EMPRESA SOCIAL DEL ESTADO

PASTO SALUD E.S.E

NIT.900091143-9

PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACION

VERSION 8.0

SAN JUAN DE PASTO
2023

PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACION
PASTO SALUD E.S.E.

ACTUALIZO

WILLIAM MONTENEGRO GUEVARA
Profesional Universitario

San Juan de Pasto
2023

TABLA DE CONTENIDO

FORMATO 225 DEL 17 DE NOVIEMBRE DE 2023 5
CONTROL DE CAMBIOS 6
INTRODUCCIÓN 7
1. OBJETIVOS 8
1.1 OBJETIVO GENERAL 8
1.2 OBJETIVOS ESPECÍFICOS 8
1.3 ALCANCE 8
2. MARCO LEGAL 9
3. MANEJO DE CONTINGENCIA 10
3.1 EQUIPAMIENTO NECESARIO PARA LA CONTINGENCIA 10
3.2 ACTIVACIÓN DE LA CONTINGENCIA 10
3.2.1 Sistema de Registros clínicos de SIOS no responde: 11
3.2.2 No hay suministro eléctrico 11
3.2.3 Fallos en horarios nocturnos 12
3.2.4 Restablecimiento del sistema de información 12
3.2.5 Pruebas del Plan de Contingencia 12
3.2.6 Informe después de la prueba del Plan de Contingencia 13
4. ACTIVIDADES DESPUÉS DE UN DESASTRE 14
4.1 EVALUACIÓN DE DAÑOS 14
4.2 PREPARACIÓN DE ACTIVIDADES DEL PLAN DE ACCIÓN 14
4.3 EJECUCIÓN DE ACTIVIDADES 14
4.4 EVALUACIÓN DE LOS RESULTADOS 15
4.5 RETROALIMENTACIÓN DEL PLAN DE CONTINGENCIA 15
4.6 RETROALIMENTACIÓN DEL PLAN DE CONTINGENCIA 15
5. ANÁLISIS DE RIESGOS 16
5.1 CONDICIONES GENERALES 16
5.2 MATRIZ DE RIESGO 16
5.3 PLAN DE RESPALDO 18
6. PLAN DE EMERGENCIA INFORMÁTICO Y RECUPERACIÓN POR DESASTRES 20
6.1 SISTEMAS DE INFORMACIÓN 20
6.2 TIEMPO DE INACTIVIDAD O DOWNTIME 20
6.3 SISTEMAS DE INFORMACIÓN ACTIVOS 22
6.4 PROVEEDORES DE SERVICIOS DE CÓMPUTO Y COMUNICACIONES 23

6.5 COPIAS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN. 24
7. GESTIÓN DE INCIDENTES 25
7.1 OBJETIVOS 25
7.2 CUADRO DE ESCALAMIENTO 25
7.3 CUADRO NIVELES DE SERVICIOS 25
7.4 CUADRO DE NIVELES DE ATENCIÓN 26
8. PLAN DE CONTINGENCIA PARA LA PRESTACIÓN DEL SERVICIO 27
8.1 REPORTE 27
8.2 REGISTRO 27
8.3 COMUNICARSE CON OFICINA ASESORA COMUNICACIONES Y SISTEMAS 27
8.4 COMUNICARLE A TODOS LOS USUARIOS AFECTADOS 27
9. DESCRIPCIÓN DE LA ACTIVIDAD 28
9.1 REPORTE DEL PROBLEMA 28
9.2 PROCESO DE RECUPERACIÓN EN CASO DE INTERRUPCIÓN DEL SERVICIO 29
10. SIMULACRO PARA VERIFICAR LA EFICIENCIA Y EFECTIVIDAD DEL PLAN DE CONTINGENCIA. 32
11. LISTA DE VERIFICACIÓN PLAN DE CONTINGENCIA 33
12. CRONOGRAMA PARA LA EJECUCIÓN DEL PLAN 35
13. GLOSARIO 36
BIBLIOGRAFÍA

EMPRESA SOCIAL DEL ESTADO PASTO SALUD E.S.E

SOLICITUD DE CREACIÓN, MODIFICACIÓN Ó ELIMINACIÓN DE DOCUMENTOS Y REGISTROS

VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
8.0	GESTION DE SISTEMAS DE INFORMACION	GSI-MDR	225

PROCESO	PROCEDIMIENTO	TIPO DE DOCUMENTO
GESTION DE SISTEMAS DE INFORMACION	GESTION DE INCIDENTES DE INFORMACION	PLAN

NOMBRE DEL DOCUMENTO	CODIGO	FECHA	TIPO DE SOLICITUD
PLAN DE CONTINGENCIA DE SISTEMAS DE INFRMACIÓN	PL- CSI	17 de noviembre de 2023	MODIFICACION/ACTUALIZACION

CAUSAS DE(Creación, Modificación o eliminación)

De acuerdo a la auditoria interna de ISO-9001 realizada al proceso de Gestión de Sistemas de Información se encontró un hallazgo en la activación del plan de contingencia para el proceso de facturación donde ya no se hace uso de talonarios de facturas físicas en su lugar se utiliza el formato GF-GFE-340

DESCRIPCION DE LAS MEJORAS

SECCIÓN MODIFICADA AL DOCUMENTO	3.2 Activación de la contingencia	ACEPTADO	SI		NO	

NOMBRES Y APELLIDOS DE QUIEN ELABORÓ	NOMBRES Y APELLIDOS DE QUIEN REVISÓ (Líder de proceso o jefe inmediato de acuerdo a la estructura organizacional de la empresa)	NOMBRES Y APELLIDOS DEL (LA) GERENTE-APRUEBA
WILLIAM MONTENEGRO GUEVARA	ARVEY VALLEJO NARVAEZ	ANA BELEN ARTEGA TORRES

CARGO	PROFESIONAL UNIVERSITARIO	CARGO	JEFE OFICINA ASESORA DE COMUNICACIONES Y SISTEMAS	CARGO	GERENTE
FIRMA		FIRMA		FIRMA	

EL PRESENTE FORMATO ES IDENTICO AL ORIGINAL APROBADO LAS MODIFICACIONES AL FORMATO NO SON VÁLIDAS SIN APROBACIÓN (FIRMAS EN FORMATO ORIGINAL) OFICINA ASESORA DE PLANEACIÓN FECHA DE CREACIÓN Y/O ACTUALIZACIÓN 22-11-2022

VIGILADO Supersalud

CONTROL DE CAMBIOS

E: Elaboración del documento
M: Modificación del documento
X: Eliminación del documento

Versión	CONTROL DE CAMBIOS	INFORMACION DE CAMBIOS					Acto Administrativo de Adopción
		E	M	X	Actividades o Justificación del cambio	Elaboró / Actualizó	
8.0	Actualización del Plan de Contingencia de Sistemas de Información.		X		**Justificación:** De acuerdo a la auditoría interna de ISO-9001 realizada al proceso de Gestión de Sistemas de Información se encontró un hallazgo en la activación del plan de contingencia para el proceso de facturación donde ya no se hace uso de talonarios de facturas físicas en su lugar se utiliza el formato GF-GFE-340	William Montenegro Guevara Profesional Universitario	Solicitud de creación, modificación o eliminación de documentos o registros GSI-MDR-225 del 17 de noviembre de 2023
7.0	Actualización del Plan de Contingencia de Sistemas de Información.		**X**		**Justificación:** En cada vigencia es necesario mantener la actualización de este plan por cuanto las condiciones de tiempos y de infraestructura que se presentan son diferentes y se requiere mejorarlas. Se realizan mejoras en la redacción del documento.	William Montenegro Guevara Profesional Universitario	Solicitud de creación, modificación o eliminación de documentos o registros GSI-MDR-225 del 22 de junio de 2023
6.0	Creación Plan de Contingencia de Sistemas de Información.	**X**			**Justificación:** El presente documento se crea teniendo en cuenta el manual de acreditación versión 3.1 de acuerdo a los estándares de gerencia de la información y para dar cumplimiento a la normatividad del Ministerio de las TICS	William Montenegro Guevara	Solicitud de creación, modificación o eliminación de documentos o registros GSI-MDR-225 del 1 de Agosto de 2019

INTRODUCCIÓN

“El plan de contingencia de Sistemas de información de la Empresa Social del Estado Pasto Salud E.S.E, es un documento que establece los lineamientos de respuesta para atender en de manera oportuna, eficiente y eficaz, la indisponibilidad del servicio de las tecnologías de la información ocasionadas por daños en equipos de cómputo, desastres, eventos naturales u otros, a causa de algún incidente tanto interno como externo a tecnologías de información. Durante el desarrollo del presente Plan, se presentan las actividades propias de gestión de contingencia que debe considerar todas las sedes de Pasto Salud E.S.E, cubriendo así los incidentes que afecten el sistema de información. Así mismos aspectos conceptuales que permitan un mayor panorama acerca del entendimiento de las contingencias y que servirán como marco de referencia, para la elaboración de las políticas, normas y procedimientos de contingencia.

