Bogotá, 23 de diciembre de 2024

Señores.
**INSTITUTO TOLIMENSE DE FORMACIÓN TÉCNICA PROFESIONAL ITFIP**
**Ibagué - Tolima**

Asunto: **Invitación Publica - IPMC-043-2024**

**REF: CRONOGRAMA DE ACTIVIAD DE MIGRACION PROCESO IPMC-043-2024**
**Objeto: RENOVACIÓN DEL ALOJAMIENTO DEL PORTAL WEB INSTITUCIONAL.**

Reciba un especial saludo de gratitud por habernos elegido,

En virtud de las obligaciones contractuales del contrato en referencia enviamos el cronograma de migración de los servidores actuales hacia la nueva infraestructura. Considerando que la infraestructura actual se encuentra alojada en servidores Linux, el plan de migración contiene actividades para migrar las Aplicaciones a plataforma **Linux CentOS**.

A continuación, el cronograma de actividades propuesto

| N° | ACTIVIDAD | PROGRAMACIÓN | | | | | |
|---|---|---|---|---|---|---|---|
| | | DÍA 1 | DÍA 2 | DÍA 3 | | DÍA 4 | DÍA 5 |
| 1 | **Instalación de Infraestructura** | GP | | | | | |
| 2 | **Configuración y Alistamiento de Infraestructura** | | GP | | | | |
| 3 | **Pruebas Exhaustivas de Factibilidad** | | | GP / ITFIP | GP / ITFIP | | |
| 4 | **Ajustes de Funcionamiento** | | | GP / ITFIP | GP / ITFIP | | |
| 5 | **Publicación de Plataforma en Pre-producción.** | | | | | GP / ITFIP | |
| 6 | **Ajustes Finales de Configuración** | | | | | | GP / ITFIP |
| 7 | **Publicación de Plataforma a Producción.** | | | | | | GP / ITFIP |

FIRMA DEL REPRESENTANTE LEGAL
Representante legal: Helmunt David Sierra Abril || C.C.: 80.184.284 de Bogotá
Razón Social: **GOPHER GROUP S.A.S. || NIT: 900425485-8**
Dirección: calle 70 # 15 – 51 Bogotá || Teléfono (1)794 5719 – 317 7134287
Correo Electrónico: soluciones@gophergroup.com.co

GopherGroup

NIT 900.425.485 - 8

# PLAN DE CONTINGENCIA
# RECUPERACIÓN DE INCIDENCIAS

PBX: (1) 794 5719

soluciones@gophergroup.com.co

Calle 70 No. 15-51
www.gophergroup.com.co

## 1. OBJETIVO

Establecer un plan de contingencia informático para los servicios informáticos de aplicaciones e infraestructura cloud.

## 2. ALCANCE

El alcance de éste procedimiento es para los servicios identificados como críticos de la infraestructura tecnológica de GOPHER GROUP. Está dirigido a todo el personal involucrado en el proceso de Informática y a los clientes de la empresa.

## 3. GLOSARIO

**CENTRO DE DATOS ALTERNO:** Es el Centro de datos encargado de absorber las operaciones del Centro de Datos Principal en caso de emergencia. Un centro de respaldo recibe estas denominaciones en función de su equipamiento

**PLAN DE CONTINGENCIA:** Es un conjunto de procedimientos alternativos para activar el funcionamiento de los procesos de Informática y tecnología cuando uno de sus servicios se afecta por un incidente interno o externo.

**INCIDENTE:** Cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción o una reducción de calidad del mismo

## 4. ABREVIATURAS

- NAS: Unidad de almacenamiento (Network Attached Storage)
- UPS: Sistema de alimentación ininterrumpida (Uninterruptible Power Supply)
- Mpls: Enlace de datos (Multiprotocol Label Switching)
- DNS: Sistema para el manejo de nombres de dominio (Domain Name System)
- DHCP: Protocolo para asignación de direcciones IP (Dynamic Host Configuration Protocol)

## 5. DESARROLLO

Se describirán los procedimientos alternos que se tienen a la operación normal, que le permiten a la empresa seguir operando ante la eventualidad de una falla de los equipos y/o servicios que componen la plataforma tecnológica.

En caso de presentarse incidentes graves como explosiones, incendios, atentados, entre otros, que puedan afectar en menor o mayor grado la operación de la empresa, se ejecutará el procedimiento establecido para la activación en uno de los data centers alternos ubicados en Canadá, Las Vegas, Texas, California, Francia o en un centro de datos nacional.

### 5.1 Políticas.

Mantener una plataforma de servicios con características de redundancia y protegida por servicios en garantía con el centro de datos prestador de servicios.

Configurar en alta disponibilidad o en Clúster, en la medida que lo justifique el costo beneficio, los componentes que afecten servicios críticos.

Activar el plan una vez se agoten los procedimientos normales de verificación y no haya sido posible la recuperación.

Asegurar la efectividad del sistema efectuando dos (2) pruebas independientes a lo largo del año de lo cual se dejará registro de ello en el Formato IT-FT-009 Registro pruebas Data Center Alterno. Las Pruebas se realizarán en horario hábil cuando se impacte menos la operación de la Entidad o en fines de semana.

