

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación



“IMPLEMENTACIÓN DE LA HERRAMIENTA SITE 24/7 PARA EL  
MONITOREO DE SERVICIOS CRÍTICOS EN UNA EMPRESA  
ADMINISTRADORA DE FONDOS”

EXAMEN DE GRADO (COMPLEXIVO)

Previo a la obtención del Título de:

MAGISTER EN SISTEMAS DE INFORMACIÓN  
GERENCIAL

Autor:

KARLA ALEXANDRA ZOLLER SAN LUCAS

GUAYAQUIL – ECUADOR

AÑO: 2021

## AGRADECIMIENTO

Agradezco a Dios por darme la vida y regalarme a la gran familia unida que tengo, que nunca me dejaron sola y siempre están a mi lado en cada momento.

A handwritten signature in black ink, appearing to read "Paula Fajal". The signature is written in a cursive, flowing style with several loops and a long horizontal stroke extending to the left.

## DEDICATORIA

Dedico este trabajo a Dios, ya que me dio las fuerzas necesarias para salir adelante; a mis padres Carlos Zöller y Melva San Lucas, y a mis hermanos Heinzl y Steffy por ese apoyo incondicional y motivación.

A mis abuelitos Consuelo Pulley y Martina Jimenez, por la confianza; a mis abuelos Roger Zöller y Carlos San Lucas, mis abuelos de ojos preciosos; que desde el cielo celebran junto a mí una más de mis metas...

A mi esposo Juan Manuel y a mi amada hija Keyra este logro también es tuyo; porque eres tú mi motor, espero te sientas orgullosa de tu mami Kalita, te amo mucho.

## TRIBUNAL DE SUSTENTACIÓN



MSIG. Lenin Freire Cobo

COORDINADOR MSIG



MSIG. Juan Carlos García

PROFESOR MSIG

## RESUMEN

Hoy en día las empresas cuentan con una gran cantidad de dispositivos como bases de datos, servidores web, aplicaciones, correo electrónico que son parte esencial del negocio.

Es por lo que ha surgido una herramienta de monitoreo como una solución para monitorear toda la infraestructura de tecnología crítica para el administrador, que brindará una mayor disponibilidad del servicio y resolverá rápidamente los problemas antes de que estos sucedan.

El objetivo de este proyecto es analizar e implementar una herramienta que le permita monitorear el estado de servidores y servicios críticos para monitorear la infraestructura.

Para el desarrollo del proyecto se utilizó la herramienta SITE 24/7 que permite analizar cada servidor de la administradora, así como también reflejar los resultados en reportes mismos que son almacenados y enviados al correo electrónico de las personas asignadas, de esta manera se podrán mantener registradas todos los eventos que surjan garantizando la funcionalidad de la infraestructura tecnológica.

El resultado del proyecto es la puesta en marcha y producción del sistema de monitoreo site 24/7 que permitirá dar seguimiento al estado de los servidores que alojan los servicios más críticos de la compañía.

## ÍNDICE GENERAL

AGRADECIMIENTO .....	ii
DEDICATORIA .....	ii
TRIBUNAL DE EVALUACIÓN .....	i
RESUMEN .....	ii
ÍNDICE GENERAL.....	iv
ABREVIATURAS Y SIMBOLOGÍA .....	vii
ÍNDICE DE FIGURAS.....	viii
ÍNDICE DE TABLAS .....	ix
INTRODUCCIÓN .....	x
CAPÍTULO 1 .....	1
GENERALIDADES .....	1
1.1. Antecedentes.....	1
1.2. Objetivos.....	2
1.2.1. Objetivo General .....	2
1.2.2. Objetivos específicos .....	3
1.2.3. Descripción del problema.....	3
1.3. Solución propuesta.....	4

CAPÍTULO 2.....	6
METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN .....	6
2.1. Planteamiento.....	6
2.1.1. Fase 1: Presentación del proyecto a Comité de Cambios Mayores	
6	
2.1.2. Fase 2: Reunión de definiciones de políticas con Proveedor ....	11
2.1.3. Fase 3: Instalación y Configuración .....	13
2.1.4. Fase 4: Revisiones post implementación auditoría .....	15
2.2. Hitos del proyecto.....	18
2.2.1. Hito 1: Definición y Alcance.....	18
2.2.2. Hito 2: Requerimientos técnicos.....	20
2.2.3. Hito 3: Definición de Equipos y servicios Críticos.....	20
2.2.4. Hito 4: Definición de umbrales de configuración .....	22
CAPÍTULO 3.....	26
RESULTADOS OBTENIDOS.....	26
3.1. Análisis de factibilidad realizado por proyectos y desarrollo	
tecnológico .....	26
3.2. Mejoras planteadas por auditoría de Sistemas.....	28
3.3. Limitaciones de la solución.....	32

CONCLUSIONES Y RECOMENDACIONES .....	32
BIBLIOGRAFÍA.....	33
ANEXOS.....	34

## **ABREVIATURAS Y SIMBOLOGÍA**

<b>PDT</b>	Proyectos y Desarrollo Tecnológico
<b>TIC</b>	Tecnologías de la información y Comunicación
<b>VPN</b>	Virtual Private Network
<b>WFH</b>	Word From Home

## ÍNDICE DE FIGURAS

Figura 1.1: Diagrama de Red Aseguradora .....	5
Figura 1.2: DMZ – Interna - Externa .....	6
Figura 2.1: Inventario de umbrales definidos en SITE 24X7 .....	23
Figura 2.2: Configuración umbrales monitoreo ping servicios.....	24
Figura 2.3: Configuración umbrales monitoreo servidor físico .....	24
Figura 2.4: Configuración umbrales utilización de memoria servidor físico...	25
Figura 2.5: Configuración disco de cada servidor centralizado.....	25
Figura 2.6: Configuración umbrales monitoreo servicios office 365.....	26
Figura 2.7: Configuración umbrales monitoreo pág. web.....	26
Figura 2.8: Configuración umbrales monitoreo servidor vmware .....	27
Figura 2.9: Configuración umbrales monitoreo servidores virtuales .....	27
Figura 3.1: Resumen de disponibilidad de servicios .....	27
Figura 3.2: Resumen de monitores activos.....	27

## ÍNDICE DE TABLAS

Tabla 1: Cuadro comparativo ofertas de proveedores .....	10
Tabla 2: Ficha Técnica Herramienta .....	15
Tabla 3: Control del proceso auditado .....	16
Tabla 4: Muestras solicitadas por auditoría.....	17
Tabla 5: Recomendaciones durante la recopilación de evidencias.....	18
Tabla 6: Requerimientos para instalación y configuración de agentes .....	20
Tabla 7: Servicios críticos .....	21
Tabla 8: Servidores críticos.....	22
Tabla 9: Mejoras post-implementación .....	31

## INTRODUCCIÓN

Esta empresa está dedicada a la administración de fondos y fideicomisos localizada en varias ciudades del Ecuador, perteneciente a un proveedor líder global de seguros, rentas y programas de beneficios para los trabajadores y que se encuentra dando servicios a más de 47 países. Este proveedor anualmente realiza una visita a fin de verificar si se cumplen con las políticas de seguridad establecidas por el grupo.

Esta última auditoría arrojó como resultado que había demasiados servidores que se quedaban offline producto de apagones, reinicios inesperados o actualizaciones automáticas provocando que sucursales enteras no puedan conectarse a los sistemas generando malestar en los partícipes y bajas en la calidad de servicio.