La elaboración del plan de contingencia implica un importante avance a la hora de superar situaciones de interrupción de las actividades y servicios prestados por Pasto Salud E.S.E. Es indispensable para el éxito del plan de contingencia, contar con personal capacitado y comprometido con la institución.”[1]

[1] https://docplayer.es/9448834-Manual-de-plan-de-contingencia-informatica.html

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Definir las acciones y procedimientos necesarios para garantizar la rápida, oportuna recuperación y puesta en operación de los sistemas de información y servicios informáticos que apoyan el cumplimiento de la misión de la entidad y los procesos administrativos, así como la protección de la integridad y confidencialidad de los datos de salud, mediante la implementación de medidas de prevención, respuesta y recuperación efectivas frente a la posible ocurrencia de incidentes de tipo Natural o tecnológico que comprometa total o parcialmente la prestación de los servicios informáticos de la Empresa Social del estado Pasto Salud E.S.E.

1.2 OBJETIVOS ESPECÍFICOS

- Identificar las aplicaciones y las plataformas consideradas críticas para la operación de la empresa.[2]

- Minimizar el tiempo de inactividad del sistema: Establecer medidas y procedimientos para reducir al mínimo el tiempo de inactividad del sistema de información en caso de fallos o interrupciones, asegurando una rápida restauración del servicio.

- Proteger la integridad de los datos de salud: Implementar mecanismos de respaldo y recuperación de datos para asegurar que la información de salud se mantenga íntegra y no se pierda en caso de incidentes o desastres.

- Realizar pruebas y simulacros periódicos: Programar y llevar a cabo pruebas regulares de contingencia para evaluar la efectividad del plan, identificar áreas de mejora y capacitar al personal en los procedimientos de respuesta ante emergencias.

- Capacitar al personal en el uso del plan de contingencia: Proporcionar formación y capacitación adecuadas a todo el personal de las sedes involucradas en el uso y ejecución del plan de contingencia, asegurando que estén preparados para actuar de manera efectiva en situaciones de crisis.

2 https://www.mintic.gov.co/gestionti/615/articles-5482_G10_Continuidad_Negocio.pdf

1.3 ALCANCE

El Plan de Contingencia de Sistemas de Información para Pasto Salud E.S.E., cubre la indisponibilidad del sistema de información y los recursos tecnológicos como infraestructura de telecomunicaciones y software y va desde la notificación de falla e indisponibilidad de los sistemas informáticos, su gestión y evaluación, hasta el restablecimiento de los servicios tecnológicos incluyendo personal encargado de administrar, mantener y utilizar los sistemas de información en salud, incluyendo al personal técnico, de TI y a los usuarios finales.

2. MARCO LEGAL

- Norma NTC-ISO 27001, Seguridad de la Información
- Decreto 2157 de 2017 - por medio del cual se adoptan directrices generales para la elaboración del plan de gestión del riesgo de desastres de las entidades públicas y privadas en el marco del artículo 42 de la ley 1523 de 2012.
- Ley 46 de 1988 - Se crea y organiza el Sistema Nacional para la Prevención y Atención de Desastres, artículo 3 numeral d) Los sistemas integrados de información y comunicación a nivel nacional, regional y local.
- Decreto Ley 919 de 1989, “Por el cual se organiza el Sistema Nacional para la Prevención y Atención de Desastres y se dictan otras disposiciones”, artículo 3 numeral d) Los sistemas integrados de información y comunicación a nivel nacional, regional y local.
- Guía Técnica Colombiana 202 de 2006, Sistema de Gestión de Continuidad del Negocio.

3. MANEJO DE CONTINGENCIA

Pasto Salud ESE, dispone de un sistema de información el cual integra toda la información de los procesos de apoyo y misionales, la información que se procesa en cada uno de estos módulos, se almacena en base de datos desde donde se recupera para su uso.

En la actualidad las actividades operativas desde cada puesto de trabajo hacen uso del sistema de información electrónico, para prestar los diferentes servicios administrativos y misionales y se pueden ver afectadas por cualquier interrupción de tipo técnico como caída de conectividad, daño en la infraestructura de hardware y software, así como fallas eléctricas, que hace que el sistema de información no funcione.

Que efecto tiene la indisponibilidad del servicio en el sistema de información:

Se podrían presentar una interrupción temporal en la prestación de los servicios y en las actividades diarias en las sedes, por cuanto no se dispone del sistema de información para registrar de manera automática los datos.

Es en este momento cuando la empresa debe disponer de un plan de contingencia de sistemas de información que le permita continuar con la prestación de los servicios misionales y administrativos sin que el usuario se vea afectado y en el menor tiempo posible sin interrumpir la prestación del servicio a los usuarios.

Lo que se espera es minimizar el impacto que pueda ocasionar la indisponibilidad del sistema de información sobre la prestación del servicio a los usuarios y sus familias.

3.1 EQUIPAMIENTO NECESARIO PARA LA CONTINGENCIA

Para el funcionamiento adecuado de este plan de contingencia es necesario determinar cuáles son los servicios más críticos que pueden verse afectados por indisponibilidad de servicios informáticos. A continuación, se establecen los servicios más críticos del área administrativa y asistencial, estos son:

- Facturación
- Servicio de consulta externa
- Servicio de urgencias
- Servicio de Hospitalización
- Imagenología.
- laboratorio clínico.

- servicio farmacéutico

Formatos o documentos Manuales

- TRIAGE URGENCIAS - GU-TU 031
- HISTORIA CLINICA DE URGENCIAS - GU-HCU 025
- HISTORIA CLINICA CONSUTLA EXTERNA - GA-HCE 341
- FORMATO ANEXO DE CERTIFICADO DE NACIDO VIVO Y ACTA DE DEFUNCIÓN
- FORMATO GF-GFE-340 (Registro de validación de datos para generación de factura electrónica)

3.2 ACTIVACIÓN DE LA CONTINGENCIA

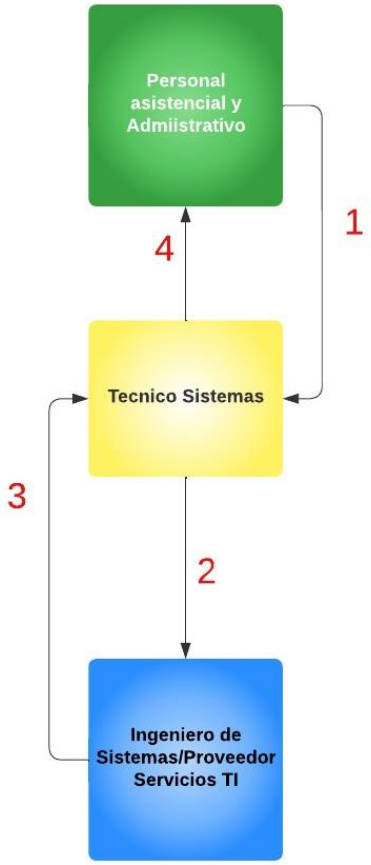
La activación del plan de contingencia se presenta de manera inmediata una vez se haya presentado la falla parcial o total en la infraestructura tecnológica y que impacte en el sistema de información. Hemos identificado las siguientes posibilidades como causas principales de fallo en los Sistemas de Información en los servicios de Facturación, Consulta externa, Hospitalización y Urgencias.