**5.2 Lineamientos.**

Los servicios de tecnología no considerados como críticos deberán ofrecer mecanismos alternativos para su operación en caso de falla.
La prioridad de atención la tienen los servicios críticos alcance de éste procedimiento
La criticidad de los servicios puede variar en el tiempo.

**5.3 Componentes del Plan**

**5.3.1 Servicios Críticos**

| | SERVICIO | SISTEMA |
|---|---|---|
| **1** | Centro de datos | **Infraestructura física** |
| **2** | Servidores físicos host / nodos | **Hardware** |
| **3** | Plataforma de administración de infraestructura | **Software** |
| **4** | Storage de Backups | **Hardware** |
| **5** | Plataforma de Backups | **Software** |

**5.3.2 Servidores**

| | SERVIDOR | FISICO | D/CENTER | ESTADO |
|---|---|---|---|---|
| 1 | NODO 1 | X | Canadá | ACTIVO |
| 2 | NODO 2 | X | Canadá | ACTIVO |
| 3 | NODO 3 | X | Canadá | ACTIVO |
| 4 | NODO 4 | X | Canadá | PASIVO |
| 5 | NODO 5 | X | Las vegas | ACTIVO |
| 6 | NODO 6 | X | Las vegas | ACTIVO |
| 7 | NODO 7 | X | Las vegas | PASIVO |
| 8 | NODO 8 | X | Francia | ACTIVO |
| 9 | NODO 9 | X | Francia | ACTIVO |
| 10 | NODO 10 | X | Francia | PASIVO |

### 5.3.3 Equipos Activos

#### 5.3.3.1 Switches Core

Los equipos core de red se encuentran conformados por 3 switches capa 3 configurados en Stack y con fuente redundante. En caso que uno de los equipos presente falla, el otro equipo toma el control de la comunicación asegurando la continuidad de la operación. Los switches interconectan las fuentes de alimentación compartiéndolas como un recurso común que conforma el core unificando las fuentes de poder y dirigiendo el consumo de energía donde el sistema core lo requiera.

#### 5.3.3.2 Switches de Borde

Los switches de borde se componen por 3 equipos conectados al core mediante puertos uplink de fibra a 10Gbps y se encuentran configurados en stack.

### 5.3.4 UPS

El centro de datos cuenta con un Sistema Ininterrumpido de Potencia UPS tipo paralelo N+1, con capacidad 100% redundante. El tiempo de autonomía es de mínimo 48 horas minutos a plena carga, en caso que uno de los dos sistemas salga de operación se garantiza un tiempo mínimo de 24 horas hasta cuando las plantas eléctricas entren en funcionamiento.

### 5.3.5 Firewall

Se tiene configurado en Clúster Activo, dos (2) equipos Firewall CISCO ASA5520

### 5.3.6 Canales de Internet

Para proporcionar el servicio de conexión a Internet se cuenta con un canal principal y un canal de respaldo ambos configurados en el Firewall para que en caso de caída de uno, el otro continúe proporcionando el servicio.

### 5.3.7 Storage de Backups

Se cuenta con dos unidades de almacenamiento NAS, una se encuentra configurada en el centro de datos principal en Canadá y la otra se encuentra en el centro de datos alterno en las vegas.

### 5.3.8 Sistemas de Información

a) Plataformas de virtualización
b) Plataforma de gestión de Backups
c) Plataforma de monitoreo

### 5.3.9 Datos

a) Sistemas operativos
b) Datos de aplicaciones
c) Bases de datos

d) Backups locales

**5.4 Situaciones de Contingencia**

**5.4.1 Falla general de Data Center**

En caso de presentarse fallo total del centro de datos principal se debe seguir Protocolo de encendido, de acuerdo con las prioridades establecidas en el Anexo No. 1 - Protocolo de encendido/apagado, una vez se haya verificado el correcto funcionamiento de las UPS.

**5.4.2 Falla del Suministro de Energía**

En caso de presentarse falla eléctrica general en centro de datos se entrará en operación con la infraestructura de redundancia para los fallos eléctricos que mantiene las mismas condiciones de alimentación que en la primaria, el bypass se realiza de forma inmediata y sin cortes de energía para el centro de datos puesto que en ese tiempo la redundancia en UPS entran en funcionamiento mientras se da el paso de alimentación eléctrica en paralelo. Si fallara la redundancia en la alimentación de la energía del centro de datos, entrará en operación el sistema ininterrumpido de potencia UPS con la autonomía de mínimo 48 a 72 horas a plena carga. En caso de falla de uno de los componentes del Sistema de UPS se debe contactar al proveedor contratado para hacer efectivo el protocolo de servicio técnico.

**5.4.3 Falla en servidores**

En caso de presentarse falla con un servidor de la Plataforma se identifica el alcance en los servicios que impacta y se activa la contingencia prevista para dicho equipo de acuerdo con los siguientes anexos:

- Anexo 2 – Relación de Servidores y su Contingencia
- Anexo 3 - Relación de servicios en ejecución por servidor

**5.4.5 Falla en switches**

En caso de presentarse falla con uno de los switches core o de borde el monitoreo activo de centro de datos inmediatamente reemplazará el hardware afectado por uno de las mismas características los cuales se manejan en stock y siempre están disponibles para su reemplazo. Estos dispositivos igualmente se viene reemplazando cada 2 años tengan o no fallos de hardware.

