1. INTRODUCCIÓN

La Gestión de la Continuidad del Servicio se preocupa de impedir que una imprevista y grave interrupción de los servicios del área de Gestión de las Tics, debido a desastres naturales u otras fuerzas de causa mayor, tenga consecuencias catastróficas para la institución.

La estrategia de la Gestión de la Continuidad del área de Gestión de las Tics, debe combinar equilibradamente-te procedimientos:

- **Proactivos:** que buscan impedir o minimizar las consecuencias de una grave interrupción del servicio.
- **Reactivos:** cuyo propósito es reanudar el servicio tan pronto como sea posible (y recomendable) tras el desastre.

Gestión

- Los planes de prevención y recuperación sean conocidos por toda la institución.
- Estos planes de adecuen a las necesidades reales de la institución.

Monitorización

- Los planes de prevención y recuperación están convenientemente actualizados.
- El área de Gestión de las Tics está capacitada para su implementación.
- Los procedimientos son los adecuados a las necesidades de la institución.

Políticas

- En la que se establezca el alcance de la misma
- Se asignen los recursos necesarios
- Se establezcan las bases para la organización del proceso.

Planificación

- Estudiar el impacto en la institución de una supuesta interrupción delos diferentes servicios del área de Gestión de las Tics.
- Analizar los riesgos y vulnerabilidades a los que está expuesta la infraestructura del área de Gestión de las Tics.
- Establecer una estrategia para la continuidad del servicio.

Implementación

- Organizar la implementación del proceso
- Elaborar los planes de prevención y recuperación del servicio.
- Establecer los protocolos de actuación en situación de crisis.

Supervisión

- Evaluar regularmente los planes de prevención y recuperación.
- Asegurar el conocimiento y formación del personal respecto a los procedimientos asociados.
- Garantizar que los planes se hallen convenientemente actualizados.

Recuperación

- Evaluar el impacto de la interrupción del servicio.
- Poner en marcha, si corresponde, los planes de recuperación.
- Supervisar el proceso.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

El objetivo del Plan de Gestión de la Continuidad de las TIC's es actuar proactivamente preparando planes de contingencia para ocasiones de desastre, asegurando que la Infraestructura (técnica y de servicios) puede recuperarse cuando así se requiera y según los acuerdos y tiempos establecidos.

2.2 OBJETIVOS ESPECIFICOS

- Garantizar la pronta recuperación de los servicios críticos y vitales del área de Gestión de las Tics tras un desastre sobre la plataforma tecnológica (Telecomunicaciones o sistemas informáticos).
- Establecer políticas y procedimientos que eviten, en la medida de lo posible las peligrosas consecuencias de un desastre o causa de fuerza mayor.
- Garantizar la continuidad de los servicios críticos y vitales del área de Gestión de las Tics tras un desastre (Servicios de Telecomunicaciones y sistemas informáticos).
- Controlar y mitigar los riesgos que se puedan materializar e impactar sobre los servicios del área de Gestión de las Tics.

3. ALCANCE

El alcance de este documento aplica para los a los sistemas de comunicación, tecnología y sistemas informáticos definidos como críticos y vitales.

4. DESARROLLO PROCEDIMENTAL

4.1 METODOLOGIA

- **Evaluación de Riesgos :** Se realiza basados en documento modelo de gestión del riesgo institucional el cual está diseñado en un modelo matemático de estimación del riesgo,

entendiendo éste como combinación de la PROBABILIDAD de ocurrencia de un evento y sus consecuencias; donde el primero pondera la posibilidad de que suceda el hecho, teniendo en cuenta la eficacia de los controles existentes para prevenir la ocurrencia del mismo y el segundo se cuantifica o estima en términos de los resultados negativos derivados del evento.
Este documento establece los criterios, herramientas y metodologías que en su conjunto conforman el Sistema de Gestión del Riesgo, que tiene como propósito identificar, priorizar, evaluar e intervenir los riesgos asistenciales, administrativos, financieros y estratégicos identificados en la institución; al igual que evaluar la eficacia de lasacciones de mejora continua, orientadas a intervenir o minimizar los riesgos detectados.

- **Estrategias de continuidad:** El área de gestión de las Tics desarrollara procedimientos orientados a garantizar la continuidad de la operación buscando alternativas manuales, automatizadas o apoyándose en ambas, describiendo medidas preventivas que eviten la interrupción de los servicios, o medidas reactivas, que recuperena un nivel aceptable de servicio en el menor tiempo posible.

- **Organización y planificación:** Una vez analizados los riesgos, vulnerabilidades, y definidas las estrategias de prevención y recuperación se asignara y organizaran los recursos necesarios, para lo cual se deben contemplar

- El desarrollo de procedimientos de planes de contingencia.
- Realizar pruebas periódicas de dichos planes.
- Revisar periódicamente los planes para adaptarlos a las necesidades reales de la institución.

- **Supervisión de la continuidad:** Una vez establecidas las políticas, estratégicas y planes de prevención y recuperación, es indispensable que el área de Gestión de las Tics esté preparada para su correcta implementación. Para esto se realizara.

- Capacitación continua al personal involucrado sobre los diferentes procedimientos de prevención y recuperación
- Realización periódica de simulacros para diferentes tipos de desastres con el fin de asegurar la capacitación al personal involucrado.
- Actualización periódica de las políticas, estrategias y planes para asegurar que responden a los requisitos de la organización.
- Evaluación de las políticas, estrategias y planes cuando se realice o vaya a realizar un cambio en la infraestructura tecnológica.

- **Control del proceso:** Periódicamente se elaborarán informes sobre la gestión que incluirán información relevante el área de Gestión de las Tics sobre los cuales se incluirán:

- Análisis sobre nuevos riesgos y evaluación de su impacto.
- Evaluación de los simulacros y desastres realizados.

- Actividades de prevención y recuperación realizadas.
- Costes asociados a los planes de prevención y recuperación.
- Preparación y capacitación del personal del Gestión de las Tics respecto a los planes y procedimientos de prevención y recuperación.

5. EVALUACIÓN

Se cuenta con unos indicadores que monitorizan esta estrategia:

EPER-TICS-01. Proporción de disponibilidad de equipos críticos.
IEPER-TICS-02. Proporción de disponibilidad de sistemas críticos.

6. ACTIVIDADES

6.1. Clasificación tecnológica crítica y vital:

Calificación de 1 a 5: Categorización de probabilidades, siendo 1 la menos posible y 5 altamente posible.

Posibilidad de ocurrencia de emergencia: Se categoriza en general como la proporción de eventos que pueden producir fallas en el funcionamiento del equipo industrial y así mismo, una emergencia.

Repercusión en usuarios: Se define como la proporción en que un evento adverso en el equipo industrial, pueda repercutir directamente afectando la seguridad de los usuarios internos y externos.

Imagen institucional: Se define en general, como la proporción en que un evento adverso, pueda producir daños en la imagen corporativa de “SES”.

Debilidad del plan de contingencia: Es la proporción en que una emergencia pueda afectar el equipo, debido a la deficiencia en su plan de contingencia.

6.1. Descripción tecnológica crítica y vital:

- Sistemas informáticos críticos y vitales.