- Cortes de fluido eléctrico
- Caída de la conectividad red de datos
- Caída de la conectividad servicio de internet
- Daño en los servidores principales o máquinas virtuales del clúster del data center
- Daño de la base de datos
- Bloqueos de Switches

3.2.1 Indisponibilidad del Sistema de Información de Operaciones en Salud (SIOS):

Durante el proceso de atención de un usuario en cualquier servicio de salud, la persona que está registrando información en el registro clínico se da cuenta que al hacer clic en algún ítem o guardar los respectivos datos muestra un mensaje que informa que no se puede acceder al sitio en este caso cualquier registro clínico, administrativo y facturación. Este error efectivamente puede tener como causa las fallas en la infraestructura antes mencionadas.

Inmediatamente al no disponer de los servicios del sistema de información se activa la cadena de llamado la cual se describe a continuación:



LLAMADO No1

La personal asistencia y/o administrativo informan de manera verbal o vía grupo de WhatsApp al técnico en sistemas del incidente ocurrido.

El técnico en sistema primero verifica si el incidente ocurrido tiene la causa en la respectiva sede o es un daño generalizado. Si el daño es en la respectiva sede procede a resolver el incidente, de lo contrario debe notificar a aun segundo nivel en este caso al personal de ingenieros de la Oficina de TI de Pasto Salud o al Proveedor de conectividad. El llamado se lo hace vía telefónica o WhatsApp.

LLAMADO No 2

El profesional Universitario quien atiende el incidente, hace el diagnóstico en el data center con los servidores o red de datos. Si el problema está al alcance de esta mesa de ayuda lo resuelve de lo contrario lo transfiere al Proveedor externo para que se dé la solución.

En este llamado se define si el tiempo de restablecimiento va a superar más de los de los 10 minutos y por lo tanto se notifica que se active el plan de contingencia a las sedes afectadas, vía llamada telefónica o WhatsApp.

Para el caso del sistema de información RUAF en el aplicativo WEB RUAF- ND v2 la activación de la contingencia se realizará a partir de las 24 horas después de la indisponibilidad del aplicativo.

LLAMADO No3

Una vez se resuelve el incidente inmediatamente se notifica en el grupo de WhatsApp a los técnicos en sistemas para que puedan levantar el plan de contingencia y se continúe con el desarrollo normal de actividades en el sistema de información.

LLAMADO No4

Los técnicos en sistemas una vez reciban el llamado de restablecimiento del sistema envían una notificación a su personal para que se levante el plan de contingencia y se continúe realizando las actividades en el sistema de información.

3.2.2 Fallos en horarios nocturnos:

Cuando el fallo del sistema se presenta en horas de la noche entre las 7:00 PM y las 7: AM en cualquiera de las sedes que tienen servicio 24 horas. La enfermera jefa que se encuentra de turno en el servicio de urgencias iniciará la cadena de llamado al técnico de sistemas de cada sede, de allí en adelante la cadena de llamada se realiza en el mismo orden de como si se presentará durante el día.

Cada incidente deberá ser reportado en la plataforma ostickets para llevar el registro, realizar su gestión y evaluación de causas que lo originaron con el fin de establecer mejoras y evitar que estos eventos se presenten con frecuencia.

3.2.3 Restablecimiento del Sistema de Información:

Una vez restablecido el fallo del sistema, se debe retornar el paso inmediato a manejo en sistema electrónico.

Los registros clínicos, así como de facturación que fueron generados en la contingencia deberán ser ingresados al sistema de información por los responsables de los mismos.

3.2.4 Simulacro Plan de Contingencia:

El responsable de Seguridad de la Información, en coordinación con la Subgerencia de Salud y las direccione operativas, llevarán a cabo anualmente una prueba al plan por el sistema de simulación, prueba sobre la mesa con escenario de incidentes simulados, en el que se representa la situación de parada de los sistemas sin activar los procedimientos correspondientes. Se evaluará el conocimiento del plan de contingencia por parte del personal asistencial y administrativo de las sedes y se comprobará que en las ubicaciones donde se llevan a cabo la prestación de los servicios a los pacientes están dotadas adecuadamente de los formularios y/o formatos necesarios y el equipamiento previsto. Se generará un CheckList de verificación del simulacro del plan. La prueba la realizará personal de la Oficina de Comunicaciones y Sistemas, ingenieros de la red de prestadores quienes verificarán la integridad y precisión del plan, el conocimiento del personal implicado en la prueba respecto de los procedimientos y la coordinación entre los profesionales. El profesional de la Oficina de Comunicaciones y Sistemas evaluará los resultados y emitirá el informe correspondiente incluyendo las deficiencias detectadas en su caso y las recomendaciones oportunas, así como los planes de mejora cuando se requieran.

3.2.5 Informe después del simulacro del Plan de Contingencia:

Se realizará un informe donde se detallen todas las actividades y tiempos que fueron empleados en la realización de las pruebas, así como el % de efectividad del simulacro en las sedes aplicadas, que evalúa el conocimiento de la ejecución del plan por parte del personal, los tiempos de activación del plan.

Posteriormente se retroalimentará al personal de técnicos en sistemas de las sedes con el fin de analizar las situaciones del simulacro y los resultados que se obtuvieron y de paso establecer acciones de mejoras.

4. ACTIVIDADES DESPUÉS DE UN INCIDENTE O DESASTRE

Después de ocurrido un siniestro o desastre es necesario realizar actividades que se detallan a continuación:

a) Evaluación de daños
b) Priorizar actividades el plan de acción
c) Ejecución de actividades
d) Evaluación de resultados
e) Retroalimentación del plan de acción

4.1 EVALUACIÓN DE DAÑOS

Inmediatamente después que el siniestro ha concluido, se debe evaluar la magnitud del daño que se ha producido, que sistemas y equipos se afectaron, que tecnología quedo no operativa, cuales se pueden recuperar y en qué tiempos.

Adicionalmente se deberá presentar un informe muy detallado de lo ocurrido a la gerencia.

4.2 PREPARACIÓN DE ACTIVIDADES DEL PLAN DE ACCIÓN

Se deben planear acciones urgentes y prioritarias teniendo en cuenta la prestación del servicio.

4.3 EJECUCIÓN DE ACTIVIDADES

La ejecución de actividades implica la creación de grupos de trabajo para realizarlas actividades previamente planificadas en el Plan de Acción.

El Jefe de la Oficina de Comunicaciones y Sistemas, será quien lidere el plan de acción con el o los equipos de trabajo que se requieran. En caso de presentarse algún problema, debe reportarse de forma inmediata al líder.

Los trabajos de recuperación tendrán dos etapas.

- Restauración haciendo uso de los recursos de la empresa incluido el talento humano.
- Restauración haciendo uso de asesoría técnica experta si el problema es más complejo y no se dispone del conocimiento del tema.

4.4 EVALUACIÓN DE LOS RESULTADOS

Una vez concluida las labores de recuperación de (los) sistema(s) que fueron afectados, por el siniestro, debemos evaluar objetivamente, todas las actividades realizadas, que tan bien se hicieron, qué tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades del plan de acción, como se comportaron los equipos de trabajo etc.

De la evaluación de los resultados y del siniestro en sí, deberían salir dos tipos de recomendaciones, una la retroalimentación del plan de contingencia y otra una lista de recomendaciones para minimizar los riesgos y perdida que ocasionaron el siniestro.

4.5 RETROALIMENTACIÓN DEL PLAN DE CONTINGENCIA

Con la evaluación de resultados, se debe optimizar el plan de acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente.

El otro elemento es evaluar cuál hubiera sido el costo de no haber tenido nuestra institución el plan de contingencia llevado a cabo.