**5.4.6 Falla en Firewall**

En caso de presentarse falla con uno de los firewall del Clúster se realiza el reemplazo del hardware de forma inmediata, entrando a funcionar el firewall redundante pasando de modo pasivo a activo de forma inmediata. Se realizaría inmediatamente el reemplazo del hardware.

**5.4.7 Falla en Canales de Internet y MPLS**

En caso de presentarse falla con uno de los canales de acceso a internet o MPLS, se tiene previsto desde centro de datos un canal paralelo de contingencia con las mismas

características que el principal con un operador diferente que interconecta los centros de datos.

#### 5.4.8 Falla en unidades de almacenamiento NAS

En caso de presentarse falla con una de las NAS, el monitor activo de centro de datos inmediatamente reporta la incidencia a los ingenieros en campo y ellos. Intervienen el hardware antes de 30 minutos pasados del reporte para realizar el cambio del hardware. Las instancias de NAS secundarias se cambian con una periodicidad en hardware de 2 años para evitar incidencias de fallos en hardware, las cuales se van alternando con las primarias en sus cambios.

### 5.4.9 Falla en Servicios

#### 5.4.9.1 DNS

Para el servicio de resolución de nombres DNS se cuenta con cuatro servidores en Clúster DNS que resuelven la zona de toda la infraestructura. Con ésta configuración en caso de falla del servidor primario DOMINIO resuelve uno de los servidores del Clúster apilados en el Clúster. En caso de falla de los dos servidores restantes se activan sus contingencias virtuales en el centro de datos principal.

#### 5.4.9.2 Falla en unidades almacenamiento

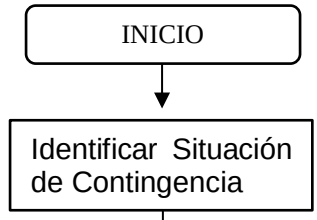
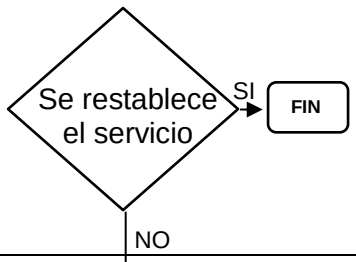
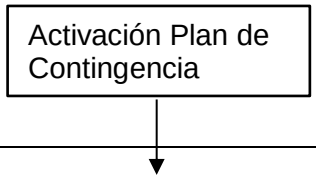
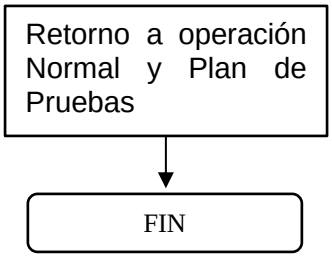
El servicio de almacenamiento de datos de GOPHER GROUP se encuentra centralizado en:

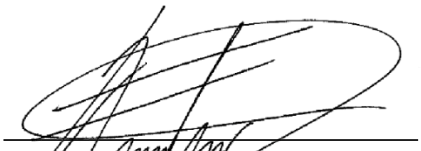
a) La infraestructura de host físicos los cuales hacen respaldo diario en NAS.
b) El Data File de Imágenes y Máquinas virtuales ubicado en la unidad de almacenamiento NAS.
c) NAS.

En caso de presentarse falla con uno de los dispositivos de almacenamiento el centro de datos interviene inmediatamente el hardware para realizar el reemplazo en un tiempo no superior a 30 minutos. Sin embargo, se tiene configurado un raid 6 con tolerancia a fallos de hasta 10 discos físicos configurados en pares diferentes dentro de los arreglos RAID configurados.

En caso de presentarse problema con los datos por pérdida o corrupción de éstos se debe remitir al procedimiento GP-PR-003 restauración de la información, para restablecer la información.

## 5.4. ACTIVIDADES.

| No. | Etapa | Responsable | Documento | Descripción de la etapa |
|---|---|---|---|---|
| 1. |  | MONITOR CENTRO DE DATOS / MONITOR GOPHER | REPORTE INCIDENCIA GP-PR-004 | Se determina el origen de la incidencia que ha terminado en la interrupción del servicio. |
| 2. |  | Coordinador infraestructura y plataforma | REPORTE INCIDENCIA GP-PR-004 | Se restauran los servicios mediante los procedimientos normales |
| 3. |  | Coordinador infraestructura y plataforma | N.A. | Se activa el Plan de Contingencia asociado al servicio crítico interrumpido |
| 4. |  | Coordinador infraestructura y plataforma | REPORTE INCIDENCIA GP-PR-004 | El servicio regresa al estado de operación normal. |



FIRMA DEL REPRESENTANTE LEGAL
Representante legal: Helmunt David Sierra Abril || C.C.: 80.184.284 de Bogotá
Razón Social: **GOPHER GROUP S.A.S. || NIT: 900425485-8**
Dirección: calle 70 # 15 – 51 Bogotá || Teléfono (1)794 5719 – 317 7134287
Correo Electrónico: soluciones@gophergroup.com.co

