EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE PITALITO EMPITALITO E.S.P.

PLAN DE CONTIGENCIA INFORMATICO Y SEGURIDAD DE LA INFORMACION

HENRY LISCANO PARRA
GERENTE

OCTUBRE DE 2023

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El presente documento define el Plan de Contingencia Informático y Recuperación de Servicios de Tecnología de la Información y Comunicaciones como un proceso continuo de planeación, desarrollo, prueba e implantación de procesos y procedimientos de recuperación en caso de una posible contingencia que pueda presentarse en la empresa de servicios públicos domiciliarios de Pitalito EMPITALITO ESP. Estas acciones buscan asegurar la reanudación eficiente y efectiva de los servicios y operaciones de Tecnologías de la Información y Comunicaciones en el menor tiempo e impacto posible.

El Plan de Contingencia Informático y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones cuenta con documentos que en conjunto permiten la gestión, ejecución, pruebas y mantenimiento, esta disgregación de documentos permiten una fácil y ágil operación por los responsables autorizados, ante situaciones de desastres.

2. MISIÓN DE EMPITALITO ESP

EMPITALITO E.S.P., es la encargada de suministrar el agua potable, prestar los servicios de aseo y alcantarillado en el sector urbano del municipio de Pitalito, con proyección comercial en otros negocios del sector, logrando estructurar un soporte y plataforma de servicios para el crecimiento urbanístico y empresarial con enfoque de sostenibilidad, generando mejores condiciones de vida a todos los habitantes y usuarios de la ciudad.

3. VISIÓN DE EMPITALITO ESP

EMPITALITO E.S.P para el 2040; será la empresa prestadora de servicios públicos domiciliarios más importante y rentable de toda la región Sur colombiana con desarrollo económico y sostenible, que estará en el tiempo garantizando con las estrategias y nuevos negocios, la infraestructura acorde y mejoria de servicios públicos, para incrementar la productividad y competitividad del municipio de Pitalito, como eje del desarrollo agroindustrial y turístico del sur de Colombia.

4. CÓDIGO DE INTEGRIDAD DE LA EMPRESA

- **HONESTIDAD**: Actúo siempre con fundamento en la verdad, cumpliendo mis deberes con transparencia, rectitud, y siempre favoreciendo el interés general.

- **RESPECTO**: Reconozco, valoro y trato de manera digna a todas las personas, con sus virtudes y defectos, sin importar su labor, su procedencia, títulos o cualquier otra condición.

- **COMPROMISO:** Soy consciente de la importancia de mi rol como servidor público y estoy en disposición permanente para comprender y resolver las necesidades de las personas con las que me relaciono en mis labores cotidianas, buscando siempre mejorar su bienestar.

- **DILIGENCIA:** Cumplo con los deberes, funciones y responsabilidades asignadas a mi cargo de la mejor manera posible, con atención, prontitud y eficiencia, para así optimizar el uso de los recursos del Estado.

- **JUSTICIA:** Actúo con imparcialidad garantizando los derechos de las personas, con equidad, igualdad y sin discriminación.

5. OBJETIVO

5.1. OBJETIVO GENERAL

Establecer los principios básicos y el marco necesario para garantizar la operatividad de los servicios y/o procesos de tecnologías de la información y comunicaciones de EMPITALITO ESP, con el propósito de asegurar y restaurar los equipos e información con las menores pérdidas posibles en forma rápida, eficiente y oportuna; buscando la mejora de la calidad en los servicios que brinda la entidad.

5.2. OBJETIVOS ESPECÍFICOS

- Identificar y analizar los riesgos posibles que pueden afectar las operaciones, procesos y servicios de tecnologías de la información y comunicaciones de la Entidad.
- Definir las actividades de planeamiento, preparación, entrenamiento y ejecución de tareas destinadas a proteger la información contra los daños y perjuicios producidos por corte de servicios, fenómenos naturales o humanos.
- Organizar y disponer al personal técnico debidamente capacitado para afrontar adecuadamente las contingencias que puedan presentarse.
- Establecer actividades que permitan evaluar los resultados y retroalimentación del presente plan.

6. FINALIDAD

Garantizar la continuidad de los servicios de tecnología de información y comunicaciones de la empresa de servicios públicos domiciliarios de Pitalito EMPITALITO ES, a fin de que se restablezcan en el menor tiempo posible, en caso de la ocurrencia de alguna eventualidad que interrumpa su funcionamiento.

7. ALCANCE

El Plan de Contingencia Informático y Recuperación de Servicios de Tecnología de la Información y Comunicaciones, incluye los elementos referidos a los sistemas de información, aplicativos informáticos, bases de datos, equipos e instalaciones tecnológicas, personal, servicios y otros administrados por la Oficina de Tecnologías de la Información y Comunicaciones (TIC), direccionado a minimizar eventuales riesgos ante situaciones adversas que atentan contra el normal funcionamiento de los servicios informáticos de la entidad.