CRITICIDAD DE LOS SISTEMAS INFORMATICOS

Equipos Variables	Posibilidad de ocurrencia de la emergencia	Repercusión en usuario	Imagen institucional	Debilidad del plan de contingencia	Total
	30%	30%	20%	20%	CALIF 1 A 5
Motor de Base de datos SQL Server	4	4	4	3	3,8
Dinámica Gerencial Hospitalaria	4	4	3	3	3,6
SIGI	3	3	2	4	3
VMware	2	4	4	1	2,8
Enterprise	4	2	1	2	2,4
Aquila RIS-PACs	4	2	1	2	2,4
Almera	1	2	2	2	1,7
CRITICIDAD TECNOLOGIA INFORMATICA Y COMUNICACIONES					
Equipos Variables **prueba**	Posibilidad de ocurrencia de la emergencia 30%	Repercusión en usuario 30%	Imagen institucional 20%	Debilidad del plan de contingencia 20%	Total CALIF 1 A 5
Firewall	3	4	4	4	3,7
Switche	2	4	4	4	3,4
Sevidores Omnivista	1	4	4	2	2,7
Switche de Fibra	1	3	2	2	2
Planta Telefonica Call	1	3	3	1	2

SOFTWARE	**MODULOS**	**SUBMODULOS**	**DESCRIPCION**
Dinámica Gerencial Hospitalaria	Administrativos y financieros	Contabilidad Niff Tesorería Cartera	Sistema de información hospitalario HIS

		Pagos	
		Activos Fijos	
		Gestión Gerencial	
	Operativos y Asistenciales	Inventarios	
		Contratos	
		Citas Medicas	
		Admisiones	
		Hospitalización	
		Facturación	
		Historias Clínicas	
		Programación de Cx	
SIGI Sistema Integrado de Gestión de la información.	Seguimiento a imágenes		Modulo que permite identificar solicitudes de procedimientos de diagnósticos y llevar su trazabilidad en el tiempo
	Seguimiento a Laboratorio		Modulo que permite identificar solicitudes de exámenes de laboratorio clínico y llevar su trazabilidad en el tiempo
	Entrega de turnos		Modulo que permite llevar un resumen del estado del paciente durante su atención y sirve para como guía para la entrega de turnos del personal asistencial

	Referencia y contra referencia		Modulo que permite llevar una trazabilidad de los pacientes comentados a la institución o de aquellos que se deben remitir a las otras instituciones
Almera	Gestión de calidad		Sistema de
	Tramites		Gestión de
	PQR		Calidad
	Riesgos		
ENTERPcRICE			Sistema de información que permite consultar resultados de laboratorio de los pacientes de la institución
MOTOR DE BASE DE DATOS SQL SERVER			Todas las bases de datos que se encuentran en la instancia Dinámica

DESCRIPCION MAQUINA VIRTUAL	NOMBRE	CRITICIDAD
FACTURACION ELECTONICA	AIRBUS-	ALTA
SIGI	ANDROMEDA	ALTA
DIRECTORIO ACTIVO PRINCIPAL	ANTONOV	ALTA
BASE DE DATOS PRINCIPAL	ARES	ALTA
AMBIENTE DESARROLLO UMANIZALES	CHENGDU J-20	ALTA
DIRECTORIO ACTIVO SECUNDARIO	DASSAULT	ALTA
DINAMICA WEB NODO 1	EMBRAER-E170_	ALTA
DINAMICA WEB NODO 2	EMBRAER-E190_	ALTA
SERVER NOMINA ANTARES	GOBLINXF-F85	ALTA
FILE SERVER (CARPETAS COMPARTIDAS	NAOS	ALTA
ALCATEL OMNIVISTA (WIFI CONTROLLER)	OV2500	ALTA

AMBIENT DE PRODUCCIÓN UMANIZALES	DOUGLASF15	MEDIA
DYALOGO_PBX	DYALOGO_PBXADMIN	MEDIA
CONTROL DE ACCESO ZKT	FOKKER	MEDIA
RPA UIPATH	MARTIN F22	MEDIA
SERVIDOR VIEJO DE NOMINA	SES_GOBLINXF-85	MEDIA
SERVER APLICATIVO CYT	SIKORSKY	MEDIA
ISABEL PBX	SUKHOI SU-57	MEDIA
SERVIDOR BD PRUEBAS	TITAN	MEDIA
VERITAS DLO	BELL_DLO	BAJA
SERVER WSUS	MCDONNELL	BAJA
IIS LABORATORIO	MIKOYAN	BAJA
SERVER APLICATIVO QURE IA	QURE.AI	BAJA
SERVER_MONITOREO_ZABBIX	SRVZABBIX6-PROXY-SES	BAJA
SERVIDOR LG SUPERSIG, OCS INVENTORY	TUPOLEV	BAJA
SERVER APLICATIVO CYT	VOUGHT	BAJA

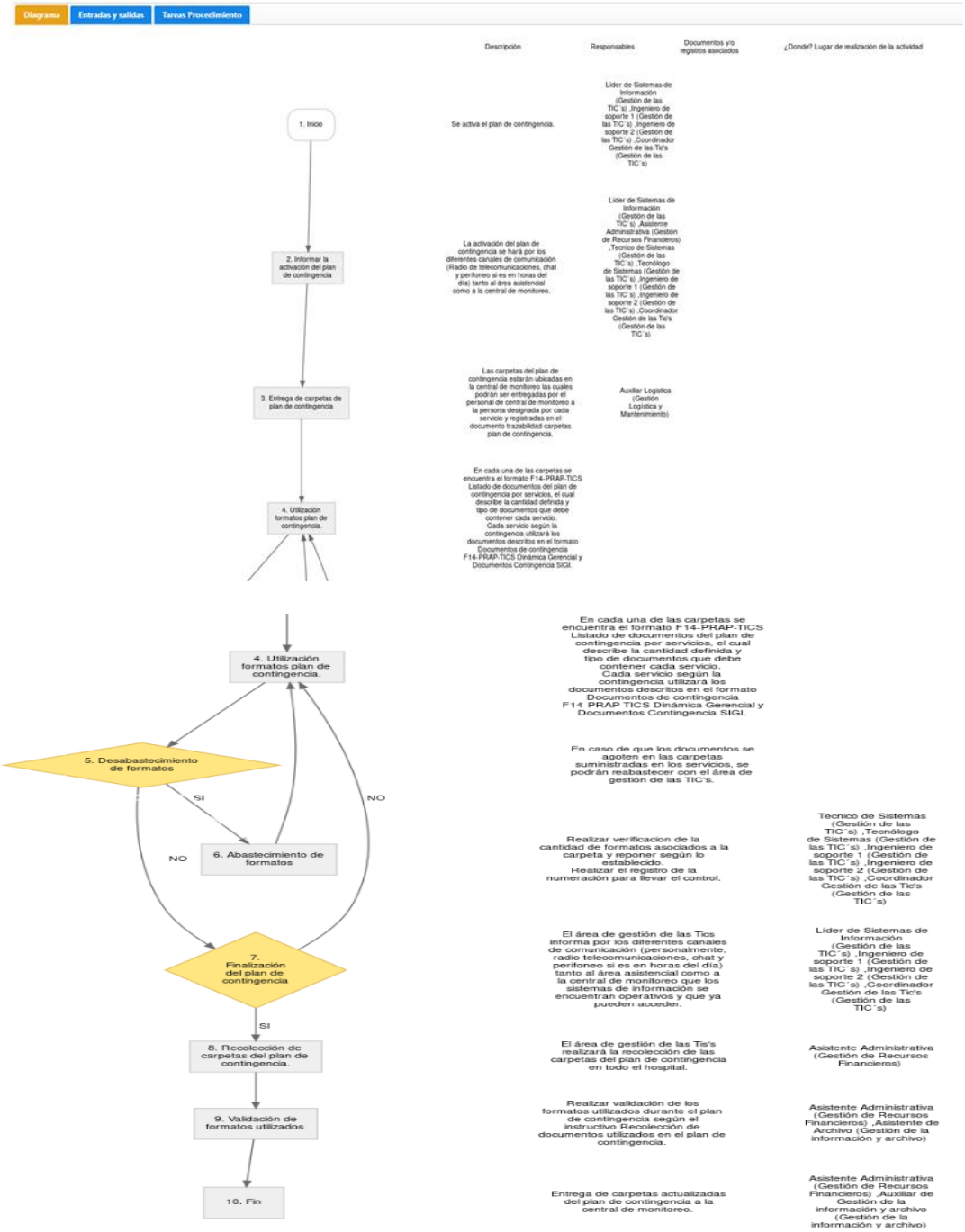
- Tecnología de comunicaciones crítica y vital.

EQUIPO	REFERNCIA	DESCRIPCION
Switch Core	ALCATEL OS6860E-U28	Dispositivo central que gestiona el tráfico de datos en una red, asegurando conectividad rápida entre switches y Access Point
Switch SAN	HPE Storage Switch M-series SN2010M	Switch que conecta el servidor de almacenamiento y los host donde están las máquinas virtuales
FIREWALL	FortiGate 200F	Dispositivo de seguridad que protege redes, controlando el tráfico y bloqueando amenazas mediante funciones avanzadas como filtrado web
PBX IP	Dyalogo CBX	controla llamadas entrantes y salientes en el call center.

