PUEYRREDON)	Desktop	1
	DELEG. SAN CAYETANO (GENERAL PUEYRREDON)	Desktop	1
	DELEG. SANTA CLARA DEL MAR (GENERAL PUEYRREDON)	Desktop	1
	DELEG. TANDIL (GENERAL PUEYRREDON)	Desktop	3
	DELEG. VELA -MARÍA IGNACIA (GENERAL PUEYRREDON)	Desktop	1
	DELEG. VILLA GESELL (GENERAL PUEYRREDON )	Desktop	1
	NICANOR OTAMENDI	Desktop	1
RJU	DCCION. REG. JUNIN	Desktop	7
	DELEG. AMEGHINO ( JUNIN )	Desktop	1
	DELEG. ARENALES ( JUNIN )	Desktop	2
	DELEG. ASCENCION ( JUNIN )	Desktop	1
	DELEG. CHACABUCO ( JUNIN )	Desktop	3
	DELEG. LINCOLN ( JUNIN )	Desktop	3
	DELEG. LOS TOLDOS - GRAL. VIAMONTE ( JUNIN )	Desktop	1
	DELEG. VEDIA L.N.ALEM ( JUNIN )	Desktop	1
RLM	DELEG. LA MATANZA - SAN JUSTO ( LA MATANZA )	Desktop	2
	DELEG. LAFERRERE ( LA MATANZA )	Desktop	2
	DELEG. LAS HERAS ( LA MATANZA )	Desktop	2
	DELEG. MARCOS PAZ ( LA MATANZA )	Desktop	2
	DELEG. RAMOS MEJIA ( LA MATANZA )	Desktop	2
	DELEG. VIRREY DEL PINO - GONZALES CATAN ( LA MATANZA )	Desktop	2
RLP	DCCION. REG. GRAN LA PLATA	Desktop	3
	DELEG. ASTILLEROS RIO SANTIAGO ( GRAN LA PLATA )	Desktop	2
	DELEG. BERISSO ( GRAN LA PLATA )	Desktop	1
	DELEG. CAÑUELAS ( GRAN LA PLATA )	Desktop	2
	DELEG. CITY BELL ( GRAN LA PLATA )	Desktop	2
	DELEG. CNEL.BRANDSEN ( GRAN LA PLATA )	Desktop	3
	DELEG. ENSENADA ( GRAN LA PLATA )	Desktop	2
	DELEG. GRAL. PAZ (RANCHOS) ( GRAN LA PLATA )	Desktop	2
	DELEG. GRAL.BELGRANO ( GRAN LA PLATA )	Desktop	2
	DELEG. LA PLATA II A.M.P ( GRAN LA PLATA )	Desktop	2
	DELEG. LA PLATA III ANEXO 7 ( GRAN LA PLATA )	Desktop	2
	DELEG. LISANDRO OLMOS ( GRAN LA PLATA )	Desktop	1
	DELEG. LOS HORNOS ( GRAN LA PLATA )	Desktop	1
	DELEG. M. B. GONNET ( GRAN LA PLATA )	Desktop	2
	DELEG. MAGDALENA ( GRAN LA PLATA )	Desktop	2

	DELEG. MELCHOR ROMERO ( GRAN LA PLATA )	Desktop	2
	DELEG. MONTE ( GRAN LA PLATA )	Desktop	2
	DELEG. PTE. PERON (GUERNICA) ( GRAN LA PLATA )	Desktop	2
	DELEG. PUNTA INDIO ( GRAN LA PLATA )	Desktop	2
	DELEG. RINGUELET( GRAN LA PLATA )	Desktop	2
	DELEG. SAN VICENTE- ALEJANDRO KORN (GRAN LA PLATA)	Desktop	2
	DELEG. TOLOSA ( GRAN LA PLATA )	Desktop	2
	DELEG. VILLA ELISA ( GRAN LA PLATA )	Desktop	2
	DELEG. VILLA ELVIRA ( GRAN LA PLATA )	Desktop	2
RLZ	DCCION. REG. LOMAS DE ZAMORA	Desktop	11
	DELEG. ALTE. BROWN ( ADROGUE ) ( LOMAS DE ZAMORA )	Desktop	2
	DELEG. AVELLANEDA ( LOMAS DE ZAMORA )	Desktop	2
	DELEG. BERAZATEGUI ( LOMAS DE ZAMORA )	Desktop	1
	DELEG. E. ECHEVERRÍA - M. GRANDE ( LOMAS DE ZAMORA )	Desktop	2
	DELEG. E. ECHEVERRÍA II - M. GRANDE ( LOMAS DE ZAMORA )	Desktop	2
	DELEG. EZEIZA ( LOMAS DE ZAMORA )	Desktop	1
	DELEG. FCIO. VARELA ( LOMAS DE ZAMORA )	Desktop	2
	DELEG. LANUS ( LOMAS DE ZAMORA )	Desktop	2
	DELEG. LOMAS DE ZAMORA ( LOMAS DE ZAMORA )	Desktop	2
	DELEG. QUILMES EZPELETA ( LOMAS DE ZAMORA )	Desktop	2
	DELEG. QUILMES OESTE ( LOMAS DE ZAMORA )	Desktop	2
	DELEG. QUILMES SOLANO ( LOMAS DE ZAMORA )	Desktop	2
RMO	DCCION. REG. MORON	Desktop	3
	DELEG. GRAL. RODRIGUEZ ( MORON )	Desktop	2
	DELEG. HURLINGHAM ( MORON )	Desktop	2
	DELEG. ITUZAINGO ( MORON )	Desktop	2
	DELEG. LUJAN ( MORON )	Desktop	2
	DELEG. MERLO ( MORON )	Desktop	2
	DELEG. MORENO ( MORON )	Desktop	2
	DELEG. TRES DE FEBRERO CASEROS ( MORON )	Desktop	1
ROL	DCCION. REG. OLAVARRIA	Desktop	7
	DELEG. AZUL ( OLAVARRIA )	Desktop	2
	DELEG. BENITO JUAREZ ( OLAVARRIA )	Desktop	2
	DELEG. BOLIVAR ( OLAVARRIA )	Desktop	2
	DELEG. CHILLAR ( OLAVARRIA )	Desktop	1
	DELEG. GRAL.ALVEAR ( OLAVARRIA )	Desktop	2
	DELEG. LAMADRID ( OLAVARRIA )	Desktop	2
	DELEG. LAPRIDA ( OLAVARRIA )	Desktop	2
	DELEG. LAS FLORES ( OLAVARRIA )	Desktop	2
	DELEG. RAUCH ( OLAVARRIA )	Desktop	2
	DELEG. TAPALQUÉ ( OLAVARRIA )	Desktop	2
RPE	DCCION. REG. PERGAMINO	Desktop	4
	DELEG. ARRECIFES ( PERGAMINO )	Desktop	2
	DELEG. BARADERO ( PERGAMINO )	Desktop	2
	DELEG. CAPITAN SARMIENTO ( PERGAMINO )	Desktop	2
	DELEG. CARMEN DE ARECO ( PERGAMINO )	Desktop	2
	DELEG. COLON ( PERGAMINO )	Desktop	2
	DELEG. RAMALLO ( PERGAMINO )	Desktop	2
	DELEG. ROJAS ( PERGAMINO )	Desktop	2
	DELEG. SALTO ( PERGAMINO )	Desktop	2
	DELEG. SAN ANDRÉS DE GILES ( PERGAMINO )	Desktop	2
	DELEG. SAN ANTONIO DE ARECO ( PERGAMINO )	Desktop	2
	DELEG. SAN NICOLAS ( PERGAMINO )	Desktop	2
	DELEG. SAN PEDRO ( PERGAMINO )	Desktop	2
RPH	DCCION. REG. PEHUAJO	Desktop	3
	DELEG. PEHUAJO ( PEHUAJO )	Desktop	4
	DELEG. 30 DE AGOSTO ( PEHUAJO )	Desktop	2

	DELEG. CARLOS CASARES ( PEHUAJO )	Desktop	2
	DELEG. CARLOS PELLEGRINI ( PEHUAJO )	Desktop	2
	DELEG. CARLOS TEJEDOR ( PEHUAJO )	Desktop	2
	DELEG. DAIREAUX ( PEHUAJO )	Desktop	2
	DELEG. GRAL. VILLEGAS ( PEHUAJO )	Desktop	2
	DELEG. HIPOLITO YRIGOYEN ( PEHUAJO )	Desktop	2
	DELEG. NUEVE DE JULIO ( PEHUAJO )	Desktop	2
	DELEG. RIVADAVIA AMERICA( PEHUAJO )	Desktop	2
	DELEG. SALLIQUELO ( PEHUAJO )	Desktop	2
	DELEG. TRENQUE LAUQUEN ( PEHUAJO )	Desktop	2
	DELEG. TRES ALGARROBOS (PEHUAJO )	Desktop	1
	DELEG. TRES LOMAS ( PEHUAJO )	Desktop	2
RSA	DCCION. REG. SALADILLO	Desktop	7
	DELEG. 25 DE MAYO (SALADILLO )	Desktop	1
	DELEG. BRAGADO (SALADILLO )	Desktop	4
	DELEG. CHIVILCOY (SALADILLO )	Desktop	4
	DELEG. LOBOS (SALADILLO )	Desktop	2
	DELEG. MERCEDES (SALADILLO )	Desktop	2
	DELEG. NAVARRO (SALADILLO )	Desktop	2
	DELEG. ROQUE PEREZ (SALADILLO )	Desktop	1
	DELEG. SUIPACHA (SALADILLO )	Desktop	1
RSI	DCCION. REG. SAN ISIDRO	Desktop	4
	DELEG. CAMPANA (SAN ISIDRO)	Desktop	2
	DELEG. ESCOBAR (SAN ISIDRO)	Desktop	2
	DELEG. EX.DE LA CRUZ CAPILLA DEL SR (SAN ISIDRO)	Desktop	2
	DELEG. JOSE C. PAZ ( SAN ISIDRO )	Desktop	2
	DELEG. MALVINAS ARGENTINAS POLVORINES (SAN ISIDRO)	Desktop	2
	DELEG. PILAR (SAN ISIDRO)	Desktop	2
	DELEG. SAN MARTIN - VILLA BALLESTER (SAN ISIDRO)	Desktop	2
	DELEG. SAN MIGUEL (SAN ISIDRO)	Desktop	2
	DELEG. SAN FERNANDO (SAN ISIDRO)	Desktop	2
	DELEG. TIGRE (SAN ISIDRO)	Desktop	2
	DELEG. VTE. LOPEZ SUT - OLIVOS (SAN ISIDRO)	Desktop	2
	DELEG. ZARATE (SAN ISIDRO)	Desktop	2

**TOTAL GENERAL 393**

#### 4. ASISTIR EN LA IMPLEMENTACIÓN DE UN NUEVO SISTEMA DE EMAIL CORPORATIVO

##### 4.1 Introducción

La actual plataforma de correo corporativa se encuentra alojada en el edificio central de IOMA sobre distribuciones de sistemas operativos sin soporte ni actualización. Adicionalmente, se detectaron los siguientes problemas principales:

- La estructura no está diseñada en base a una arquitectura de roles, lo que hace que todos estos se encuentren en un mismo servidor.
- La interconexión con diferentes dispositivos hace que la demora de entrega y recepción la haga una plataforma poco confiable.
- Sin control de ABM de usuarios.
- Etc.

Todo eso hace a la plataforma deficiente para las necesidades actuales de la organización.

##### 4.2 Alcance

El proyecto constó en asistir a la Dirección de Sistemas de IOMA en la implementación de una plataforma de correo corporativo en las tareas de: relevamiento del estado actual, análisis de soluciones accesibles para implementar, diseño de la arquitectura y en la posterior implementación de los entornos para su migración.

### 4.3. Plan de trabajo

#### 4.3.1. Análisis de soluciones posibles

Se analizaron las alternativas de plataformas del tipo world class tanto pagas como Open Source, y en forma paralela se analizó en la órbita del Gobierno de la Provincia de Buenos Aires si existían prestadores de este servicio, ya sea servicio por uso o colaboración en la implementación y puesta en marcha; todo con el requisito principal que cualquier solución debía de cumplir la interconectividad de múltiple plataformas y poder integrarse con el Active Directory de IOMA para un gestión de cuentas centralizada.

#### 4.3.2. Ejecución de tareas

Relevado todo lo anterior se procedió brindar asistencia técnica al personal especializado de la Dirección de Sistemas de IOMA en:

- 7) Dimensionamiento de las necesidades de infraestructura para dar servicio a toda la Institución.
- 8) Preparación de la infraestructura necesaria.
- 9) Instalación de la nueva plataforma de email corporativo.
- 10) Ejecución de pruebas integrales.
- 11) Proporcionar los accesos necesarios para que el equipo correspondiente al instituto procesa con la migración.

### 4.4. Implementación

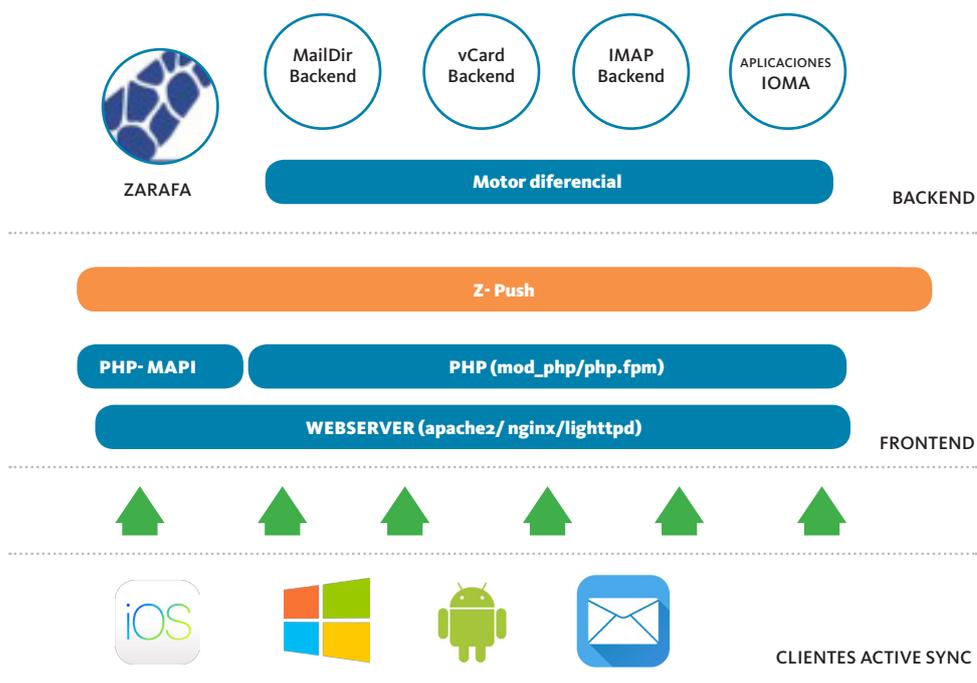
#### 4.4.1. Características de la solución implementada

La solución de correo electrónico que se ejecutó en el proyecto fue utilizando la solución de Zimbra Collaboration Open Source + Z-Push, con las siguientes características:

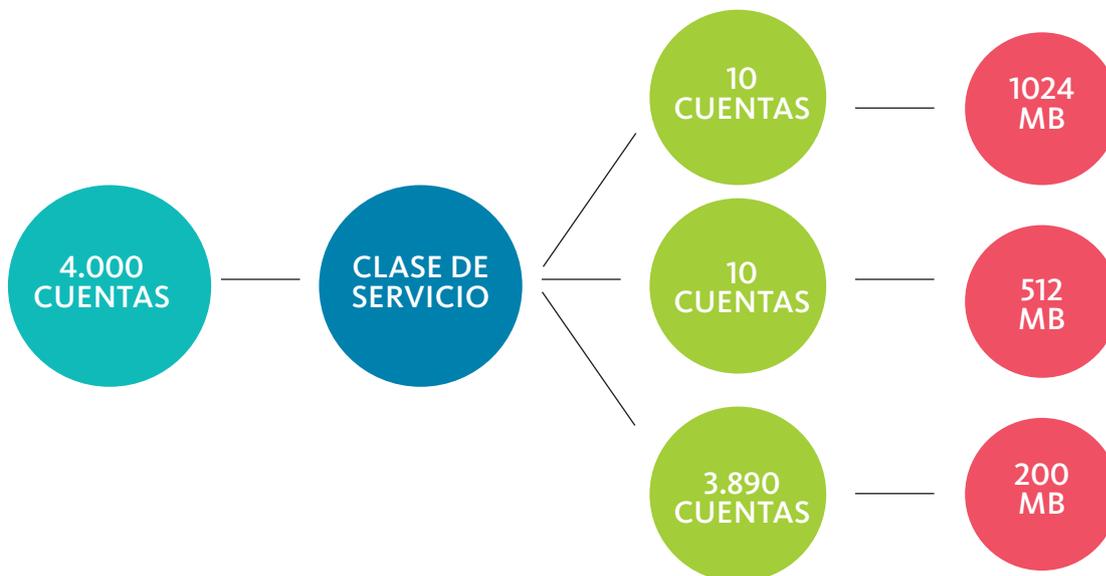
- Consola de administración web para la gestión de usuarios.
- Administración desde línea de comandos.
- Ejecuta sobre plataforma RHEL, webmail, calendario, agenda, libreta de direcciones en la interfaz del cliente.
- Instalando un complemento de ZeXtras se tiene la posibilidad de chat entre los usuarios activos.
- Integrada con autenticación de Active Directory.

#### 4.4.2. Esquema

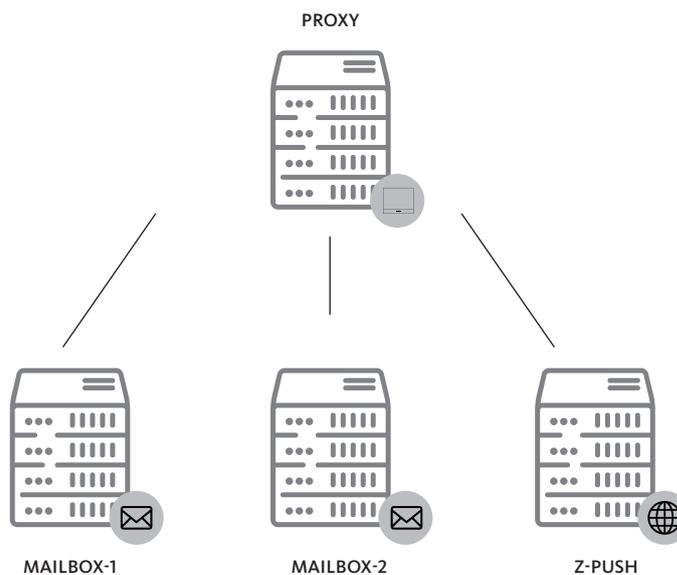
Esquemáticamente, se puede visualizar de la siguiente manera:



#### 4.4.3. Dimensionamiento de la plataforma



#### 4.4.4. Diagrama de servidores



- 2 Mailbox Servers
- 1 Proxy Server
- 1 Z-Push Server (ActiveSync)

Todos los servidores cuentan con Redhat Enterprise 7.5 de 64-bit virtualizados en infraestructura de la Dirección Provincial de Sistemas dedicada para IOMA.