GopherGroup

NIT 900.425.485 - 8

# ARQUITECTURA TOLERANTE A FALLOS

PBX: (1) 794 5719

soluciones@gophergroup.com.co

Calle 70 No. 15-51
www.gophergroup.com.co

# CONTENIDO

CONTENIDO ..... 2
ARTQUITECTURA TOLERANTE A FALLOS ..... 3
Resumen ..... 3
1 Introducción ..... 3
2 Arquitectura de la solución ..... 4
2.1 Infraestructura ..... 4
Suministro Eléctrico. ..... 4
Fallos las fuentes de alimentación locales de los equipos. ..... 4
Fluctuaciones de Tensión. ..... 4
Cortes totales del suministro Eléctrico. ..... 5
Infraestructura de comunicaciones. ..... 6
2.2 Servidores ..... 6
Clusters. ..... 6
RAIDs. ..... 6
2.3 Sistema de mensajería Electrónica ..... 7
2.4 Arquitectura Web ..... 7
El método Load Balancing Switches. ..... 7
El segundo método implementado en nuestra empresa Microsoft NLB. ..... 8
2.5 Seguridad ..... 8
Código dañino. ..... 8
Ataques a través de Internet. ..... 8
Copias de seguridad. ..... 9



PBX: (1) 794 5719
soluciones@gophergroup.com.co
Calle 70 No. 15-51
www.gophergroup.com.co

# ARTQUITECTURA TOLERANTE A FALLOS

**Resumen.** En **GOPHER GROUP** tenemos implementado un esquema de tolerancia a fallos, aseguramos la disponibilidad en nuestros equipos y los servicios que suministramos de manera fiable y sin interrupción las 24 horas del día durante siete días a la semana, poniendo a disposición los elementos software y hardware necesarios para que los elementos redundantes actúen cooperativamente, de forma activa-activa o activa-pasiva, pero siempre de forma transparente para nuestros clientes. En el presente documento daremos a conocer la forma como evitamos, reducimos y aplicamos soluciones a las incidencias que se puedan presentar en los servicios que prestamos a cada uno nuestros clientes.

## 1 Introducción

La disponibilidad es una medida relativa a la preparación para su utilización de un sistema informático, mientras que la fiabilidad es una medida relativa a su capacidad para mantenerse operativo en el tiempo. Ambas propiedades están englobadas dentro de una propiedad mucho más amplia, la confiabilidad, que también incluye aspectos de seguridad, confidencialidad e integridad de datos.

Todas ellas conllevan a un elevado aumento del coste invertido en hardware y software. Es por esta razón que **GOPHER GROUP** realizó una exhaustiva evaluación para elegir correctamente los componentes de nuestro sistema que permite fácilmente alcanzar un sistema disponible el 99% del tiempo.

Las métricas comúnmente utilizadas para medir la disponibilidad y fiabilidad de nuestro sistema son el tiempo medio entre fallos o MTTF (mean time to failure) que mide el tiempo medio transcurrido hasta que un dispositivo falla, y el tiempo medio de recuperación o MTTR (mean time to recover) que mide el tiempo medio tomado en restablecerse la situación normal una vez que se ha producido el fallo. Lógicamente, **GOPHER GROUP** tiene como principal objetivo aumentar el MTTF y reducir el MTTR de forma que minimicemos ese tiempo.


PBX: (1) 794 5719
soluciones@gophergroup.com.co
Calle 70 No. 15-51
www.gophergroup.com.co

# 2 Arquitectura de la solución

Ante una incidencia es importante para **GOPHER GROUP** tener en cuenta los siguientes cinco aspectos: infraestructura, servidores, mensajería, arquitectura Web y seguridad.

## 2.1 Infraestructura

La línea de división entre la infraestructura y la arquitectura de un sistema informático es, a menudo, muy difícil de ver. Sobre todo porque si nos planteamos la arquitectura de una organización desde un punto de vista evolutivo, los elementos que en un momento dado se consideran como propios de la arquitectura pasan a ser posteriormente parte de la infraestructura. Esto, por ejemplo, ha ocurrido ya con las redes locales y está empezando a ocurrir con los sistemas de mensajería. Aquí trataremos dentro de este capítulo exclusivamente los problemas derivados del suministro eléctrico y los sistemas de comunicaciones.

**Suministro Eléctrico.** La primera causa de fallos que debemos contemplar en nuestro sistema es la provocada por interrupciones o anomalías en el suministro eléctrico. Si, por el motivo que sea, nuestros equipos se quedan sin energía o ésta les llega alterada nuestro sistema no funcionará en absoluto o no lo hará correctamente. Tres son los posibles problemas que se nos pueden presentar en este aspecto:

- Fallos en las fuentes de alimentación locales de los equipos.
- Fluctuaciones de tensión en el suministro eléctrico.
- Cortes totales de suministro eléctrico.

**Fallos las fuentes de alimentación locales de los equipos.** Las partes más débiles de los sistemas informáticos, y las que fallan más a menudo son las fuentes de alimentación. Todos los filtros, generadores externos y sistemas de alimentación ininterrumpida no tienen valor de nada si lo que falla es la fuente de alimentación local de uno de nuestros equipos. Afortunadamente, **GOPHER GROUP** cuenta con servidores de gama alta y fueron fabricados con una fuente de alimentación redundante.