-

Procedimientos

Plan de Contingencia Sistema de información Dinámica Gerencial



6.4 Simulación y Simulacros

6.4.1 Objetivos

- Evaluar periódicamente los planes descritos en los procedimientos de contingencia del área de Gestión de las TICs
- Detectar puntos débiles o fallas ante la activación de un plan de contingencia relacionado con sistemas de comunicación y sistemas informáticos.
- Identificar la capacidad de respuesta de los colaboradores de la institución ante la activación de un plan de contingencia relacionado con sistema de comunicación y sistemas informáticos.
- Disminuir y optimizar el tiempo de respuesta ante la activación de un plan de contingencia relacionado con sistemas de comunicación, y sistemas informáticos.
- Promover la difusión de los planes a cargo del área de Gestión de las Tics

6.4.2. Simulación

Ejercicio de manejo de información, para la toma de decisiones, la educación y la evaluación; basados en un supuesto desastre ocurrido en un lugar y tiempo específicos.

Alcance de la simulación

Se realizaran ejercicios de simulación, 2 veces por año en los cuales participarán todos los integrantes del área de Gestión de las Tics, con el fin de asegurar la capacitación de los mismos y poder así desarrollar habilidades de coordinación, manejo y determinaciónde las diferentes posibles respuestas ante un evento o falla relacionada con los sistemas informáticos, tecnología informática y de comunicaciones

6.4.3 Simulacros

Es un ejercicio práctico para representar una situación de emergencia que afecte la institución en sus sistemas comunicaciones, sistemas, involucrando a los colaboradores de la institución con el fin de medir y evaluar en tiempo la respuesta a las acciones realizadas y los recursos utilizados.

Alcance de la simulación

Se realizaran ejercicios de simulacro, 2 veces por año en los cuales participarán todos los integrantes del área de Gestión de las Tics y los colaboradores del área que aplique, con el fin de asegurar la capacitación de los mismos y poder así desarrollar habilidades de coordinación, manejo y determinación de las diferentes posibles respuestas ante un evento o falla relacionada con los sistemas informáticos, tecnología informática y de comunicaciones.

1. BACKUPS

1.1. Objetivo General

Proteger y resguardar la información de los Sistemas informáticos críticos y la documentación crítica y vital para la entidad, así como la restauración de la misma en el momento que se necesite con el fin de garantizar la continuidad del negocio.

1.2. Objetivos Específicos

- Realizar una descripción general de la información que se custodia con su ubicación
- Describir el proceso de ejecución de los backups con fechas y horas.
- Describir para cada proceso el RPO y el RTO.

1.3. Alcance

Comprende desde la realización de la copia de respaldo a las bases de datos de los sistemas informáticos denominados como críticos y vitales, la documentación crítica y vital para la entidad además de la clasificación de los archivos en las computadoras por parte de cada uno de los usuarios, el almacenamiento de las copias de seguridad hasta la restauración de las mismas.

1.4. Descripción del proceso.

A continuación se hace una descripción detallada de los nombres de las bases de datos la ubicación de sus archivos la periodicidad de las tareas y los tiempos de ejecución.

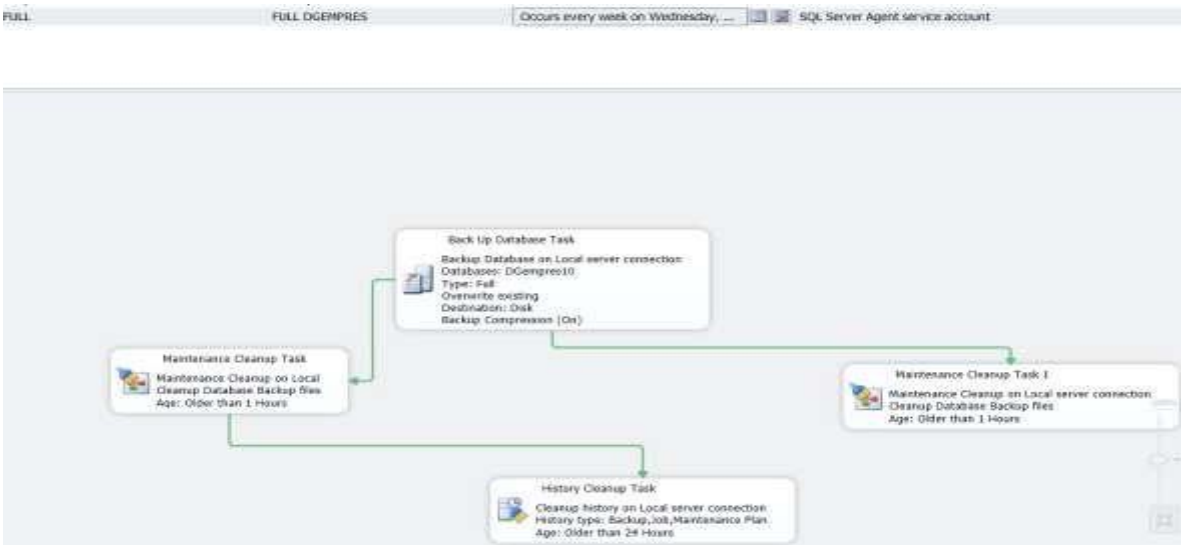
1.4.1. Bases de datos de Sistemas informáticos críticos y vitales

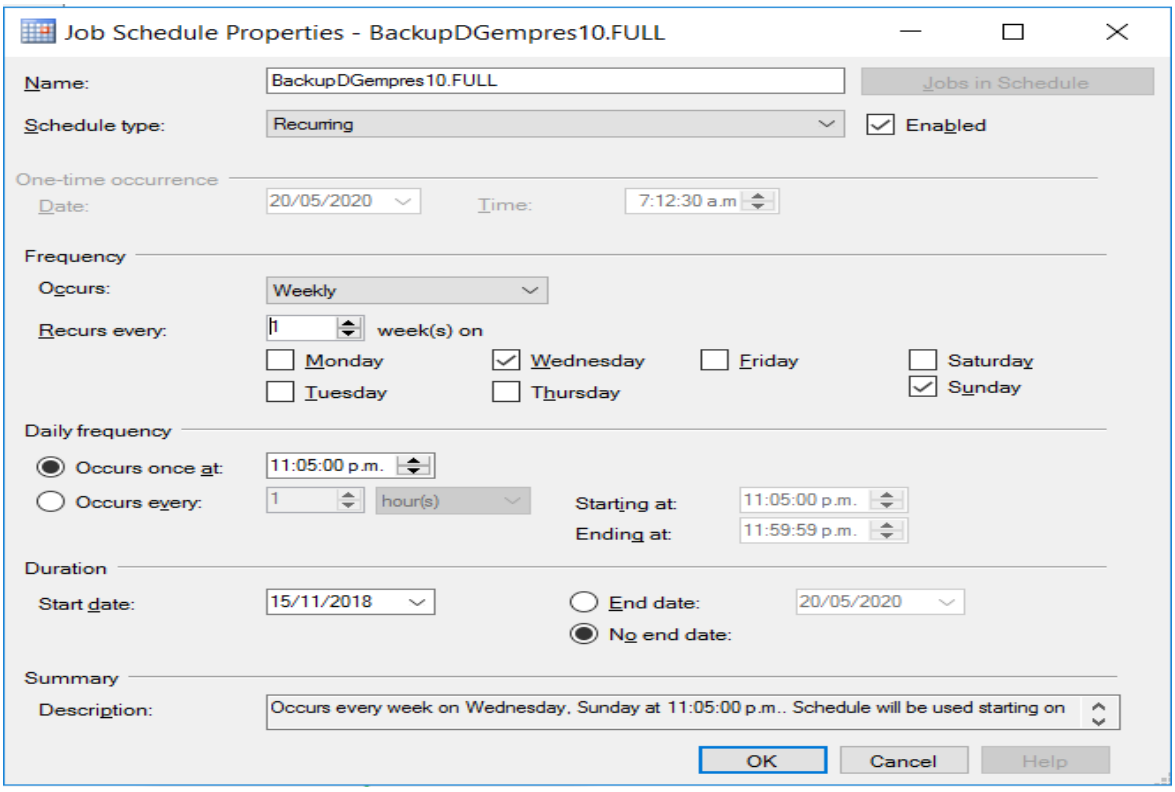
1.4.1.1. Dinámica Gerencial Hospitalaria

La base de datos del sistema de información Dinámica Gerencial Hospitalaria es una base de datos SQL Server la se encuentra ubicada en el servidor llamado Ares el cual tiene como dirección IP 192.168.10.38 e instancia SQL Dinámica (Ares\Dinámica). El nombrede la base de datos es DGempres10 su archivo .mdf se encuentra ubicado en la partición E:/DataUserSQL y su archivo .ldf se encuentra ubicado en la partición F:/LogUserSQL. La copia de seguridad para esta base de datos está programada para que se ejecute una full(BackupDGempres10FULL) cada semana comprimida por el SQL y copias transaccionales(BackupDGempres10TRN) cada 5 minutos.