Basado en las recomendaciones dadas se procede a realizar un análisis exhaustivo de la situación actual de la empresa, identificando los servidores con aplicaciones y servicios considerados como críticos, así como también los administradores y backup; ambos responsables de la administración y correcto funcionamiento de la herramienta.

Actualmente existen muchas herramientas que permiten verificar estado o la salud de un equipo tecnológico, por lo que se cotiza con varios proveedores, seleccionando 3 opciones, mismas que deberán ser analizadas por el comité de compras para su aprobación y posterior adquisición.

La herramienta seleccionada y a implementar se llama SITE 24/7, la cual funciona censando el estado todos los equipos registrados en un servidor centralizado, obteniendo los datos proporcionados y enviando notificaciones vía correo electrónico en caso de que se presente algún incidente o error en los mismos; teniendo en cuenta que, para registrar un sensor es necesario conocer el servicio al que se orienta y así encasillarlo con los que ya fueron proporcionados por la herramienta o elaborando un sensor acoplado a las necesidades de la empresa. [1]

Generalmente estos problemas no eran detectados debido a la gran cantidad de dispositivos con los que cuenta la administradora es por ello que en base al análisis realizado se determinaron umbrales y configuraciones de línea base a fin de recibir todo el tiempo notificaciones e inclusive mucho antes de que se presente un problema que impida que un equipo esté disponible.

# **CAPÍTULO 1**

## **GENERALIDADES**

### **1.1. Antecedentes**

La compañía administradora de fondos con sede en un país de América Latina; y que a su vez pertenece a uno de los principales proveedores globales de seguros, programas de ingresos y beneficios para trabajadores con presencia en más de 47 países, siendo pioneros y líderes en el desarrollo y administración de fondos de largo plazo en el país, ofrece fondos de mediano plazo, desarrollados con soporte tecnológico y dentro de los altos estándares de calidad del grupo al que pertenece.

Por esta razón y como parte de los estándares de cumplimiento del grupo al que pertenece esta empresa, se sujeta internamente a un código de conducta que define y desarrolla los principios de comportamiento ético de

negocio y actividades, estableciendo las pautas necesarias para asegurar la responsabilidad corporativa reflejada en las relaciones con todos los partícipes (empleados, ejecutivos, proveedores y terceros).

La competencia particular se basa en el enfoque exclusivo y especializado de la gestión de fondos de inversión, considerando que el compromiso empresarial es una fuente de creación de valor sostenible y el principal requisito para mantener la confianza de la sociedad en cualquier institución. [2]

Por ello, es importante analizar el funcionamiento de los equipos de red para asegurar la calidad del servicio con el fin de ser una empresa más competitiva y atractiva en el mercado.

## **1.2. Objetivos**

### **1.2.1. Objetivo General**

Implementar una herramienta que permita monitorear la infraestructura tecnológica de los servidores y servicios críticos obteniendo una visibilidad detallada de los indicadores clave de rendimiento desde una solución única e integral.

### **1.2.2. Objetivos específicos**

- ✓ Implementar una herramienta de monitoreo de servidores.
- ✓ Obtener KPI'S que permitan llevar un control de incidentes.
- ✓ Optimizar tiempos de gestión y atención de equipos críticos.
- ✓ Elaborar documentación entendible de la herramienta para el personal de infraestructura.

### **1.2.3. Descripción del problema**

La empresa administradora de fondos cuenta con servicios en línea, por lo que es indispensable velar por el correcto funcionamiento de sus servidores. Censar todos sus equipos críticos es muy tedioso más aún si hay que realizar bitácoras que demandan mucho tiempo considerando que no es la única tarea a la que se dedica la persona encargada de infraestructura y soporte.

Esta empresa cuenta con solo dos personas altamente capacitadas en el área de infraestructura, mismas que se encargan no solo de velar por la salud física de los equipos mencionados sino también de monitorear el desempeño de estos.

El contar con servicios en línea conlleva abarcar una gran cantidad de problemas que pueden aparecer inesperadamente inclusive en la madrugada, el personal de Infraestructura y soporte no posee dentro de su contrato horas STANDBY de manera permanente por lo que se tiene que esperar al día siguiente para que estos incidentes se conozcan, muchas veces se reestablecen solos y el personal no se entera porque no hay un reporte con los sucesos ocurridos en todos los servidores.

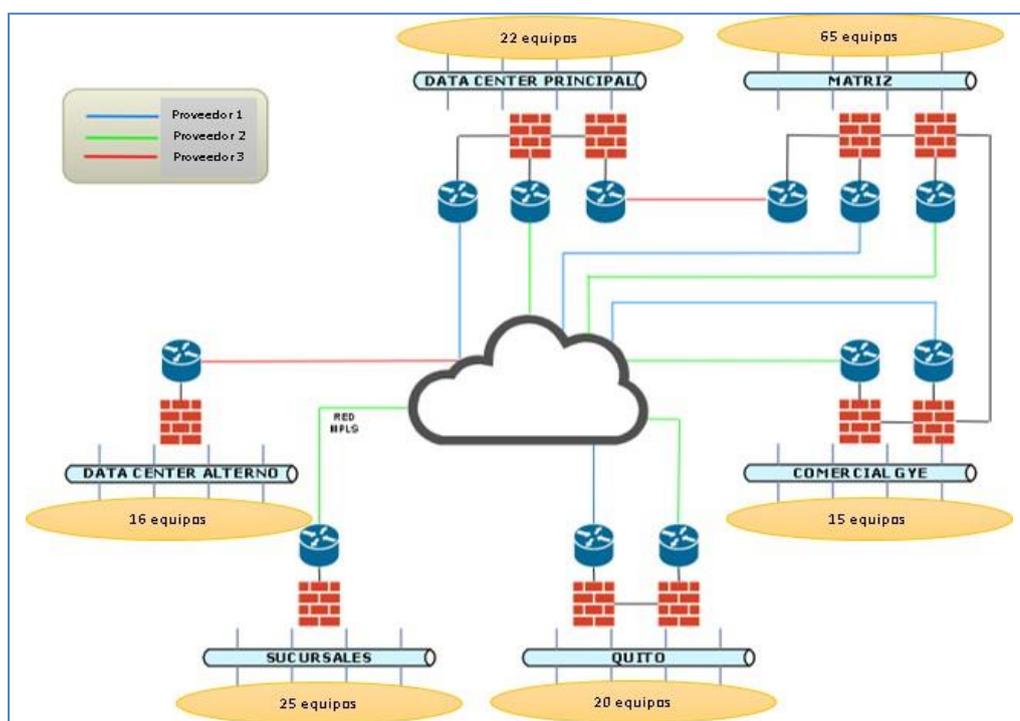
Se requiere un análisis para poder seleccionar herramientas de excelente calidad y precio que permitan detectar eventos o sucesos a tiempo evitando que estos representen negativos para la empresa.