**Fluctuaciones de Tensión.** Incluso en las mejores áreas de suministro la corriente eléctrica pueden sufrir variaciones. Podemos hablar de cuatro fenómenos distintos englobados dentro de esta categoría: picos de tensión (spikes), sobretensiones (surges), caídas (sags) y bajadas de tensión (brownouts).
Los picos de tensión son grandes incrementos de la misma de duración infinitesimal. Es posiblemente el fenómeno más peligroso y más difícil de tratar. La mayoría de las veces son ocasionadas por factores externos que están totalmente fuera de nuestro control (como el arranque en las proximidades de un gran motor eléctrico o la recuperación después de un corte de suministro de la central eléctrica.

**GOPHER GROUP** dispone de un protector contra estos fenómenos que permite que la velocidad de reacción del elemento ante los picos sea lo más elevada posible y que, ante


PBX: (1) 794 5719
soluciones@gophergroup.com.co
Calle 70 No. 15-5 ı
www.gophergroup.com.co

las puntas más severas, el protector se autodestruya a sí mismo aislando nuestro sistema de la red eléctrica como última medida de salvaguarda. Asimismo este protector trabaja creando un camino eléctrico alternativo para derivar esos picos de tensión sin que lleguen a afectar alguno de nuestros equipos.

Las sobretensiones son ocasionadas por causas similares a las que generan los picos de tensión, pero suelen ser de mayor duración (unos cientos de milisegundos) y de menor intensidad. Para esta incidencia **GOPHER GROUP** cuenta con una buena UPS con protección y suministro de tensión constante que permite solucionar el percance que se pueda llegar a presentar.

Las caídas de tensión son el fenómeno opuesto a los picos. No llegan a ser cortes efectivos del suministro, sino meramente descensos muy bruscos de duración infinitesimal que, sin la protección adecuada, puede causar el reseteo de nuestros equipos. Es por esta razón que **GOPHER GROUP** cuenta con transformadores de tensión constante que soluciona el problema de las caídas menos severas.

Por último, las bajadas de tensión son descensos de alrededor de un 5 o 10 % de la tensión de suministro que, para defenderse de las sobrecargas, las compañías eléctricas realizan deliberadamente. Las UPS con las que cuenta **GOPHER GROUP** proporcionan una protección constante que aíslan este fenómeno.

**Cortes totales del suministro Eléctrico.** Dentro de los cortes totales de suministro podemos distinguir tres casos: los que duran unos milisegundos (micro-cortes), aquellos que duran unos minutos y los que duran desde una hora hasta varios días.

Los micro-cortes pueden provocar, en el mejor de los casos, que los equipos se reinicien y, en el peor, fallos inesperados e imprevisibles de memoria, lectura o escritura en disco, etc. Tienen un efecto particularmente perjudicial cuando se reproducen continuadamente varios de estos cortes, lo que provoca una gran fatiga a los componentes electrónicos de los equipos. No es raro tampoco que uno o varios microcortes vayan acompañados, seguida o intercaladamente, de picos de tensión. Al disponer **GOPHER GROUP** de UPS protege contra los picos de tensión que se puedan presentar.

Los cortes que duran entre unos minutos y una hora pueden solventarse con los UPS que cuenta **GOPHER GROUP**, es por esta razón que la empresa dimensiona la duración de las baterías de la misma en función de la carga de nuestro sistema.

Como anticipamos en la introducción, **GOPHER GROUP** tiene como compromiso entre la disponibilidad que pretendemos y el coste del sistema.

En el caso que nos ocupa, uno de los criterios discriminatorios a la hora de **GOPHER GROUP** para escoger los elementos críticos de la red (servidores, cabinas externas de discos y routers) fue la posibilidad de que incluyesen fuentes de alimentación redundantes.


PBX: (1) 794 5719
soluciones@gophergroup.com.co
Calle 70 No. 15-5 |
www.gophergroup.com.co

Se utilizaron, en todos los casos, UPS con protección contra picos y estabilizador de salida de tensión constante de la casa CENER. Se instalaron además sendos generadores de tensión y en uno de ellos y se colocaron además protectores específicos contra estos fenómenos.

**Infraestructura de comunicaciones. GOPHER GROUP** dentro de este punto tiene en cuenta dos apartados: el primero relativo a la infraestructura de comunicaciones local y el segundo los medios de comunicaciones inter-centros.

En lo referente a las comunicaciones locales, **GOPHER GROUP** cuenta con segmentos de backup para los equipos de nuestro sistema y un concentrador de reserva en caso de que se tenga la necesidad de sustituirlo.

En cuanto a las comunicaciones inter-centros, **GOPHER GROUP** dispone de dos medios alternativos de distintas tecnologías: dos operadores de comunicaciones diferentes en cada uno de ellos. Ya que **GOPHER GROUP** contempla que de nada vale disponer de dos líneas de RDSI para nuestra operativa normal y otras dos de backup puesto que, si la avería ocurre precisamente en la centralita quedarán inoperativas.

En lo referente a tecnología, **GOPHER GROUP** cuenta fundamentalmente con cuatro opciones:

- Frame Relay o Red de Retransmisión de Tramas.
- RDSI o Red Digital de Servicios Integrados.
- ADSL o Asymmetric Digital Subscriber Line.
- Redes ATM o de Transferencia Asíncrona.

La elección que **GOPHER GROUP** haga de una u otra depende del uso que vayamos a darle y de las necesidades del servicio que vayamos a proveer a nuestro cliente.