4.6 RETROALIMENTACIÓN DEL PLAN DE CONTINGENCIA

Implementación

En la fase de implementación se recomienda que debe ser prioridad el despliegue del plan de contingencia a todo el personal administrativo y asistencial que se vea involucrado y que se vean afectados por el incidente. Dentro de esta etapa se debe preparar muy bien al personal de acuerdo a los lineamientos establecidos en dicho plan.

Monitoreo y Evaluación

La fase de evaluación y monitoreo nos dará de alguna manera la seguridad con la que se pueda reaccionar en el tiempo esperado y con la acción correcta. Se debe lograr crear cultura en el personal ante una eventualidad de amerite activar un plan de contingencia, para ello se debe preguntar al personal cual es el momento en que se activa el plan, cual es la cadena de llamado que se debe seguir y cuáles son las actividades de su competencia dentro del plan.

5. ANÁLISIS DE RIESGOS(1)

5.1 CONDICIONES GENERALES

Para el actual análisis de riesgos realizado se tuvieron en cuenta los siguientes criterios generales que aplican para cualquier sistema de información de Pasto Salud E.S.E.

TIPO DE RIESGO	FACTOR DE RIESGO	PREVENCIÓN Y MITIGACIÓN
"El Fuego: destrucción de equipos y archivos.	Bajo	Extintores, aspersores automáticos, detectores de humo, pólizas de seguros.
El robo común: pérdida de equipos y archivos.	Medio	Seguridad Privada, Alarma, Seguro contra todo riesgo y copias de respaldo (BackUp)
El vandalismo: daño a los equipos y archivos	Medio	Seguro contra todo riesgo, copias de respaldo.
Fallas en los equipos: daño a los archivos	Medio	Mantenimiento, equipos de respaldo, garantía y Copias de respaldo.
Equivocaciones: daño a los archivos.	Bajo	Capacitación, copias de respaldo, políticas de Seguridad.
Acción de Virus: daño a los equipos y archivos	Alto	Actualizaciones del sistema operativo, Antivirus Actualizados, copias de respaldo.
Desastres naturales: destrucción de equipo y archivos	Bajo	Seguro contra todo riesgo, copias de respaldo. Las sedes cumplen con las normas Antisísmicas.
Accesos no autorizados: filtrado no autorizado de datos	Bajo	Cambio de claves de acceso mínimo cada seis Meses. Política de seguridad para acceso a personal competente.
Robo de datos: difusión de datos sin el debido cubrimiento de su costo.	Bajo	Cambio de claves de acceso mínimo cada seis meses, custodia de las copias de respaldo.
Fraude: modificación y/o desvío de la información y fondos de la institución.	Bajo	Sistemas de información seguros con dos usuarios para autorizar transacciones, procedimiento de control y registro de transacciones en tablas de auditoría."[3]

5.2 MATRIZ DE RIESGO

La Oficina Asesora de Comunicaciones y Sistemas cuenta con el matriz de riesgos con el fin de recolectar en forma sistemática y organizada los datos relacionados con los factores de riesgo existentes y de esta manera planificar las medidas de prevención y control de manera adecuada y oportuna. Ver Anexo 1: Matriz de Riesgos – Gestión de Sistemas de Información.

Del análisis de detallado de riesgos, se dispondrá de información suficiente, para proponer diferentes medidas de prevención y recuperación que se adapten a las necesidades de la organización. La prevención frente a riesgos genéricos y poco probables puede ser muy costosa y no estar siempre justificada, sin embargo, las medidas preventivas o de recuperación frente a riesgos específicos pueden resultar sencillas, de rápida implementación y relativamente baratas

3 https://iderf.gov.co/wp-content/uploads/2020/10/PLAN-DE-CONTINGENCIA-Y-POLITICAS-DE-SEGURIDAD-DE-SISTEMAS-DE-INFORMACION.pdf

5.3 PLAN DE RESPALDO

A continuación, se presenta las actividades que se deben realizar con el objeto de prever, mitigar o eliminar los riesgos conocidos para Pasto Salud ESE.

No	ACTIVIDAD	ELEMENTOS	LUGAR Y RESULTADO
1	Copias de seguridad de la información y Documentos existentes en los discos duros de los computadores de todas las áreas Pasto Salud y copias de seguridad en los servidores de backup de cada rede operativa como sede administrativa, lo cual se estipula en el Procedimiento de Gestión de Copias de Seguridad GSI-PD 119.	Documentos en formatos Word, Excel, PDF, PowerPoint, imágenes, audio y archivos de correos electrónicos.	Copias de seguridad realizadas por parte de cada usuario responsable de la producción de la información.
2	Copias de seguridad de los sistemas de Información y Bases de Datos de Pasto Salud, lo cual se estipula en el Procedimiento de Gestión de Copias de Seguridad GSI-PD 119.	Bases de datos del motor de base de datos SQLSERVER como SIOS, Génova, Nomina, BDCALIDAD, BD_HVEQUIPOS, contratistasSoporteDIAN, BD_LAVADOMANOS, BD_FINANCIERA, FACTURASPT, FUID (Formato Único de Inventario Documental). Base de datos del motor de base de datos Postgresql para ORFEO (Sistema de información de gestión documental)	Programación de Copias de seguridad así: - SIOS: 1 Copia Full el fin de semana y 2 copias diarias diferenciales en la tarde y noche respectivamente - GENOVA: 1 Copia Full el fin de semana y 2 copias diarias diferenciales en la tarde y noche respectivamente - NOMINA: 1 Copias Full el fin de semana y 1 copia Diaria diferencial en la noche - ORFEO: 2 copias Full diarias en la mañana y tarde de lunes a viernes - BDCALIDAD: 1 copia Full diaria - BD_HVEQUIPOS: 1 copia Full semanalmente los lunes, miércoles, viernes - ContratistaSoporteDIAN: 1 copia Full semanalmente de lunes a viernes - BD_LAVADOMANOS: 1 copia Full diaria - BD_FINANCIERA: 1 copia Full mensual - FACTURASPT: 1 copia Full semanalmente los lunes, miércoles, viernes - FUID: 1 copia Full semanalmente de lunes a viernes

No	ACTIVIDAD	ELEMENTOS	LUGAR Y RESULTADO
3	Contar mínimo con un kit de instalación para restaurar los archivos del sistema operativo y aplicaciones de un computador o servidor en caso de falla o virus.	-Sistema operativo (Windows 10/11) -Paquetes de ofimática. (Office Standard, Office Profesional) -Bases de datos (Sql Server Standard, etc.) -Drivers y utilitarios de impresoras, tarjetas de red, computadores, etc.	Carpeta compartida donde se almacenan copias de los originales del licenciamiento de Pasto Salud ESE Responsable: Profesional U Sistemas y Técnicos IPS
4	Mantener pólizas de seguros vigentes, asegurando por el valor real, contra todo riesgo los equipos y bienes	Equipos eléctricos y/o electrónicos, móviles, portátiles, software y equipos de comunicación.	Póliza vigente contra todo riesgo de daño y/o pérdida Física por cualquier causa. Responsable: secretaria general
5	Mantenimientos, revisiones preventivas y correctivas de equipos de computación y comunicación, extintores, alarmas y sistemas contra incendio, para mantenerlos en óptimas condiciones.	Equipos de computación y comunicación periféricos, sistemas eléctricos UPS, Aire acondicionado, Alarmas, Sistemas contra incendio, Extintores, reglamento del edificio.	Contratos anuales de mantenimiento preventivo y correctivo, garantías vigentes, control del mantenimiento de los equipos. Responsable: Supervisor de contrato de mantenimiento.
6	Actualizar las claves o contraseña de acceso a las aplicaciones y bases de datos de los sistemas de Pasto Salud.	Base de Datos, y sistema de Información SIOS.	Mínimo cada 90 días como política del directorio activo, para el ingreso al sistema operativo. Cada tres meses se valida a usuarios que no a interactuado con el sistema de información SIOS y se los bloquea Responsable: Todos los funcionarios de la Entidad que manejen sistemas de información y Profesional Universitario.