La ubicación de las copias es:

Servidor: Ares
I:\BackupSQL\DGEMPRES\Copia_SYAC\transac\DGempres10





I:\BackupSQL\DGEMPRES\Copia_SYAC\transac\TRN

Estas copias hacen partes de los planes de mantenimiento del motor SQL Server

Nombre del plan de mantenimiento FULL : BackupDGempres10FULL
Nombre del plan de mantenimiento TRN : BackupDGempres10TRN

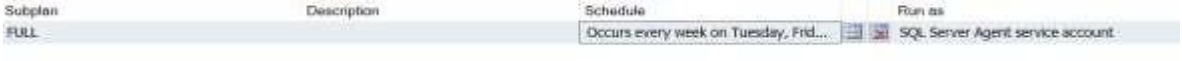
Recovery Point Objective (RPO) = 5 minutos.
Recovery Time Objective (RTO) = 45 minutos.

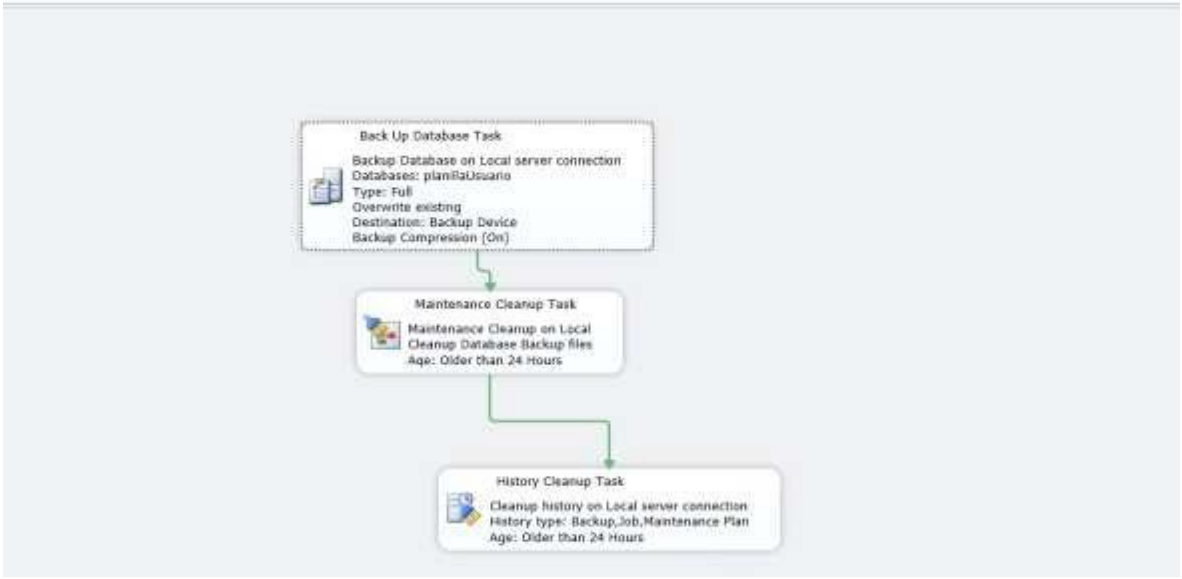
1.4.1.2. SIGI Sistema Integrado de Gestión de la información.

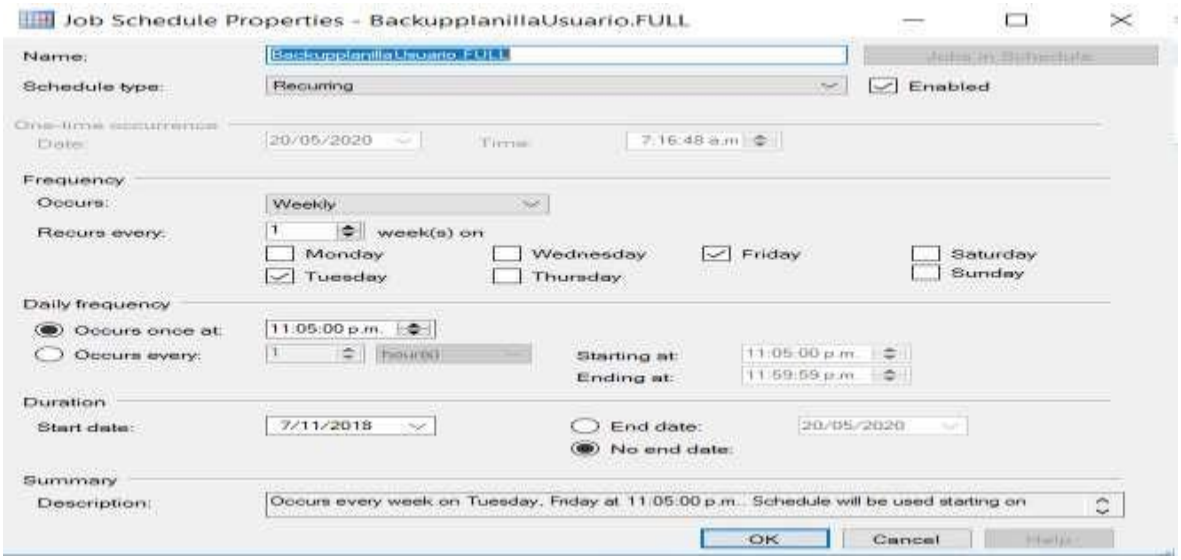
La base de datos del sistema de SIGI es una base de datos SQL Server ubicada en el servidor llamado Ares el cual tiene como dirección IP 192.168.10.38 e instancia SQL Dinámica (Ares\Dinámica). El nombre de la base de datos es planillaUsuario su archivo .mdf se encuentra ubicado en la partición E:/DataUserSQL y su archivo .ldf se encuentra ubicado en la partición F:/LogUserSQL. La copia de seguridad para esta base de datos esta programada para que se ejecute una full(BackupplanillaUFULL) cada semana comprimida por el SQL y copias transaccionales(BackupplanillaUsuarioTRN) cada 5 minutos.

La ubicación de las copias es:

Servidor : Ares
I:\BackupSQL\PLANILLAUSUARIO\FULL







I:\BackupSQL\PLANILLAUSUARIO\TRN

Estas copias hacen partes de los planes de mantenimiento del motor SQL Server.

Nombre del plan de mantenimiento FULL : BackupplanillaUFULL

Nombre del plan de mantenimiento TRN : BackupplanillaUsuarioTRN

Recovery Point Objective (RPO) = 5 minutos.
Recovery Time Objective (RTO) = 60 minutos.