## 2.2 Servidores

Las características fundamentales y la configuración de nuestros servidores:

**Clusters.** Un cluster de ordenadores es, básicamente, un sistema distribuido en paralelo que consiste en dos o más servidores interconectados compartiendo sus recursos y que son vistos como si se tratase de uno solo. Esta es la medida que **GOPHER GROUP** incrementa enormemente la disponibilidad de un sistema, no sólo ante fallos, sino también contemplando las necesarias actualizaciones periódicas del sistema que nos obligan a sacarlos momentáneamente de producción.

**RAIDs.** La tecnología RAID (Redundant Array of Independent Disks) permite a **GOPHER GROUP**, mediante hardware o software, combinar dos o más discos de forma que sean vistos como una única unidad lógica. La información se almacena en ellos de forma redundante proporcionando distintos niveles de tolerancia a fallos. La empresa tiene presente que el esquema RAID puede ser controlado por el propio sistema operativo, por software especializado o por un adaptador hardware específico que usa un procesador dedicado para aligerar la carga de la CPU del servidor. Con el uso de un buen hardware


PBX: (1) 794 5719 soluciones@gophergroup.com.co Calle 70 No. 15-5
www.gophergroup.com.co

**GOPHER GROUP** tiene mayor tolerancia a fallos, mejor rendimiento de lectura y escritura (gracias a caches dedicadas) y funcionalidades extras como el hot-swap y el hot-spare.

**GOPHER GROUP** cuenta con **RAID 5**. Este esquema usa bandas para almacenar los datos y paridad para proporcionar tolerancia a fallos. La principal diferencia respecto a RAID 3 y RAID 4 es que no dedica un disco en exclusiva para la paridad, sino que almacena ésta en bandas intercaladas entre los datos de todos los discos. Requiere un mínimo de tres discos y su eficacia en cuanto a espacio de almacenamiento es idéntica a la proporcionada por los dos RAID's anteriores. La distribución de las bandas de paridad entre todos los discos elimina el cuello de botella existente en las escrituras. Otro punto a tener en cuenta es que este esquema nos proporciona mayor velocidad de acceso y escritura y menor pérdida de capacidad utilizando discos pequeños en mayor cantidad, frente al uso de menor número de discos de mayor tamaño.

## 2.3 Sistema de mensajería Electrónica

Los sistemas de mensajería se están convirtiendo en uno de los puntos vitales de las nuevas empresas. **GOPHER GROUP** ha implementado unas restricciones en este aspecto puesto que un sistema de mensajería electrónica sin ningún tipo de restricción puede ser muy peligroso: el mal uso de los usuarios puede ocasionar que las líneas se colapsen y dejar que el sistema que se está ofreciendo quede fuera de servicio durante prolongados períodos de tiempo.

## 2.4 Arquitectura Web

**GOPHER GROUP** consigue, aparte de una alta disponibilidad, un sistema fácilmente escalable. La estrategia comúnmente usada por **GOPHER GROUP** para diseñar una sede Web o de servidores FTP de alta disponibilidad es lo que se denomina una granja de servidores (Web Farm) con algún sistema de balanceo de carga entre los servidores que componen la granja. Mediante el sistema de balanceo de carga las peticiones entrantes de los distintos clientes son repartidas de distintas formas. Existen dos formas implementadas por la empresa en la distribución de la cargas.

En nuestra empresa se opta por usar NLB para el reparto de carga, combinado con Microsoft Clúster Service para aumentar la disponibilidad y escalabilidad del sistema.

**El método Load Balancing Switches.** Es una solución robusta y muy escalable. Los switches se colocan entre la conección a Internet y la granja de servidores. Todas las peticiones de los clientes llegan al switch usando la misma dirección IP y es éste, en base a diferentes algoritmos implementados en él, quien dirige el requerimiento de servicio a uno de los servidores de la granja. El switch dirige periódicamente un ping a cada uno de los servidores que componen la granja de forma que puede determinar en cada momento cuales están activos y cuáles no. Asimismo, usa el tiempo de respuesta de los mismos para determinar la carga de trabajo de cada uno y utilizar este parámetro en sus algoritmos de encaminamiento, proporcionándonos de esta forma un balanceo de carga inteligente.


PBX: (1) 794 5719
soluciones@gophergroup.com.co
Calle 70 No. 15-5
www.gophergroup.com.co

**El segundo método implementado en nuestra empresa Microsoft NLB.** Este sistema utiliza una dirección IP virtual para el clúster de servidores, distribuyendo la carga de los clientes entre los servidores reales de forma transparente para los clientes. NLB se implementa usando un driver de red situado lógicamente entre el nivel más alto del protocolo TCP/IP y el adaptador de red del servidor. Todos los servidores que componen el clúster reciben la totalidad de las peticiones de los clientes. El driver de red de NLB actúa como filtro y permite que el servidor procese únicamente parte del tráfico que recibe.

## 2.5 Seguridad

La seguridad física y lógica de todos los servicios ofrecidos por nuestra empresa, es el último punto de este documento. Si buscamos construir un sistema confiable y altamente disponible debemos de hacerlo seguro.

Dentro de la seguridad **GOPHER GROUP** tiene en cuenta los siguientes puntos:

- Ubicación de los servidores y elementos críticos de nuestra red.
- Contraseñas de BIOS y de consola.
- Seguridad general del hardware.