#### 4.4.5. Accesos y entorno grafico

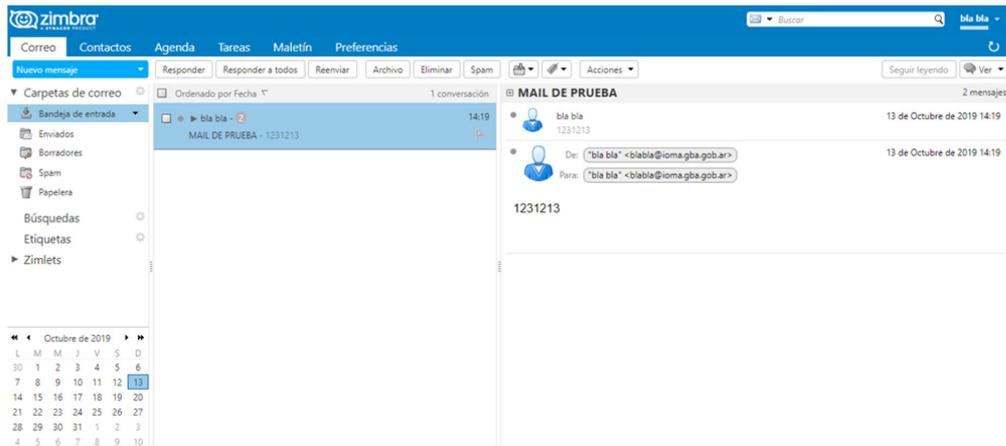
##### 4.4.5.1. Portal web (URL de acceso)

El portal de correo corporativo es accesible a través de la siguiente dirección web:

**<https://webmail.ioma.gba.gob.ar/>**



#### 4.4.5.2. Entorno del web mail



#### 4.4.6. Acceso al tablero de gestión

Por medio de la IP de gestión con la credencial de Active Directory, se puede realizar la gestión de la plataforma, tanto ABM de cuentas como servicios particulares del correo:

<https://10.2.252.107:7071/zimbraAdmin/>

##### 4.4.6.1. Entorno del tablero de gestión



#### 4.4.7. Acceso a los servidores

A continuación, se detallan los servidores involucrados en la solución con sus direccionamientos:

IP	Hostname	Acceso
10.2.252.106	zproxy01	SSH
10.2.252.107	mailbox-1	SSH
10.2.252.108	mailbox-2	SSH
10.2.252.109	zpush1	SSH

- **IP Pública:** 170.155.9.145
- **Registro DNS:** webmail.ioma.gba.gob.ar

## 5. GENERAR UNA POLÍTICA ORGANIZACIONAL PARA NORMALIZAR LOS PROCESOS DE BACKUP Y RESTORE DE LA INFORMACIÓN

### 5.1 Introducción

Tanto los sistemas de información como los datos son activos muy valiosos para IOMA, y se ha realizado una inversión muy importante en recursos humanos y financieros para crear estos sistemas. En consecuencia, resulta crítico la creación de una Política de Backup Corporativa, que permita:

- Minimizar los riesgos de pérdida de datos.
- Resguardar la confidencialidad e integridad de la información contenida en los sistemas de IOMA.
- Asegurar la disponibilidad de aquellos datos críticos, de forma tal que la información pueda ser utilizada como el activo crítico que es.
- Reducir riesgo del negocio y legales.

Todos los datos (críticos o no) se almacenan en el datacenter de la Dirección de Sistemas de IOMA, en los servidores de aplicación y en equipos locales. Estos datos pueden ser categorizados en:

- 1 Datos personales de un usuario
- 2 Datos de una unidad de negocio
- 3 Datos compartidos
- 4 Bases de datos
- 5 Datos de aplicaciones y sistemas

### 5.2. Objetivo

El presente documento especifica las políticas de backup, describe los servidores cuyos datos se resguardan, el personal autorizado a operar los backup y restauraciones, los datos a resguardar, el momento en que se ejecutan lo backup, el manejo de los datos almacenados, y las responsabilidades de los operadores y demás personas involucradas.

### 5.3. Responsabilidades

De los sistemas centrales: el administrador de sistemas de IOMA es responsable de conocer, adoptar e implementar la presente política de backup.

De las estaciones de trabajo o PC de escritorio: el usuario es responsable de los respaldos de los equipos personales. Los usuarios deberán respaldar diariamente la información sensible y crítica que se encuentre en sus computadoras personales o estaciones de trabajo.

**NOTA:** Tanto para las Estaciones de Trabajo como para los Sistemas Centrales no se harán backup de los ficheros con extensiones: avi, mp3, mp4, divx, mpg, wvm, mkv o extensiones de características similares. Si por motivos de trabajo se crean este tipo de archivos se deberá notificar a la “Mesa de Ayuda” vía email, junto con una descripción del motivo. La “Mesa de Ayuda” junto con las autoridades del departamento de Sistemas de IOMA estudiará el caso y tomará una decisión que será notificada.

No se realizarán backups de máquinas personales.

## 5.4. Alcance

Aplica a todos los datos alojados en servidores bajo resguardo acorde a los objetivos de seguridad de los datos establecidos por el área, y a los datos de usuarios que se incluyan (por mutuo acuerdo) en algún plan de backup brindado por el área.

## 5.5. Desarrollo de la política

### 5.5.1. Tipos de respaldo

El volumen de la información a respaldar condicionará las decisiones que se tomen sobre la política de backup, en una primera consideración está compuesto por el conjunto de datos que deben estar incluidos, sin embargo, se pueden adoptar diferentes estrategias respecto a la forma del respaldo, que condicionan el volumen de información a copiar, las cuales pueden ser:

- ❶ Servidor completo (incluyendo sistema operativo instalado) en el caso de servidores virtuales.
- ❷ Software Base (Paquetes y/o Lenguajes de Programación con los cuales han sido desarrollados o interactúan nuestros Aplicativos Institucionales).
- ❸ Software aplicativo (Considerando tanto los programas fuentes, como los programas objetos correspondientes, y cualquier otro software o procedimiento que también trabaje con los datos, para producir los resultados con los cuales trabaja el usuario final). Se deben considerar las copias de los listados fuentes de los programas definitivos, para casos de problemas.
- ❹ Datos y estructura de datos (Bases de Datos, Índices, tablas de validación, contraseñas, tablas, usuarios, roles, configuraciones y todo archivo necesario para el funcionamiento de los Sistemas de Información de la Institución y la pronta recuperación de los mismos en caso de fallas).

### 5.5.2. Especificaciones y normas para la elaboración de los backup

Según corresponda y se encuentre disponible los backup pueden ser almacenados en DVD de primera marca o cintas de backup (ver en dispositivo) con etiquetas que contengan la siguiente información mínima:

- Nombre del Sistema y/o del Servidor.
- Versión / Año.
- Ubicación de las fuentes (en el caso de software aplicativo).
- Ubicación de los compilados (si corresponde, en el caso de software aplicativo).
- Ubicación de los instaladores (si corresponde, en el caso de software aplicativo).
- Número de DVD o Cinta (en formato [número] de [cantidad total], ej. 2 de 3).

En caso de que sea disco rígido: Se deberá referenciar el arreglo de disco y equipo storage, como así también el nombre del sistema y/o del servidor.

### 5.5.3. Periodicidad

Se llevará un registro del medio en uso indicando como mínimo

- Fecha o tipo de ejecución del respaldo
- DVD, cintas o arreglo de disco que integren el backup de los equipos
- Cantidad de veces que usa la cinta. Una cinta tiene un máximo de 250 veces de sobre escritura (vida útil). Luego deberá procederse a su respectivo cambio.
- Las cintas de backup se almacenarán en un lugar bajo llave con las condiciones ambientales descritas en la política.
- El administrador del sistema de backup revisará periódicamente que se cumpla con este registro en tiempo y forma.
- La ubicación de resguardo de dichos backup será la sala de servidores local donde se esté resguardando y un duplicado en un sitio externo.

#### 5.5.3.1. Criterios de Periodicidad

La frecuencia de obtención de estos backup variará según los siguientes criterios:

**Servicios externos:** serán aquellos que presten servicios a clientes y contengan información que requiera por normas Gubernamentales contar con un resguardo prolongado en el tiempo, el plazo será de 10 años distribuidos de la siguiente manera:

- a) Toma diaria por 2 (dos) semanas.
- b) Toma semanal por 4 (cuatro) semanas.
- c) Toma mensual por 12 (doce) meses.

**Servicios internos:** serán aquellos que presten servicios a la operatoria interna y de ellos dependan cualquier equipo de la red, el plazo será al menos 1 año distribuidos de la siguiente manera:

- a) Toma diaria por 2 (dos) semanas.
- b) Toma semanal por 4 (cuatro) semanas.
- c) Toma mensual por 12 (doce) meses.

#### 5.5.4. Criterios de elección de software para la gestión de backup

En este aspecto, en el mercado se dispone de un conjunto de utilitarios de propósito general que permiten efectuar procesos de respaldo de información, por lo tanto, se debe disponer de criterios o metodologías apropiadas que permitan el uso de estos utilitarios de acuerdo con:

- Sistema operativo del origen.
- Sistema a resguardar y posibilidades de generar exportaciones de datos en tiempo real desde el mismo.
- Volumen de información a resguardar.
- Volumen de almacenamiento disponible en el servidor de backup y la posibilidad de comprimir los respaldos.
- Frecuencia de actualización de la información.
- Importancia de la información.

En los casos especiales en que no se disponga de un software apropiado para la generación del respaldo en cuestión, se deberá implementar un sistema confeccionado a medida de las necesidades particulares basado en los criterios y periodicidades ya descritos.

#### 5.6. Rutinas de seguimiento y control

Para prevenir fallas en la restauración de datos de servidores, la información almacenada en los backup debe ser verificada mensualmente y en forma íntegra. Para ello se deben realizar rutinas de control de backup. Éstas consisten en la prueba integral de los respaldos; desde su restauración desde el servidor de backup a otro de testeo (duplicado del servidor original en producción), descompresión e importación de datos hasta las pruebas correspondientes de funcionamiento (según el sistema que se esté recuperando). Ya que, por cuestiones de volúmenes de datos y tiempos, sería imposible realizar la comprobación de todos los backup, se tomarán muestras de entre 5 y 10 backup aleatoria y rotativamente, para llevar adelante este proceso.

#### 5.7. Posibles pérdidas de datos

Para que haya pérdida total de datos, deberán ocurrir los siguientes tres eventos simultáneamente:

- Pérdida de los datos en el servidor original, ya sea por negligencia o falla de hardware.
- Pérdida de los resguardos en el archivo en el/los servidor/es de backup, si se realizan a archivo.
- Pérdida de los datos en sistemas magnéticos o extraíbles, si se realiza este tipo de backup.

#### 5.8. Dispositivos

Existen ciertas condiciones con las que se deben guardar los respaldos, con el fin de garantizar una adecuada conservación de la información.

A continuación, se indican las condiciones que se deben tener en cuenta para el óptimo funcionamiento de los dispositivos de cintas:

- La humedad relativa del ambiente se debe encontrar entre el 20 % al 80 %, La temperatura puede oscilar entre 5°C a 45°C.
- El ambiente debe contar con aire acondicionado o ventilación.
- Las cintas deben ser guardadas dentro de su caja plástica.
- Los dispositivos deben mantenerse alejados de campos magnéticos.
- Para realizar un respaldo se debe contar como mínimo con un dispositivo de almacenamiento externo, este puede ser, una cinta o disco removible. Si no se cuenta con un dispositivo de almacenamiento externo es recomendable utilizar al menos y de manera temporal el disco duro de otra máquina. Esta es una medida temporal mientras se adquiere un dispositivo de almacenamiento externo más seguro para aplicar el procedimiento de respaldos correctamente.
- Es recomendable contar con un sitio externo a la institución para guardar algunas copias de respaldos semestrales
- Que todos los servidores tengan los datos importantes en particiones con RAID de nivel mayor que 0.
- Que se disponga de una red separada para la ejecución de los backup. De no ser posible, usar una VLAN.

- Que los servidores que resguarden un volumen grande de datos tengan interfaces de red de velocidad gigabit.
- Que la red de backup esté a velocidad gigabit. De no ser posible, por lo menos asegurar que ninguna de las interfaces por donde pasan los datos esté a menos de 100 mbps.
- Que los servidores destinados a backup, tengan fuente redundante.

Como contingencia en caso de desastre. Entre los soportes más habituales, podemos destacar las cintas magnéticas, discos compactos o cualquier dispositivo capaz de almacenar los datos que se pretenden salvaguardar.

## 6. ACTUALIZAR Y NORMALIZAR LOS SISTEMAS OPERATIVOS DE LOS SERVIDORES DEL DATACENTER IOMA

### 6.1. Introducción

En los complejos sistemas de Organizaciones en nuestros días, la "peor pesadilla" para un directivo de sistemas tiene que ver con aquella infraestructura que son difíciles de diseñar, desplegar, mantener y administrar. Estos factores no generan únicamente frustración en los responsables, sino también producen problemas adicionales: costos elevados, tiempos de despliegue muy prolongados, incremento de los tiempos de downtime de las aplicaciones, y muchas dificultades a la hora de considerar la escalabilidad de la plataforma.

Una de las claves para la resolución de estos problemas tiene que ver con incrementar la eficiencia de toda la Dirección de Sistemas a través de la estandarización del datacenter (considerando cables, racks, dispositivos de seguridad, servicios, servidores, sistemas operativos, etc.). Cuando los componentes de un datacenter son intercambiables, escalables, repetibles, entendibles e integrados, hay un vasto potencial para el ahorro de costos, de tiempos, para la mejora del diseño, instalación, operación y mantenimiento.

El usar infraestructura estandarizada, eliminando el potencial para el surgimiento de problemas complejos, únicos y difíciles de resolver, ofrece muchos beneficios.

#### 6.1.1. Escalabilidad simple

La densidad y capacidad que un datacenter requiere hoy, no tiene nada que ver con lo que requerirá dentro de 5 o 7 años. Este es el concepto por el cual es clave preparar la infraestructura para el futuro, tratando de predecir lo que será necesario más adelante, y si seremos capaces de lograr acomodar todos los agregados de infraestructura.

La estandarización de un datacenter permite lograr una configuración óptima del espacio, estableciendo una infraestructura hoy, con la confianza en que será muy fácil de hacerla crecer en el futuro (escalabilidad) sin incalculables costos o expansiones físicas del datacenter.

A medida que cambian los requerimientos tecnológicos, por el crecimiento natural de la organización, "bloques de construcción" adicionales puede ser agregados sin la necesidad de realizar grandes proyectos de reingeniería.

#### 6.1.2. Gestión de los recursos humanos

Cuando se implementan componentes estandarizados en un datacenter, se requiere menos capacitación y tiempo para la resolución de problemas. Todo trabaja de la misma forma, el equipamiento es fácil de entender, y con un set de skills acotado es posible el mantenimiento del hardware, todo porque los componentes de los sistemas se ven, funcionan y responden de una forma similar.

Componentes únicos requieren consideración especial, agregando complejidad a la administración del datacenter.

En vez de pasar horas "apagando incendios", los administradores del datacenter puede dedicar más recursos a la capa de TI soportada por la misma infraestructura.

#### 6.1.3. Mantenimiento optimizado

El datacenter actual de IOMA presenta muchas dificultades para la administración de parches, actualizaciones y en general para su mantenimiento, principalmente por la variedad de soluciones de diferentes proveedores.

Utilizar un hardware estandarizado permite el tener que gestionar soluciones de los mismos proveedores, recurriendo a pocos canales de soporte y con menos problemas de compatibilidad.

#### 6.1.4. Menores tiempos de downtime

La mayoría de los tiempos de downtime en un datacenter tienen que ver con el error humano. Al reducir este factor,

necesariamente bajamos los tiempos que los sistemas permanecen caídos.

Los errores pasan en casi cualquier contexto, desde problemas de fabricación hasta casos de mala praxis en un paciente, esto no es discutible. Estandarizando procesos y sistemas de un datacenter el personal técnico estará muy familiarizado con la documentación, el mantenimiento y las reparaciones involucradas en los problemas que puedan surgir, lo que resultará en menos errores por falta de conocimiento de uso. Se reduce significativamente el error humano relativo al tipeo de un comando erróneo, el activar un switch equivocado o sacar el cable que no corresponde.

Si bien el error humano nunca podrá ser eliminado, una vez que sucede, el contar con un datacenter estandarizado permitirá que el arreglo y consiguiente vuelta a la operatividad sea en tiempos mucho más reducidos.

**6.1.5. Despliegues más rápidos**

La configuración y el despliegue de cualquier tecnología sucede más rápidamente cuando los componentes y conectores son más simples. Si se tiene un datacenter estandarizado, también es posible que existan menos piezas que requieran instalación. De la misma forma, la configuración sucede de una forma mucho más intuitiva, dado que los conocimientos se corresponden entre diferentes sistemas.

**6.2. Alcance y requerimientos**

Las organizaciones y empresas de hoy en día deben estar atentas a las actualizaciones de los programas y sistemas operativos por la seguridad de los datos. No se trata solo de mejorar la funcionalidad de un programa con una nueva versión, sino de mantener la seguridad de los mismos a medida que se van descubriendo vulnerabilidades. Esta tarea es responsabilidad del Departamento de Sistemas en general, y en particular, del administrador del equipo servidor. A fin de poder mantener los sistemas actualizados, se debe tener en cuenta los siguientes requisitos:

- Conocer la cantidad de equipos físicos y virtuales.
- Conocer el tipo de sistema operativo de cada equipo.
- Mantenerse informado de las nuevas vulnerabilidades que puedan afectar a cada SO.
- Establecer un cronograma de actualización para cada nueva versión que informe el fabricante del sistema operativo.

**6.3. Fundamentos del proyecto**

Actualmente la Dirección de Sistemas de IOMA no cuenta con un estándar de sistemas operativos ni para servidores ni para estaciones de trabajo. Para necesidades similares, se cuenta con diferentes sistemas operativos, esto trae como consecuencia la complicación para la administración y mantenimiento.

Puntos adicionales detectados:

- Sin un estándar de versiones entre las distribuciones (en el caso de LINUX)
- Sin mantenimiento contractual vigente en muchas versiones (caso de Windows XP y Windows 7)
- No existe un WSUS (rutina automatizada para instalación desatendida de parches y actualizaciones).Inexistencia de tareas programadas de update para los equipos que cuentan con sistema operativo LINUX.

**6.4. Objetivos del proyecto**

Llevar adelante un plan de trabajo que permita la estandarización de los sistemas operativos del datacenter IOMA, a partir de las definiciones de la Dirección.

Una vez finalizado el trabajo, se confeccionará un informe final detallando la situación inicial y situación final.