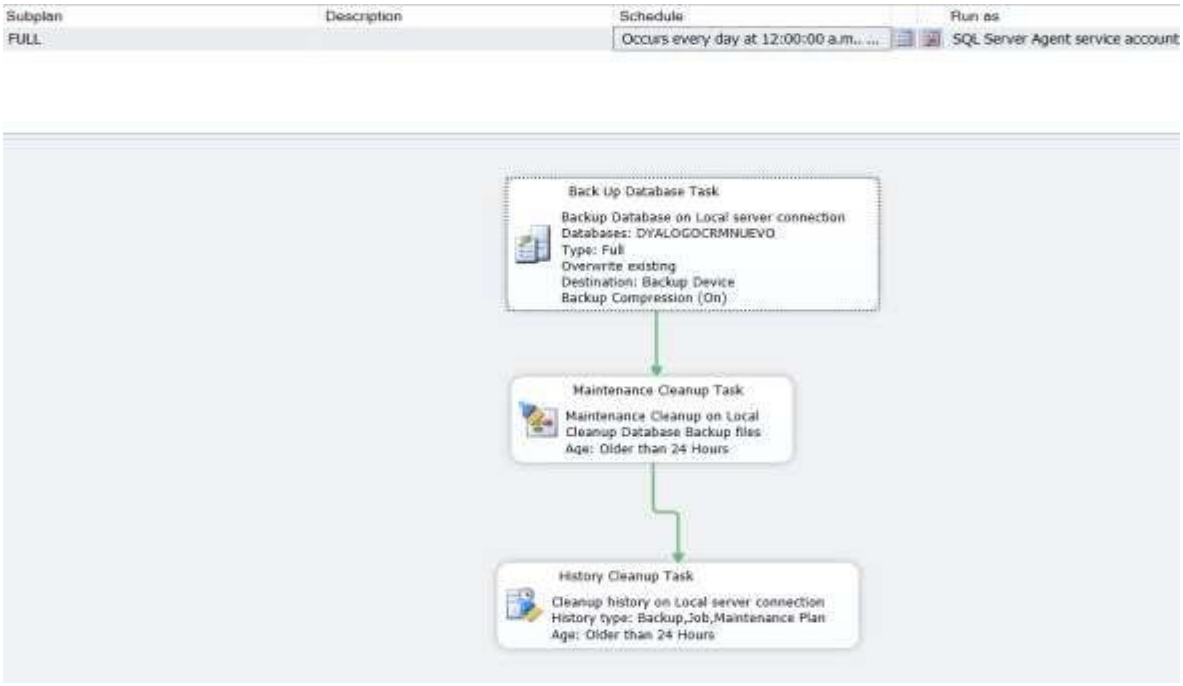
1.4.1.3. DYALOGO Nuevo

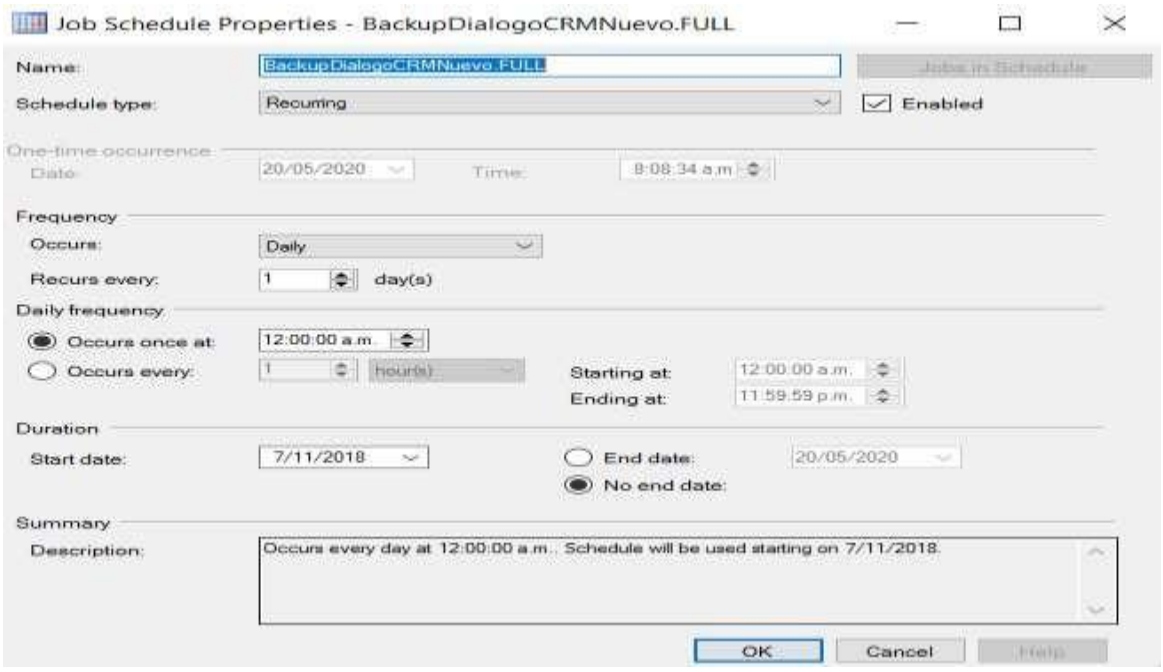
La base de datos del sistema DYALOGO es una base de datos SQL Server ubicada en el servidor llamado Ares el cual tiene como dirección IP 192.168.10.39 e instancia SQL Dinámica (Ares\Dinámica). El nombre de la base de datos es DYALOGOCRM su archivo .mdf se encuentra ubicado en la partición E:/DataUserSQL y su archivo .ldf se encuentra ubicado en la partición F:/LogUserSQL.

La copia de seguridad para esta base de datos está programada para que se ejecute una full(BackupDyalogoCRMNuevoFULL) cada semana comprimida por el SQL y copias diferenciales(BackupDyalogoCRMNuevoDIF) cada 20 minutos.

La ubicación de las copias es:

Servidor: Ares
I:\BackupSQL\DYALOGOCRMNUEVO\FULL





I:\BackupSQL\DYALOGOCRMNUEVO\DIF

Estas copias hacen partes de los planes de mantenimiento del motor SQL Server

Nombre del plan de mantenimiento FULL : BackuDyalogoCRMNuevoFULL

Nombre del plan de mantenimiento DIF : BackuDyalogoCRMNuevoDIF

Recovery Point Objective (RPO) = 20 minutos.
Recovery Time Objective (RTO) = 60 minutos.

1.4.1.4. Manillas

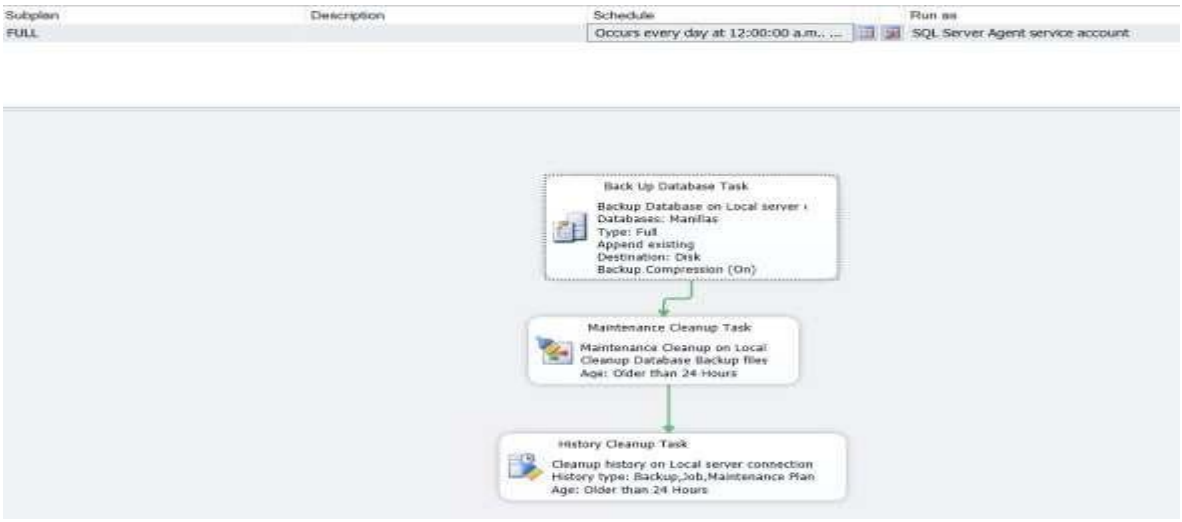
La base de datos del sistema Manillas es una base de datos SQL Server ubicada en el servidor llamado Ares el cual tiene como dirección IP 192.168.10.39 e instancia SQL Dinámica (Ares\Dinámica). El nombre de la base de datos es Manillas su archivo .mdf se encuentra ubicado en la partición E:/DataUserSQL y su archivo .ldf se encuentra ubicado en la partición F:/LogUserSQL.