Los servidores de la empresa están ubicados en un espacio aislado, de acceso controlado y bien diferenciado. Poseen un ambiente refrigerado y libre de emisiones de polvo, humos y cualquier otro agente agresivo para los mismos. Asimismo, los servidores están protegidos mediante contraseñas de BIOS y de consola. Dichas contraseñas son conocidas exclusivamente por las personas indispensables, cumplir ciertas normas de seguridad (combinaciones sin sentido de símbolos, números y letras en mayúsculas y minúsculas), guardarse en un sobre lacrado para emergencias, cambiarse periódicamente y nunca jamás dejar las contraseñas por defecto que el fabricante o distribuidor proporcione.

**Código dañino.** Hace alusión a los programas no autorizados que realizan funciones que el usuario no conoce y probablemente no desea, bien porque han sido modificados para alterar su funcionalidad o porque han sido diseñados ex- profeso para permanecer ocultos y destruir o robar datos. Los más frecuentes ejemplos de código dañino son los virus y los troyanos.

La detección del código dañino una vez introducido en nuestro sistema puede ser una tarea muy complicada, así que **GOPHER GROUP** extrema las precauciones en cuanto al software que es introducido en nuestros equipos, permitiendo exclusivamente la instalación de software homologado por la dirección técnica de la empresa y realizando esta siempre de forma controlada por personal especializado y nunca por el usuario en cuestión.

**Ataques a través de Internet.** Siempre que conectemos nuestra red con el mundo exterior estamos entrando en un terreno hostil. La mejor defensa para evitar ataques externos es un firewall. Un firewall es un dispositivo que evita que personas


PBX: (1) 794 5719 soluciones@gophergroup.com.co Calle 70 No. 15-5 | www.gophergroup.com.co

desautorizadas entren en nuestra red. Puede tratarse de un ordenador autónomo con filtro de paquetes o de un dispositivo hardware que realiza tales funciones. Los firewalls funcionan como punto único de entrada, evaluando las diversas peticiones y comprobando cuándo están autorizadas y cuándo no, permitiendo también realizar bloqueos contra determinados protocolos y contenidos. En definitiva, un firewall controla quién puede entrar, qué puede entrar y dónde y cómo pueden entrar en nuestra red.

Habitualmente el firewall separa nuestra red interna de los equipos que necesariamente deben de estar conectados directamente al mundo exterior. La zona donde se encuentran estos últimos se denomina habitualmente zona desmilitarizada o DMZ.

**Copias de seguridad.** Un correcto programa de copias de seguridad es indispensable para **GOPHER GROUP** asegurar la disponibilidad de los datos en nuestro sistema. Es así que la empresa trabaja con un autoloader o robot de backups el cual almacena la información del cliente en un storage externo al servidor para mitigar cualquier riesgo de pérdida de información. Adicionalmente, se mantienen copias en tipo snap de los clientes que cuenten con este servicio de forma permanente o por demanda.


PBX: (1) 794 5719
soluciones@gophergroup.com.co
Calle 70 No. 15-5
www.gophergroup.com.co

**NIT: 900.466.147-9**

Bogotá D.C. 19 de enero 2024

**ADM-COR0152**

**ACTA DE ENTREGA**

Por medio de la presente **ANDEANTRADE GROUP LATAM S.A.S.**, hace entrega oficial de licencias relacionadas a continuación:

| ITEM | DESCRIPCION | CANT |
|---|---|---|
| 1 | Licencias Veeam | |
| V-ESSSTD-VS-P0ARE-00 | Annual Basic Maintenance Renewal Expired - Veeam Backup Essentials Standard 2 socket bundle | 1 |
| V-ESSSTD-VS-P0ARW-00 | Annual Basic Maintenance Renewal Expired (Fee Waived) - Veeam Backup Essentials Standard 2 socket bundle | 1 |
| V-ESSSTD-VS-P01AR-00 | Annual Basic Maintenance Renewal - Veeam Backup Essentials Standard 2 socket bundle | 1 |

Adjuntamos el contenido del correo electrónico enviado a ustedes por VEEAM

Para constancia de lo anterior se firma en Bogotá, a los once (19) días del mes de enero de 2024.

Atentamente,

Alexander Prieto
Gerente de Cuenta
ANDEANTRAD GROUP LATAM S.A.S.

Recibí a satisfacción,

**NIT: 900.466.147-9**

Helmunt Sierra
Director Comercial
GOPHER GROUP

Thank you for your interest in Veeam products.

**Product download**

| | |
|---|---|
| Veeam Backup & Replication | Primary download or Alternative download |
| Veeam ONE | Primary download or Alternative download |

You can manage your product license online using the Veeam License Management Portal and read Veeam's Licensing FAQ.