**6.5. Plan de trabajo**

TAREA	MES 1	MES 2	MES 3	MES 4
Relevamiento integral de los sistemas operativos				
Relevamiento integral de actualizaciones importantes Recomendadas - Opcionales por SO				
Cronograma de back up y/o punto de restauración de equipos a actualizar				
Implementación de ventana horaria de tarea de actualización				
Instalación de actualizaciones				
Verificación de equipo				

### 6.5.1. Cronograma de ejecución

### 6.5.2. Situación actual

Actualmente, el Instituto de Obra Médico Asistencial (IOMA) cuenta con una granja de servidores en su datacenter. Dicha granja, está compuesta por equipos físicos y equipos virtuales que poseen diversos sistemas operativos (Windows 2000/2003/2008/2012; Debian 3.1/5/6/7/8; Linux; RedHat 9 en versiones de 32 y 64 bits). En el apartado 6 se detalla el relevamiento realizado sobre la infraestructura del datacenter.

### 6.5.3. Ejecución del plan de trabajo previsto

Se tomó como base para el relevamiento a la información obtenida en la primera etapa de la Consultoría. Al tratarse de información con cierto tiempo de obtenida, se intentó por todos los medios que el personal de la Dirección responsable del datacenter le brindara a los consultores la información actualizada del parque, a fin de poder tener una visión clara y precisa de la situación actual.

Los pedidos se hicieron en reiteradas oportunidades, pero no fue posible obtener una respuesta satisfactoria a los mismos.

En virtud de esta situación, el proyecto queda suspendido, debido a que resulta inviable continuar con un plan de renovación de sistemas operativos sin tener la foto exacta sobre la situación actual.

Sin embargo, el trabajo realizado en el presente informe sirve como base para un futuro proyecto que permita llevar adelante las tareas programadas.

## 6.6. Relevamiento de la infraestructura

Nro	Rack/ Blade/ Torre	Marca	Marca y modelo procesador	Capacidad disponible en discos	Cantidad de Discos	Total GB en uso	Memoria RAM	S.O.	Estado	Comentarios
1	2U	IBM x3650 M4	Dos Intel Xeon 6C E5-2620 95W	-	0	-	64Gb	VMWare- ESXi	uso	Aplicaciones/ Base de Datos
2	2U	IBM x3650 M4	Dos Intel Xeon 6C E5-2620 95W	-	0	-	64Gb	VMWare- ESXi	uso	Aplicaciones/ Base de Datos
3	2U	IBM x3650 M4	Dos Intel Xeon 6C E5-2620 95W	-	0	-	64Gb	VMWare- ESXi	uso	Aplicaciones/ Base de Datos
4	2U	IBM x3650 M4	Dos Intel Xeon 6C E5-2620 95W	-	0	-	64Gb	VMWare- ESXi	uso	Aplicaciones/ Base de Datos
5	2U	IBM x3650 M4	Dos Intel Xeon 6C E5-2620 95W	-	0	-	64Gb	VMWare- ESXi	uso	Aplicaciones / Base de Datos
6	2U	IBM x3650 M4	Dos Intel Xeon 6C E5-2620 95W	-	0	-	64Gb	VMWare- ESXi	uso	Aplicaciones/ Base de Datos
7	1U	IBM x3550 M4 E5-2620 95W	Dos Intel Xeon 6C	6,6Tb	8	6,6Tb -Total-	16Gb	Windows Server2012	uso	Backup
8	2U	HP Proliant 380 G8	Dos Intel Xeon 6C E5-2630	1,5Tb	5	1,2Tb	16Gb	VMWare- ESXi	uso	Aplicaciones/ Base de Datos
9	2U	HP Proliant 380 G6	Dos Intel Xeon 6c	484Gb	4	484Gb -Total-	12Gb	Windows Server 2012	uso	Clúster Físico Base de Datos
10	2U G6	HP Proliant 380	Dos Intel Xeon 6c	876Gb	6	876Gb -Total-	12Gb	Windows Server 2003	uso	Base de Datos
11	2U 380 G5	HP Proliant	Dos Intel Xeon 4c	876Gb	6	500Gb	4Gb	Windows Server2012	uso	Clúster Físico Base de Datos
12	4U	HP Proliant 350	Dos Intel Xeon	432Gb	6	300Gb	4Gb	Windows Server 2003	uso	File Server
13	4U	HP Proliant 350	Dos Intel Xeon	432Gb	6	250Gb	4Gb	Windows Server 2003	uso	File Server
14	Torre	HP Proliant 350	Dos Intel Xeon	432Gb	6	270Gb	4Gb	Windows Server 2003	uso	File Server
15	Torre	HP Proliant 350	Dos Intel Xeon	584Gb	4		4Gb	Windows Server 2003	uso	File Server
16	4U	HP Proliant 370	Dos Intel Xeon	144Gb	2		4Gb	-	No uso	Problemas funcion.
17	1U	HP Proliant DL 360	Dos Intel Xeon	144Gb	2		2Gb	-	No uso	Problemas funcion.

### 6.6.1. Servidores físicos

NRO SERVIDOR	ROL MAQUINA VIRTUAL	VERSIÓN S.O.	COMENTARIOS
1	Desarrollo Web	Debian 3.1 - 32 bits	Apache 2.0.54/PHP 4.4.2/MySQL 4.0.12/Freetds 0.62.4
2	Servidor Web Sitio Oficial y aplicaciones PHP	Red Hat 9 - 32 bits	Apache 2.0.54/PHP 4.3.11/MySQL 4.1.12/Freetds 0.63
3	Servidor de Correo Pop3 e Imap	Debian 5 - 32 bits	Cyrus SASL / IMAP 2.1.18 / Postfix 2.1.5 / SpamAssassin 3.0.3 / ClamAV 0.84 / Squirrelmail 1.4.4 / Apache 2.2.9
4	Servidor DNS y Proxy	Debian 6 - 64 bits	BIND9 9.7.3/Squid 2.7
5	Administración y Actualizaciones de F-Secure	Windows Server 2012	F-Secure Policy Manager 11.31
4	Servidor MySQL dedicado a sistema Peri-Natal	Debian 7 - 64 bits	MySQL 5.5.31
5	Servidor ADABAS/Natural	Windows 2000 Server	Entire Net-Work 2.6.1.0/ADABAS "c" 3.1/Natural 4.1.2
6	Servidor Proxy (acceso alternativo)	Debian 7 - 64 bits	Squid 2.7
7	Servidor Control de Ingreso personal 8vo. Piso	Windows Server 2008 R2 - 64 bits	Sara Operativo v5.05.01/SQL Server 2005
8	Controlador de Dominio Primario	Windows Server 2012 R2 - 64 bits	Active Directory Primario /DNS/DFS
9	Controlador de Dominio Secundario	Windows Server 2012 R2 - 64 bits	Active Directory Primario /DNS/DFS
10	Servidor DHCP de la LAN	Debian 7 - 64 bits	isc-dhcp 4.2.2
11	Servidor para Sistemas de Digitalizacion Lexmark	Windows Server 2008 R2 - 64 bits	Apache Tomcat 8.0 Perceptive Content Image Now 71.0
12	Servidor para Sistemas de Digitalizacion Lexmark	Windows Server 2008 R2 - 64 bits	Administracion Impresoras Lexmark FireBird FlameRobin
13	Servidor FTP para uso solo dentro de la red de gobernacion	Debian 3.1 - 32 bits	proftpd 1.2.10
14	Servidor Web IIS de Desarrollo Windows Server 2003 - 32 bits	IIS 6	
15	Servidor Web IIS de Produccion	Windows Server 2003 - 32 bits	IIS 6
16	Servidor MySQL de Produccion Servidor MySQL de Produccion	MySQL 5.0.22	
17	Vmware vCenter Server Appliance 1 v.5.5.0	Linux	Administra los Vmware 1, 2 y 3
18	VMware vCenter 1 (VMware 1, 2 y 3)	Linux	Administra los Vmware 4, 5 y 6
19	DNS Impresoras de Digitaliz. de las Regiones	Debian 8 - 64 bits	BIND9 9.9.5
20	Balaceo de carga de Terminal Server	Debian 6.0 - 64 bits	Haproxy 1.4
21	Testing Base de datos produccion	Windows Server 2012 R2 - 64 bits	MSSQL 2008 R2
22	Servidor de Archivos	Windows Server 2008 R2 - 64 bits	Servidor de Archivos
23	Servidor Horario NTP	Debian 8 - 64 bits	NTP 1:4.2.6
24	Servidor de Actualizaciones de Microsoft	Windows Server 2012 R2 - 64 bits	WSUS 3.0 IIS 8
25	Servidor de Terminal Server	Windows 2003 Server	Terminal Server - Sol
26	Servidor de Terminal Server Region La Plata	Windows server 2008 - 32 bits	Terminal Server - Sol
27	Servidor de Terminal Server para las Regiones	Windows server 2008 - 32 bits	Terminal Server - Sol
28	Servidor de Terminal Server para las Regiones	Windows server 2008 - 32 bits	Terminal Server - Sol
29	Servidor de Terminal Server para las Regiones	Windows server 2008 - 32 bits	Terminal Server - Sol
30	Servidor de Licencias Terminal Server	Windows server 2008 - 32 bits	
31	Servidor VPN Producción	Debian 8 - 64 bits	Openvpn
32	Servidor Web para Desarrollo con PHP 5	Debian 8 - 64 bits	Apache 2.4.10/ PHP 5.6/ MySQL 5.5.44/ FreeTDS 0.91
33	Mirador de Distribuciones Debian	Debian 8 - 64 bits	Apache 2.4.10
34	Servidor Base Datos Producción 1	Windows Server 2008 R2 - 64 bits	MSSQL 2008 R2
35	Servidor Base Datos Producción 2	Windows Server 2003	MSSQL 2005
36	Servidor Base Datos Desarrollo	Windows Server 2003	MSSQL 2005
37	Servidor Base Datos suplente de producción 2	Windows Server 2003	MSSQL 2005
38	Servidor Base Datos Sistema Digitaliz. Lexmark	Windows Server 2012 R2 - 64 bits	SQL Server 2008 R2
39	Servidor de Archivos - IIS - Servicios .Net	Windows Server 2012	
40	Servidor WEB	RedHat 9	
41	Vmware vCenter Server Appliance 2 v.5.5.0	Linux	Administra los Vmware 4, 5 y 6
42	Servidor Web IIS sistema de Digesto (win isis)	Windows Server 2012 R2 - 64 bits	IIS 8 FTP (accesible solo por el usuario que maneja el sistema)
43	Clientes Livianos instalados en Planta Baja	Windows 7 - 32 bis	
44	Clientes Livianos instalados en Planta Baja	Windows 7 - 32 bis	
45	Clientes Livianos instalados en Planta Baja	Windows 7 - 32 bis	
46	Clientes Livianos instalados en Planta Baja	Windows 7 - 32 bis	
47	Clientes Livianos instalados en Planta Baja	Windows 7 - 32 bis	
48	Clientes Livianos instalados en Planta Baja	Windows 7 - 32 bis	
49	Clientes Livianos instalados en Planta Baja	Windows 7 - 32 bis	
50	Clientes Livianos instalados en Planta Baja	Windows 7 - 32 bis	
51	Servidor de Archivos - Perna	Windows Server 2012	
52	VPN01 VLAN-Fibercorp	Linux debian 8	Servidor VPN conectividad resd Fibercorp
53	LB1 Backend	Linux debian 8	Servidor Balanceador de servidores Backend
54	LB1 Front	Linux debian 8	Servidor Balanceador de servidores Front
55	LB1 Front_Autogestionv	Linux debian 8	Servidor Balanceador de servidores Front Autogestión
56	LB2 Backend	Linux debian 8	Servidor Balanceador de servidores Backend

### 6.6.4. Dispositivos de comunicaciones

57	LB2 Front	Linux debian 8	Servidor Balanceador de servidores Front
58	LB2 Front Autogestion	Linux debian 8	Servidor Balanceador de servidores Front Autogestión
59	Afil01	Windows Server 2012 R2 - 64 bits	Servidor Front Sistema Credenciales IIS8
60	AutoGestion01	Windows Server 2012 R2 - 64 bits	Servidor Front Sistema Autogestión IIS8
6	AutoGestion02	Windows Server 2012 R2 - 64 bits	Servidor Front Sistema Autogestión IIS8
62	Identity01	Windows Server 2012 R2 - 64 bits	Servidor Front Sistema Identificación IIS8
63	Identity02	Windows Server 2012 R2 - 64 bits	Servidor Front Sistema Identificación IIS8
64	Sql-Nodo-A-Prod -- Cluster	Windows Server 2012 R2 - 64 bits	Servidor base de Datos Producción Sistema Credenciales- MSSQL 2014
65	Sql-Nodo-B-Prod - Cluster	Windows Server 2012 R2 - 64 bits	Servidor base de Datos Producción Sistema Credenciales-MSSQL 2014
66	Sql-Nodo-C-Prod - Cluster	Windows Server 2012 R2 - 64 bits	Servidor base de Datos Producción Sistema Credenciales - MSSQL 2014
67	Sql-Nodo1-Testing - Cluster	Windows Server 2012 R2 - 64 bits	Servidor base de Datos Testing Sistema Credenciales - MSSQL 2014
68	Sql-Nodo2-Testing - Cluster	Windows Server 2012 R2 - 64 bits	Servidor base de Datos Testing Sistema Credenciales - MSSQL 2014
69	Sql-Nodo3-Testing - Cluster	Windows Server 2012 R2 - 64 bits	Servidor base de Datos Testing Sistema Credenciales - MSSQL 2014
70	Aplicaciones 1	Windows Server 2012 R2 - 64 bits	Servidor de aplicaciones Sistema Credenciales IIS8
71	Aplicaciones 2	Windows Server 2012 R2 - 64 bits	Servidor de aplicaciones Sistema Credenciales IIS8
72	Aplicaciones 3	Windows Server 2012 R2 - 64 bits	Servidor de aplicaciones Sistema Credenciales IIS8
73	System Center	Windows Server 2012 R2 - 64 bits	Inventario Hardware y Software / escritorio e instalación remota de sistemas operativos

### 6.6.2. Servidores lógicos

MARCA	MODELO	CAPACIDAD TOTAL	CAPACIDAD UTILIZADA	SOPORTE DEL FABRICANTE	COMENTARIOS
IBM	V3700 24 ejes	15Tb	11Tb	Garantía	Requiere ampliación urgente
IBM	V3700 24 ejes	15Tb	12Tb	Garantía	Requiere ampliación urgente
HP	StoraWork P2000 G3 24 ejes	2.6Tb	2Tb	No	
HP	StoraWork P2000 G3 24 ejes	220Mb	-	No	Solo tiene 2 discos

### 6.6.3. Storages

RACK	MARCA	MODELO	PUERTOS	ROL	COMENTARIOS
1U en rack de comunicaciones	Mikrotik	Router CCR 1036	12 UTP 100/1000 + 4SFP	Router/Firewall	
1U en rack de comunicaciones	D-Link	DGS-3100-24TG	8 UTP 100/1000 + 16SFP	Switch	Backbone Fibra a pisos
1U en rack de comunicaciones	D-Link	DGS-3120-24SC	8 UTP 100/1000 + 16 SFP + 8 combo	Switch	Backbone Fibra a pisos
1U en rack de comunicaciones	D-Link	DGS-3120-TC	24 UTP 100/1000 + 4 SFP	Switch	Switch de Piso
1U en rack de comunicaciones	Alcatel	OmniSwitch 6602-24	24 UTP 10/100 + 2 SFP	Switch	Switch de Piso
1U en rack de comunicaciones	Alcatel	OmniSwitch 6602-48	48 UTP 10/100 + 2 SFP	Switch	Switch de Piso
1U en rack de Servidores	AVAYA	4826GTS	24 UTP 100/1000 + 4 SFP	Switch	Switch de Servidores
1U en rack de Servidores	AVAYA	4826GTS		Switch	Switch de Servidores

## 7. ASISTENCIA EN LA IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO PARA EL DATACENTER IOMA

### 7.1. Introducción

Dada la no existencia de un conjunto de elementos de monitoreo para el / los servicios de datacenter, que permitan detectar eventos con la suficiente antelación para poder actuar en consecuencia, es que se asiste en la implementación de una plataforma de monitoreo.

#### 7.1.1. Alcance

El proyecto consistió en asistir al personal de la Dirección de Sistemas en la implementación de la plataforma, relevando el estado actual, analizando las soluciones accesibles para implementar, diseñando a su vez la arquitectura e implementado los entornos listos para su utilización, promoviendo la aplicación de mejores prácticas de la industria para este tipo de trabajos y colaborando con las tareas específicas.

### 7.1.2. Plan de trabajo

Se analizó las alternativas de plataformas world class tanto pagas como open source, dado que existía un presupuesto para la adquisición de una plataforma se ejecutó la adquisición de una plataforma paga.

Tareas realizadas:

12. Confeccionar el requerimiento técnico para derivarlo al área de compras.
13. Dimensionar las necesidades de infraestructura en paralelo a la gestión de la compra.
14. Preparar la infraestructura necesaria.
15. Estandarizar la forma de monitoreo.
16. Pruebas integrales
17. Brindar los accesos para que el equipo correspondiente al instituto procesa con la migración.

## 7.2. Solución implementada

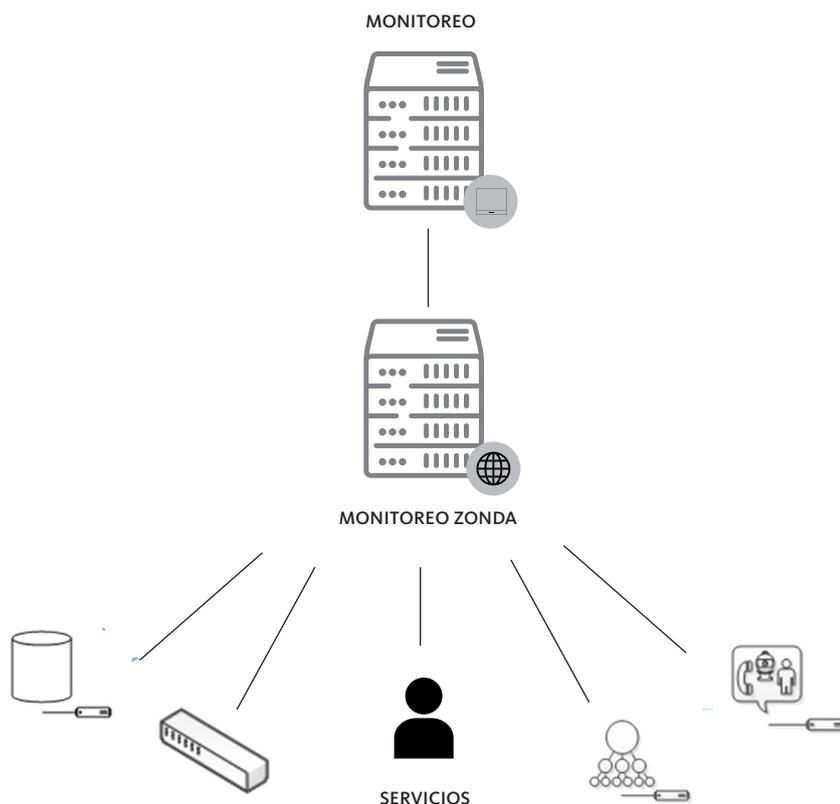
La solución implementada para la monitoria fue de la plataforma PRTG, la misma se licencia por sensores permite utilizar 100 sensores de forma gratuita, pero para la solución final se contempló la cantidad de 1000 con soporte por 3 años pudiendo contar con updates y soporte de la plataforma.