### **1.3. Solución propuesta**

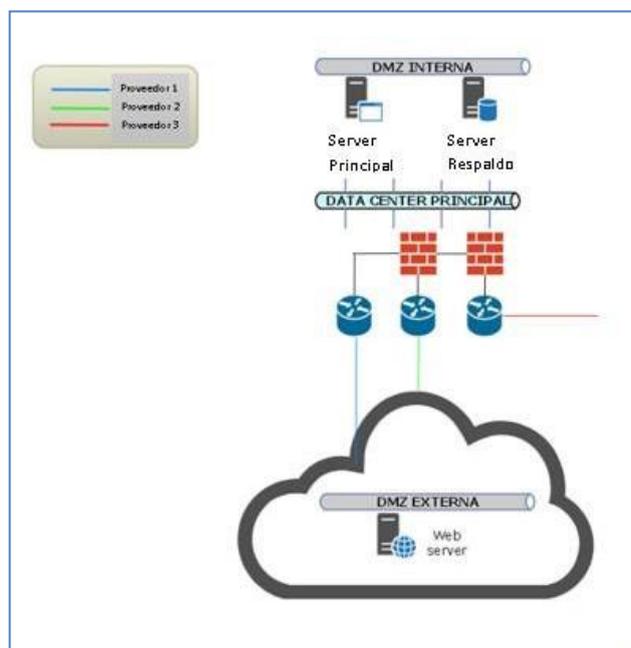
Fallos de red, fallas energéticas o falta de recursos en los servidores son los principales eventos reportados por parte del personal de infraestructura; generalmente una aplicación tiene conexión directa a la base de datos, dando paso al almacenamiento de información, cortar la conexión con la base de datos impediría registrar las transacciones del Core de negocio e impediría dar un buen servicio.

Es por ello que se debe precautelar por las comunicaciones entre servidores, bases de datos y demás equipos que conforman la red de la Administradora, así como también de la optimización de los recursos tales como Disco, Memoria, Carga, para la evaluación y monitoreo del rendimiento y salud de los equipos se instalará dentro de un servidor robusto el sistema de monitoreo llamado SITE 24/7.

Se espera trabajar de manera preventiva y no reactiva por lo que se motivará dentro de la cultura organizacional las capacitaciones y se elaborará la suficiente documentación técnica para el fácil uso de la herramienta.



**Figura 1.1:** Diagrama de Red Aseguradora  
Elaborado por: Autor



**Figura 1.2: DMZ – Interna - Externa**  
**Elaborado por: Autor**

## **CAPÍTULO 2**

### **METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN**

#### **2.1. Planteamiento.**

##### **2.1.1. Fase 1: Presentación del proyecto a Comité de Cambios**

##### **Mayores**

El Área de Proyectos, deberá asegurar el cumplimiento de todos requerimientos de novedades o incidencias por lo que se deberá ingresar un tiquete mediante la Mesa de Ayuda, estos cambios deben ser planificados y probado antes y después de su implementación, en un ambiente controlado, documentando cada uno de los pasos, incluyendo información que soporte dichas pruebas.

Los pases a producción no se podrán realizar si no se entregan todos los documentos establecidos para el pase. Exceptuando los cambios urgentes que deben ser aprobados por la Gerencia general.

El comité de gestión de cambios está conformado por los siguientes colaboradores:

- Gerencia general
- Gerente Administrativo Financiero
- Gerente comercial
- Oficial de Seguridad de la Información
- Jefe de Proyectos y Desarrollo tecnológico

En caso de ausencia del titula, podrán presidir la reunión del Comité de Gestión de Cambios los siguientes colaboradores:

- Jefe de Riesgos – Reemplazando al Oficial de Seguridad de la Información
- Líder de Desarrollo – Reemplazando al jefe de Proyectos y Desarrollo tecnológico

Y; en calidad de observadores podrán presidir la reunión del Comité de Gestión de Cambios los siguientes colaboradores:

- Auditor General
- Auditor IT
- Asistente de Coordinación y Control

Para la aprobación de los requerimientos mayores todos los integrantes deberán estar de acuerdo en su ejecución.

#### Sustentación de la compra

Durante la visita realizada por el proveedor global del exterior realizada en Septiembre/2019 se solicitó implementar el monitoreo automatizado de servicios IT, que pueden comprometer la continua operación de los servicios brindados por la Aseguradora, por esta razón se necesita contar con una herramienta automática para el monitoreo de los 365 días del año y las 24 horas del día (monitoreo 365x24x7).

## Metodología de Trabajo

El servicio de monitoreo se brindará mediante una herramienta de software y configuración de agentes para controlar el buen funcionamiento de la infraestructura tecnológica tales como servidores, enlaces, ambientes virtuales, switches, etc.

Esto con el objetivo de mantener el monitoreo permanente sobre la infraestructura tecnológica de la organización, lo que nos permitirá tener una alerta al momento de que sucede el evento y poder tomar medidas de corrección inmediatamente, se procede a cotizar con varios proveedores teniendo como resultado el siguiente cuadro comparativo.

Proveedor	Descripción	Tiempo entrega	Valor instalación	Pago Anual	Valor Total	Anticipación
SECUINFOR	Monitoreo de infraestructura para 77 equipos con notificaciones por correo y llamadas telef.	10 días	2800.0	8064.0	10864.0	100% instalación
EURODATA	Monitoreo de infraestructura para 77	60 días	1960.0	4620.0	6580.0	0%

	equipos con notificaciones correo/SMS					
SYNERGY	Monitoreo de infraestructura para 77 equipos con notificaciones correo/SMS	Sujeto a disponibilidad	1881.6	4166.0	5048.0	0%
TECHNET	Monitoreo de infraestructura para 77 equipos con notificaciones correo/SMS	Sujeto a disponibilidad	2016.0	4132.8	6148.8	0%

**Tabla 1:** Cuadro comparativo ofertas de proveedores  
**Elaborado por:** Autor

En base al cuadro comparativo la opción más viable por solución brindada y por costos es SYNERGY.

El departamento de Proyectos y desarrollo tecnológico cuenta con presupuesto para llevar a cabo este proyecto, este valor se encuentra reportado en un control de inversiones que se genera anualmente a inicios de año para su aprobación y seguimiento.

Se procede con el proceso administrativo de adquisición de licencias mediante la Cotización de compra #30234.

### **2.1.2. Fase 2: Reunión de definiciones de políticas con Proveedor**

La empresa administradora de fondos ha contratado los servicios de SYNERGY para realizar la implementación de la solución de monitoreo Site24x7 de Zoho Corporation, con la finalidad de analizar la solución de gestión de rendimiento de su infraestructura.

Site24x7 le permite supervisar, y gestionar la disponibilidad y el rendimiento de sus activos y servicios de TI dentro de los centros de datos tradicionales, así como en los entornos de nube pública más recientes. [1]

Con Site24x7 el equipo de operaciones de TI accederá rápida y fácilmente a la información que necesitan para mejorar la calidad, la previsibilidad y la eficiencia del servicio dando prioridad a la resolución de problemas según el impacto que tengan sobre el negocio, haciendo así más fácil la reducción de los tiempos de inactividad, mejorando la experiencia del usuario final y, en último término, capitalizando los objetivos del negocio.

### Condiciones Generales

- En caso de productos/licencias el tiempo de entrega está sujeto a disponibilidad.
- En caso de servicio/soporte el tiempo de entrega está sujeto a previa coordinación.
- Una vez aprobada la propuesta no se aceptan cambios a ésta.
- Los montos ofertados en esta propuesta, incluso cuando están por separado, solo son válidos cuando son considerados en un único paquete. Cualquier cambio en las fechas, cantidades y productos, requiere revisión de los montos y condiciones.

### Observaciones:

- En caso de querer monitorear alguna métrica en particular de los Dispositivos de red, se debe tener la información del MIB y OIDs del dispositivo.
- Precio mensual válido para contrato mínimo de 1 año de duración.
- Notificaciones por correo electrónico ilimitados
- Incluye 200 créditos para SMS/Llamadas de Voz
  - 1 SMS = 1 crédito

- 1 Llamada de Voz = 2 créditos

Mejoras de Servicios de Monitoreo como valor agregado:

- Configuración de 1 Dashboard de Disponibilidad de Servicios
- Configuración de 2 Acciones automatizadas
- Configuración de 1 Reporte de caídas y SLA
- Configuración de Monitores pendientes: 4 básicos y 5 avanzados

### **2.1.3. Fase 3: Instalación y Configuración**

A continuación, se detalla las acciones realizadas para la instalación y configuración del agente de monitoreo Site24x7:

1. Desde la consola de Site24x7 vaya a Servidor > Monitor de servidor > Servidores (+) > Windows
2. Hacer clic en Descargar Site24x7 Windows Server Agent. Haga doble clic en el archivo .msi. Haga clic en siguiente.
3. Ingresar la clave del dispositivo en el campo provisto. Esto se encuentra en la página Agregar monitor de Windows en el cliente web.