6. PLAN DE CONTINGENCIA INFORMÁTICO Y RECUPERACIÓN POR DESASTRES(2)

Cuando ocurra un desastre, es esencial que se conozca al detalle el motivo que lo originó y el daño producido para permitir recuperar en el menor tiempo posible el proceso perdido. Los procedimientos de recuperación y verificación son de ejecución obligatoria y bajo la responsabilidad de los encargados de la realización de los mismos. En estos procedimientos están involucrados todos los funcionarios de la Oficina Asesora de Comunicaciones y Sistemas de Pasto Salud ESE.

Las actividades previas a la ocurrencia de un desastre o falla son aquellas relacionadas con la planeación, preparación, entrenamiento y ejecución de actividades de resguardo de la información, que aseguren un proceso de recuperación con el menor costo posible para Pasto Salud. En la fase de planeación se debe tener la siguiente información disponible para proceder.

6.1 SISTEMAS DE INFORMACIÓN

Se identifican los Sistemas de Información con los que cuenta Pasto salud ESE, tanto los desarrollados por el área de sistemas como los contratados por la entidad con otras empresas.

6.2TIEMPO DE INACTIVIDAD O DOWNTIME

El término tiempo de inactividad (downtime) es usado para definir cuando los sistemas de información o hardware no están disponible (solo para servidores). Los casos DOWNTIME pueden ser planeados o no planeados. Los casos de tiempos de inactividad en servidores planeados pueden ser por mantenimiento, cambio de sistema operativo, recuperación de bases de datos, reconfiguración de los sistemas o reinicio de servicios. Los casos de tiempos de inactividad no planeadas pueden ser provocados por fallas del sistema, daño en los servidores, fallas de la red de datos, fallas en el fluido eléctrico

No	Criticidad	Nombre del sistema	Lenguaje de Desarrollo	Áreas y Procesos	No de Usuarios Conectados a la Base de Datos	Equipamiento mínimo de funcionamiento	Actividades de recuperación	Tiempo de recuperación máximo
1	Alta	SIOS (Sistema de Operaciones en Salud)	Visual.Net	Todas las áreas y procesos de la organización	390 usuarios concurrentes	Máquina Virtual, SO Windows 2008 Server Standard, Memoria 128 Gigas, DD 500 gigas.	1.Recuperación Máquina virtual 2.Recuperación de la Base de Datos	8 horas
2	Media	ORFEO	PHP	Todas las áreas y procesos de la organización	229 usuarios	Máquina Virtual, SO Linux Standard, Memoria 8 Gigas, DD 500 gigas.	1.Recuperación Máquina virtual 2.Recuperación de la Base de Datos	1 hora
3	Alta	Correo Electrónico		Todas las áreas y procesos de la organización	272 cuentas	Google	Recuperacion Google	1 hora.
4.	Media	OsTicket	PHP	Todas las áreas y procesos de la organización	32 usuarios	CloudLinux 6 64 bit	1. Restauración de la base de datos. 2. Restauración de la página de la aplicación.	1 horas.

6.3 SISTEMAS DE INFORMACIÓN ACTIVOS

INFRAESTRUCTURA TECNOLÓGICA Y DE COMUNICACIONES

No	Criticidad	EQUIPO	Áreas y Procesos	Equipamiento mínimo de funcionamiento	Actividades de recuperación	Tiempo de recuperación máximo
1	Alta	SERVIDORES	Todas las áreas y procesos de la organización	Servidor SO Windows 2008 Server Enterprise, HyperV Memoria 128 Gigas, DD 500 gigas.	Notificar a almacén y hacer valida la garantía Remplazo Servidor por un alterno (MV)	24 horas

No	Criticidad	EQUIPO	Áreas y Procesos	Equipamiento mínimo de funcionamiento	Actividades de recuperación	Tiempo de recuperación máximo
2	Media	COMPUTADORES	Sede Administrativa	Equipo SO Windows 7, 2 Gigas, DD 70 Gigas, Monitor, Mouse, Teclado.	Notificar a almacén y hacer valida la garantía Reparar equipo, reportar a tercero	24 horas
3	Alta	COMPUTADORES	Historia Clínica, facturación	Equipo SO Windows 7, 2 Gigas, DD 70 Gigas, Monitor, Mouse, Teclado.	Notificar a almacén y hacer valida la garantía Reparar equipo, reportar a tercero	24 horas
4	Alta	IMPRESORAS	Facturación	Monocromática, Trabajo en Red	Notificar a tercero para remplazar Impresora	2 horas
5	Media	IMPRESORAS	Otros Procesos administrativos	Monocromática, Trabajo en Red	Notificar a tercero para remplazar Impresora.	24 horas
6	Alta	INTERNET	Todas las áreas y procesos de la organización	500 megas enlaces inalámbricos	Reportar incidente tercero	10 minutos después del reporte de caída
7	Alta	CANAL DE DATOS	Todas las áreas y procesos de la organización	50 MBPS Enlaces Inalámbricos	Reportar incidente tercero	10 minutos después del reporte de caída

6.4 PROVEEDORES DE SERVICIOS DE CÓMPUTO Y COMUNICACIONES

No	Empresa Contratista	Contacto Técnico	Objeto Contractual	Vigencia Contrato	Estado del Contrato
1	SISTEMAS PALACIOS	INGENIERO JESUS RUIZ 310 8669682	Prestación del servicio de conectividad y fibra óptica de las IPS urbanas y rurales proveer y configurar los dispositivos necesarios para garantizar la seguridad perimetral entre las IPS y la Sede Central.	01 de febrero al 31 de diciembre de 2023.	Activo
2	SOPHOS INFORTEC	JHON JAMIOY	Soporte técnico herramienta de seguridad Antivirus edpoint	01 de enero al 31 de diciembre	Activo

No	Empresa Contratista	Contacto Técnico	Objeto Contractual	Vigencia Contrato	Estado del Contrato
3	BIOELECTROMEDICAL	CAROLINA GOMEZ 301 4361627	Prestación de servicio de mantenimiento preventivo y correctivo de equipos de Informática, UPS y equipos de comunicaciones	01 de enero al 31 de diciembre de 2023.	Activo
4	COPYRENT	JOSE FERNANDO SANCHEZ ORTIZ Cel. 300 3164632	Prestación de servicio de arrendamiento de impresoras	01 de enero al 31 de agosto de 2023	Activo
5	TELEFÓNICA MOVISTAR	Líneas de atención al cliente 018000910909 móvil: #600	Prestación de servicio telefónico fijo y móvil	01 de enero al 31 de diciembre de 2023.	Activo
6	DONGEE	Mesa de Ayuda On-line Web Bogotá: Calle 59 8-21 of M01 +57 6013819002 manager.dongee.com/	Prestar el servicio de alojamiento de la página web institucional Hosting.	01 de enero al 31 de diciembre de 2023.	Activo
7.	NUVA	Mesa de soporte: https://soporte.nuva.co/portal/es/signin	Prestar el servicio de soporte de correo electrónico institucional.	01 de enero al 31 de diciembre de 2023.	Activo
7.	DITEC DE COLOMBIA	JHON VELASQUEZ DAVILA 3117131418 - 3153455865	Prestación del servicio de uso y goce del Espectro Radio Eléctrico, en modalidad de mono canal de voz y repetidor digital.	01 de enero al 31 de diciembre de 2023.	Activo

6.5 COPIAS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN.

Las copias de seguridad tienen por objeto proveer el respaldo de la información actualizada a cada sistema de información de acuerdo con os siguientes criterios.

No	ACTIVIDAD	FRECUENCIA	RESPONSABLES	MEDIDAS DE CONTROL
1	Copias de seguridad de la información y documentos residentes en los discos duros de los computadores de todas las áreas Pasto Salud. Documentos en formatos Word, Excel, PDF, PowerPoint, imágenes, audio y archivos de correos electrónicos.	**Periodo:** Copias de seguridad diarias: -Sios: 1 Full fin de semana y 2 diarias -Génova: 1 Full fin de semana y 2 diarias -Nomina: 1 diaria -Orfeo: 2 Diaria de lunes a viernes Array5 Unidad E y Array1 Unidad G Servidor 192.168.10.9 Copias de Documentos del personal: **Medio:** Unidad de Almacenamiento 192.168.10.206 **Nota:** El usuario es responsable de guardar los archivos en la carpeta de red asignada a cada usuario del directorio activo.	Funcionarios y contratistas de Pasto Salud ESE. Profesionales Universitarios Sistemas. Técnicos sistemas Contratistas	Verificación anual De los procedimientos establecidos.