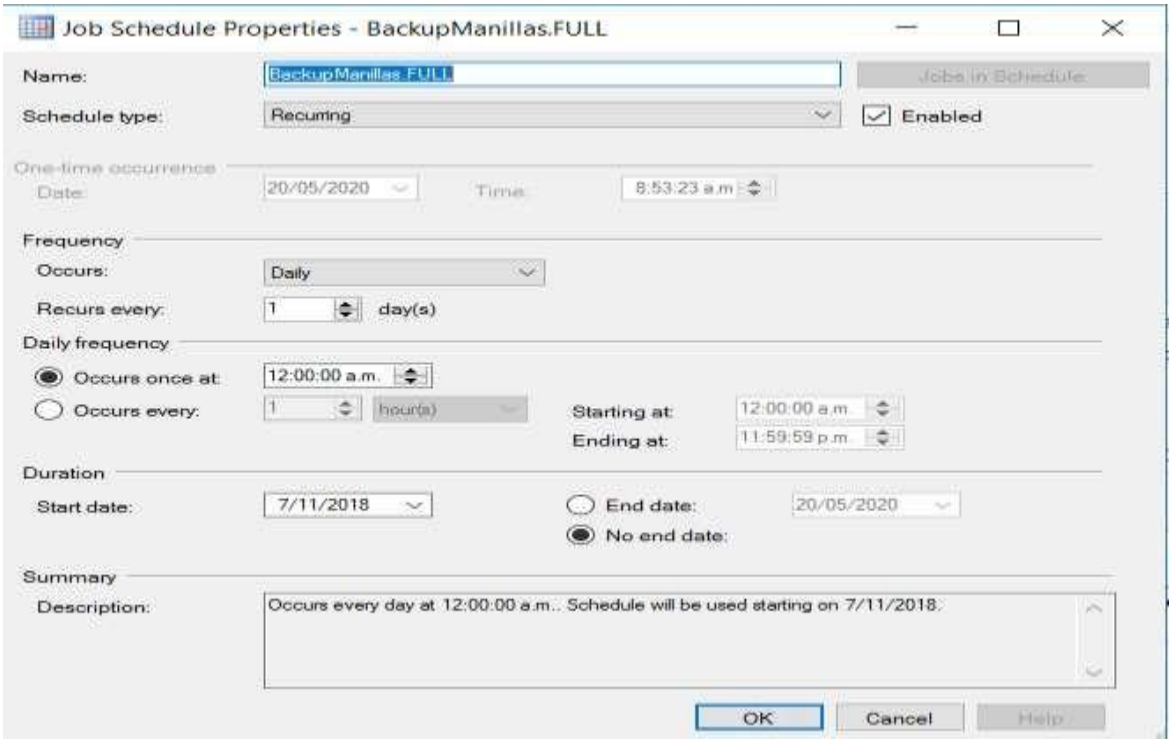
La copia de seguridad para esta base de datos está programada para que se ejecute una full(BackupManillasFULL) cada 24 horas.

La ubicación de las copias es:
Servidor: Ares
I:\BackupSQL\MANILLAS

Estas copias hacen partes de los planes de mantenimiento del motor SQL Server

Nombre del plan de mantenimiento FULL : BackupManillasFULL





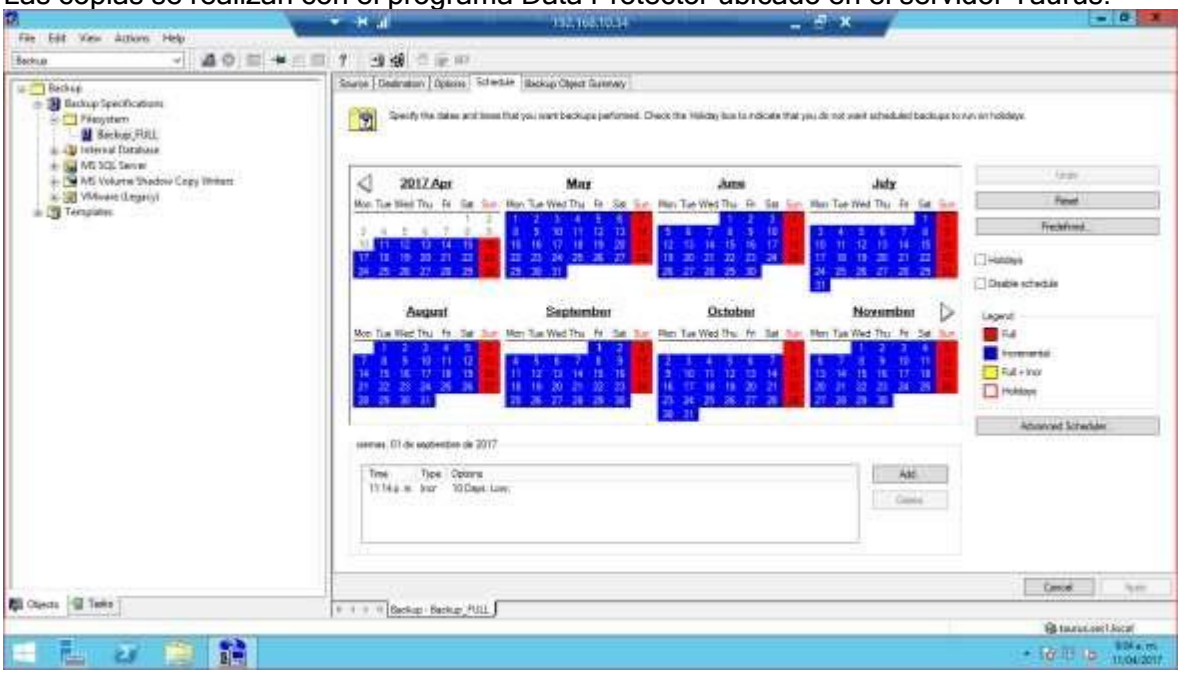
Recovery Point Objective (RPO) = 5 minutos.
Recovery Time Objective (RTO) = 60 minutos.

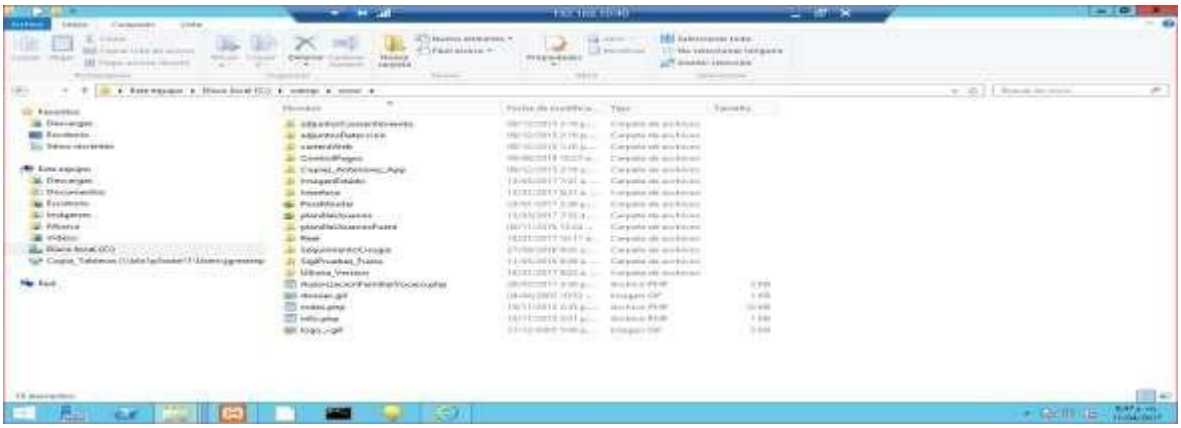
1.4.2. Código fuente de datos de Sistemas informáticos críticos y vitales.

El código fuente de los distintos aplicativos se encuentra ubicado en el servidor Andromeda en C:\wamp\www.

La copia de seguridad para estos archivos está programada para que se ejecute una full (Todos los domingos) a la 1:00 a.m. he incrementales una vez al día de lunes a sábado con a las 11:14 pm.

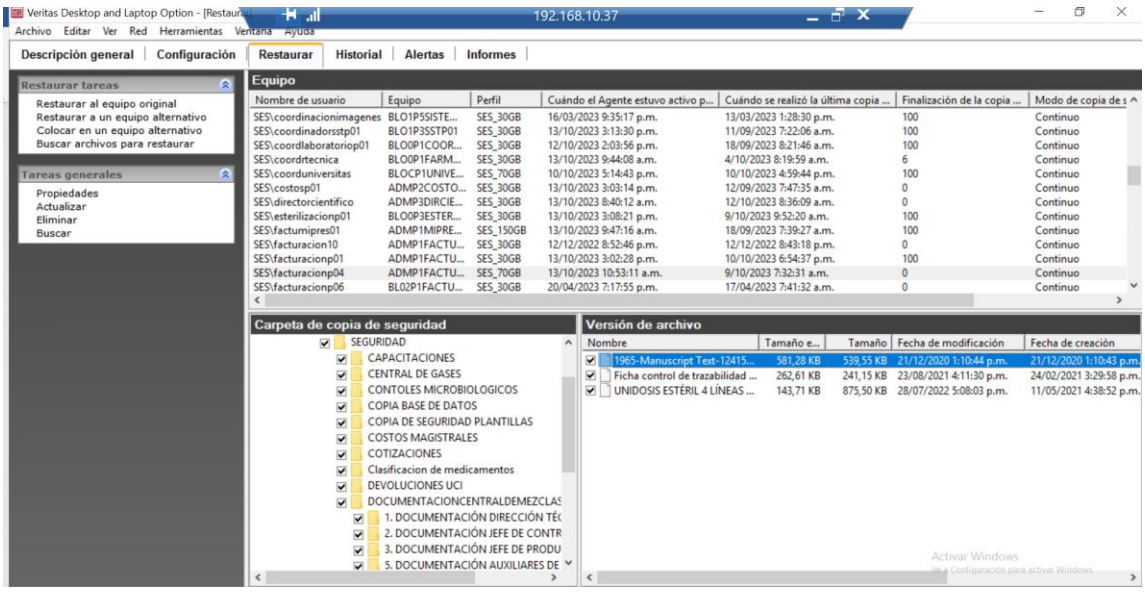
Las copias se realizan con el programa Data Protector ubicado en el servidor Taurus.