4. Seleccionar una carpeta de instalación donde desee colocar el agente. Asegúrese de que la carpeta tenga permiso de lectura y escritura
  
5. Una vez que el agente se haya instalado correctamente, puede ver el monitor en Servidor > Monitor de servidor > Servidores. Una vez que el agente esté instalado, aparecerá un icono de bandeja en la barra de inicio rápido o aparecerá en Inicio > Todos los programas > Site24x7 Windows Monitor > Icono de bandeja.

Este proceso se realizó para todos los otros servidores que requerían agente

Se pueden visualizar los servidores monitoreados actualmente y los recursos de performance de cada uno.

6. Para el monitoreo de componentes vmware se añadieron las credenciales del vCenter para poder monitorear las máquinas virtuales, datastore requeridas.

7. Para el monitoreo de los enlaces de todas las localidades se agregó monitores de PING que se encuentran monitoreando a nivel del ISP y equipo interno.
  
8. Para el monitoreo de Office 365 se agregaron las credenciales requeridas, y como se muestra en la imagen, el agente recopila información de todos los servicios de Office 365.
  
9. Parte del monitoreo también es a la disponibilidad de la página de la empresa.

#### 2.1.4. Fase 4: Revisiones post implementación auditoría

El objetivo de la auditoría es verificar la implementación de monitoreos automatizados de servicios críticos de TI resultantes de recomendación por visita realizada en agosto/2019 por Seguridad de Información del proveedor global.

Información técnica	
Herramienta de software:	Herramienta automática desarrollada por Sinergy (Agente Site 24x7)
Notificaciones habilitadas por:	Correo electrónico
Remitente de Informes:	Site247@synecuador.com
Remitente de Alertas:	Site247@synecuador.comreporte

**Tabla 2:** Ficha Técnica Herramienta  
**Elaborado por:** Autor

---

CONTROL DEL PROCESO	
FRECUENCIA DE REPORTES:	Desde su implementación en Mayo del 2020 hasta el 20 de Septiembre el área de IT dispone de reportes todos los días lunes de cada semana. Diarios desde el lunes 21 de septiembre.
RESPONSABLE:	Asistente de Servidores, Redes y Seguridad.
DEFINICIÓN DE BACK UP:	Jefe de Proyectos y DT
OBJETIVO DEL MONITOREO POR IT:	Mantener un monitoreo permanente sobre la IT de la organización, que permitirá contar con alertas efectivas desde el momento que ocurre un evento (Pico de interrupción) y poder así tomar medidas de corrección inmediatas con los proveedores de los servicios.
PROCESO DOCUMENTADO:	Monitoreo de servicios de los procesos críticos- (Requiere mejoras, observaciones emitidas 26 Nov 2020)
COMENTARIO DE AUDITORIA	Revisiones y evaluación de alertas implementadas, verificación de uptime con conformidad del proceso implantado por PDT, sólo requiere mejoras del proceso e inventarios.

**Tabla 3:** Control del proceso auditado  
**Elaborado por:** Autor

MONITOREO DE SERVICIOS POR AUDITORIA							
MES-AÑO	TIPO DE SOLICITUD	SEMANA, (LUNES)	DIA DEL MES	INFORME	ALERTA	ESTADO INF.	COMENTARIOS AUDITORIA
may-20	MUESTRA	4	-	X		—	CONFORMIDAD
	MUESTRA	18		X		—	CONFORMIDAD
jun-20	MUESTRA	1	-	X		—	CONFORMIDAD
	MUESTRA	22	-	X		—	CONFORMIDAD
	MUESTRA	29	-	X		—	CONFORMIDAD
	MUESTRA	-	30		X	—	CONFORMIDAD
jul-20	MUESTRA	6	-	X		—	CONFORMIDAD
	MUESTRA	13	-			—	CONFORMIDAD
	MUESTRA	20	-	X		—	CONFORMIDAD
	MUESTRA		15		X	—	CONFORMIDAD
	MUESTRA		16		X	—	CONFORMIDAD
ago-20	MUESTRA	27	-			—	CONFORMIDAD
	MUESTRA	3	-	X		—	CONFORMIDAD
	MUESTRA	17		X		—	CONFORMIDAD
	MUESTRA	-	15		X	—	CONFORMIDAD
	MUESTRA	-	27		X	—	CONFORMIDAD
sep-20	MUESTRA	24	-			—	CONFORMIDAD
	MUESTRA	7	-	X		—	CONFORMIDAD
	MUESTRA	14	-	X		—	CONFORMIDAD
	EJECUCIÓN DIARIA	-	18		X	—	CONFORMIDAD

	EJECUCIÓN DIARIA	-	19		X	-	CONFORMIDAD
	EJECUCIÓN DIARIA	-	21		X	-	CONFORMIDAD
	EJECUCIÓN DIARIA	-	29	X		-	CONFORMIDAD
	EJECUCIÓN DIARIA	-	30	X		-	CONFORMIDAD

**Tabla 4:** Muestras solicitadas por auditoría  
**Elaborado por:** Autor

### Alcances de actuación de auditoria en sistemas

Desde el 1/Octubre/2020 a la fecha el control de los monitoreos es diario por Auditoria, mail remitido de reportes automáticos y alertas según la necesidad de revisión de Auditoria por Asistente de Coordinación y control con la coordinación del Asistente de Redes y servidores.

ACCIONES IMPLANTADAS-RECOMENDACIONES EN LA RECOPIACIÓN DE EVIDENCIAS		
Recomendaciones emitidas	Comentario Auditoria	ESTADO
Alertas por picos de inactividad solo son enviados a Asistente Servidores, Redes y Seguridades, no definido back up para cubrir contingencia o ausencias del principal.	19/Nov procedimiento operativo consta formalizado que en el back es el Jefe de PDT 26/Nov Jefe PDT quien actúa como backup remite evidencia de inclusión en los mails de notificación diaria del monitoreo de servicios	Regularizado
Se constató que ciertos informes automáticos enviados de Oct y Nov ( 9 en total) no pueden ser abiertos.	Se solicita configurar la herramienta de tal manera que el informe generado actualmente en pdf, también se genere en otro formato. En reemplazo a los reportes se solicita el envío de las alertas para	Regularizado

	confirmar si existen incidentes o no en esos días, no existiendo novedad alguna por reportar.	
Se identifican saltos y picos de interrupciones que no constan en el reporte de incidentes que se notifica a Seguridad de Información y a Auditoria.	Se justifica por las actualizaciones realizadas en los servidores según mantenimientos planificados, parches por vulnerabilidades, proceso relevado el 19/Octubre y en sesiones de Nov/2020.	Regularizado
Inventario de incidentes requiere mejoras ya que no incorpora la notificación automática del agente, que difiere en minutos del horario de inicio y de término reportado del evento ocurrido.	Se implementará mejoras en el Reporte de incidentes al cierre de Nov/2020 que incluya 2 parámetros (Notificación alerta automática y horarios de Gestión) . Bosquejo fue enviado el 25/Nov/2020 a Auditoria de resultados de Oct/2020.	Regularizado
Monitoreo de Servidor de directorio activo secundario no consta en la configuración definida de los procesos críticos, pese a que consta en los 15 procesos inventariados según control de S.I.	25/Nov/2020 => Configuración con el proveedor para inclusión del monitoreo de AD secundario, sólo figuraba el principal. Se remite evidencia del monitoreo diario del 26/Nov donde ya se encuentra incluido el directorio activo secundario.	Regularizado

**Tabla 5:** Recomendaciones durante la recopilación de evidencias  
**Elaborado por:** Autor

## 2.2. Hitos del proyecto

### 2.2.1. Hito 1: Definición y Alcance

Se desea mantener el monitoreo permanente sobre la infraestructura tecnológica de la organización, lo que va a permitir tener una alerta al momento de que sucede el evento o antes de

que este se de para de esta forma poder tomar medidas de corrección de manera inmediata.