### 7.2.1. Características

A continuación, se detallan las características de la herramienta implementada:

- Monitoreo de Ancho de Banda.
- Monitoreo SNMP v2/v3.
- Compatibilidad con IPv4 e IPv6.
- Posibilidad de integración Active Directory.
- Monitoreo de Base de Datos.
- Monitoreo de Servidores Físicos y Virtuales.
- Dashboard de Alarmas y Mapas.
- Módulo de Reporteria con posibilidad de envíos por Mail o CSV.
- Posibilidad de utilización de Sondas remotas.
- Capacidad para monitorear desde 1000 Elementos.
- Disponibilidad de NETFLOW para control de flujos.
- Disponibilidad de envíos de alarmas por Mails y SMS.

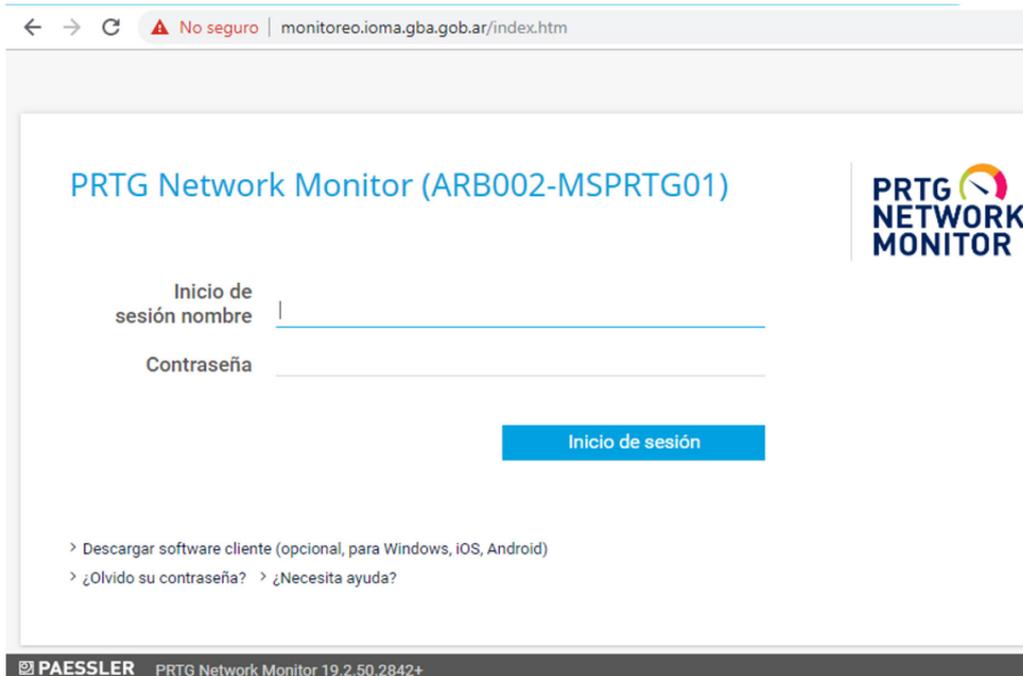
### 7.2.2. Esquema de monitoreo



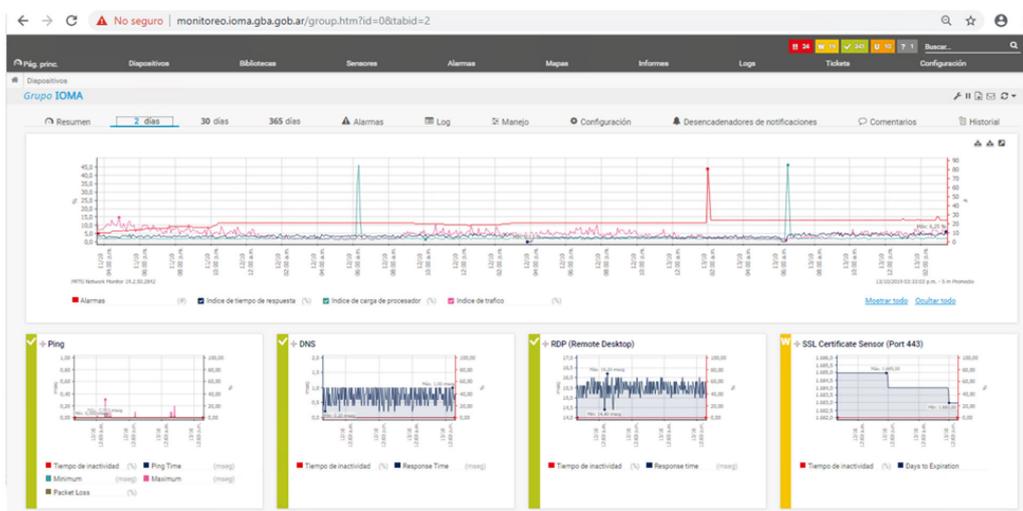
### 7.2.3. Accesos y entorno grafico

#### 7.2.3.1. Portal web

https://monitoreo.ioma.gba.gov.ar/index.htm



#### 7.2.3.2. Entorno del web mail



#### 7.2.4. Acceso a los servidores

A continuación, se detallan los servidores involucrados en la solución con sus direccionamientos:

IP	Hostname	Acceso
10.2.252.99	arbo02-msprtgo1	RDP
10.31.1.65	arbo01-msprtgo1	RDP

Comunidad SNMP: IOMA-SNMP

## 8. GENERACIÓN DE PLIEGO TÉCNICO PARA LA ADQUISICIÓN DE TODO EL MATERIAL NECESARIO Y LAS TAREAS PARA RE-CABLEAR LA RED LAN DEL EDIFICIO DE CASA CENTRAL Y LAS PRINCIPALES DELEGACIONES IOMA Y DE ADQUISICIÓN DE EQUIPAMIENTO PARA IMPLEMENTAR UNA RED WIFI CORPORATIVA EN EL EDIFICIO DE CASA CENTRAL Y PRINCIPALES DELEGACIONES IOMA

### 8.1. Situación actual

El edificio cuenta con trece (13) plantas y dos subsuelos. En cada uno de ellos, hay un rack de 20 unidades que concentra los equipos de comunicación de FO (fibra óptica), los equipos de datos, patcheras de datos, patcheras analógicas, UPS y banco de baterías.

Por una bandeja metálica de 400 mm se distribuye el cableado troncal, la fibra óptica y, en muchos casos, la energía eléctrica de los racks.

Se observa que la interconexión de los puestos desde las patcheras hacia los equipos de comunicación no se encuentra debidamente acomodados en organizadores (por la falta de estos), y los cables de conexión no corresponden a la CAT6. Por otra parte, no todos los racks cuentan con ventiladores de extracción de aire caliente y, muchos de ellos, tampoco tienen llaves que impidan el acceso a los equipos de comunicación de personal no autorizado.

### 8.2. Propuesta

Ante esta situación, se propone:

- Asegurar el acceso a los racks y equipos de comunicación cerrando los mismos con llave.
- Agregar ventilación en los racks que carezcan de equipos de extracción de aire.
- Reemplazar patcheras CAT5 y CAT5E por patcheras CAT6.
- Agregar organizadores y reemplazar los patchcords por cables CAT6.
- Reemplazar el cableado horizontal y vertical del edificio en CAT6.
- Incluir canales de tensión de cinco (5) tomas para conectar los equipos de comunicación.

### 8.3. Descripción del trabajo

En base a los planos de planta del edificio de IOMA Delegación Central, entregados oportunamente por IOMA, en formato digital CAD, se procedió a verificar la ubicación de los puestos de datos y telefonía IP que abarca el proyecto.

Se han seguido las indicaciones del personal de la IOMA Delegación Central abocados a la tarea de relevamiento e identificación de requerimientos.

Además, se buscó obtener las trazas óptimas de las canalizaciones interiores del edificio, tanto verticales y horizontales que contendrán el cableado estructurado, eligiendo la ubicación de los gabinetes para lograr el objetivo.

### 8.4. Desarrollo Del Trabajo

#### 8.4.1. Procedimiento de Identificación de Redes de área local

Este procedimiento se realizará de acuerdo con las directivas emitidas por IOMA Delegación Central denominada Nomenclatura, y este detalla el modo de identificación de las partes de la red de cableado estructurado.

- 1 Serán rotulados todos los cables del cableado horizontal en sus extremos y en los equipos terminales de datos (ETD) y partes de interconexión.
- 2 Los rótulos, ya sean adhesivos o insertables, cumplirán los requisitos de legibilidad, protección contra el deterioro y adhesión especificados en el estándar UL969.

- 3 Resumiendo, se identificarán los cables UTP en ambos extremos del tendido horizontal, las placas en las tomas de las Estaciones de Trabajo y los Paneles de Conexión.
- 4 La nomenclatura a utilizar es la descrita en el siguiente apartado.

#### 8.4.1.1. Identificación de bocas en cada puesto

Se solicita la implementación del siguiente código de rotulado para cada uno de los puestos.

Piso del cuarto de equipos/ distribución	Identificación del cuarto de equipos/ distribución	Gabinete	Patchera	Boca y tipo
Nº o Letra de 2 dígitos	Letra A-Z	Nº de 2 dígitos	Letra A-Z	Nº de 2 dígitos y letra D, V o A
01	A	03	C / B / A	07D / 07V / 01A

**Ejemplo para boca de datos:** 01-A-03-C-07D  
**Ejemplo para boca de voz:** 01-A-03-B-07V  
**Ejemplo para boca de voz analógica:** 01-A-03-A-01A

#### FORMATO

- PISO del Cuarto de equipos/distribución: Número o letra de dos dígitos. Subsuelo (SS), Entre Piso (EP), Planta Baja (PB), primer piso (01), segundo piso (02), etc.
- Cuarto de equipos/distribución: Letra de la A- Z.
- Identificador del Gabinete por cuarto de distribución: Se identifica con un número de dos dígitos.
- Posición en el Gabinete: Posición en donde se instala el “Panel de interconexión”. Se identifica con una letra de la A-Z.
- Puerto de conexión en el Panel de interconexión: Número de dos dígitos, más la letra D, V o A.

Para los equipos de 48 puertos, la identificación de estos en el panel de interconexión será de 1 a 24 para el panel denominado n-1 y de 25 a 48 para el panel denominado n-2, donde n identifica la letra de las patcheras pertenecientes al concentrador. De esta manera quedan inequívocamente determinadas todas las patcheras con sus equipos correspondientes.

#### 8.4.1.2. Identificación en el cuarto de distribución

Para efectos de ilustración, se adjunta un gráfico que aplica el procedimiento de identificación de la red local.

- Piso donde se ubica el cuarto de distribución: 01
- Cuarto de equipos: A
- Gabinete: 01
- Posición del Panel de interconexión: B
- Puerto de conexión en el panel de interconexión: 04 D

**01 A 01 B 04D**

#### 8.4.1.3. Identificación de la caja de conexión

El identificador se asocia directamente con el extremo del cable que se conecta en el Cuarto de distribución. De manera que el código de identificación se conforma de igual manera.

**01 A 01 B 04D**

#### 8.4.1.4. Identificación de los extremos del cable con la etiqueta de identificación

Los identificadores se asocian directamente con la identificación efectuada en la caja de conexión y en cuarto de distribución correspondiente.

#### 8.4.2. Planos planta de la red

Los planos de planta detallan el recorrido del cableado a lo largo de todo el edificio indicando los lugares elegidos para realizar los tendidos verticales y horizontales de la red que nos ocupa y están dibujados en CAD.

Los planos están realizados sobre la base del plano de planta del edificio entregado por IOMA. Se adjuntan los archivos CAD de cada planta del edificio.

El contenido de los planos de planta muestra la ubicación de los:

- Cuartos de Distribución
- Las oficinas con la ubicación de las “Cajas de Conexión” dentro de las mismas.
- Cableado horizontal, muestra el recorrido y tipo de ductos utilizados en cada tramo, bandeja, caño, etc.
- Altura a la cual deben ser instalados los ductos
- Cantidad de cables por tramo
- Cableado vertical, ubicación de los montantes, detalles constructivos.
- El plano de planta tendrá una capa con las cotas del tendido.
- Identificación del cableado. El plano de planta tendrá una capa donde se identifican todos los puestos de la red bajo la nomenclatura requerida por IOMA.

## 8.5. Topología de la red

La red que nos ocupa se desarrolla en 14 plantas: Subsuelo 1, Planta Baja, 1ºP, 2ºP, 3ºP, 4ºP, 5ºP, 6ºP, 7ºP, 8ºP, 9ºP, 10ºP, 11ºP, 12ºP y 13ºP.

La topología de red propuesta es una estrella jerárquica con centro en el cuarto de distribución ubicado en el octavo piso, denominado 08 A 01.

El cableado horizontal está realizado con cable UTP CAT6. Se respetará en todos los puestos no superar los 90 metros de extensión del cableado según lo requiere la norma EIA/TIA 568A. Los equipos estarán instalados en racks standard de 20 unidades

Los racks estarán equipados con los accesorios necesarios para asegurar la calidad de la distribución del cableado en su interior.

## 8.6. Pliego técnico

### PLIEGO DE ESPECIFICACIONES TÉCNICAS (PET)

#### Solución Integral de Conectividad para la Red de Área Local de IOMA

#### ARTÍCULO 1 – OBJETO DEL DOCUMENTO

El presente documento establece el conjunto de Especificaciones Técnicas a satisfacer para implantar la Red de Área Local (LAN) en el edificio de central de IOMA y en sus 14 Regiones de la Provincia de Buenos Aires con las 195 delegaciones dependientes.

Atento a las características de la contratación, que implica el acceso a las redes de información, configura la exigencia de realizar operaciones de carácter reservado, a fin de proteger y dar seguridad a los datos e infraestructura informática frente a ciberataques que puedan afectar a la Administración de IOMA en consecuencia a los ciudadanos.

El / los Adjudicatario/s debe/n proveer, implantar, poner en marcha con la modalidad llave en mano y mantener preventiva y correctivamente, cuando corresponda.

El Oferente debe integrar a su Oferta, una descripción pormenorizada de la solución técnica propuesta. La descripción deberá incluir, en el texto, todos los detalles que permitan evaluar el cumplimiento técnico de la propuesta; cualquier elemento no descrito en el texto se considerará inexistente independientemente que pudiera haberse incluido en un diagrama adjunto. Además de la descripción textual, la propuesta deberá incluir todos los diagramas conceptuales y técnicos de uso habitual, y las especificaciones técnicas de cada uno de los diferentes equipos o elementos que forman parte del sistema propuesto, con indicación de marca, modelo y opciones de hardware cuando corresponda.

#### ARTÍCULO 2 – OFERTA TÉCNICA

Contendrá el desarrollo y descripción en forma pormenorizada de los Bloques por los cuales presente su propuesta y el detalle de equipos, materiales y accesorios a utilizar.

Se integrará con:

- a) Descripción técnica detallada para cada Bloque ofertado;
- b) La documentación en la que conste las características técnicas de los equipos e instalación que forman parte de la propuesta que el Oferente planea emplear para satisfacer lo solicitado, que permita conocer o identificar con toda claridad, los equipos cotizados.
- c) Planillas de Cumplimiento, detallando de qué manera su Oferta se ajusta a los requerimientos Técnicos exigidos en las Especificaciones Técnicas.

Para ello, debe confeccionar una tabla como respuesta a cada uno de los puntos de dicha sección, presentada en el mismo orden, que contenga las siguientes columnas.

1. Identificar a que Punto de las Especificaciones Técnicas se refiere.
2. Cumplimiento del punto. Se debe responder taxativamente Sí o No. La respuesta “Si” implica el total cumplimiento y aceptación de la cláusula. En ningún caso se responderá con frase del tipo “Cumple según pliego” u otras de similar tenor, las que de existir serán asimiladas a NO CUMPLE;
3. Foja de la Oferta en la que se encuentra la justificación Técnica detallada;
4. Detalles y Observaciones relevantes al Punto.

**ARTÍCULO 3 – DETERMINACIÓN DE LA MEJOR OFERTA**

La preadjudicación se efectuará para cada Bloque, teniendo en cuenta el valor ponderado de las ofertas., a partir del procedimiento de ponderación de Ofertas establecidos a continuación:

**a) Bloque 1, Renglón 1:**

1. En el Anexo IX se detallan los puntos deseables, pero no obligatorios que forman parte de la solución. Cada punto tiene asignado un puntaje que evalúa la percepción del Comitente de esa característica en particular.
2. La Preadjudicación se hará a la Oferta que obtenga el menor Valor Ponderado.
3. Considerando el puntaje obtenido por las características técnicas de la Oferta se calculará el Valor Ponderado con la siguiente ecuación:

**Dónde:**

**Puntaje:** es la sumatoria de puntos que corresponden a la solución técnica presentada, calculados de acuerdo al cumplimiento de las características detalladas en el Anexo IX.

**b) Bloque 2:**

Al no existir puntos OBLIGATORIOS se adjudicará a la oferta de menor valor económico.

**c) Bloque 3:**

Al no existir puntos OBLIGATORIOS se adjudicará a la oferta de menor valor económico.

**d) Bloque 4:**

Al no existir puntos OBLIGATORIOS se adjudicará a la oferta de menor valor económico.

**e) Bloque 5:**

Al no existir puntos OBLIGATORIOS se adjudicará a la oferta de menor valor económico.

**ARTÍCULO 4 – ESPECIFICACIONES TECNICAS BASICAS**

**BLOQUE 1 - ELECTRÓNICA DE LAN**

**Renglón 1:** Equipamiento

**1.1. Conmutador (Switch) de Core Modular y Administrable – Cantidad 2 (dos)**

**1.1.1.** Concentrador Switch de Core modular con las siguientes características:

- 1.1.1.1. Concentrador Switch para conmutación de tramas LAN.
- 1.1.1.2. Deberá contar con servicios de red de capa 2 y 3 (network layer 2 y 3).
- 1.1.1.3. Deberá contar con “stack dual” IPv4/IPv6.
- 1.1.1.4. Deberá incluir los accesorios necesarios para montar en racks estándar de 19”.
- 1.1.1.5. Debe ocupar una altura no superior a 5 (cinco) unidades de rack.
- 1.1.1.6. Deberá contar con un mínimo de 4 bahías para alojar módulos de interfaces 1/10GE
- 1.1.1.7. Cada unidad deberá ser entregada con 1 (uno) juego de manuales de configuración de hardware y software. Estos manuales podrán ser entregados en formato papel o mediante medios de almacenamiento digitales.
- 1.1.1.8. Los equipos deberán ser alimentados de 220 V - 50 Hz, monofásico con toma de 3 patas planas, sin necesidad de requerir un transformador adicional.
- 1.1.1.9. Compatibilidad mínima: Gigabit Ethernet en cobre (IEEE 802.3ab), Gigabit Ethernet en fibra (IEEE 802.3z) y 10 Gigabit Ethernet (IEEE 802.3ae).