**MY ACCOUNT**

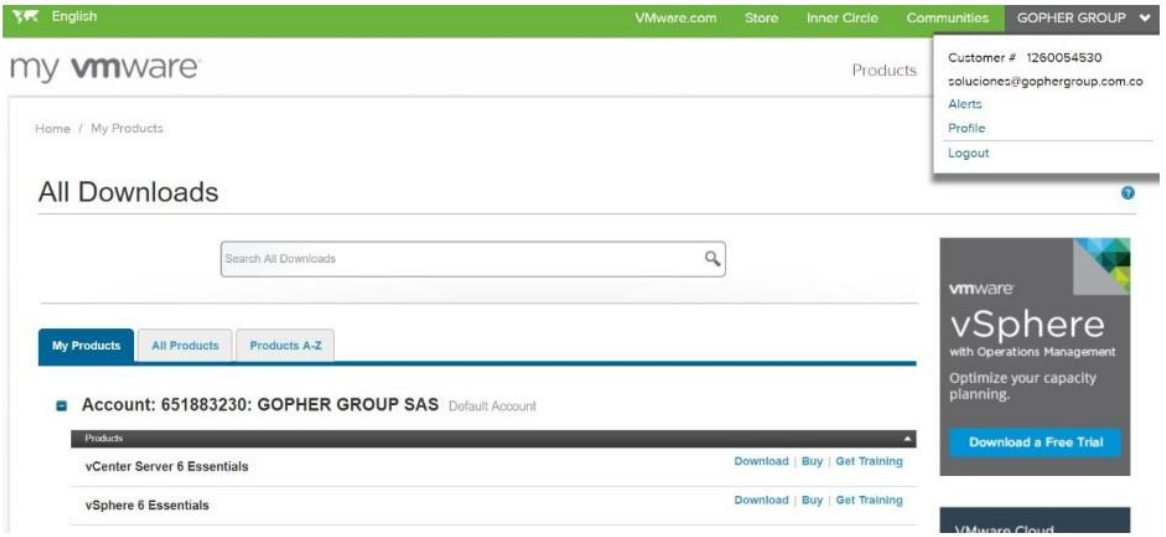
Manage license keys
Contact sales
Get help
Download Veeam products

We enhance our products based on customer feedback. If you have a suggestion regarding Veeam products, please post it in on the Veeam Community Forums.

Regards,
Veeam Team

**GOPHER GROUP S.A.S**
**NIT: 900.425.485-8**

**CERTIFICACION VMWARE**:




**HELMUNT DAVID SIERRA ABRIL**
**C.C. 80.184. 284 de Bta.**
**Representante Legal**
**Gopher Group S.A.S**
**PBX. 7945719 Ext. 108**

**CERTIFICACIÓN TIER IV**
**CENTRO DE DATOS**

Nos complace confirmar que su centro de datos es **SWITCH SUPERNAP A switch Company** ubicado en **CANADA**, el cual corresponde con la **certificación TIER IV**. Esto nos permite ofrecer equipos en alta disponibilidad que son fácilmente recuperables ante un fallo en cualquiera de estos centros de datos. Se trata de uno de los centros de datos mejor consolidados en estados unidos y dueño de más de 282 patentes para el diseño de centros de datos.




*Certificación verificable desde el sitio web oficial de UPTIME INSTITUTE CERTIFIED y desde la página web del proveedor respectivamente.*
*https://es.uptimeinstitute.com/TierCertification/allCertifications.php?page=1&ipp=All*
*http://www.supernap.com/tier-iv-gold.html*

Por otro lado, la disponibilidad de servicio es garantizada según el estándar **TIER IV** a un 99.97%, el cual maneja servidores de respaldo en su propia infraestructura en **Collocation**, lo cual nos permite manejar la redundancia a nivel de servidores además de la redundancia ya ofrecida por el centro de datos.

Con lo anterior certificamos que efectivamente ofrecemos la redundancia en el servicio ofertado,

**CERTIFICACIÓN DE SOPORTE**

Bogotá, 23 de diciembre de 2024

Señores
**INSTITUTO TOLIMENSE DE FORMACIÓN TÉCNICA PROFESIONAL ITFIP**
La Ciudad.

**Asunto: Mínima cuantía No. IPMC-043-2024**
**Objeto*:*** RENOVACIÓN DEL ALOJAMIENTO DEL PORTAL WEB INSTITUCIONAL

El suscrito **Helmunt David Sierra Abril**, identificado con cédula de ciudadanía N° **80.184.284,** expedida en **Bogotá**, actuando en representación de **GOPHER GROUP S.A.S. NIT 900.425.485**, con domicilio en **Bogotá,** debidamente autorizado, según consta en el certificado de existencia y representación legal expedido por la Cámara de Comercio de **Bogotá**, bajo la gravedad de juramento garantizo la prestación del servicio de soporte técnico, el cual se llevara a cabo en la oficina principal de la empresa ubicada en la Calle 70 No 15 – 51 de Bogotá, con un equipo de cuatro ingenieros de soporte calificados con amplia experiencia, quienes manejan cuatro canales de soporte vinculados a chat, correo electrónico, escritorio remoto y HELP DESK. Este equipo de trabajo estará disponible 7 x 24 x 365, recibiendo respuesta inmediata después del requerimiento.

Los canales de comunicación al equipo de soporte son:
Correo: soporte@gophergroup.com.co
PBX: (031) 794 57 19 ext. 1006
Móvil y WhatsApp: 314-393 76 11 y 317-713 42 87

Atentamente.

FIRMA DEL REPRESENTANTE LEGAL
Representante legal: Helmunt David Sierra Abril || C.C.: 80.184.284 de Bogotá
Matrícula Profesional No.: 70255-264906 TLM
Razón Social: **GOPHER GROUP S.A.S. || NIT: 900425485-8**
Dirección: calle 70 # 15 – 51 Bogotá || Teléfono (1)794 5719 – 317 7134287
Correo Electrónico: soluciones@gophergroup.com.co