7. GESTIÓN DE INCIDENTES

7.1 OBJETIVOS

- Detectar cualquiera alteración en los servicios TI.
- Registrar y clasificar estas alteraciones en la plataforma habilitada para este fin (osTicket).
- Informar al tercero o asignar el personal encargado de restaurar el servicio.

Los funcionarios de Pasto Salud ESE pueden reportar un problema presentado en la infraestructura tecnológica y física de manera electrónica a través de la plataforma osTicket.

Una vez se registra la solicitud en el sistema se inicia un proceso de escalamiento de acuerdo a los siguientes niveles establecidos.

7.2 CUADRO DE ESCALAMIENTO

Nivel	PUNTO DE ESCALAMIENTO
1	Técnicos Contratistas
2	Administrador del sistemas Ingeniero de Sistemas Soporte SIOS Profesional Universitario
3	Proveedor de servicios

7.3 CUADRO NIVELES DE SERVICIOS

No	Descripción General del Problema	Nivel de servicios requeridos
1	Denegación de servicios por fallas del software o conectividad que afecten de forma general el sistema que impida el acceso a los servicios con impacto significativo operacional, entre un 90% al 100% de los usuarios. PRIORIDAD DE SOLUCIÓN ALTA.	Nivel 1: 1 hora Nivel 2: 2 hora Nivel 3: Entre 1 y 4 horas
2	Degradación de servicios por fallas sobre las estructuras de datos, hardware, comunicaciones y software que NO impide por completo el acceso a los servicios con impacto operacional medio-alto, entre un 30% y un 90% de los usuarios. PRIORIDAD DE SOLUCIÓN MEDIA.	Nivel 1: 3 horas Nivel 2: 3 horas Nivel 3: 8 horas
3	Degradación de servicios por fallas sobre las estructuras de datos, hardware, comunicaciones y software que NO impide por completo el acceso a los servicios con impacto operacional medio-alto, entre un 1% y un 30% de los usuarios. PRIORIDAD DE SOLUCIÓN BAJA.	Nivel 1: 8 horas Nivel 2: 12 día Nivel 3: 24 horas

El tiempo de solución establecido en el anterior cuadro de niveles de servicio, según la prioridad y niveles de escalamiento, corresponde al tiempo transcurrido entre la comunicación oficial del problema y la solución del problema en el cuarto de máquinas de cada sede o Sede Administrativa.

7.4 CUADRO DE NIVELES DE ATENCIÓN

Nivel	NIVEL DE ATENCION
1	**ATENCION PRIORITARIA**: Sistemas de información y equipos que requieran alta disponibilidad de atención a los usuarios externos y manejen alto volumen de información. (Sios, Radicación y correspondencia, Conectividad, Impresoras de facturación, equipos de historia clínica y facturación.
2	**ATENCION NORMAL:** Sistemas de información y equipos no relacionados con la atención a los usuarios y manejen bajo volumen de información. (Impresoras, equipos de áreas administrativas sede central, sistemas que no requirieran Conectividad y que cuenten con mayor plazo para la consulta y disponibilidad de información,

PLAN DE CONTINGENCIA PARA LA PRESTACIÓN DEL SERVICIO

Los funcionarios y personal contratista de Pasto Salud deben continuar con la prestación del servicio a los usuarios externos en caso de que ocurra una interrupción del servicio en los sistemas de información administrativos y asistenciales, para ello se deben tener en cuenta las siguientes consideraciones:

8.1 REPORTE

Reportar el incidente al área de sistemas en primera instancia a través de la plataforma, en caso de no tener el servicio de internet, se deberá realizar de manera telefónica.

8.2 REGISTRO

Para el caso de los procesos que tienen mayor impacto en el tiempo de atención al usuario, como facturación y registros clínicos, se requiere realizar de manera manual el registro de la facturación y diligenciamiento de los registros clínicos. Una vez de restablezca el servicio se deberá ingresar los registros clínicos y la facturación al sistema SIOS.

8.3 COMUNICARSE CON LA OFICINA ASESORA DE COMUNICACIONES Y SISTEMAS

En caso de no tener red de Internet, servicio de electricidad, los responsables de cada oficina deben comunicarse con el personal de la Oficina Asesora de Comunicaciones y Sistemas.

8.4 COMUNICARLE A TODOS LOS USUARIOS AFECTADOS

Una vez resuelta la falla se debe informar vía plataforma electrónica, correo electrónico o comunicado vía Spark o el medio que en ese momento esté disponible a todos los usuarios afectados.

9. DESCRIPCIÓN DE LA ACTIVIDAD

9.1 REPORTE DEL PROBLEMA

No	Nombre de la actividad	Descripción	Responsable
1	Comunicar el problema o falla.	El funcionario o contratistas del sistema identifican el problema o falla del sistema de información y comunican de forma inmediata, abriendo un ticket en la plataforma dispuesta para ello o telefónicamente los pormenores del caso. El ticket debe contener un resumen del problema y el detalle de la falla presentada puede ir acompañada de toda información adicional como imágenes de pantallazos necesarios para identificar el problema.	Funcionario o contratista del área de sistemas asignado para solución y seguimiento del reporte.
2	Analizar y evaluar el problema o falla. Diagnóstico	El ingeniero o técnico a quien se le haya asignado el caso mediante ticket numerado realizará la verificación, análisis y evaluación de los mismos, los soluciona si está a su alcance, y realiza la comunicación al interesado; de lo contrario, escala el caso.	Funcionario o contratista del área de sistemas asignado para solución y seguimiento del reporte.
3	Escalar y gestionar la solución del problema	El profesional Universitario o Técnico de sistemas abre el caso en el sistema de tickets para reporte, seguimiento y control de la solución del problema. Se categoriza el problema de acuerdo con la prioridad y se escala al responsable de acuerdo con el nivel de servicio del numeral 5.1. Si el problema va a ser solucionado por personal externo a la entidad se debe asignar el respectivo ticket al proveedor responsable del servicio solicitado.	Funcionario o contratista del área de sistemas asignado para solución y seguimiento del reporte.
4	Ejecutar pruebas	Después del diagnóstico, si se encuentra solución, se implanta la misma y se recupera la operación normal de lo contrario se escala al siguiente nivel y se verifica nuevamente el problema hasta encontrar la solución. Para los casos que requieran realizar pruebas, Se realizan pruebas para verificar la efectiva solución, luego se implementa en el ambiente de producción. Se realiza seguimiento y monitoreo durante un periodo de tiempo hasta que se vuelva a presentar, si no vuelve a presentarse se cierra el problema y se hace reapertura si es necesario. Una vez solucionado el problema se responde el ticket con la descripción de la solución del problema, fecha, responsable. Se envía la comunicación de la solución al funcionario que reportó el problema y a las partes interesadas del proceso, para verificación de la solución.	Funcionario o contratista del área de sistemas asignado para solución y seguimiento del reporte.
5	Verificar solución y período de prueba.	Los funcionarios usuarios del sistema deben verificar que la solución dada sea satisfactoria durante un período no superior a dos días, de lo contrario comunicarán al área de sistemas la inconformidad para la reapertura del caso y se devuelve a la actividad 4. Si los usuarios no presentan ninguna observación durante el período de prueba, se entiende por recibida a satisfacción la solución del problema.	Todos los funcionarios usuarios de sistemas de información de Pasto salud

No	Nombre de la actividad	Descripción	Responsable
6	Cerrar el caso	Se cierra el caso, una vez finalizado el tiempo de prueba o si existe recibo a satisfacción por parte de los usuarios del sistema sobre la solución dada.	Funcionario o contratista del área de sistemas asignado para solución y seguimiento del reporte
7	Fin del procedimiento		