**1.1.2. Conectividad**

- 1.1.2.1. La cantidad de puertos de concentración inicial deberá proveerse mediante la instalación de los módulos correspondientes para los tipos indicados en la tabla que se incluye más abajo.
- 1.1.2.2. En caso de que el acceso a la interfaz física sea implementado mediante transceptores enchufables, los mismos deberán ser del tipo SFP o SFP+.
- 1.1.2.3. Cantidad y tipo de bocas mínimo a incluir en el switch: Se deberá contar con la cantidad solicitada (mínima) en etapa inicial y capacidad de crecimiento remanente en el switch para llegar a capacidad (máxima) solo con el agregado de tarjetas/módulos adicionales.
- 1.1.2.4. Tipo y cantidad mínima de ports de entrada/concentración/distribución requerida:

<b>TIPO DE PUERTO (SÓLO SE PUEDE ELEGIR UN TIPO)</b>	<b>PUERTOS (MÍNIMO)</b>	<b>PUERTOS (MÁXIMO)</b>
1/10 Gigabit Ethernet SFP/SFP+	48	80

**1.1.2.5.** De la tabla anterior se desglosa:

- 1.1.2.5.1. 2 puertos en cada switch para interconexión entre ambos switches de CORE, que deberán actuar como una única unidad lógica mediante configuración de Virtual Switch. Esos dos puertos deben ser de 10GE

cada uno (20GE en port channel) y el tipo de interfaz (cobre o fibra) podrá ser determinado por el oferente.

**1.1.2.5.2.** 30 puertos en cada switch para conexión hacia los switches/extensores de acceso. Estos deberán ser 10 Gigabit base-LR

**1.1.2.5.3.** 8 puertos en cada switch para conexión hacia los Equipos de Data Center. Estos deberán ser 10 Gigabit base-LR

**1.1.2.5.3.4.** puertos en cada switch para conexión hacia la red MAN. Estos deberán ser 10 Gigabit base-LR, ER, ZR (según la distancia)

**1.1.2.6.** Todos los puertos deberán soportar IEEE 802.3ad LACP (Link Aggregation Control Protocol) para agrupamiento de enlaces en un único canal de mayor ancho de banda.

**1.1.2.7.** Al configurarse el par de equipos como Virtual Switch, el LACP deberá poder configurarse utilizando puertos de ambas unidades para formar parte del mismo port channel LACP.

**1.1.2.8.** Soporte de Jumbo Frames de al menos 9216 bytes de longitud.

### 1.1.3. Rendimiento:

**1.1.3.1.** La matriz de conmutación en Layer 2 (switch fabric) deberá contar con una velocidad de conmutación inicial no inferior a la sumatoria del ancho de banda de todos los puertos solicitados en la configuración inicial, considerando que los mismos operan en modo full-duplex.

**1.1.3.2.** La matriz de conmutación en Layer 2 (switch fabric) deberá tener capacidad de escalar, hasta una velocidad de conmutación no inferior a 2 Tbps.

**1.1.3.3.** El redireccionamiento en Layer 3 para IPv4 (Layer 3 packet forwarding) será no inferior a 300 Mpps

**1.1.3.4.** El redireccionamiento en Layer 3 para IPv6 (Layer 3 packet forwarding) será no inferior a 150 Mpps

**1.1.3.5.** Deberá soportar Netflow en hardware, con no menos de 2.5M de entradas.

### 1.1.4. Capacidades de Capa 2 (Layer 2)

**1.1.4.1.** Soporte de al menos 128000 MAC address de red.

**1.1.4.2.** Capacidad de soportar definición de dominios de broadcast VLANs (Virtual LANs) en cualquier puerto según IEEE 802.1 p/Q o por reglas de asignación por port y address MAC.

**1.1.4.3.** Deberá soportar no menos de 4000 VLANs.

**1.1.4.4.** Soporte de IEEE802.1ad QinQ (transporte de VLANs locales sobre VLANs externas).

**1.1.4.5.** Soporte de Spanning Tree Protocol según IEEE 802.1D y Rapid Spanning Tree Protocol según IEEE 802.1w.

**1.1.4.6.** Soporte de Múltiple Spanning Tree Protocol según IEEE 802.1s para mejorar la eficiencia de convergencia en entornos VLAN.

### 1.1.5. Capacidades de Capa 3 (Layer 3)

**1.1.5.1.** Soporte de ruteo estático.

**1.1.5.2.** Soporte de "Router Information Protocol", RIPv1, RIPv2.

**1.1.5.3.** Soporte de ruteo avanzado mediante OSPFv2 (IPv4) y OSPFv3 (IPv6) ("Open Shortest Path First"), y BGPv4 ("Border Gateway Protocol") o protocolos mejorados.

**1.1.5.4.** Deberá efectuar Routing entre Virtual LANs con protocolos IP (mínimo).

**1.1.5.5.** Soporte de multidifusión mediante protocolo IGMPv2 e IGMPv3 ("Internet Group Management Protocol") de acuerdo al RFC-2236, y soporte de PIM ("Protocol Independent Multicast") en modos "sparse" (SM) y "dense" (DM). Con soporte de 32.000 grupos IGMP como mínimo.

**1.1.5.6.** Soporte de MPLS:

**1.1.5.6.1.** MPLS-P: conmutación de etiquetas

**1.1.5.6.2.** MPLS-PE: imposición/deposición de etiquetas

**1.1.5.6.3.** MPLS-RSVP-TE: Ingeniería de tráfico con reserve de recursos

**1.1.5.6.4.** MPLS VPN

**1.1.5.6.5.** EoMPLS

**1.1.5.6.6.** VPLS

**1.1.5.7.** Deberá soportar como mínimo 256.000 rutas (IPv4) y/o 128.000 rutas (IPv6)

**1.1.5.8.** Soporte de Multicast, con 128.000 rutas (IPv4/IPv6) como mínimo.

**1.1.5.9.** Soporte de encapsulamiento IPV4 e IPv6 en IPv6

**1.1.5.10.** Soporte de encapsulamiento IPV6 en IPv4 (6to4, GRE, ISATAP)

### 1.1.6. Calidad de Servicio (QoS)

**1.1.6.1.** Deberá implementar mecanismos para clasificación de tráfico tanto en IPv4 como IPv6.

**1.1.6.2.** Deberá poseer al menos 8 colas de priorización de tráfico por puerto, y al menos una de las colas deberá tener prioridad absoluta en la conmutación de su tráfico por sobre todas las demás, esto es, mientras esta cola tenga tráfico en espera, no podrá procesarse ninguna otra cola.

**1.1.6.3.** Permitirá el manejo de políticas de QoS con criterios asignables sobre layer 2 y 3 (mínimo).

**1.1.6.4.** Deberá soportar al menos 64.000 entradas para marcado de tráfico.

- 1.1.6.5.** Deberá soportar IEEE 802.1p/Q para clasificación y priorización de tráfico, IP ToS y DiffServ.
- 1.1.6.6.** En cada puerto deberá aceptar la conmutación de tráfico clasificado (TAG) aunque sin rechazar otros tráficos no clasificados (UNTAG), a fin de permitir la conexión de un teléfono IP y una PC en un mismo puerto.
- 1.1.6.7.** Deberá poder realizar mapeos 802.1p/Q a DiffServ/ToS y DiffServ/ToS a 802.1p/Q.

#### 1.1.7. Seguridad

- 1.1.7.1.** Manejo de Listas de Control de Acceso (ACL) sobre layer 2 a 4 (mínimo); soportando un mínimo de 64.000 ACLs
- 1.1.7.2.** Soporte de autenticación IEEE 802.1x
- 1.1.7.3.** Soporte de autenticación múltiple (multi-host) IEEE 802.1x
- 1.1.7.4.** Deberá ser capaz de realizar autenticación IEEE 802.1x a través de una consulta a un servidor de autenticación del tipo RADIUS acorde a RFC-2138.
- 1.1.7.5.** Soporte de Reverse Path Forwarding (RPF) y uRPF Check (para IPv4 e IPv6)
- 1.1.7.6.** Soporte contra ataques de Distributed Denial of Service (DDoS) con control de procesos de CPU
- 1.1.7.7.** Soporte de Políticas de uso para protección del panel de control (CoPP)
- 1.1.7.8.** Soporte IEEE 802.1ae MACsec en HW

#### 1.1.8. Administración

- 1.1.8.1.** Soporte de administración encriptada mediante SNMPv3, SSL o SSH.
- 1.1.8.2.** Agente SNMP según RFC 1157 que permita monitorear el estado y el tráfico del dispositivo en forma remota desde entorno Windows / X Windows. Soporte de MIB II según RFC 1213.
- 1.1.8.3.** Se deberán proveer en un medio extraíble todos los bloques de información de management (MIBs) necesarios.
- 1.1.8.4.** Capacidad de soportar al menos 4 grupos de RMON.
- 1.1.8.5.** Almacenamiento de sistema operativo y configuración en memoria Flash reescribible con las siguientes características:
  - 1.1.8.5.1.** Capacidad de actualización por medio de protocolo FTP según RFC 959 ó TFTP según RFC 1350 (cliente y servidor).
  - 1.1.8.5.2.** El sistema deberá permitir actualizaciones de software en línea sin necesidad de interrumpir su funcionamiento.
  - 1.1.8.5.3.** Asimismo, deberá permitir realizar una copia de resguardo del sistema actual, a fin de tener la capacidad de recuperarlo en caso de que la actualización no funcione adecuadamente.
  - 1.1.8.5.4.** Servicio de configuración por medio de consola remota Telnet según RFCs 854/855 sobre transporte TCP/IP según RFCs 793/791.
  - 1.1.8.5.5.** Soporte de replicación o copiado de tráfico configurable, ya sea mediante ACL, port, MAC address o VLAN hacia un puerto específico definido por el administrador para su estudio y análisis.

#### 1.1.9. Redundancia y Alta Disponibilidad

- 1.1.9.1.** Uso de módulos Hot-Swap para evitar detener el equipo en caso de falla.
- 1.1.9.2.** Deberá permitir la configuración en arquitectura de virtual switch (VSS) entre 2 o más equipos, que deberán comportarse como solo uno, desde el punto de vista de administración y gestión.
- 1.1.9.3.** En configuración Virtual Switching (VSS) los módulos de Administración y monitoreo de cada equipo de core deben comportarse como un módulo con su redundancia.
- 1.1.9.4.** En configuración Virtual Switching (VSS) las switch fabric redundante de cada equipo de core, deben comportarse como un módulo con su redundancia.
- 1.1.9.5.** Deberá soportar Stateful Switchover (SSO) y Non-Stop-Forwarding (NSF), en modalidad Virtual Switch (VSS)
- 1.1.9.6.** Deberá soportar upgrade de software en línea sin pérdida de paquetes (ISSU), en modalidad Virtual Switch (VSS)
- 1.1.9.7.** Fuente de alimentación redundante (mínimo 1+1).
- 1.1.9.8.** Ventiladores redundantes, reemplazables en caliente.

### 1.2 Switches de Acceso o Extensores con PoE de 48 (Cuarenta y Ocho) ports y 2 (dos) / 4 (cuatro) de Uplink – Cantidad: 56 (Cincuenta y Seis)

- 1.2.1.** Concentrador Switch o Extensor Ethernet / Fast Ethernet / Gigabit Ethernet con conexión a backbone de 1 / 10 Gigabit Ethernet con las siguientes características:
  - 1.2.1.1. Nota:** cuando se habla de extensores, se refiere a ciertas arquitecturas disponibles, donde el switch de acceso funciona en realidad como un módulo remoto del switch de CORE. De esta manera, se logra administrar toda la red LAN como si se tratase de un único switch central.
  - 1.2.1.2. NO OBLIGATORIO:** Si el oferente dispone de ambas tecnologías, switches y extensores; esta última será la preferida dado que simplifica enormemente la administración de la red.
  - 1.2.1.3.** Switch concentrador para conmutación de tramas Ethernet, que incluye servicios de red de capa 2 y capa 3; o extensor del switch de Core, con las mismas características.
  - 1.2.1.4.** Deberá incluir los accesorios necesarios para montar en racks estándar de 19”.
  - 1.2.1.5.** Compatibilidad mínima: Ethernet IEEE 802.3, Fast Ethernet IEEE 802.3u, Gigabit Ethernet en cobre (IEEE 802.3ab), Gigabit Ethernet en fibra (IEEE 802.3z) y 10 Gigabit Ethernet (IEEE 802.3ae).

- 1.2.1.6. Cada unidad deberá ser entregada con 1 (uno) juego de manuales de configuración de hardware y software. Estos manuales podrán ser entregados en formato papel o mediante medios de almacenamiento digitales.
- 1.2.1.7. Los equipos deberán ser alimentados de 220 V -50 Hz, monofásico con toma de 3 patas planas, sin necesidad de requerir un transformador adicional.
- 1.2.1.8. Fuente de alimentación redundante (mínimo 1+1).

## 1.2.2. Conectividad

- 1.2.2.1. La cantidad de puertos de concentración inicial deberá proveerse mediante la instalación de los módulos correspondientes para los tipos indicados en punto 1.2.2.3.1 siguiente.
- 1.2.2.2. En caso de que el acceso a la interfaz física sea implementada mediante transceptores enchufables, los mismos deberán ser del tipo SFP/SFP+.
- 1.2.2.3. Cantidad y tipo de bocas mínimo a incluir en el switch:
  - 1.2.2.3.1. Tipo y cantidad mínima de ports de entrada/concentración:
    - 1.2.2.3.1.1. Gigabit Ethernet 10/100/1000BaseT autosensing (RJ45): 48 (Cuarenta y ocho)
    - 1.2.2.3.1.2. Slot para 1/10 Gigabit Ethernet SFP/SFP+: 2 (dos) o 4 (Cuatro)
- 1.2.2.4. Se deberán proveer los siguientes elementos para los switches solicitados:
  - 1.2.2.4.1. 1 (uno) Cables de Stacking de 0,5m.
  - 1.2.2.4.2. 1 (uno) módulos de 10 GbE SFP+ (LR)
  - 1.2.2.4.3. 1 (uno) para stack de switches de piso cada 2 switches.
  - 1.2.2.4.4. Todos los puertos de cobre 10/100/1000BaseT deberán soportar la funcionalidad de Power over Ethernet (PoE) con una capacidad de 15,4W por puerto, debiendo soportarse todos los puertos en simultáneo a máxima potencia. (740W)
  - 1.2.2.4.5. El equipo deberá tener la capacidad de soportar PoE+ (30W) en sus puertos, siempre que alcancen los 740W de potencia total.
  - 1.2.2.4.6. Todos los puertos de cobre 10/100/1000BaseT deberán soportar la característica Auto-MDIX, es decir el conector deberá ajustar automáticamente su funcionamiento sin importar si se enchufa un cable directo o uno cruzado.
  - 1.2.2.4.7. Para modo full dúplex los puertos deberán soportar control de flujo mediante IEEE 802.3X.
  - 1.2.2.4.8. Soporte de Jumbo Frames de al menos 9216 bytes de longitud
  - 1.2.2.4.9. Soporte de IEEE 802.3az Energy-Efficient Ethernet (EEE)
  - 1.2.2.4.10. Ports de uplink/salida:
  - 1.2.2.4.11. Los equipos deberán contar con al menos 2 slots disponibles para interfaces SFP+ de 10Gbps (No se admiten soluciones que compartan el puerto de Uplink con los puertos de usuarios)

## 1.2.3. Apilamiento (Stacking)

- 1.2.3.1. Los equipos deberán soportar la funcionalidad de Stacking de al menos 5 unidades.
- 1.2.3.2. Los equipos que formen parte de mismo stack deberán poder operar en forma virtualizada como una sola unidad, tanto a nivel de administración, procesamiento y enrutamiento
- 1.2.3.3. El stack deberá soportar la funcionalidad de agregación de vínculos en forma distribuida entre los distintos equipos que conforman el Stack. (Link aggregation distribuido).
- 1.2.3.4. Proveer las interfaces de Stacking, que deberán ser distintas a las interfaces solicitadas y deberán ser provistas con sus respectivos cables de conexión.
- 1.2.3.5. La velocidad del stack deberá ser como mínimo de 80 Gbps.

## 1.2.4. Funcionalidad de Capa 2 (Layer 2)

- 1.2.4.1. Soporte de al menos 128000 MAC address de red.
- 1.2.4.2. Capacidad de soportar definición de dominios de broadcast VLANs (Virtual LANs) en cualquier puerto según IEEE 802.1 p/Q o por reglas de asignación por port y address MAC.
- 1.2.4.3. Deberá soportar no menos de 4000 VLANs.
- 1.2.4.4. Soporte de IEEE802.1ad QinQ (transporte de VLANs locales sobre VLANs externas).
- 1.2.4.5. Soporte de Spanning Tree Protocol según IEEE 802.1D y Rapid Spanning Tree Protocol según IEEE 802.1w.
- 1.2.4.6. Soporte de Multiple Spanning Tree Protocol según IEEE 802.1s para mejorar la eficiencia de convergencia en entornos VLAN.

## 1.2.5 Capacidad de Capa 3 (Layer 3)

- 1.2.5.1. Soporte de ruteo estático.
- 1.2.5.2. Soporte de "Router Information Protocol", RIPv1, RIPv2.
- 1.2.5.3. Soporte de ruteo avanzado mediante OSPFv2 (IPv4) y OSPFv3 (IPv6) ("Open Shortest Path First") y BGPv4 ("Border Gateway Protocol") o protocolos mejorados.
- 1.2.5.4. Deberá efectuar Routing entre Virtual LANs con protocolos IP (mínimo).
- 1.2.5.5. Soporte de multidifusión mediante protocolo IGMPv2 e IGMPv3 ("Internet Group Management Protocol") de acuerdo al RFC-2236, y soporte de PIM ("Protocol Independent Multicast") en modos "sparse" (SM) y "dense" (DM). Con soporte de 32.000 grupos IGMP como mínimo.