Los elementos para monitorear son los siguientes:

- 12 Servidores críticos
- host
- 1 URL monitoring
- 15 equipos de red
- 22 enlaces de red
- 1 instancia de office 365
- 7 servidores app

Servicios:

- Notificaciones por correo electrónico ilimitados
- Incluye 200 créditos para SMS/Llamadas de Voz
  - o 1 SMS = 1 crédito
  - o 1 Llamada de Voz = 2 créditos

Valores agregados:

- Configuración de 1 Dashboard de Disponibilidad de Servicios
- Configuración de 2 Acciones automatizadas
- Configuración de 1 Reporte de caídas y SLA

- Configuración de Monitores pendientes: 4 básicos y 5 avanzados

### 2.2.2. Hito 2: Requerimientos técnicos

A continuación, se muestran los requerimientos necesarios para la instalación y configuración de los agentes de Site24/7:

Nombre del Agente:	Site 24x7
Puerto de salida:	HTTPS 443
Dominios destinos:	Dms.zoho.com Plus.site24x7.com Puls2.site24x7.com Plus3.site24x7.com

**Tabla 6:** Requerimientos para instalación y configuración de agentes  
**Elaborado por:** Autor

Adicionalmente se requerirá:

- Credenciales con permisos de administrador para instalar el agente de Monitoreo.

### 2.2.3. Hito 3: Definición de Equipos y servicios Críticos

Se consideran críticos a toda aquella infraestructura o servicios que pueden comprometer la continuidad de la atención y servicios brindados por la empresa. La disponibilidad y el rendimiento de la infraestructura y procesos críticos se detallan a continuación:

- Enlaces de datos de todas las oficinas.
- Disponibilidad de internet.
- Enlaces de acceso a data center alternativo.
- Disponibilidad en servicios de firewall.
- Disponibilidad en data center principal.
- Servicios web.
- Ambiente virtual.
- Servicio de correo office 365.
- Servidores de aplicaciones.
- Directorio activo, principal y secundario.
- Switches Core.
- Acceso a bases de datos.
- Acceso a red de todas las oficinas.

### Servicios críticos

#	Servicio	Monitor 24x7
1	Servicio virtualización	Si
2	Servicio de clúster Producción	Si
3	Microsoft IIS	Si
4	Active Directory de Microsoft	Si
5	Sincronización Microsoft 365 - Correos	Si
6	Servicios de virtualización 1	Si
7	Resources	Si

**Tabla 7:** Servicios críticos  
**Elaborado por:** Autor

## Servidores críticos

Equipo Físico	Equipos Virtuales	Monitor 24x7
Servidor físico ESXG8TB1	Servidor MySQL289	Si
	Servidor app Apoyo2	Si
	Servidor Citrix Contry	Si
	Servidor Citrix Oficina	Si
	Servidor BiomJsig	Si
	Servidor PowApp	Si
Servidor físico ESXUGTB2	Servidor DirecAct	Si
	Servidor Webupsyu	Si
	Servidor LDAP23	Si
	Servidor VeenBack	Si
	Servidor Suc_Citrix	Si
	Servidor Servicios en línea	Si
	Servidor Sql en línea	Si
	Servidor transWeb	Si
Servidor WSTUPUS GYE		Si

**Tabla 8:** Servidores críticos  
**Elaborado por:** Autor

### **2.2.4. Hito 4: Definición de umbrales de configuración**

Inventario de los umbrales definidos en la solución de monitoreo Site24x7.

Nombre	Umbral	PROBLEMA			CRÍTICO		
		Condición	Umbral	Valor sonda	Condición	Umbral	Valor sonda
Default Threshold - Ring	Pérdida de paquetes	>	20%	5			
	Tiempo de respuesta para la ubicación principal de monitorización	>	200ms	5	>	300ms	10
Default Threshold - Server	Notificar cuando el proceso no funcione	Si		1			
	Utilización de CPU	>	90%	5			
	Utilización de memoria	>	90%	5	>	95%	5
	Utilización de disco	>	90%	5	>	90%	5
	Utilización de disco de partición (%)	>	90%	5			
Default Threshold - Data store	Espacio libre (en porcentaje)	>	70%				
Default Threshold - Office 365	Notificar cuando el servicio esté inactivo	Si					
	Notificar cuando la función del servicio esté inactivo	Si					
Default Threshold - UI	Tiempo de respuesta para la ubicación principal de monitorización	>	300ms	5			
Default Threshold - VMWare ESX	Notificar cuando un sensor de energía está inactivo/con problemas/crítico	Si					
	Notificar cuando un sensor de ventilador está inactivo/con problemas/crítico	Si					
	Notificar cuando un sensor de temperatura está inactivo/con problemas/crítico	Si					
	Notificar cuando un sensor de procesador está inactivo/con problemas/crítico	Si					
	Notificar cuando un sensor de memoria está inactivo/con problemas/crítico	Si					
	Notificar cuando un sensor de almacenamiento está inactivo/con problemas/crítico	Si					
	Notificar cuando un sensor de batería está inactivo/con problemas/crítico	Si					
	Notificar cuando un sensor de guardián está inactivo/con problemas/crítico	Si					
	Notificar cuando un sensor de tensión está inactivo/con problemas/crítico	Si					
	Notificar cuando un procesador está inactivo/con problemas/crítico	Si					
	Uso de CPU	>	90%	5	>	0.95	5
	Utilización de memoria	>	90%	5	>	0.95	5
Default Threshold - VMWare VM	Notificar errores del agente	Si					
	Notify when an NIC gets disconnected	No					
	Uso de CPU	>	95%	5			
	Uso de memoria	>	95%	5			
Default Threshold - AD Server	Lecturas	>	110kb/s	5			
	Escrituras	>	110kb/s	5			

**Figura 2.1:** Inventario de umbrales definidos en SITE 24X7  
**Elaborado por:** Autor

## Ping

The screenshot shows the 'Editar el Perfil del Umbral' (Edit Threshold Profile) window. At the top, the 'Tipo de monitor' (Monitor Type) is set to 'Hacer Ping' (Ping), and the 'Nombre a mostrar' (Name to display) is 'Default Threshold - PING', indicated by a red arrow. Below this, the 'Reglas de tiempo de inactividad' (Inactivity Time Rules) section shows 'Número de ubicaciones para informar que el monitor no funciona' (Number of locations to report that the monitor is not working) set to '3 ubicaciones'. The 'Configuración de umbral' (Threshold Configuration) section contains two threshold rules:

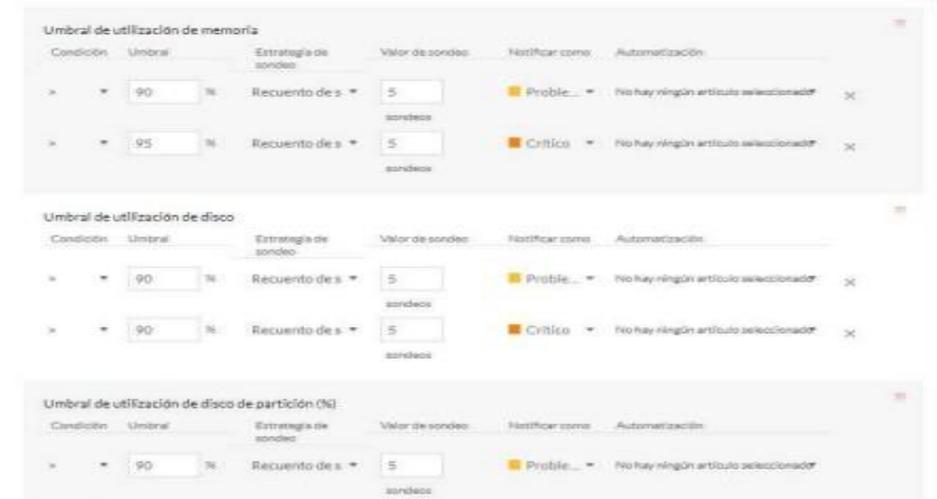
Condición	Umbral	Estrategia de sondes	Valor de sondes	Notificar como
<	20	%	5 sondes	Proble...
Add Critical Threshold				
>	200	ms	5 sondes	Proble...
>	300	ms	10 sondes	Critico

**Figura 2.2:** Configuración umbrales monitoreo ping servicios  
**Elaborado por:** Autor

## Servidores Físicos

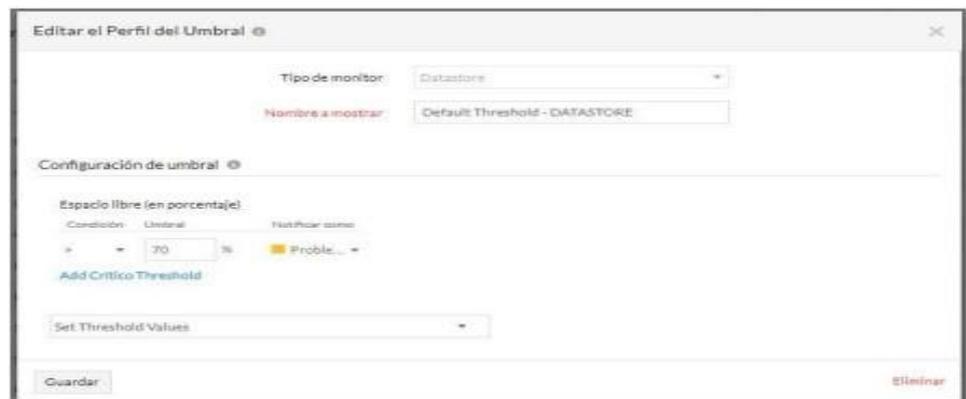
The screenshot shows the 'Configuración de umbral' (Threshold Configuration) window. The 'Nombre a mostrar' (Name to display) is 'Default Threshold - SERVER'. The 'Notificar cuando el proceso no funcione' (Notify when the process is not working) section is visible, with 'Estrategia de sondes' (Probe Strategy) set to 'No' and 'Recuento de sondes' (Probe Count) set to '1'. The 'Notify As' dropdown is set to 'Proble...', and the 'Automation' dropdown is set to 'No hay ningún artículo seleccionado'.

**Figura 2.3:** Configuración umbrales monitoreo servidor físico  
**Elaborado por:** Autor



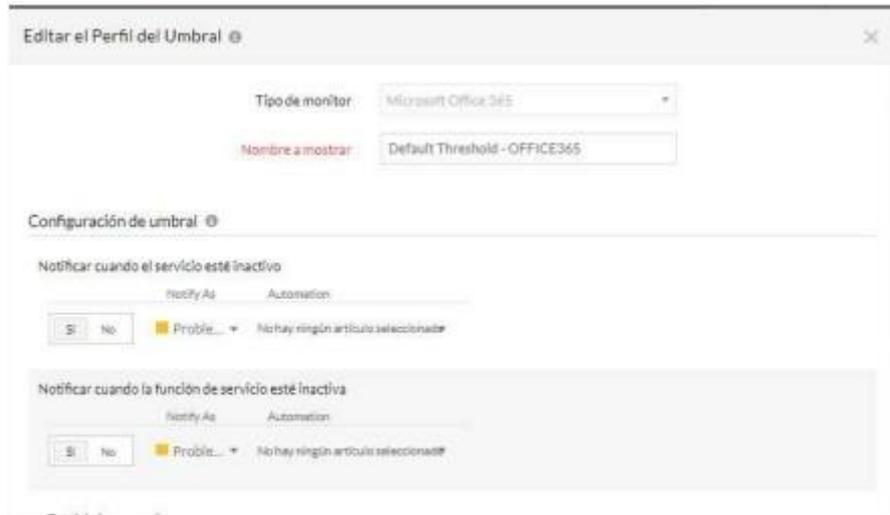
**Figura 2.4:** Configuración umbrales utilización de memoria servidor físico  
**Elaborado por:** Autor

Disco de cada servidor de almacenamiento centralizado



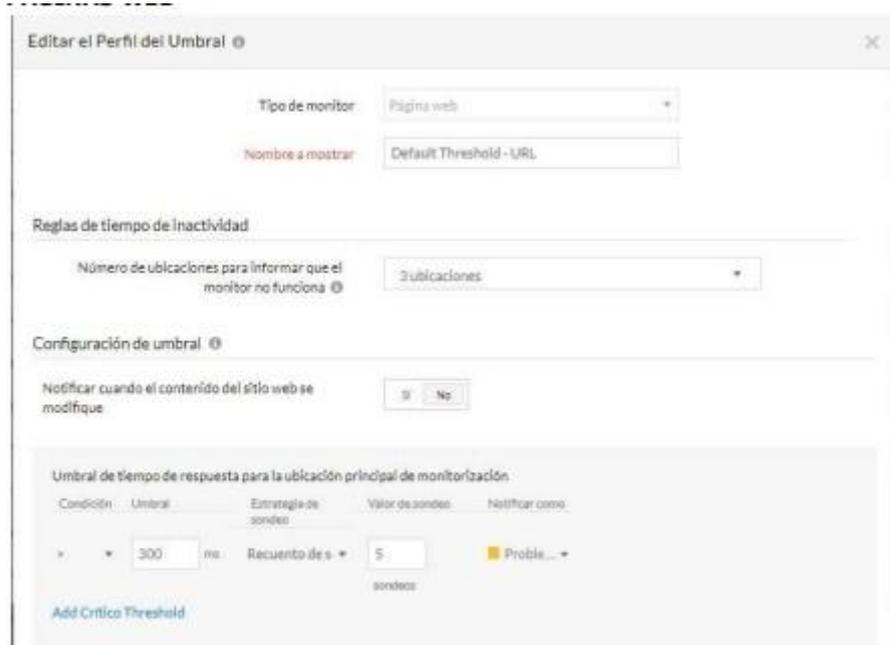
**Figura 2.5:** Configuración disco de cada servidor centralizado  
**Elaborado por:** Autor

Servicios de Office 265



**Figura 2.6:** Configuración umbrales monitoreo servicios office 365  
**Elaborado por:** Autor

## Página web



**Figura 2.7:** Configuración umbrales monitoreo pág. web  
**Elaborado por:** Autor

## Servidor físico VMWARE

The screenshot shows the 'Editar el Perfil del Umbral' (Edit Threshold Profile) window for a physical VMware server. The 'Tipo de monitor' (Monitoring Type) is set to 'Servidor de VMware ESX/ESD'. The 'Nombre a mostrar' (Display Name) is 'Default Threshold - VMWAREESX'. Under 'Configuración de umbral' (Threshold Configuration), there are four sections for notifying when sensors are inactive or have critical problems:

- Notificar cuando un sensor de energía está inactivo/con problemas/crítico: Notify As:  Sí  No  Problema...
- Notificar cuando un sensor de ventilador está inactivo/con problemas/crítico: Notify As:  Sí  No  Problema...
- Notificar cuando un sensor de temperatura está inactivo/con problemas/crítico: Notify As:  Sí  No  Problema...
- Notificar cuando un sensor de procesador está inactivo/con problemas/crítico: Notify As:  Sí  No  Problema...