9.2 PROCESO DE RECUPERACIÓN EN CASO DE INTERRUPCIÓN DEL SERVICIO.

No	Nombre de la actividad	Descripción	Responsable
1	Comunicar la falla	Los funcionarios de Pasto Salud ESE tienen la responsabilidad de comunicar de forma inmediata, por cualquier medio de comunicación disponible, al área de sistemas la interrupción parcial o total del servicio de un sistema de información y/o comunicación de la Entidad	Todos los funcionarios usuarios de sistemas de información de Pasto salud.
2	Iniciar plan de recuperación.	Los ingenieros de sistemas de Pasto Salud ESE realizarán pruebas preliminares para constatar la veracidad del incidente y constatar la suspensión total o parcial del servicio del sistema de información. En principio se deben tomar en cuenta los siguientes aspectos del plan de emergencias: 1. Evaluación del impacto y urgencia de la situación del desastre en la infraestructura de los sistemas de información y/o Comunicación. 1. Asignación de funciones de emergencia a los funcionarios del área de sistemas. 2. Verificación de disponibilidad de recursos para la contingencia como: manuales técnicos de instalación del sistema de información, almacenamiento de datos, sistemas eléctricos, comunicación, hardware y copias de seguridad. 3. Comunicación a los usuarios de la interrupción o degradación del servicio indicando el tiempo estimado de restablecimiento del servicio si se puede determinar. 4. Procedimiento de contacto y colaboración con los proveedores involucrados.	Funcionario del área de sistemas asignado para la recuperación y seguimiento de la solución.

No	Nombre de la actividad	Descripción	Responsable
3	Ejecutar el plan de recuperación .	Si el sistema se encuentra funcionado parcialmente y es posible realizar una copia de seguridad, se suspende el servicio para que los usuarios no registren más transacciones y se realiza la copia de seguridad. El responsable asignado ejecuta los siguientes pasos para la recuperación del sistema de acuerdo al nivel de la falla: 1. Instalación y puesta a punto de un equipo de cómputo compatible y hardware necesarios para la instalación del sistema de información con las características mínimas exigidas. 2. Instalación y configuración del sistema operativo, drivers y servicios necesarios para el funcionamiento del sistema de información a recuperar. 3. Instalación y configuración del sistema de información y el motor de la base de datos y niveles de seguridad. 4. Instalación de aplicaciones adicionales necesarias para el funcionamiento del sistema de información. 5. Realización del procedimiento restauración de la base de datos con la última copia de seguridad disponible de acuerdo al procedimiento de restauración establecido: Copia completa y la última diferencial. 6. Reiniciación del servicio, prueba y afinamiento del sistema de información. 7. En un horario de baja demanda de tráfico en la red y servicios, se realiza la recuperación de otras aplicaciones y actualizaciones que no influyen directamente en el funcionamiento del sistema de información recuperado. 8. Si el equipo de cómputo no requiere cambiarse por fallas técnicas de hardware y se cuenta con una copia en el disco duro, únicamente es necesario restaurar la copia de seguridad de la información, sin realizar los pasos del 1 al 4. 9. Para los sistemas de información web únicamente se requiere copiar la carpeta donde se encuentra el software ejecutable y actualizar la carpeta de la base de datos con el último backup automático almacenado en el disco duro. De acuerdo con la complejidad y especialidad del sistema de información de la Entidad, o si la actividad 4 no ha sido satisfactoria, se debe escalar y determinar el nivel de servicio de acuerdo a los cuadros del numeral 5.1	Funcionario o contratista del área de sistemas asignado para la recuperación y seguimiento de la solución.
4	Comunicar el restablecimiento del servicio.	Una vez puesta en marcha y funcionamiento el sistema de información, se comunica a los usuarios del mismo usando el medio de comunicación más masivo. Se realiza un seguimiento en las primeras dos horas sobre el comportamiento y rendimiento del sistema para verificar su correcto funcionamiento. Se lleva a cabo una solicitud de opinión o encuesta sobre del funcionamiento del sistema de información, como retroalimentación para el cierre del proceso.	Funcionario o contratista del área de sistemas asignado para la recuperación y seguimiento de la solución.
5	Cerrar el proceso de recuperación en caso de contingencia	Se cierra el proceso, una vez finalizado el período de seguimiento y no exista ninguna observación por parte de los usuarios.	Funcionario del área de sistemas asignado para la recuperación y seguimiento de la solución.

10. SIMULACRO PARA VERIFICAR LA EFICIENCIA Y EFECTIVIDAD DEL PLAN DE CONTINGENCIA

No	Nombre de la actividad	Descripción	Responsable
1	Planificar simulacro plan de contingencia	1. Realizar la programación anual del simulacro de recuperación de los sistemas de información. 2. Difusión y actualización de los planes de prevención y recuperación de sistemas. 3. Capacitación específica sobre los diferentes procedimientos de prevención y recuperación, dentro del proceso de inducción a los funcionarios nuevos que ingresan a la Entidad. 4. Verificación de disponibilidad de manuales o guías técnicas actualizadas para la instalación de sistemas de información. 5. Disponibilidad de recursos informáticos para habilitar el servicio de un sistema de información en el menor tiempo posible.	Profesional responsable del área de sistemas
2	Preparar recursos para el simulacro de recuperación.	Los funcionarios de la Oficina de Comunicaciones y Sistemas de Pasto Salud ESE verifican la disponibilidad de los recursos o requerimientos mínimos para la ejecución del simulacro: 1. Disponibilidad de recursos para la contingencia como: Manuales o guías técnicas de instalación del sistema de información, almacenamiento de datos, sistemas eléctricos, comunicación, de hardware, y copias de seguridad. 2. Disposición de equipos de cómputo (servidor o computador) con las características técnicas mínimas para la instalación y recuperación del sistema de información. 3. Verificación de disponibilidad de los proveedores o contratista involucrados para el soporte en caso de requerirse.	Profesional responsable del área de sistemas.
4	Ejecutar el simulacro del plan de contingencia.	Se ejecuta el procedimiento del simulacro realizando el procedimiento descrito en la actividad 4 del numeral 7.2 “Ejecutar el plan de recuperación” para verificar la eficiencia, eficacia y efectividad del plan de contingencia correspondiente a cada sistema de información. En esta fase hay que tener muy presente que el plan no busca resolver la causa del problema, sino asegurar la continuidad de las tareas críticas de la Entidad.	Profesional responsable del área de sistemas.
5	Realizar pruebas	Se realizan las pruebas pertinentes para intentar valorar el impacto real de un posible problema dentro de los escenarios establecidos como posibles. En caso de que los resultados obtenidos difieran de los esperados, se devuelve a la actividad anterior para verificación, e inicia nuevamente la prueba. El adecuado conocimiento por parte de los participantes del plan de contingencia y la documentación técnica de los sistemas de información, ayudarán a identificar las posibles carencias del plan. Una vez finalizado el plan, se elabora un acta que contenga los resultados de su ejecución cuyas conclusiones servirán para elaborar los planes de mejoramiento al sistema de atención de contingencias.	Profesional responsable del área de sistemas