- 1.2.5.6.** Soporte de MPLS:
  - 1.2.5.6.1.** MPLS-P: conmutación de etiquetas
  - 1.2.5.6.2.** MPLS-PE: imposición/deposición de etiquetas
  - 1.2.5.6.3.** MPLS-RSVP-TE: Ingeniería de tráfico con reserve de recursos
  - 1.2.5.6.4.** MPLS VPN
  - 1.2.5.6.5.** EoMPLS
  - 1.2.5.6.6.** VPLS
- 1.2.5.7.** Deberá soportar como mínimo 256.000 rutas (IPv4) y/o 128.000 rutas (IPv6)
- 1.2.5.8.** Soporte de Multicast, con 128.000 rutas como mínimo.
- 1.2.5.9.** Soporte de encapsulamiento IPV4 e IPV6 en IPV6
- 1.2.5.10.** Soporte de encapsulamiento IPV6 en IPV4 (6to4, GRE, ISATAP)

#### 1.2.6. Manejo de QoS (Calidad de Servicio)

- 1.2.6.1.** Deberá implementar mecanismos para clasificación de tráfico tanto en IPv4 como IPv6.
- 1.2.6.2.** Deberá poseer al menos 4 colas de priorización de tráfico por puerto, y al menos una de las colas deberá tener prioridad absoluta en la conmutación de su tráfico por sobre todas las demás, esto es, mientras esta cola tenga tráfico en espera, no podrá procesarse ninguna otra cola.
- 1.2.6.3.** Permitirá el manejo de políticas de QoS con criterios asignables sobre layer 2 y 3 (mínimo).
- 1.2.6.4.** Deberá soportar al menos 64.000 entradas para marcado de tráfico.
- 1.2.6.5.** Deberá soportar IEEE 802.1p/Q para clasificación y priorización de tráfico, IP ToS y DiffServ.
- 1.2.6.6.** En cada puerto deberá aceptar la conmutación de tráfico clasificado (TAG) aunque sin rechazar otros tráficos no clasificados (UNTAG), a fin de permitir la conexión de un teléfono IP y una PC en un mismo puerto.
- 1.2.6.7.** Deberá poder realizar mapeos 802.1p/Q a DiffServ/ToS y DiffServ/ToS a 802.1p/Q.

#### 1.2.7. Seguridad de Acceso

- 1.2.7.1.** Soporte de autenticación IEEE 802.1x
- 1.2.7.2.** Soporte de administración encriptada mediante SNMPv3, SSL o SSH.
- 1.2.7.3.** Manejo de Listas de Control de Acceso (ACL) sobre layer 2 a 4 (mínimo).
- 1.2.7.4.** Soporte de Port ACL, VLAN ACL y IPv6 ACL
- 1.2.7.5.** Soporte de autenticación basada en MAC Address
- 1.2.7.6.** Soporte de mecanismos de seguridad como:
  - 1.2.7.6.1.** Bloqueo de BPDU sobre puertos que no requieren recibir este tipo de paquetes
  - 1.2.7.6.2.** Bloqueo de paquetes de DHCP desde servidores no autorizados
  - 1.2.7.6.3.** IP source Guard para prevenir ataques de IP spoofing
  - 1.2.7.6.4.** STP root guard
  - 1.2.7.6.5.** Permitir el acceso solo a direcciones MAC específicas.
- 1.2.7.7.** Soporte de RADIUS para autenticación de usuarios.

#### 1.2.8. Administración

- 1.2.8.1.** Agente SNMP según RFC 1157 que permita monitorear el estado y el tráfico del dispositivo en forma remota desde entorno Windows / X Windows. Soporte de MIB II según RFC 1213.
- 1.2.8.2.** Se deberán proveer en un medio extraíble todos los bloques de información de management (MIBs) necesarios.
- 1.2.8.3.** Capacidad de soportar al menos 4 grupos de RMON.
- 1.2.8.4.** Capacidad para soportar Netflow y/o SFLOW en cualquiera de los puertos
- 1.2.8.5.** Almacenamiento de sistema operativo y configuración en memoria Flash re escribible. Capacidad de actualización por medio de protocolo FTP según RFC 959 ó TFTP según RFC 1350 (cliente y servidor).
- 1.2.8.6.** Servicio de configuración por medio de consola remota Telnet según RFCs 854/855 sobre transporte TCP/IP según RFCs 793/791.
- 1.2.8.7.** Logging de sesiones y eventos
- 1.2.8.8.** Debe soportar distintos niveles de acceso al equipo.
- 1.2.8.9.** Soporte de 802.1AB - Link Layer Discovery Protocol (LLDP)
- 1.2.8.10.** Soporte de Port y VLAN mirroring
- 1.2.8.11.** Soporte de Device Link Detection Protocol (DLDP)

### 1.3 Controladores de Red Inalámbrica, Controladores de Puntos de Acceso Inalámbricos, administración y gestión centralizada: 2 (Dos)

#### 1.3.1. Escalabilidad

- 1.3.1.1.** Indicar los niveles de escalabilidad respecto de cantidad de APs soportados por el controlador.
- 1.3.1.2.** Indicar los niveles de escalabilidad respecto de cantidad de clientes soportados (usuarios conectados a un AP).
- 1.3.1.3.** Indicar los niveles de escalabilidad respecto de cantidad de VLANs soportadas
- 1.3.1.4.** Indicar cantidad y tipo de interfaces disponibles en los controladores

### 1.3.2. Alta Disponibilidad y Redundancia

- 1.3.2.1. Debido a la alta criticidad del tráfico de gestión y monitoreo, los equipos propuestos deberán proveer alta disponibilidad (99,999%).
- 1.3.2.2. Los controladores deberán funcionar en configuración redundante.
- 1.3.2.3. Detallar todas las opciones que existan para realizar la redundancia.
- 1.3.2.4. En condiciones normales, con una configuración 1+1, los controladores deben realizar el balanceo de APs y ante una contingencia que falle uno de ellos, el equipo que queda debe tomar el control de todos los APs.
- 1.3.2.5. NO OBLIGATORIO: Los Access Points continúan brindando el servicio normalmente cuando falla su controlador primario. Explicar que sucede con las sesiones activas de usuarios.
- 1.3.2.6. Redundancia de entradas de alimentación: el equipamiento propuesto debe contar con redundancia de entrada de alimentación.
- 1.3.2.7. Redundancia de fuente de alimentación: el equipamiento propuesto debe contar con dos o más fuentes de alimentación con módulos independientes.
- 1.3.2.8. Redundancia de fuente de alimentación: el equipamiento propuesto debe poder funcionar con 1 sola fuente de alimentación en caso de falla en las fuentes redundantes, pudiendo reemplazar una en caso de falla sin afectación en el equipo y sus servicios.
- 1.3.2.9. NO OBLIGATORIO: Todas las placas y fuentes pueden ser reemplazadas en línea, sin interrupción de servicio (hot swappable).

### 1.3.3. Características físicas del Hardware

- 1.3.3.1. Realizar un gráfico para los equipos propuestos, dimensiones y unidades de rack que ocupa.
- 1.3.3.2. Detallar especificaciones técnicas sobre ventilación y flujo de aire para la refrigeración del equipo.
- 1.3.3.3. Detallar márgenes y umbrales de temperatura y, en el caso de que los tuviera, mecanismos de seguridad que presenta, ante fallas de refrigeración.

### 1.3.4. Management

- 1.3.4.1. NO OBLIGATORIO: El equipo propuesto cuenta con interfaces para realizar gestión y monitoreo outband. Detallar cuántas interfaces y de qué tipo son.
- 1.3.4.2. NO OBLIGATORIO: Las interfaces físicas para realizar gestión outband, soportan velocidades 10/100/1000 tanto half como full duplex.
- 1.3.4.3. Debe soportar SNMP v1, v2c y v3
- 1.3.4.4. Debe soportar RFC 854 Telnet
- 1.3.4.5. Debe soportar RFC 4253 SSH Transport Layer Protocol
- 1.3.4.6. Debe soportar RFC 1155 Management Information for TCP/IP-Based Internet
- 1.3.4.7. Debe soportar RFC 1156 MIB
- 1.3.4.8. Debe soportar RFC 1157 SNMP
- 1.3.4.9. Debe soportar RFC 1213 SNMP MIB II
- 1.3.4.10. Debe soportar RFC 1350 TFTP
- 1.3.4.11. Debe soportar RFC 1643 Ethernet MIB
- 1.3.4.12. Debe soportar RFC 2030 Sntp
- 1.3.4.13. Debe soportar RFC 2616 http
- 1.3.4.14. Debe soportar RFC 2665 Ethernet-Like Interface types MIB
- 1.3.4.15. Debe soportar RFC 2819 RMON MIB
- 1.3.4.16. Debe soportar RFC 2863 Interfaces Group MIB
- 1.3.4.17. Debe soportar RFC 3164 Syslog. Indicar cada cuánto tiempo y por cuánto tiempo se guardan los logs.
- 1.3.4.18. Debe soportar RFC 3414 User-Based Security Model (USM) for SNMPv3
- 1.3.4.19. Debe soportar RFC 3418 MIB for SNMP
- 1.3.4.20. Debe soportar RFC 3636 Definitions of Managed Objects for IEEE 802.3 MAUs
- 1.3.4.21. NO OBLIGATORIO: El controlador permite ver en tiempo real y guardar un histórico acerca de la performance de radio y niveles de interferencia a los cuales están expuestos los APs.
- 1.3.4.22. Detalla
- 1.3.4.23. NO OBLIGATORIO: El controlador permite manejo de estadísticas y KPIs.
- 1.3.4.24. NO OBLIGATORIO: Es posible generar KPIs propios, Detallar
- 1.3.4.25. Los mecanismos de accounting deben permitir realizar accounting x SSID. Detallar como funciona y que opciones se permiten.
- 1.3.4.26. Debe soportar la opción de configurar varios SSID por APs.
- 1.3.4.27. NO OBLIGATORIO: La cantidad de SSID soportados, depende solo del modelo de AP. Indicar el máximo número de SSID que pueden configurarse.
- 1.3.4.28. Debe soportar la opción de configurar los APs en Mesh
- 1.3.4.29. Debe soportar la opción de definir diferentes grupos o zonas de APs
- 1.3.4.30. NO OBLIGATORIO: Se pueden bajar de manera automática diferentes configuraciones para los APs de determinadas zonas. Explicar todas las opciones que existen respecto de la configuración de zonas y los beneficios de utilizar zonas.

- 1.3.4.31. Debe soportar Real-time location service (RTLs)
- 1.3.4.32. Debe soportar autoconfiguración de los APs
- 1.3.4.33. Debe soportar selección automática del canal
- 1.3.4.34. Debe soportar upgrade de software para los APs
- 1.3.4.35. NO OBLIGATORIO: Es posible hacer un roll back de la versión de firmware del controlador.
- 1.3.4.36. NO OBLIGATORIO: Puedo hacer un roll back de la versión de firmware de los APs.
- 1.3.4.37. Debe soportar el troubleshooting de los clientes
- 1.3.4.38. NO OBLIGATORIO: Provee alguna funcionalidad que permita asignar un pool distinto de IPs dependiendo el SSID al cual se conecte el cliente
- 1.3.4.39. Detallar las diferentes opciones que puedan tener (por ejemplo, opción 82 DHCP)
- 1.3.4.40. El controlador debe permitir realizar balanceo de carga de los APs en el controlador. Detallar como es el funcionamiento de este tipo de balanceo.
- 1.3.4.41. El controlador debe permitir realizar balanceo de carga de los clientes en los APs. Detallar como es el funcionamiento de este tipo de balanceo.
- 1.3.4.42. Debe soportar Handover/Roaming. Describir como es el proceso o los procesos en caso de que haya varias opciones y si es transparente para el usuario.

### 1.3.5. Soporte de estándares Wireless

- 1.3.5.1. Debe soportar el estándar IEEE 802.11a
- 1.3.5.2. Debe soportar el estándar IEEE 802.11b
- 1.3.5.3. Debe soportar el estándar IEEE 802.11g
- 1.3.5.4. Debe soportar el estándar IEEE 802.11n
- 1.3.5.5. Debe soportar el estándar IEEE 802.11ac
- 1.3.5.6. Debe soportar el estándar IEEE 802.11e
- 1.3.5.7. Debe soportar el estándar IEEE 802.11h
- 1.3.5.8. Debe soportar el estándar IEEE 802.11k
- 1.3.5.9. Debe soportar el estándar IEEE 802.11r
- 1.3.5.10. Debe soportar el estándar IEEE 802.11u
- 1.3.5.11. Debe soportar el estándar IEEE 802.11w
- 1.3.5.12. Debe soportar el estándar IEEE 802.11d
- 1.3.5.13. Debe estar certificado por Passpoint (Hotspot 2.0)

### 1.3.6 Soporte de estándares

- 1.3.6.1. El controlador debe soportar túneles CAPWAP, especificar las diferentes opciones respecto del tráfico que se puede enviar a través del túnel (tráfico de usuario, solo señalización, etc.).
- 1.3.6.2. Recomendar lo que el proveedor considera como la mejor alternativa y en caso de terminar solo los túneles con el tráfico de señalización, especificar donde terminaría el tráfico de usuario. Detallar
- 1.3.6.3. Soporte de IEEE 802.3, Standard definido por la IEEE para el intercambio de información entre sistemas de redes tanto para áreas locales como metropolitanas
- 1.3.6.4. Debería soportar IEEE 802.1p COS
- 1.3.6.5. Debería soportar IEEE 802.1p QoS para distintos tipos de servicios. Indicar para cuantos tipos de servicio.
- 1.3.6.6. Indicar si soporta IEEE 802.1q Virtual bridge Domain
- 1.3.6.7. Se requiere que el equipo soporte ARP según RFC 826. Esto significa que las interfaces puedan solicitar y también responder ARP.
- 1.3.6.8. Debe soportar RFC 768 UDP
- 1.3.6.9. Debe soportar RFC 791 IP
- 1.3.6.10. Debe soportar RFC 2460 IPv6 (pass through Bridging mode only)
- 1.3.6.11. Debe soportar RFC 792 ICMP
- 1.3.6.12. Debe soportar RFC 793 TCP
- 1.3.6.13. Debe soportar RFC 1122 Requirements for Internet Hosts
- 1.3.6.14. Debe soportar RFC 1519 CIDR
- 1.3.6.15. Debe soportar RFC 1542 BOOTP
- 1.3.6.16. Debe soportar RFC 2131 DHCP
- 1.3.6.17. Debe soportar IPv6

### 1.3.7. Seguridad y Autenticación

- 1.3.7.1. NO OBLIGATORIO: Soporta algún mecanismo para la seguridad de equipos outdoor Ejemplo, si en el controlador no agrego la MAC de este APs, el mismo no se conecta a la red.
- 1.3.7.2. Debe soportar la detección de rogue APs. Detallar.
- 1.3.7.3. Debe soportar la detección de ataques de denegación de servicios. Detallar.
- 1.3.7.4. Debe soportar la detección de AP spoofing. Detallar.
- 1.3.7.5. Debe soportar WPA
- 1.3.7.6. Debe soportar WPA2

- 1.3.7.7. Debe soportar 802.11i
- 1.3.7.8. Debe soportar autenticación por MAC Address
- 1.3.7.9. Debe soportar RFC 1321 MD5 Message-Digest Algorithm
- 1.3.7.10. Debe soportar RFC 4346 TLS Protocol Versión 1.0 y 1.1
- 1.3.7.11. Debe soportar RFC 2104 HMAC: Keyed Hashing for Message Authentication
- 1.3.7.12. Debe soportar RFC 2401 Security Architecture for the Internet Protocol
- 1.3.7.13. Debe soportar Wired Equivalent Privacy (WEP)
- 1.3.7.14. Debe soportar Temporal Key Integrity Protocol-Message Integrity Check (TKIP-MIC)
- 1.3.7.15. Debe soportar Advanced Encryption Standard (AES)
- 1.3.7.16. Debe soportar Data Encryption Standard (DES): DES-CBC, 3DES
- 1.3.7.17. Debe soportar Secure Sockets Layer (SSL) and Transport Layer Security (TLS): RC4 128-bit and RSA 1024-bit and 2048-bit
- 1.3.7.18. Debe soportar Datagram Transport Layer Security (DTLS): AES-CBC
- 1.3.7.19. Debe soportar IPsec: DES-CBC, 3DES, AES-CBC
- 1.3.7.20. Debe soportar RFC 4347 Datagram Transport Layer Security
- 1.3.7.21. Debe soportar RFC 3280 Internet X.509 PKI Certificate and CRL Profile
- 1.3.7.22. Debe soportar RFC 2451 ESP CBC-Mode Cipher Algorithms
- 1.3.7.23. Debe soportar RFC 2409 IKE
- 1.3.7.24. Debe soportar RFC 2407 Interpretation for ISAKMP
- 1.3.7.25. Debe soportar RFC 2405 ESP DES-CBC Cipher Algorithm with Explicit IV
- 1.3.7.26. Debe soportar RFC 2404 HMAC-SHA-1-96 within ESP and AH
- 1.3.7.27. Debe soportar RFC 2403 HMAC-MD5-96 within ESP and AH
- 1.3.7.28. Debe soportar el aislamiento de clientes inalámbricos de diferentes SSID.

#### 1.3.8. Portal

- 1.3.8.1. La plataforma deberá soportar la conexión del cliente a través de la selección de una red WiFi abierta y ser redirigido a un portal
- 1.3.8.2. La plataforma deberá soportar un portal que tenga una interfaz de bienvenida, en donde se requieran los datos del cliente para comenzar a usar el servicio. En esta instancia el cliente no tiene servicio, solo puede ver esta interfaz.
- 1.3.8.3. La plataforma deberá soportar una instancia en el portal donde se acepten términos y condiciones, debe presentarse luego de estar registrado e identificado. En esta instancia aún no se tiene servicio
- 1.3.8.4. La plataforma deberá soportar en el portal la autenticación con Usuario y Contraseña. Detallar las interfaces entre los equipos de la solución necesarios para esta autenticación.
- 1.3.8.5. La plataforma deberá soportar la generación de nuevos usuarios desde el portal.
- 1.3.8.6. La plataforma deberá soportar la generación de un servicio temporal.
- 1.3.8.7. La plataforma deberá brindar información de ubicación del usuario para poder enviar publicidad dirigida en forma dinámica mediante el uso de aplicaciones externas, y deberá contar con interfaces de integración hacia las mismas.

#### 1.4 Puntos de Acceso Inalámbricos (AP) - Access Point 802.11ac – Cantidad: 284 Doscientos Ochenta y Cuatro, Sujeto a Site Survey (Punto 1.9)

##### 1.4.1. Generalidades:

- 1.4.1.1. Indicar peso del Access Point (si posee antenas externas o equipamiento adicional indicarlo en el campo detalle).
- 1.4.1.2. Indicar dimensiones del Access Point (si posee antenas externas o equipamiento adicional indicarlo en el campo detalle).
- 1.4.1.1. Especificar rango de temperatura de operación.
- 1.4.1.2. Especificar rango de humedad de operación.
- 1.4.1.3. Especificar el color/colores del dispositivo disponibles.
- 1.4.1.4. Indicar el material de construcción.
- 1.4.1.5. Debe cumplir como mínimo con normas NEMA 1 y/o IP10 (protección contra el polvo, la luz y salpicaduras indirectas).
- 1.4.1.6. Especificar la máxima cantidad de usuarios conectados soportado por el Access Point.
- 1.4.1.7. Especificar la máxima cantidad de usuarios activos (generando tráfico) soportado por el Access Point.
- 1.4.1.8. Especifique cual fue el protocolo de prueba para obtener los datos.
- 1.4.1.9. Debe poderse limitar la cantidad máxima de usuarios conectados al Access Point. Detallar.
- 1.4.1.10. Especificar cuánto tiempo permanecen las MAC Address de los dispositivos (STA) en las Access List del Access Point.
- 1.4.1.11. Especificar throughput máximo teórico y real soportado por el Access Point.
- 1.4.1.12. Especificar si el Access Point permite la implementación de Real-time location service (RTLS).
- 1.4.1.13. El Access Point debe estar homologado/certificado por la CNC o autoridad competente.
- 1.4.1.14. El Access Point debe poseer un puerto de consola para la gestión local del mismo.
- 1.4.1.15. El Access Point debe admitir conexión de forma local para su administración a través interfaz gráfica. Especificar.
- 1.4.1.16. El Access Point debe poseer indicaciones lumínicas para indicar el estado de las alarmas del dispositivo y su modo de operación.