**Figura 2.8:** Configuración umbrales monitoreo servidor vmware  
**Elaborado por:** Autor

## Servidores virtuales

The screenshot shows the 'Editar el Perfil del Umbral' (Edit Threshold Profile) window for virtual servers. The 'Tipo de monitor' (Monitoring Type) is set to 'VM de VMware'. The 'Nombre a mostrar' (Display Name) is 'Default Threshold - VMWAREVM'. Under 'Configuración de umbral' (Threshold Configuration), there are three sections:

- Notificar errores del agente: Notify As:  Sí  No  Problema... (No hay ningún artículo seleccionado)
- Notify when an NIC gets Disconnected: Notify As:  Sí  No  Problema... (No hay ningún artículo seleccionado)
- Uso de CPU: Condición: Umbral. Estrategia de sondeo: Recuento de s. Valor de sondeo: 5. Notificar como:  Sí  No  Problema... (No hay ningún artículo seleccionado). Automatización:  Sí  No  Problema... (No hay ningún artículo seleccionado).

At the bottom, there is a link to 'Add Critical Threshold'.

**Figura 2.9:** Configuración umbrales monitoreo servidores virtuales  
**Elaborado por:** Autor

## **CAPÍTULO 3**

### **RESULTADOS OBTENIDOS**

#### **3.1. Análisis de factibilidad realizado por proyectos y desarrollo tecnológico**

Mediante la contratación de los servicios de SYNERGY se implementó la solución de monitoreo Site24x7 de Zoho Corporation.

Con la solución de monitoreo Site24x7 el Asistente de Servidores, Redes y Seguridad accede a la información que necesitan para mejorar la calidad, la previsibilidad y la eficiencia del servicio dando prioridad a la resolución de problemas según el impacto que tengan sobre el negocio, permitiéndole la reducción de los tiempos de inactividad, mejorando la experiencia del usuario final y, en último término, capitalizando los objetivos del negocio.

La solución de monitoreo Site 24x7 emite por correo electrónico todos los días de forma automática un informe de la disponibilidad de los Activos de TI monitoreados mediante el correo Site247@synecuador.com; con el respectivo informe es recibido por el Asistente de Servidores, Redes y Seguridad.



**Figura 3.1:** Resumen de disponibilidad de servicios  
Elaborado por: Autor

Vista general de Monitores activos de la solución de monitoreo Site24x7 de toda la infraestructura de la empresa. El Asistente de Servidores, Redes y Seguridad gestiona las tareas respectivas para solucionar los servicios monitoreados que se encuentren con el estado Abajo, Crítico y Problema.



**Figura 3.2:** Resumen de monitores activos  
Elaborado por: Autor

- **Abajo:** El servicio no puede ser monitoreado debido a que se encuentra inactivo.
- **Crítico:** El servicio monitoreado tiene alertas del tipo Crítico según configuración de umbrales.
- **Problema:** El servicio monitoreado tiene alertas del tipo Problema según configuración de umbrales.
- **Arriba:** El servicio monitoreado se encuentra operativo correctamente según configuraciones de umbrales.

### 3.2. Mejoras planteadas por auditoría de Sistemas

El objetivo es dar seguimiento a las actividades pendientes Post-Implementación Monitoreo automático de servicios críticos.

PUNTOS PENDIENTES MONITOREO POST IMPLEMENTACIÓN OMM 24/7		
PLANES DE ACCIÓN PDT	ESTADO	COMENTARIOS AUDITORIA
Confirmar si se dio solución con el proveedor para contar con formato adicional de presentación del informe diario, se cuenta con informe en pdf que algunas veces se ha tenido que acudir al mail de alertas porque dicho archivo está dañado.		Ok solucionado con fecha 26/Nov/2020. Se remite el 3/Dic/2020 OK regularizado.
Alertas por picos de inactividad solo son enviados a Asistente Servidores, Redes y Seguridades, no		Ok solucionado con fecha 26/Nov/2020. Se remite el 26/Nov/2020 evidencia por Jefatura de Proyectos y Desarrollo tecnológico // OK regularizado.

definido back up para cubrir contingencia o ausencias del principal.		
Inclusión tónica de monitoreo de servicios en Comité de Gestión de TI y Requerimientos.		Ok regularizado Comité celebrado el 2/Dic/2020- Evidencias remitida PDT con fecha 4/Dic/2020
Proceso inventario que consta en la matriz de S.I. que pese a que no es crítico forma parte de acciones definidas: "Verificación de servicio de wifi en horarios establecidos"		<a href="#">Por confirmar con Riesgos/Seguridad de Información</a> Queda sin efecto dado que no está dentro de los servicios críticos el wifi.
Según cuadro de control de actividad seguida por el área de Seguridad de Información, consta inventariado 15 actividades por ejecutar monitoreo, de los cuales falta incluir la verificación de acceso a páginas de bancos por proceso de débitos automáticos.		<a href="#">Por confirmar con Riesgos/Seguridad de Información</a> Producto de la implementación del Monitoreo 24/7 para revisión del uptime de ciertos servicios críticos, Auditoría le había solicitado que en modalidad teletrabajo debería contemplarse el acceso web para el proceso de débitos automáticos que se realiza por páginas web, lo cual en escenario normal está contemplado en el ítem "Verificación de disponibilidad de internet"; sin embargo en WFH, el internet depende del servicio de datos del colaborador, por lo cual solicita se pueda asignar línea dedicada de internet al personal que realiza este proceso. -> <a href="#">Se revisó en reunión con las Gerencias, TTHH, Proyectos y Riesgos y se definió la malla de recursos con líneas dedicadas. La instalación ya se encuentra activa.</a>
Inclusión de procedimiento operativo de monitoreos de servicios- adaptar observaciones de Auditoría		Previa revisión segundo borrador remitido 3/Dic. Auditoría notificó 04/Dic propuesta para la mejora del documento, fecha máxima de envío 07/Dic. 07/12/2020=> Ok, recibido
Archivo umbrales de monitoreos de servicios 24 x7		4/Dic => Se solicitó inclusión en el mismo manual operativo y no como documento independiente.
Inventario de servidores críticos monitoreados		Información será remitida hasta el 07/Dic/2020 por PDT.