11. LISTA DE VERIFICACIÓN PLAN DE CONTINGENCIA

No	ACTIVIDAD	OFICINA	RESULTADO	SI	NO	OBSERVACIONES
1	Copias de seguridad de la información y documentos de los discos duros de los computadores de Pasto Salud ESE.(Documentos en formatos Word, Excel, Power Point, audio y correos electrónicos)		Se encuentran disponibles las copias de seguridad de los archivos y documentos de los usuarios en la carpeta de cada usuario en la unidad de almacenamiento 192.168.10.20	X		
2	Copias de seguridad de los sistemas de información y bases de datos de Pasto Salud ESE.		Se encuentra disponible una copia de seguridad mensual para la vigencia actual de las siguientes bases. 1. SIOS 2. Génova. 3. Nomina 4. Orfeo En el servidor central y la unidad 192.168.10.79	X		
3	Contar mínimo con un kit de instalación para restaurar los archivos del sistema operativo y aplicaciones de un computador o servidor en caso de falla o virus.		Se encuentra disponible un KIT de instalación para cada uno de los siguientes productos y periféricos en la oficina de Pasto Salud ESE. 1. Sistema Operativo Windows XP, Vista, Windows seven, 2008 Server standard 2. Sql Server 2008 R2 3. Drivers para Impresora Epson FX 1170DN 4. Microsoft Office Estándar Edition y Profesional.	X		
4	Mantener descentralizados Los servicios que requieren restauración inmediata.	Todas las oficinas de Pasto Salud ESE.	Pasto Salud ESE tiene los servicios de Directorio activo y IIS, Máquinas virtuales de Sql Server, y ¿y Sophos en equipos físicos alternos servidores?	X		
5	Mantener pólizas de seguros vigentes, asegurando por el valor real, contra todo riesgo los equipos y bienes de Pasto Salud.	Todas las oficinas de Pasto Salud ESE.	Pasto Salud ESE cuenta con Pólizas vigentes contra todo riesgo de daño y/o pérdida física por cualquier causa.	X		
6	Mantenimientos, revisiones preventivas y correctivas de equipos de computación y Comunicaciones, extintores, alarmas y sistemas contra incendio, para mantenerlos en óptimas condiciones.	Todas las oficinas de Pasto Salud ESE.	Pasto Salud cuenta con un plan de mantenimiento y contratos de mantenimientos vigentes para los equipos de cómputo de la Entidad.	X		

No	ACTIVIDAD	OFICINA	RESULTADO	SI	NO	OBSERVACIONES
7	Actualizar las claves o contraseña de acceso a las aplicaciones y bases de datos de los sistemas de información de Pasto Salud.	Todas las oficinas de Pasto Salud ESE	Se tiene implementada la política de actualización de claves de acceso para todos los sistemas de información de la Entidad en el directorio activo.	**X**		
8	Mantener actualizados los sistemas operativos, antivirus y aplicaciones de Pasto Salud ESE.		Se cuenta con un sistema de seguridad con seguimiento e informes para detectar vulnerabilidades de riesgo por virus informático.	**X**		
9	Mantener los servidores en condiciones ambientales óptimas de tal forma que no Fallen o se deterioren por uso inadecuado.		Verificación del cuarto de servidores y comunicaciones que cuente con sistemas de seguridad de acceso y ambiente adecuado de temperaturas.	**X**		
10	Mantener como respaldo un inventario adicional con equipos de cómputo, repuestos, consumibles, para su reemplazo inmediato en caso de falla.		Verificar que existan equipos y repuestos de respaldo en almacén y en cada sede.	**X**		

12. GLOSARIO(2)

"Acceso: Es la lectura o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta una Base de Datos, los datos son primero accedidos y suministrados a la computadora y luego transmitidos a la pantalla del equipo.

Amenaza: Cualquier evento que pueda interferir con el funcionamiento de un computador o causar la difusión no autorizada de información confiada a un computador como por ejemplo: Fallas del suministro eléctrico, virus, saboteos o descuido del usuario.

Ataque: Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático o el intento de obtener de modo no autorizado la información confiada a un computador.

Base de Datos: Es un conjunto de datos organizados, entre los cuales existe una correlación y que además están almacenados con criterios independientes de los programas que los utilizan. Entre sus principales características se encuentran brindar seguridad e integridad a los datos, proveer lenguajes de consulta, de captura y edición de los datos en forma interactiva, proveer independencia de los datos.

Datos: Los datos son hechos y/o valores que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos en el presente documento. En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y Bases de Datos, textos (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), videos (secuencia de tramas), etc.

Golpe (breach): Es la violación exitosa de las medidas de seguridad, como el robo de información, la eliminación de archivos de datos valiosos, el robo de equipos, PC, etc.

Incidente: Cuando se produce un ataque o se materializa una amenaza se tiene un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de eliminación de un archivo protegido.

Integridad: Los valores consignados en los datos se han de mantener de tal manera que representen la realidad y su modificación debe ser registrada en bitácoras del sistema que permitan la auditoría de los acontecimientos. Las

técnicas de integridad sirven para prevenir el ingreso de valores errados en los datos sea esta situación provocada por el software de la Base de Datos, por fallas de los programas, del sistema, el hardware o, simplemente, por errores humanos.

Privacidad: Se define como el derecho que tiene Pasto Salud ESE para determinar, a quién, cuándo y qué información de su propiedad podrá ser difundida o transmitida a terceros.

Seguridad: Se refiere a las medidas que toma Pasto Salud ESE con el objeto de preservar la integridad de sus datos o información procurando que no sean modificados, destruidos o divulgados ya sea en forma accidental, no autorizada o intencional. En el caso de los datos e información contenidos en los sistemas de información del Pasto Salud ESE, la privacidad y seguridad guardan estrecha relación entre sí, aunque la diferencia entre ellas radica en que la primera se refiere a la distribución autorizada de información y la segunda al acceso no autorizado.

Sistemas De Información: Es el término empleado en el ambiente del procesamiento de datos para referirse al almacenamiento de los datos de una organización y ponerlos a disposición de su personal. Pueden ser registros simples como archivos de Word y Excel, o pueden ser complejos como una aplicación de software con base de datos.

Cortafuegos (firewall): Es un sistema diseñado para bloquear el acceso no autorizado de comunicaciones. Se trata de un dispositivo configurado para permitir, limitar, cifrar y descifrar el tráfico de mensajes entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios. Los cortafuegos se utilizan para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets."[4]

Data Center: Lugares físicos de la entidad donde se encuentren alojados los servidores y demás equipos de comunicaciones.

"Plan de Continuidad de Negocio: Procedimientos documentados que guían orientan a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel pre-definido de operación debido una vez presentada / tras la interrupción. NOTA: Típicamente, esto incluye los recursos, servicios y actividades necesarios para garantizar la continuidad de las funciones críticas del negocio. [Fuente: ISO 22301].

Nivel de Criticidad: Descripción cualitativa usada para enfatizar la importancia de un recurso, proceso o función que debe estar disponible y operativa

4 https://iderf.gov.co/wp-content/uploads/2020/10/PLAN-DE-CONTINGENCIA-Y-POLITICAS-DE-SEGURIDAD-DE-SISTEMAS-DE-INFORMACION.pdf

constantemente o disponible y operativa al menor tiempo posible después de que un incidente, emergencia o desastre ocurra.

Interrupción: Incidente, bien sea anticipado (ej. huracanes) o no anticipados (ej. Fallas de potencia, terremotos, o ataques a la infraestructura o sistemas de tecnología y telecomunicaciones) los cuales pueden afectar el normal curso de las operaciones en alguna de las ubicaciones de la organización.

Recuperación de desastres de tecnología y telecomunicaciones (ITCTIC): Habilidad Capacidad de los elementos de tecnología y telecomunicaciones (ITC) de las TIC de la organización para soportar sus funciones críticas a un nivel aceptable dentro de un periodo predeterminado de tiempo después de una interrupción.

Modo de falla: Manera Forma en por la cual se observa una falla es observada."[5]

[5] https://www.mintic.gov.co/gestionti/615/articles-5482_G10_Continuidad_Negocio.pdf

BIBLIOGRAFÍA

1. 14:00-17:00. ISO. [citado 10 de julio de 2023]. ISO/IEC 27001 Standard – Information Security Management Systems. Disponible en: https://www.iso.org/standard/27001

2. articles-5482_G10_Continuidad_Negocio.pdf [Internet]. [citado 10 de julio de 2023]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G10_Continuidad_Negocio.pdf

Fin del documento.

ACTUALIZADO POR:

WILLIAM MONTENEGRO GUEVARA
Profesional Universitario

REVISADO POR:

HARVEY ALEXISVALLEJO NARVAEZ
Jefe oficina Asesora de Comunicaciones y Sistemas

APROBADO POR:

ANA BELEN ARTEAGA TORRES
Gerente