**1.4.2. Montaje**

- 1.4.2.1. Debe incluir soporte o estar adaptado para la colocación sobre mesada.
- 1.4.2.2. Debe incluir soporte o estar adaptado para la colocación sobre pared.
- 1.4.2.3. Debe incluir soporte o estar adaptado para la colocación sobre techo.
- 1.4.2.4. El dispositivo debe incluir un Kit de instalación. Especificar el contenido del mismo.
- 1.4.2.5. El dispositivo debe incluir un soporte/accesorio de tipo anti-vandálico.

**1.4.3. Modo de Operación**

- 1.4.3.1. El dispositivo debe poder operar en modalidad "Autónoma" / "Thick AP" / "Stand Alone".
- 1.4.3.2. El dispositivo debe poder operar en modalidad "Centralizada" / "Thin AP" / "Dependent AP".
- 1.4.3.3. Especificar los diferentes mecanismos que utilizan los APs para realizar el discover de los posibles controladores para asociarse. Explicarlos y nombrar ventajas y desventajas.
- 1.4.3.4. El Access Point debe soportar el cambio de modo a través del "controlador/sistema de gestión". Mencionar si existe otra forma.

**1.4.4. Radio**

- 1.4.4.1. El Access Point debe soportar la norma IEEE 802.11 y todas las revisiones a/g/n/ac. En caso de soportar otras revisiones especificarlo.
- 1.4.4.2. Debe cumplir con una potencia mínima de transmisión igual o superior a 22dBm para la banda de 2,4 GHz. Detallar la potencia máxima de transmisión para cada una de las revisiones.
- 1.4.4.3. Debe cumplir con una potencia mínima de transmisión igual o superior a 22dBm para la banda de 5 GHz. Detallar la potencia máxima de transmisión para cada una de las revisiones.
- 1.4.4.4. Especificar el SNR mínimo soportado por el Access Point para establecer una conexión en cada una de sus bandas (2,4 y 5 GHz).
- 1.4.4.5. Debe poseer antenas externas. Especificar el tipo de antena (omni / sectorial / array), adjuntando el patrón de radiación para cada tipo de antena y bandas de operación. Adjuntar imágenes de las mismas.
- 1.4.4.6. Debe poseer por lo menos 4 antenas duales (2,4 y 5 GHz). Especificar la ganancia en cada banda.
- 1.4.4.7. Debe poseer entrada auxiliar para conectar antenas externas (o en su defecto debe incluirse un modelo análogo exclusivamente con antenas externas). Especificar el tipo de conector y el tipo (omni / sectorial / array), marca y modelo de antena, adjuntando el patrón de radiación para cada tipo de antena y bandas. Adjuntar hojas de datos de las mismas.
- 1.4.4.8. Debe soportar los siguientes Data Rates: 802.11a (6, 9, 12, 18, 24, 36, 48, 54 Mbps), 802.11g (1, 2, 5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps). Informar velocidades de 802.11ac soportadas.
- 1.4.4.9. Especificar la sensibilidad en recepción para cada uno de los Data Rates en las revisiones a/g soportados por el Access Point, para cada una de las bandas (2,4 y 5GHz).
- 1.4.4.10. Especificar los MCSs index soportados por el Access Point (revisiones n/ac).
- 1.4.4.11. Especificar la sensibilidad en recepción para cada uno de los MCSs (esquemas de modulación) en la revisión n, soportados por el Access Point, para cada una de las bandas (2,4 y 5GHz). Especificarlo en el ancho de banda de 20 y 40 MHz.
- 1.4.4.12. Debe soportar la configuración de múltiples SSIDs. Especificar el máximo.
- 1.4.4.13. Debe soportar MIMO. Especificar qué tipo de configuración MIMO es soportada (Tx X Rx) y máximo número de spatial streams soportados.
- 1.4.4.14. Especificar si soporta Beamforming y que mecanismos utiliza el Access Point para cumplir con esta funcionalidad.
- 1.4.4.15. Debe soportar QoS según la norma IEEE 802.11e (también conocido como WME o WMM).
- 1.4.4.16. Debe contar con analizador de espectro por hardware incluido en cada AP, para análisis. Clasificación y mitigación de interferencias

**1.4.5. Alimentación**

- 1.4.5.1. Debe soportar alimentación PoE según norma IEEE 802.3af.

**1.4.6. Conectividad**

- 1.4.6.1. Debe soportar interfaz Ethernet (10/100/1000 BaseT).
- 1.4.6.2. El Access Point deberá estar preparado para soportar un esquema de direccionamiento IPv6 (forwarding de paquetes IPv6, etc.). Detallar e indicar Roadmap en caso necesario.
- 1.4.6.3. Especificar si la conectividad entre APs y el Controlador es Layer 2 y/o Layer 3.
- 1.4.6.4. Especificar qué tipo de túnel utiliza (GRE, CAPWAP, etc.). Indicar si el túnel soportado es estándar.
- 1.4.6.5. Indicar si el AP puede levantar el túnel y todos los servicios contra un Controlador de APs de otro fabricante.
- 1.4.6.6. Indicar entre qué equipos se arma dicho túnel (AP <> Controlador, AP <> Router, etc.).
- 1.4.6.7. Soporta configurar dos IPs para túnel activo y túnel backup contra controladores distintos para un esquema de controladores activo/backup? Detallar.
- 1.4.6.8. Debe soportar IEEE 802.1Q VLANs
- 1.4.6.9. Debe soportar IEEE 802.1p QoS

#### 1.4.7. Performance

- 1.4.7.1. Especificar si el Access Point posee algún mecanismo de mitigación ante interferencia (no WiFi). Detallar su funcionamiento.
- 1.4.7.2. El Access Point debe poseer mecanismo de Band Steering (Balanceo de carga entre bandas 2,4-5 GHz) para la mejora de performance.
- 1.4.7.3. Indique si el Access Point posee alguna funcionalidad adicional que permita mejorar la performance de conexión.

#### 1.4.8. Seguridad y Autenticación

- 1.4.8.1. ¿Soporta algún mecanismo para la seguridad de equipos outdoor que vayan en la vía pública? Ejemplo, si en el controlador no agrega la MAC de este APs, el mismo no se conecta a la red.
- 1.4.8.2. Debe soportar la detección de rogue APs. Detallar.
- 1.4.8.3. Debe soportar la detección de ataques de denegación de servicios. Detallar.
- 1.4.8.4. Debe soportar la detección de AP spoofing. Detallar
- 1.4.8.5. Debe soportar WPA
- 1.4.8.6. Debe soportar WPA2
- 1.4.8.7. Debe soportar 802.11i
- 1.4.8.8. Debe soportar autenticación por MAC Address.
- 1.4.8.9. Debe soportar RFC 1321 MD5 Message-Digest Algorithm
- 1.4.8.10. Debe soportar RFC 4346 TLS Protocol Versión 1.0 y 1.1
- 1.4.8.11. Debe soportar RFC 2104 HMAC: Keyed Hashing for Message Authentication
- 1.4.8.12. Debe soportar RFC 2401 Security Architecture for the Internet Protocol
- 1.4.8.13. Debe soportar Wired Equivalent Privacy (WEP)
- 1.4.8.14. Debe soportar Temporal Key Integrity Protocol-Message Integrity Check (TKIP-MIC)
- 1.4.8.15. Debe soportar Advanced Encryption Standard (AES)
- 1.4.8.16. Debe soportar Data Encryption Standard (DES): DES-CBC, 3DES
- 1.4.8.17. Debe soportar Secure Sockets Layer (SSL) and Transport Layer Security (TLS): RC4 128-bit and RSA 1024-bit and 2048-bit
- 1.4.8.18. Debe soportar Datagram Transport Layer Security (DTLS): AES-CBC
- 1.4.8.19. Debe soportar IPsec: DES-CBC, 3DES, AES-CBC
- 1.4.8.20. Debe soportar RFC 4347 Datagram Transport Layer Security
- 1.4.8.21. Debe soportar RFC 3280 Internet X.509 PKI Certificate and CRL Profile
- 1.4.8.22. Debe soportar RFC 2451 ESP CBC-Mode Cipher Algorithms
- 1.4.8.23. Debe soportar RFC 2409 IKE
- 1.4.8.24. Debe soportar RFC 2407 Interpretation for ISAKMP
- 1.4.8.25. Debe soportar RFC 2405 ESP DES-CBC Cipher Algorithm with Explicit IV
- 1.4.8.26. Debe soportar RFC 2404 HMAC-SHA-1-96 within ESP and AH
- 1.4.8.27. Debe soportar RFC 2403 HMAC-MD5-96 within ESP and AH
- 1.4.8.28. Debe soportar el aislamiento de clientes inalámbricos de diferentes SSID.

#### 1.5. Servidor de Direccionamiento IP (DHCP) – Cantidad: 1 (uno)

##### 1.5.1. DHCP Server

- 1.5.1.1. Debe soportar:
  - 1.5.1.1.1. Portal: Primero se asigna dirección IP, el tráfico de cliente se redirige al portal para acceder al servicio.
  - 1.5.1.1.2. AAA: Con cliente propio, este se autentica usando 802.1x a través del AAA existente
  - 1.5.1.1.3. La solución provista debe incluir un servidor de DHCP que deberá ser capaz de soportar el dimensionamiento de la solución completa.
  - 1.5.1.1.4. Detallar el hardware de la solución de DHCP ofrecida (preferentemente por arquitecturas basadas en Intel, RHEL como OS y VMware de hipervisor –si fuera posible-).
  - 1.5.1.1.5. Dar la lista de características del DHCP ofrecido.
  - 1.5.1.1.6. Indicar número máximo concurrente de discovers por segundo que puede soportar la solución ofrecida.
  - 1.5.1.1.7. Indicar número máximo concurrente de request por segundo que puede soportar el DHCP propuesto.
  - 1.5.1.1.8. Proveer la documentación completa del DHCP ofrecido.
  - 1.5.1.1.9. El servidor DHCP ofrecido debe ser redundante.
  - 1.5.1.1.10. Sería deseable que soporte redundancia geográfica.
  - 1.5.1.1.11. El servidor DHCP debe ser escalable. Detallar la capacidad del servidor DHCP en su configuración mínima e indicar como escala.
  - 1.5.1.1.12. El servidor DHCP debe soportar los protocolos DHCPv4 y DHCPv6.
  - 1.5.1.1.13. El servidor DHCP debe soportar la configuración de diferentes rangos de direcciones IP (scopes).
  - 1.5.1.1.14. En el servidor DHCP se deben poder configurar los scopes como redes y máscaras, luego dentro de esas redes se establecerán los rangos de IP a asignar y se podrán establecer direcciones IP reservadas, dirección IP del gateway, etc.
  - 1.5.1.1.15. El servidor DHCP será capaz de procesar campos y opciones DHCP para asignar direcciones IP de

acuerdo a reglas. Detallar qué opciones y campos maneja y las reglas soportadas.

**1.5.1.1.16.** El servidor DHCP debe permitir enviar opciones DHCP específicas al dispositivo cliente en base a reglas. Detallar qué opciones maneja y las reglas soportadas.

**1.5.1.1.17.** El servidor DHCP debe ser capaz de asignar IP reservada a ciertos clientes de acuerdo a cierto criterio, por ejemplo, MAC del dispositivo cliente. Detallar.

**1.5.1.1.18.** El servidor DHCP debe ser capaz de manejar scopes que se solapen. Por ejemplo, en el caso de usar redes privadas repetidas que luego pasan por un NAT diferente cada una.

**1.5.1.1.19.** El servidor DHCP debe generar logs de asignación de direcciones y errores.

**1.5.1.1.20.** Debe generar traps de SNMP cuando alcance umbrales, por ejemplo, de uso de scopes, por un número de solicitudes (discovers, requests, etc.) o cualquier elemento que afecte concurrentes.

**1.5.1.1.21.** Debe trabajar con una base de datos abierta e incluso poder usar bases de datos externas

## 1.6 Sistema de identificación de usuarios y control de acceso

**1.6.1.** El sistema deberá ser centralizado, y tendrá la capacidad de identificar los usuarios que acceden a la red, ya sea cableado en un puerto de switch o inalámbrico.

### 1.6.2. Funcionalidad

**1.6.2.1.** Policy Enforcement: deberá proveer un modelo de políticas de acceso basado en atributos, incluyendo el punto de acceso (alámbrico o inalámbrico), el protocolo de autenticación, el perfil del usuario, etc.

**1.6.2.2.** Debe tener la capacidad de integrarse con repositorios de usuarios externos como Active Directory, LDAP, Radius, RSA-OTP

**1.6.2.3.** Control de acceso, incluyendo listas (ACLs) descargables, asignación de VLAN, redireccionamiento URL, VLANs nominadas.

**1.6.2.4.** Deberá permitir un acceso seguro, sin necesidad de configurar clientes (endpoints) para su autenticación y autorización.

**1.6.2.5.** Deberá implementar el uso de una red para invitados, con capacidad de autogestión, con posibilidad de incluir banners o algún video institucional como experiencia de acceso a la red, ya sea por medios alámbricos (Switch) o inalámbricos (Access Point)

**1.6.2.6.** Deberá utilizar RADUIS para Autorización, Autenticación y Accounting (AAA), soportando los siguientes protocolos: PAP, MS-CHAP, Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), EAP-Flexible Authentication vía Secure Tunneling (FAST), EAP-Transport Layer Security (TLS) y EAP-Tunneled Transport Layer Security (TTLS).

**1.6.2.7.** Tiene que poder oficiar como autoridad certificante interna, evitando en una primera etapa la complejidad de sumar una autoridad externa.

**1.6.2.8.** Debe manejar el protocolo de certificados estándar OCSP y poder revocar un certificado si un dispositivo es sustraído.

**1.6.2.9.** Deberá poder armar perfiles de dispositivos (por ejemplo: impresoras, PC Windows, Notebook Windows, Smartphone Android, Iphone, etc.) a modo de poder aplicar políticas basados en dichos templates.

**1.6.2.10.** Deberá soportar updates automáticos de perfiles de diferentes vendedores.

**1.6.2.11.** Tanto para PCs como para dispositivos móviles, deberá no sólo autenticar al usuario, sino también poder realizar un relevamiento de seguridad del dispositivo antes de habilitar su acceso a la red interna. Por ejemplo, debe probar la versión del sistema operativo, últimos updates, si tienen corriendo el antivirus, antispysware, encriptación del disco, etc.

**1.6.2.12.** En caso de no cumplir la política establecida en alguno del software del punto k, deberá redirigir al usuario a una VLAN de cuarentena, donde poder bajar la imagen correspondiente.

### 1.6.3. Administración y Gestión

**1.6.3.1.** La consola de administración deberá ser centralizada, vía GUI basada en web, pudiendo configurar perfiles, postura, invitados, autenticación y autorización.

**1.6.3.2.** Deberá incluir consola embebida para monitoreo, reportes y troubleshooting para ayudar a los administradores a resolver problemas.

**1.6.3.3.** Deberá contar con reportes real-time e históricos para todos los servicios.

### 1.6.4. Plataforma

**1.6.4.1.** Serán aceptados dispositivos que corran sobre servidores de uso específico, pero preferidos aquéllos que sean virtualizables sobre VMWare o KVM.

## 1.7 Sistema de Gestión

**1.7.1.** El proveedor deberá brindar la siguiente información acerca de los detalles específicos de funcionalidad de sus productos para el software de gestión de los equipos presentados en la solución, el SG se encarga de ver toda la red completa, permite gestionar los equipos, visualizar alarmas y generar estadísticas de toda la red y su utilización.

El Sistema de Gestión propuesto debe ser flexible y auditable, es decir, debe simplificar las tareas de la operación y control de los equipos. El manejo deberá ser simple y eficaz, y deberán estar cubiertas todas las tareas necesarias para administrar la solución. Se desea también saber qué nivel de control de gestión se tiene sin el software propuesto, utilizando sólo CLI y/o SNMP de manera de poder administrarlo con nuestros sistemas actuales.

El proveedor deberá responder de cuantos paquetes de “software” cuenta su sistema de gestión y monitoreo propuesto.

### 1.7.2. General

- 1.7.2.1. Completar la siguiente tabla contenida en el Anexo I referida al sistema de Gestión.
- 1.7.2.2. El Sistema de Gestión deberá tener capacidad de monitoreo dinámico y control en tiempo real de las siguientes funcionalidades de gestión:
  - 1.7.2.2.1. Gestión de fallas/mantenimiento
  - 1.7.2.2.2. Gestión de performance
  - 1.7.2.2.3. Gestión de configuración
  - 1.7.2.2.4. Gestión del software del sistema
  - 1.7.2.2.5. Gestión de seguridad
  - 1.7.2.2.6. Gestión de topología
  - 1.7.2.2.7. Gestión de interfaz Northbound
  - 1.7.2.2.8. Gestión de licenciamiento
  - 1.7.2.2.9. Confiabilidad del sistema
- 1.7.2.3. Especificar si todas las funcionalidades de gestión descritas anteriormente se ejecutan en una única plataforma o en forma distribuida.
- 1.7.2.4. Dispondrá de la posibilidad de recolectar información, de usos, localización y demás con alguna plataforma de analytics permitiendo brindar servicios basados en localización, publicidad dirigida y demás.
- 1.7.2.5. La aplicación del Sistema de gestión deberá estar basada en una plataforma confiable y altamente disponible. Dicha aplicación debe ofrecer redundancia para evitar cualquier tipo de falla y garantizar una confiabilidad máxima.
- 1.7.2.6. Se deberá describir el esquema de redundancia del sistema de gestión.
- 1.7.2.7. Se deberá proveer detalles completos sobre los proveedores de plataformas de hardware y software, módulos, confiabilidad, tiempo medio entre fallas (MTBF), redundancia, etc.
- 1.7.2.8. El oferente deberá suministrar una aplicación de documentación preferentemente online, con actualizaciones automáticas que contenga toda la información sobre tipos de hardware, características, descripción técnica, descripción de comandos, procedimiento de Operación y Mantenimiento, etc. de todos los módulos y equipos componentes del sistema.
- 1.7.2.9. Los diferentes elementos de red que componen la solución deberán tener la posibilidad de ser gestionados mediante el protocolo SNMP. Indicar la versión del protocolo y las funcionalidades soportadas.
- 1.7.2.10. Indicar los protocolos de gestión y aprovisionamiento soportados por los diferentes elementos de red ofrecidos.