reportados por PDT no concuerda con los monitoreados según informe diario de monitoreos de servicios críticos 24/7.		20/01/2021.- PDT se compromete a enviar bitácora de servicios críticos.
Reestructurar el reporte de eventos/incidentes para que incorpore información de las alertas del monitoreo de servicios		Se remitió preliminar con corte a Oct/2020 el 26/Nov. Por formalizar cambios en el envío de reporte de incidentes al cierre de Nov/2020 20/01/2021.- PDT se compromete a enviar junto a la bitácora de incidentes los correos con los tickets del proveedor informando lo sucedido con los enlaces.
En la evaluación del despliegue de MPLS en sucursales se confirmará si el licenciamiento abarcará un punto o dos como se lo hace en la actualidad (Internet y VPN).		Por coordinarse una nueva sesión con el proveedor, prevista en el transcurso de la semana del 7 al 11 de Dic. Se remitirá mail de justificación de gestiones por coordinarse el 6/Dic 06/12/2020 => OK recibido.
Justificación de picos por interrupciones Nov 2020-Dic 2020		Esta bitácora consolidada fue remitida por Auditoria con fecha 30/Nov/2020 acordado contar con el análisis y sustentos por PDT hasta el 11/Dic/2020 20/01/2021.- En reunión se informa que se ha enviado con corte al día Lunes 19/01/2021 la bitácora con picos de inactividad para su justificación. 15/03/2021.- PDT formaliza mediante correo que los valores de inactividad de los meses de nov/dic se deben a que la herramienta se encontraba en una etapa de reafinamiento, razón por la cual estos valores no son confiables.
Bitácora mensual de las actualizaciones instaladas en los servidores críticos y envío del cronograma de mantenimientos establecidos para justificar picos de interrupción que no se origina de eventos.		Compromisos definidos: El Afinamiento de este proceso se realizará durante el mes de diciembre para ejecutar dicha implantación a partir del mes de enero del 2020. 20/01/2021.- Se trata tema con proveedor por lo que se estabilizará hasta finales del mes de enero y se procederá a enviar de manera mensual para la revisión y seguimiento

		15/3/2021.- PDT envía correo formalizando reporte de parchados programados por el proveedor.
Se consultará con el proveedor si en vez de poner un totalizado de horas de interrupción, se puede colocar un promedio de interrupciones por día.		Se tendrá que realizar una segunda sesión con el proveedor, prevista en el transcurso del 7 al 11 de diciembre del 2020 20/01/2021.- PDT indica que consultará una vez más a proveedor la posibilidad de acoplar esta mejora al informe actual. 15/03/2021.- PDT envía correo formalizando que el reporte emitido por la herramienta se mantiene con el formato actual
Quedan 4 licencias que no cubrirán el monitoreo de los débitos automáticos que no fue contemplado en el proceso inicial.		Acción por evaluar con el jefe PDT la inclusión de más licencias o en su defecto redefinir si con el despliegue de MPLS se liberarán licencias o no. Por confirmar hasta el 18 Dic 2020 Queda sin efecto dado que solo se están considerando los servidores, firewalls y servicios críticos revisados y aprobados.
En la evaluación de los monitoreos con corte al mes de noviembre se evidencia que el monitor MS Office 365 tiene problemas desde el 04-nov, sin embargo, el rendimiento consta como 100% disponible		Se tendrá que realizar una segunda sesión con el proveedor, prevista en el transcurso del 7 al 11 de diciembre del 2020 a fin de mitigar por qué consta como un servidor con problemas y en la parte inferior como 100% disponible. Se ajustará en la plataforma ya que el Monitor MS Office 365 muestra monitoreos de varios servicios que no se usan, es decir que de los 20 hay que identificar cuáles de estos son los que se debería mantener. 20/01/2021.- Se indica que se levantará ticket con proveedor a fin de que se segreguen por servicios y que no consideren los que no se usan

**Tabla 9:** Mejoras post-implementación  
Elaborado por: Autor

### **3.3. Limitaciones de la solución**

- Cuando un servidor se apaga, puede tomar cierto tiempo reconocer que vuelve a estar en servicio.
- Los reportes de alerta que se emiten dentro de la aplicación están configurados de fábrica y si se desea modificar alguna variable descuadra el reporte.
- Si hay errores de fábrica es necesario

## CONCLUSIONES Y RECOMENDACIONES

1. Para acceder a la consola Web de Monitoreo Site24x7, se debe enrolar cada usuario, para este paso se envió un correo electrónico para que puedan realizarlo.
2. Pueden descargarse el aplicativo móvil para Site24x7, donde pueden acceder a las mismas vistas que se han mostrado en este documento.  
Valido para Android y Apple.
3. Se ha habilitado las notificaciones por correo electrónico para todos los monitores de la empresa Administradora de Fondos, llegará como remitente: Site247@synecuador.com.

## BIBLIOGRAFÍA

- [1] ZohoCorp, «Site24X7,» 2021. [En línea]. Available: <https://www.site24x7.com/es/application-performance-monitoring.html>.  
[Último acceso: 10 10 2021].
- [2] D. A. Freire Aleaga y R. W. Sánchez Balarezo, «DSPACE,» 2016. [En línea]. Available: <https://dspace.ups.edu.ec/handle/123456789/12655>.

## ANEXOS

	MANUAL DE PROCEDIMIENTOS OPERATIVOS
	MONITOREO DE SERVICIOS DE LOS PROCESOS CRÍTICOS
DEPARTAMENTO: PROYECTOS Y DESARROLLO TECNOLÓGICO	CÓDIGO: MP-SA-PFES-314

Control de cambios:

Versión	Fecha de revisión / actualización	Fecha de vigencia	Breve descripción del cambio
1	19/11/2020	01/12/2020	Elaboración de documento.

### 1. OBJETIVO

Establecer las políticas y procedimientos para el monitoreo de los servicios de los procesos críticos.

### 2. POLÍTICA

El Asistente de Servidores, Redes y Seguridad será responsable de monitorear el estado de los servidores de los procesos críticos.

El Asistente de Servidores, Redes y Seguridad será el responsable de solucionar los problemas reportados por el incorrecto funcionamiento de un servicio.

El jefe de Proyectos y Desarrollo Tecnológico asumirá las responsabilidades del monitoreo de servicios de los procesos críticos en caso de ausencia del Asistente de Servidores, Redes y Seguridad.

### **3. PROCEDIMIENTOS**

#### **3.1. MONITOREO DE LOS SERVICIOS DE LOS PROCESOS CRÍTICOS**

##### **Asistente de Servidores, Redes y Seguridad**

1. Todos los días por la mañana, verifica el correcto estado de los servicios de los procesos críticos.

- 1.1. En caso de que un servicio no se encuentra funcionando correctamente entonces, ejecuta las tareas, desde el paso 4, indicadas en el procedimiento *“GESTIÓN DE LA ALERTA POR EL ESTADO INCORRECTO DE UN SERVICIO”*

#### **3.2. GESTIÓN DE LA ALERTA POR EL ESTADO INCORRECTO DE UN SERVICIO**

##### **Aplicativo de Monitoreo Automático / Colaborador**

1. Reporta al Asistente de Servidores, Redes y Seguridad sobre el estado incorrecto de un servicio.

##### **Asistente de Servidores, Redes y Seguridad**

2. Recibe una alerta por correo electrónico por el estado incorrecto de un servicio.
3. Verifica el servicio reportado.

4. Realizar las correcciones pertinentes para el correcto funcionamiento del servicio.
  - 4.1. Coordina acciones con un proveedor en caso de ser necesario.
  
5. Valora la alerta y la registra en la “Bitácora de Eventos” en el caso de que haya sido un incidente.

ELABORACIÓN / ACTUALIZACIÓN	ASISTENTE DE COORDINACIÓN Y CONTROL	
REVISIÓN	ASISTENTE DE SERVIDORES, REDES Y SEGURIDAD	
	JEFE DE PROYECTOS Y DESARROLLO TECNOLÓGICO	
APROBACIÓN	GERENTE ADMINISTRATIVO FINANCIERO	