7.4.4. Backup usuarios finales

El backup de documentos de los usuarios se realiza con el programa “DLO” de “VERITAS”, para este proceso se creo un servidor llamado “BELL IP 192.168.10.37 donde la información queda almacenada en la unidad “D” en la carpeta “DLO\SES-nombre de usuario”.



El Backup de usuarios finales solo se realiza a los documentos que se encuentran en la carpeta de seguridad de cada equipo de computo.

La programación de los backup de usuarios está configurada para que se realice en el momento de que un documento de la carpeta “SEGURIDAD” sea modificado.

- La copia se realiza cuando el documento es modificado.
- Esta es almacenada en los servidores centrales y en un Robot de cintas.
- El sistema tiene la capacidad de guardar hasta 3 versiones de los documentos.

7.4.5. Prueba de recuperación de Backups.

Para asegurar la integridad de los resguardos realizados, una vez por mes se ejecutará el siguiente procedimiento:

1. Se seleccionarán al menos un soporte de backup full por mes.
2. Se elegirán para recuperar como mínimo 10 archivos transaccionales.
3. Se creara un caso en sigi en la opción seguridad informática/backups
4. Se debe especificar en SIGI la base de datos a recuperar.
5. Se debe especificar la fecha del backup full y los trn si aplica.
6. Poner en tramite el caso y adjuntar evidencias un vez se termine la restauración.
7. Al finalizar se debe cerrar el caso especifiando

· Backup con su fecha

- Trn recuperados
- Tiempo de recuperación.
- Se recuperó correctamente el archivo: Si/No
- Base de datos operativa SI/NO
- Problemas encontrados si aplica

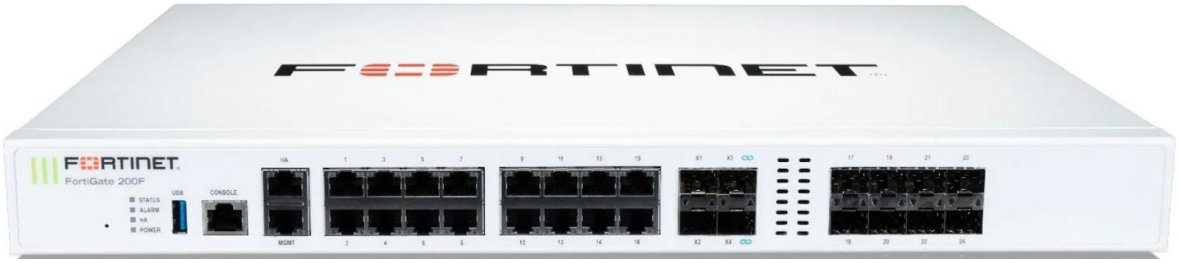
8. El área responsable de la Seguridad Informática revisará que se esté cumpliendo en tiempo y forma con el procedimiento; además podrá pedir la ejecución de una prueba cuando lo considere necesario.

7.4.6. Infraestructura de Networking

A continuación se describe el plan de continuidad de negocio para la infraestructura de networking del área de Tecnología del SES Hospital Universitario de Caldas. Este plan garantizará la disponibilidad, integridad y confidencialidad de los servicios de red en caso de incidentes que puedan afectar la operatividad normal del hospital.

Firewall

FortiGate 200F



Contamos con 2 Firewall FortiGate 200F (FG-200F) cuya principal función es otorgar Protección perimetral , gestión de tráfico y políticas de seguridad.

Descripción del FortiGate 200F:

1. **Interfaces:**

- Varias interfaces de 1 GE (Gigabit Ethernet) y 10 GE.
- Soporte para interfaces SFP/SFP+ (Fibra Optica).
- Interfaces de administración dedicadas.

2. **Seguridad:**

- Protección avanzada contra amenazas (ATP).
- Sistema de prevención de intrusiones (IPS).
- Filtrado web, control de aplicaciones y protección contra malware.

3. **Funciones Adicionales:**

- VPN (IPSec y SSL) para conexiones seguras.
- Balanceo de carga y failover.

Contingencia

Alta Disponibilidad

Los dos dispositivos FortiGate 200F se encuentran conectados entre si por medio del puerto HA y con la parametrización interna donde se le da una prioridad a cada uno y se establece la replicación / balanceo continuo de configuración y recursos.

Ventajas de tener el FortiGate 200F en HA (High Availability):

1. **Redundancia y Disponibilidad:**

- Failover Rápido: En caso de fallo del hardware o software en un dispositivo, el otro toma el control automáticamente, asegurando mínima interrupción.
- Zero Downtime: Minimiza el tiempo de inactividad, garantizando que los servicios críticos permanezcan accesibles.

2. **Balanceo de Carga:**

- Distribuye el tráfico de red entre múltiples dispositivos, optimizando el rendimiento y asegurando que ningún dispositivo esté sobrecargado.

3. **Escalabilidad:**

- Facilita la adición de capacidad adicional sin interrupciones significativas, permitiendo que la infraestructura crezca con las necesidades de la institucion.

4. **Mantenimiento Sin Interrupciones:**

- Permite la actualización y mantenimiento de los dispositivos sin necesidad de desconectar los servicios, ya que uno puede seguir operando mientras el otro se actualiza.

5. **Seguridad Mejorada:**

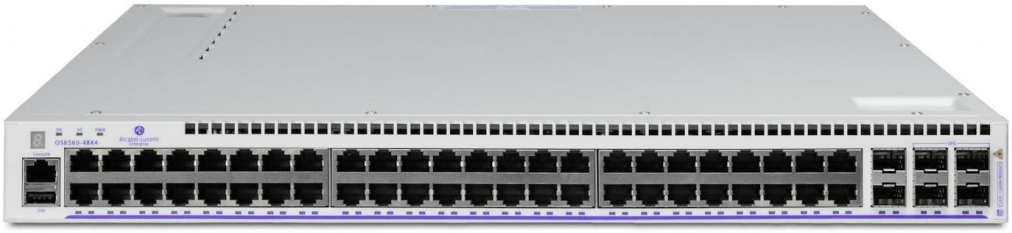
- La alta disponibilidad garantiza que las políticas de seguridad se apliquen continuamente sin interrupciones, manteniendo una postura de seguridad consistente.

CANALES DE INTERNET

SES Hospital Universitario de Caldas cuenta con dos proveedores de servicios de Internet (ISP), Claro y Tigo, que proporcionan la conectividad esencial para sus operaciones diarias.

SWITCH

Alcatel-Lucent OmniSwitch OS6560-48X4



Actualmente la Institución cuenta con 30 Switch encargados de ofrecer una conectividad de alta velocidad, fiable y segura comunicados entre sí por 2 rutas diferentes de fibra óptica y distribuidos por 10 cuartos de datos .