### 1.7.3. Gestión de Fallas

- 1.7.3.1. El SG deberá notificar en tiempo real los eventos de generación y eliminación de alarmas.
- 1.7.3.2. Se deberá proveer un control de alarmas de los elementos de la red gestionada mediante una representación gráfica.
- 1.7.3.3. El control de alarmas deberá utilizar los códigos de color predeterminados para indicar las diferentes categorías de alarmas (nivel de gravedad, no reconocida, reconocida, en mantenimiento, etc.).
- 1.7.3.4. El SG deberá permitir establecer más de un umbral para cada tipo de alarma
- 1.7.3.5. Al detectarse nuevas alarmas, dicha información deberá visualizarse en la representación gráfica de la red mediante señales sonoras como característica opcional.
- 1.7.3.6. El SG deberá proporcionar logs de alarmas que contengan todo el historial de las alarmas de la red.
- 1.7.3.7. El SG deberá soportar filtrado y clasificación de alarmas.
- 1.7.3.8. El SG deberá proporcionar notificaciones automáticas por mensaje de texto, e-mail, fax o impresora.
- 1.7.3.9. El reconocimiento de la alarma deberá implicar cambios de su estado y color en el SG.
- 1.7.3.10. El historial de alarmas debe ser almacenado y debe tener capacidad para guardar datos u otros elementos específicos para un futuro análisis de las fallas de la red. Especificar tiempo de almacenamiento y capacidad en base a la granularidad de los datos.
- 1.7.3.11. El SG deberá poder capturar alarmas de entorno.
- 1.7.3.12. Las notificaciones de alarmas y eventos que se generen y envíen desde el SG deberán incluir información suficiente para permitir identificar inequívocamente el tipo de notificación de que se trata y el equipo que genera la alarma/evento.
- 1.7.3.13. El SG deberá proporcionar datos de todos los equipos que reciben alarmas y eventos como también las categorías que se le asignarán a las alarmas y eventos.
- 1.7.3.14. Las notificaciones de alarmas y eventos deberán incluir detalles correspondientes a la instancia de alarmas o eventos. La información contenida en una notificación de alarma deberá ser suficiente para:
  - 1.7.3.14.1. Ubicar las fallas de hardware dentro del elemento de red;
  - 1.7.3.14.2. Suministrar la información de diagnóstico necesaria para determinar la causa real del evento y determinar la acción correctiva apropiada.
- 1.7.3.15. El SG deberá presentar el estado de la alarma de los elementos de red en la interfaz gráfica de usuario de topología por medio de colores o cambios gráficos.
- 1.7.3.16. El SG deberá permitir a los usuarios ubicar el elemento de red en el mapa topológico en la ventana de

consultas de alarmas o en la ventana para búsquedas en tiempo real.

**1.7.3.17.** El SG deberá permitir a los usuarios administradores cambiar en el sistema el nivel de gravedad de cada alarma.

**1.7.3.18.** El SG deberá permitir a los usuarios administradores modificar/agregar en el sistema la definición de las alarmas.

**1.7.3.19.** El SG deberá permitir a los usuarios registrar las experiencias en el tratamiento de fallas en la base de conocimiento. La base de conocimiento de alarmas deberá soportar operaciones de importación y exportación.

**1.7.3.20.** El SG deberá detectar en forma automática las alarmas de fallas no eliminadas que han permanecido por un período de tiempo prolongado y luego notificar a los usuarios resaltando dichas alarmas en las ventanas de alarmas. Este período de tiempo se deberá poder personalizar.

**1.7.3.21.** El SG deberá permitir filtrar por tipo de falla/alarma y establecer ranking de elementos de red o fallas con mayor concurrencia.

#### 1.7.4. Gestión de Performance

**1.7.4.1.** El Sistema de Gestión de Performance ofrecido deberá soportar las siguientes facilidades para medir los datos de performance de la red y proporcionar estadísticas para permitir al usuario identificar desviaciones que se presenten en el sistema.

**1.7.4.1.1.** (1) Generación y recopilación de datos

**1.7.4.1.2.** (2) Almacenamiento de datos

**1.7.4.1.3.** (3) Procesamiento y presentación de datos

**1.7.4.2.** El SG deberá tener una presentación gráfica para todos los datos de medición de performance.

**1.7.4.3.** El SG ofrecido deberá implementar indicadores de performance flexibles que permitan definir sus propios indicadores, además del conjunto de indicadores que establezca el oferente.

**1.7.4.4.** El SG ofrecido deberá tener la posibilidad de agrupar indicadores y realizar operaciones entre los mismos para generar nuevos indicadores producto de la operatoria de los anteriores.

**1.7.4.5.** El SG ofrecido deberá proveer informes de KPI (Key Performance Indicator). Estos informes deberán estar disponibles para cualquier tipo de elemento de red o funcionalidad o grupo de ellos. Como mínimo los siguientes tipos de informes deberán estar disponibles:

**1.7.4.5.1.** Informe de comparación de múltiples objetos: Cada gráfico de este informe deberá comparar los objetos gestionados respecto de un conjunto de indicadores a una fecha y con una periodicidad determinada (hora, día, semana o mes).

**1.7.4.5.2.** Informe de evolución de objeto único: Cada gráfico de este informe deberá presentar la evolución de un conjunto de indicadores para un objeto gestionado (o grupo de objetos) entre dos fechas y con la periodicidad seleccionada (hora, día, semana o mes).

**1.7.4.5.3.** Informe de advertencias: Cada gráfico de este informe deberá presentar una lista ordenada de los objetos gestionados en función de ciertos criterios de selección sobre un indicador a una fecha y con una periodicidad determinada (día, semana, mes).

**1.7.4.6.** El SG ofrecido deberá tener la capacidad de modificar o crear cualquier tipo de informes, permitiendo definir qué tipo de indicadores deberán presentarse en el informe.

**1.7.4.7.** El oferente deberá proporcionar una base de datos de las estadísticas recopiladas desde el sistema. Se deberá especificar el tipo de base de datos, la disponibilidad, el nombre, su capacidad y atributos. Se deberá otorgar acceso de lectura/escritura.

**1.7.4.8.** La base de datos deberá permitir almacenar todo tipo de datos de estadísticas. El oferente deberá proporcionar información completa de la capacidad de almacenamiento de la base de datos e indicar los elementos de red y contadores soportados y la cantidad de días en que las estadísticas pueden almacenarse.

**1.7.4.9.** El oferente deberá proveer un sistema de alerta de performance en tiempo real para indicar en forma inmediata cualquier degradación de la calidad del servicio o sobrecarga en los recursos del elemento de red, sobre la base de mediciones de performance.

**1.7.4.10.** El SG deberá ser capaz de exportar los datos del sistema en diferentes formatos.

**1.7.4.11.** El SG deberá permitir a los usuarios especificar los umbrales de alarma para los indicadores. Un indicador deberá poder tener más de un umbral para diferentes objetos de medición o diferentes tiempos de medición.

**1.7.4.12.** El SG deberá ofrecer la posibilidad de mostrar los datos en tiempo real en forma gráfica.

#### 1.7.5. Gestión de Configuración

**1.7.5.1.** El sistema ofrecido deberá soportar descubrimiento automático de nuevos elementos de red y su inclusión en la gestión.

**1.7.5.2.** Deberá ser posible realizar el aprovisionamiento de parámetros de configuración de manera automática al detectar un nuevo elemento en la red.

**1.7.5.3.** El sistema de gestión deberá ofrecer una interfaz de interconexión con el CRM para el aprovisionamiento automático de los elementos de red. Especificar los campos posibles a utilizar.

**1.7.5.4.** Deberá ser posible hacer fácilmente un backup en los archivos de log de la configuración operativa de los elementos de red.

- 1.7.5.5.** Deberá ser posible restablecer con facilidad configuraciones de los elementos de red desde un backup de configuración.
- 1.7.5.6.** El SG deberá proporcionar el panel de equipos, donde se muestre la información del bastidor, de las placas, alarmas y del estado.
- 1.7.5.7.** Deberá ser posible reiniciar elementos de red o placas de forma remota.
- 1.7.5.8.** Deberá ser posible realizar configuraciones de forma masiva y centralizada a distintos elementos de red.
- 1.7.5.9.** Deberá ser posible gestionar de manera centralizada y en forma masiva APs en modo autónomo (Thin)
- 1.7.5.10.** Deberá ser posible gestionar de manera centralizada y en forma masiva APs en modo centralizado (Thick)
- 1.7.5.11.** El operador deberá contar con una topología intuitiva para verificar el estado del hardware.
- 1.7.5.12.** El SG deberá proporcionar la función de gestión de estado de los elementos de red. El estado de los equipos o puertos deberá ser verificado e informado al usuario. El usuario deberá poder reiniciar/bloquear/desbloquear/apagar el equipo o el puerto.
- 1.7.5.13.** El usuario deberá tener la posibilidad de consultar los parámetros principales del estado del hardware como ser estado del procesador, memoria, temperatura de operación, etc.
- 1.7.5.14.** SG deberá soportar monitoreo en línea del estado de ejecución del sistema y del estado del hardware incluyendo:
  - 1.7.5.14.1.** Estado del servicio y proceso
  - 1.7.5.14.2.** Utilización de la CPU
  - 1.7.5.14.3.** Utilización de la memoria
  - 1.7.5.14.4.** Utilidad de la base de datos
  - 1.7.5.14.5.** Utilidad del disco
- 1.7.5.15.** Los AP deberán soportar la gestión local por consola, detallar su modo de ejecución.
- 1.7.5.16.** Indicar si los APs poseen gestión local por interfaz web.
- 1.7.5.17.** Los elementos de red deberán soportar un sistema de seguridad para impedir que un usuario no identificado pueda gestionar el elemento de red de manera local (Consola/Web). Especificar.
- 1.7.5.18.** Indicar si la gestión de los elementos de red se realiza inband/outband

#### **1.7.6. Gestión del Software del Sistema**

- 1.7.6.1.** La gestión de software deberá incluir como mínimo los siguientes ítems:
  - 1.7.6.1.1.** Cambios y actualización de software
  - 1.7.6.1.2.** Reinicio en caso de fallas
  - 1.7.6.1.3.** Recuperación de software y del sistema
  - 1.7.6.1.4.** Activación de software
  - 1.7.6.1.5.** Consulta de versiones de software
- 1.7.6.2.** Las nuevas versiones de software para los elementos de la red y la gestión deberán ser descargables desde el Sistema de Gestión. La descarga deberá llevarse a cabo sin afectar el funcionamiento normal del elemento gestionado ni del Sistema de Gestión. Asimismo, deberá ser posible programar el Downgrade/Upgrade de software.
- 1.7.6.3.** El Sistema de Gestión deberá contar con la funcionalidad para proveer backup y recarga de software. El oferente deberá claramente especificar la duración requerida para el proceso de backup y de recarga, así como también especificar si cualquiera de los elementos de red pueda quedar fuera de servicio durante este proceso.
- 1.7.6.4.** El oferente deberá soportar la carga de nuevo software para diferentes nodos desde el Sistema de Gestión (mediante la carga del SW en el Sistema de Gestión desde medios externos y luego a través de la descarga de dicho SW en los elementos de red) así como también la carga de un elemento de red en forma local. (Ambas opciones deberán estar disponibles).

#### **1.7.7. Gestión de Seguridad**

- 1.7.7.1.** El acceso al SG se controlará a través del inicio de sesión con el nombre de usuario y la contraseña.
- 1.7.7.2.** Se detectará y evitará el acceso de usuarios no autorizados al Sistema de Gestión. El Proveedor deberá brindar los detalles acerca de las técnicas utilizadas a tal fin.
- 1.7.7.3.** Se deberá detectar y prevenir el acceso de usuarios no autorizados entre el servidor del SG y los elementos de red gestionados. El Proveedor deberá brindar detalles acerca de las técnicas utilizadas a tal fin.
- 1.7.7.4.** Se deberá detectar y prevenir el acceso de usuarios no autorizados desde la interfaz northbound si hubiere. El Proveedor deberá brindar detalles acerca de las técnicas utilizadas a tal fin.
- 1.7.7.5.** La transmisión entre el Sistema de Gestión ofrecido y los elementos de red debe realizarse de manera codificada y segura.
- 1.7.7.6.** La transmisión entre el servidor del SG y los cliente del SG debe realizarse en forma codificada y segura.
- 1.7.7.7.** El SG deberá permitir establecer usuarios con diferente privilegios y niveles de acceso.
- 1.7.7.8.** El SG deberá permitir establecer grupos de usuarios y asignarles diferentes privilegios y niveles de acceso.
- 1.7.7.9.** El SG deberá permitir establecer accesos a diferentes grupos de elementos de red a los diferentes usuarios según sus privilegios y niveles de acceso.
- 1.7.7.10.** El SG debe asegurar que un terminal quede automáticamente bloqueado si no se realiza ninguna operación durante un período determinado. El terminal bloqueado solo puede ser desbloqueado por la cuenta de usuario administrador.

**1.7.7.11** El SG debe permitir a los usuarios administradores controlar a todos los usuarios del sistema de gestión. Información tal como el nombre de usuario, acciones que realiza, hora en que realiza tales acciones, resultados, terminales, etc. se deberán exhibir en la interfaz de monitoreo de gestión de seguridad de los usuarios administradores y deberá quedar registrado en una base de datos por un tiempo determinado (indicar el tiempo de almacenamiento).

**1.7.7.12** El SG debe permitir a los usuarios administradores la remoción forzosa de un usuario determinado.

**1.7.7.13.** El Administrador del SG deberá poder crear y administrar nuevos perfiles de Operador. El Proveedor deberá detallar lo siguiente:

**1.7.7.13.1** Todos los ítems que están disponibles para caracterizar un perfil de Operador en particular.

**1.7.7.13.2.** Todas las operaciones que pueden llevarse a cabo en un perfil de Operador en particular.

**1.7.7.14.** El Administrador del SG deberá poder especificar las políticas relacionadas con el inicio de sesión y la contraseña del operador. Detallar las posibilidades ofrecidas al Administrador en esta área.

**1.7.7.15.** El SG proveerá las funciones necesarias para operar los logs del Operador. Se deberá detallar la forma de acceder a los logs así como las funciones disponibles para su operación.

### 1.7.8. Gestión de Licenciamiento

**1.7.8.1** El SG deberá ofrecer la posibilidad de gestionar todo tipo de licencias de los elementos de red y funcionalidades del sistema de una manera gráfica y con una interfaz de usuario sencilla.

**1.7.8.2** El SG deberá ofrecer la posibilidad de gestionar las licencias de cada uno de los elementos de red.

**1.7.8.3** El SG deberá ofrecer la posibilidad de gestionar las licencias de cada una de las diferentes funcionalidades soportadas por cada elemento de red.

**1.7.8.4** El SG deberá ofrecer la posibilidad de gestionar de manera dinámica las licencias por usuario.

### 179. Confiabilidad del Sistema

**1.7.9.1** Los discos rígidos integrados deben soportar configuración redundante RAID1 (espejamiento de discos 1+1).

**1.7.9.2** Los bancos de discos deben soportar la configuración redundante RAID5+Hotspare.

**1.7.9.3** El sistema ofrecido debe soportar redundancia de enlaces de comunicación para garantizar la confiabilidad de la red de gestión.

**1.7.9.4** El SG debe soportar HA, es decir, deben existir dos servidores que forman un clúster y operan como servidores stand by uno del otro. Cuando falla el servidor principal, el sistema cambia automáticamente a un servidor adicional.

**1.7.9.5** El SG debe soportar la función de backup y restauración de los datos del sistema y de los datos de usuarios operadores/administradores. Si se produce una falla en el sistema, el usuario administrador puede recuperar todos los datos del backup para que el sistema vuelva al estado en que se encontraba antes de la falla.

### 1.8 Equipos Spare

Dada la eventual necesidad de solucionar problemas en la operatoria diaria se solicitan los siguientes dispositivos como repuesto en la instalación del Comitente.

#### EQUIPOS SPARE

<b>Access Point</b>	15
<b>Extensores</b>	2

### 1.9 Site survey

Se deberá realizar un estudio de Site Survey para la instalación de los Puntos de Acceso Inalámbricos, el oferente indicará el software e instrumentos con los que lo realizará, como así también el procedimiento aplicado pudiendo así modificar la cantidad como también las características del AP dada la densidad de los lugares a realizar el estudio.

### Renglón 2: Soporte y Mantenimiento

**2.1.** El adjudicatario deberá proveer, a partir de la fecha de recepción y por el período mínimo de TRES (3) años, un servicio de garantía integral (partes, repuestos y accesorios, mano de obra y reemplazo de las partes, repuestos y accesorios dañados) para todo el hardware ofertado (entendiéndose por "recepción" no su simple entrega, sino instalados y funcionando debiendo extenderse la correspondiente constancia con indicación de lugar, fecha y firma del funcionario receptor), con atención en el lugar de instalación (In-Situ) incluyendo repuestos, traslados y mano de obra.

**2.2.** La garantía de funcionamiento y el servicio técnico de mantenimiento será integral; es decir, que comprenderá el servicio de reparación con provisión de repuestos y/o cambio de las partes que sean necesarias sin cargo alguno para la Dirección Provincial de Telecomunicaciones. El proveedor garantizará que el servicio técnico será brindado por personal especializado de la empresa fabricante de los productos ofrecidos, o en su defecto por su propio plantel especializado el que deberá estar debidamente certificado por los fabricantes de los productos ofrecidos para esa tarea específica.

- 2.3.** A tal fin el oferente deberá adjuntar a la oferta una nota emitida por el fabricante donde este indique con claridad que la garantía será brindada a través del fabricante, sin condicionamientos ni limitaciones.
- 2.4.** Los materiales y repuestos a emplear deberán ser originales de fábrica, nuevos y sin uso, debiendo presentarse la documentación que respalde las citadas características.
- 2.5.** El proveedor se obliga a proveer los repuestos necesarios en tiempo y forma para garantizar la continuidad operativa de los equipos en su funcionamiento ante eventuales fallas.
- 2.6.** Durante el periodo de garantía, el proveedor deberá brindar el mantenimiento preventivo del equipo, en donde deberá efectuar tareas como la actualización de firmware, parches o cualquier otro mantenimiento necesario, según las recomendaciones del fabricante para asegurar el correcto funcionamiento del equipamiento.
- 2.7.** Asimismo, se deberán incluir los servicios profesionales para realizar de manera semestral (cada seis meses) la optimización del sistema, upgrades de firmware, BIOS, fix, parches y actualización de software de virtualización, previo al análisis y a la confirmación por parte del personal encargado de la Dirección Provincial de Telecomunicaciones para la aplicación de dichas mejoras.
- 2.8.** No se aceptarán posteriores adiciones a la lista explícita de elementos y/o situaciones no cubiertas por la garantía.
- 2.9.** Todas las características del servicio ofrecido se deberán encontrar operativas al día de la apertura de esta licitación.
- 2.10.** En caso de requerirse la sustitución total del equipo, los equipos provistos como sustitución deberán ser iguales a los averiados o de mayores prestaciones. En ningún caso se aceptará que la sustitución exija la modificación de la estructura de la red o provoque reducción en las funcionalidades del sistema. Todas las reconfiguraciones de software que sean necesarias como consecuencia de la sustitución deberán ser realizadas por el proveedor. La garantía deberá ser brindada por técnicos especializados y suministrada por un servicio técnico autorizado y certificado por el fabricante de los equipos.