Contingencia

Cada uno de los swtich tienen conexión entre si por medio de 2 puertos troncales en modo Link Agregation donde se maneja una alta disponibilidad en la interconexión de los mismos y a nivel de centro de datos la institución cuenta con 2 rutas de fibra óptica que interconecta cada unos de los centro de datos con el Firewall Principal

ACCESS POINT

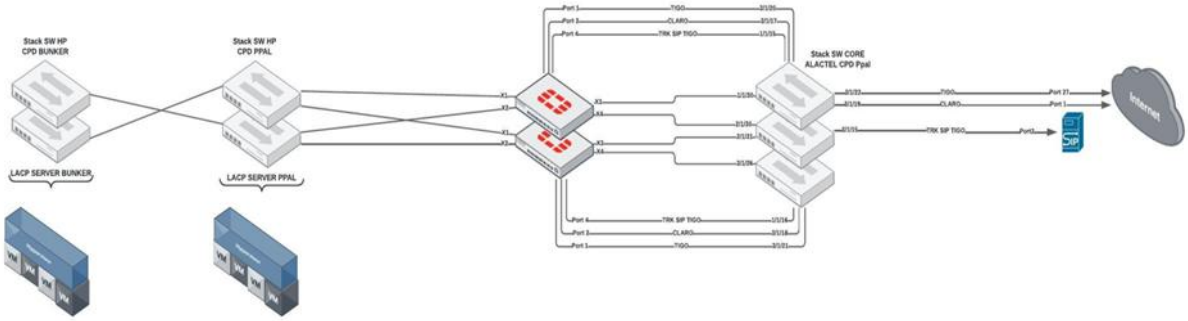
Alcatel Lucent - OmniAccess Stellar AP1220

La red WIFI de la institución es gestionada por los Access Point Alcatel Lucent - OmniAccess Stellar AP1220 los cuales son administrados en su totalidad por medio de la consola Omnivista

Contingencia

La contingencia para los access points Alcatel-Lucent OmniAccess Stellar AP1220 se basa en el respaldo regular de la configuración del servidor donde se encuentra la consola OmniVista. Esto garantiza que, en caso de fallo del servidor, la configuración se pueda restaurar rápidamente, minimizando el impacto en el servicio WiFi.

TOPOLOGIA DE RED



INFRAESTRUCTURA DE SERVIDORES

A continuación se describe el Plan de Continuidad de de las operaciones críticas en caso de un desastre que afecte al datacenter principal.

1. Desarrollo

Aplicación

Cada vez que se presente un incidente que afecte la disponibilidad, según el RTO (Recovery Time Objective) y RPO (Recovery Point Objective) que se tiene contemplado en los planes de contingencia.

Fallas

- Incidentes serios de seguridad en los sistemas, como delitos cibernéticos, pérdida de información, robo de información sensible o su distribución accidental, fallos en los sistemas IT, errores de operación en los sistemas, etc.
- Daños en las infraestructuras o en los servicios, fallos en el suministro eléctrico, fallos en las

comunicaciones, bloqueo en los accesos de las sedes de la compañía.

- Fallos en los equipos o en los sistemas del centro de datos, incluyendo fallos en las fuentes de alimentación o en los equipos de refrigeración.
- Daños deliberados como actos de terrorismo o de sabotaje, guerras, robos, huelgas, etc.
- Daños por situaciones físicas y de ambiente, como sismo, etc.

Infraestructura Actual de Servidores

Ambiente de Producción

En el ambiente de producción de nuestra infraestructura tecnológica, contamos con dos servidores HPE Proliant DL360 Gen10 Plus. Cada uno de estos servidores está equipado con VMware 8.0, proporcionando una plataforma robusta y escalable para **la** virtualización de nuestras cargas de trabajo.

La administración centralizada de estos servidores se realiza a través de VMware VCenter 8.0, lo que nos permite gestionar y optimizar eficientemente los recursos disponibles, así como garantizar un alto nivel de disponibilidad y rendimiento para nuestros servicios críticos.

Dentro de este entorno, hemos implementado un total de 30 máquinas virtuales. Estas máquinas virtuales están configuradas para ofrecer una variedad de servicios esenciales, que incluyen:

Servicios de bases de datos: Alojamos múltiples instancias de bases de datos que soportan las aplicaciones y operaciones empresariales, garantizando la integridad, disponibilidad y seguridad de nuestros datos.

Aplicativos internos: Las aplicaciones desarrolladas y utilizadas internamente por la institución se ejecutan en este entorno virtualizado, facilitando la gestión y el mantenimiento de nuestros procesos operativos.

Directorio Activo: Nuestro sistema de autenticación y administración de usuarios está basado en Active Directory, proporcionando un control centralizado de los recursos y mejorando la seguridad de la red.

File server: El almacenamiento y gestión de archivos se realiza a través de servidores de archivos virtuales, permitiendo un acceso rápido y seguro a la información compartida entre los diferentes departamentos de la organización.

Esta configuración nos permite no solo optimizar el uso de nuestros recursos de hardware y software, sino también asegurar una alta disponibilidad y redundancia, minimizando el riesgo de interrupciones en el servicio y asegurando una operación continua y eficiente de nuestra infraestructura tecnológica.

Ambiente de Respaldo

En el ambiente de Respaldo, contamos con dos servidores HPE Proliant DL380 Gen10 Plus, cada uno equipado con VMware 8.0. Estos servidores están gestionados a través de VMware VCenter 8.0, proporcionando una administración centralizada y eficiente de los recursos virtuales. En este entorno, se alojan las réplicas de las máquinas virtuales de producción, garantizando que todos los datos críticos y aplicaciones esenciales estén respaldados y disponibles en caso de fallos en el ambiente de producción.

Las tareas de replicación se realizan utilizando el sistema Zerto, una solución avanzada de recuperación ante desastres y continuidad del negocio. Zerto nos permite replicar de manera continua y en tiempo real las máquinas virtuales, asegurando que las copias de seguridad estén siempre actualizadas y listas para ser activadas cuando sea necesario. Esta configuración robusta nos proporciona una alta disponibilidad y una recuperación rápida ante cualquier eventualidad, garantizando la continuidad del negocio y la integridad de nuestros datos. Con Zerto, podemos gestionar y monitorizar fácilmente el proceso de replicación, asegurando que nuestros objetivos de recuperación se cumplan de manera efectiva y eficiente.

Estrategias de Continuidad

Evaluación de criticidad de los Servidores

El plan de continuidad de seguridad de la información se realizará teniendo en cuenta la evaluación de impacto de cada servicio Afectado:

Criticidad	Tiempo Objetivo de Recuperación (RTO)	Tipo de Servicio
Alta	**Hasta 1 hora**	**Servidores de Bases de Datos** **Servidores de Aplicativos** **Servidor de directorio activo**
Media	**2 a 4 horas**	**Servidor de Facturación**
Baja	**Mayor a 24 horas**	**Servidor de Biométricos** **Servidor de Parqueadero**

Replicación de Datos con Zerto

Replicación de datos en tiempo real entre los hosts del datacenter principal y los hosts del datacenter de respaldo.

Esta replicación se realiza de forma continua y garantiza

Copia de Seguridad

Realizar copias de seguridad completas e incrementales diariamente. Almacena las copias de seguridad en un sitio alterno(fuera de sitio).

Procedimientos de Respuesta a Incidentes

Detección de Incidentes

Monitoreo continuo de la infraestructura mediante herramientas especializadas que generen alertas.

Activación del Plan

Definir criterios claros para la activación del PCN, como la detección de un fallo crítico en los hosts del datacenter principal.

Procedimientos de Recuperación

- Fallo de un Host en el Datacenter Principal.
- Detección: Notificación automática del fallo del host.
- Respuesta Inmediata: El equipo de TI evalúa el fallo y trata de restablecer el host.
- Activación de Redundancia: Si no es posible restablecer el host rápidamente, los servicios se migran automáticamente al otro host funcional en el datacenter principal.

Fallo Total del Datacenter Principal

- Validación: Verificar la funcionalidad completa de los servicios en el datacenter de respaldo.

8. Pruebas y Mantenimiento

- Pruebas Regulares: Realizar pruebas semestrales del PCN para asegurar su efectividad.
- Revisión y Actualización: Revisar y actualizar el PCN anualmente o después de cualquier cambio significativo en la infraestructura.

9. Documentación y Registros

- Registros de Incidentes: Mantener registros detallados de todos los incidentes y las acciones tomadas.

Revisiones del PCN: Documentar todas las revisiones y actualizaciones del PCN.

TABLA DE CONTROL DE CAMBIOS

VERSION	DESCRIPCIÓN U ORIGENDEL CAMBIO	FECHA
00	Creación del Documento	26/10/2013
01	Incorporación del numeral 7. BACKUPS	30/05/2017
02	Se actualizan los indicadores ylos planes de backup	01/05/2020
04	Se actualiza capitulo Infraestructura de Networking	30/09/2023
05	Actualiza capítulo de infraestructura de servidores	30/08/2024