8. DEFINICIONES

- **TI**: es la aplicación de ordenadores y equipos de telecomunicación para almacenar, recuperar, transmitir y manipular datos, con frecuencia utilizado en el contexto de los negocios u otras empresas.
- **AMENAZA:** probabilidad de ocurrencia, durante un periodo específico y dentro de un área determinada, de un fenómeno que puede potencialmente causar daños en los elementos en riesgo
- **CONTIGENCIA:** Evento o suceso que ocurre, en la mayoría de los casos, en forma inesperada y que causa alteraciones en los patrones normales de funcionamiento de una organización.
- **ELEMENTOS EN RIESGO:** Se refiere a la población, las construcciones, la infraestructura, las edificaciones de las actividades económicas y otros espacios donde éstas se desarrollan, los servicios públicos y el medio ambiente natural que son susceptibles de daños como consecuencia de la ocurrencia de un fenómeno natural o producido por el hombre (artificial).
- **VULNERABILIDAD:** La vulnerabilidad se refiere al grado de pérdidas relacionadas con un elemento en riesgo (o un conjunto de elementos en riesgo), que resulta como consecuencia de un fenómeno natural o artificial con una determinada magnitud. Se expresa de una escala de "0" (no hay daños) a "1" (daño total).
- **RIESGO:** Se refiere a la cuantificación de los posibles daños ocasionados a los elementos en riesgo como consecuencia de un fenómeno natural o artificial en términos de vidas perdidas, personas heridas, daños materiales y ambientales e interrupciones de la actividad económica.
- **GRAVEDAD:** Se refiere a la magnitud resultante de los daños provocados por un siniestro. Esta es subdividida en ninguna, insignificante, marginal, crítica y catastrófica y se definen según el factor de evaluación (víctimas, pérdidas económicas, suspensión de operación, daño ambiental).
- **SEGURIDAD:** Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que, en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.
- **DATOS:** Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos.
- **INCIDENTE:** Es una violación con éxito de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, etc.
- **ACTIVO:** Son todo aquellos recursos o componentes de la institución, tanto físico (tangibles), como lógicos (intangibles) que constituyen su infraestructura, patrimonio, conocimiento y reputación en el mercado.
- **PLAN DE CONTIGENCIA:** Es una estrategia que se compone de una serie de procedimientos que facilitan una solución alternativa que permite restituir rápidamente el funcionamiento de los servicios críticos de la Fundación ante la eventualidad que lo afecte de forma parcial o total.

- **MINTIC**: El Ministerio de Tecnologías de la Información y las Comunicaciones, según la Ley 1341 o Ley de TIC, es la entidad que se encarga de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones.
- **Arquitectura Empresarial (AE)**: Es una práctica estratégica que consiste en analizar integralmente las empresas desde diferentes perspectivas o dimensiones, con el propósito de obtener, evaluar y diagnosticar su estado actual y establecer la transformación necesaria. El objetivo es generar valor a través de las Tecnologías de la Información para que se ayude a materializar la visión de la empresa.
- **ERP**: Una definición sencilla de qué es un ERP (Enterprise Resource Planning – Planificación de Recursos Empresariales) es un conjunto de sistemas de información que permite la integración de las operaciones de una empresa, como, por ejemplo; producción, logística, inventario, tesorería, contabilidad etc.
- **VPN**: Es una red privada virtual (VPN) construida dentro de una infraestructura de red pública, tal como la red mundial de Internet. Las empresas pueden usar redes privadas virtuales para conectar en forma segura oficinas y usuarios remotos a través de accesos a Internet.
- **Gestión tecnológica**: Es un sistema de conocimientos y prácticas relacionados con los procesos de creación, desarrollo, transferencia y uso de la tecnologia.
- **Recursos tecnológicos**: Conjunto total de medios materiales e inmateriales, métodos, procesos, competencias y saber hacer de las personas, tanto si éstos llegan a utilizarse como si no.
- **Estrategia TI**: Conjunto de principios, objetivos y acciones concretas que reflejan la forma en la cual una empresa decide utilizar las Tecnologías de la Información para permitir el logro de su misión de una manera eficaz. La Estrategia TI es una parte integral de la estrategia de una empresa.
- **Gestión de Seguridad y Privacidad de la Información**: Conjunto de actividades que permiten planear, administrar, operar, hacer seguimiento y evaluar, apropiadamente con base en la aplicación de las mejores prácticas y con el propósito de agregar valor para la organización, la definición y gestión de los controles y mecanismos para alcanzar los niveles requeridos de seguridad, privacidad y trazabilidad de los Componentes de Información, de los Sistemas de información, de los Servicios Tecnológicos.
- **Gestión de Servicios Tecnológicos**: Conjunto de actividades que permiten planear, administrar, operar, hacer seguimiento y evaluar, apropiadamente con base en la aplicación de las mejores prácticas y con el propósito de agregar valor para la organización, la definición y diseño de la Arquitectura de la infraestructura tecnológica que se requiere para soportar los Sistemas de Información y el portafolio de servicios.
- **Gestión de Sistemas de Información**: Conjunto de actividades que permiten planear, administrar, operar, hacer seguimiento y evaluar, apropiadamente con base en la aplicación de las mejores prácticas y con el propósito de agregar valor para la organización, los Sistemas de Información (misional, de apoyo, portales digitales y de direccionamiento estratégico).

- **Gestión TI:** Es una práctica que permite operar, innovar, administrar, desarrollar y usar apropiadamente las tecnologías de la información (TI), con el propósito de agregar valor para la organización. La gestión de TI permite a una organización optimizar los recursos, mejorar los procesos de negocio y de comunicación y aplicar las mejores prácticas.
- **Gobierno de TI**: Es una práctica, orientada a establecer unas estructuras de relación que alinean los procesos de negocio con los procesos, recursos y estrategias de TI, para agregar valor a las organizaciones y apoyar el cumplimiento de sus objetivos estratégicos. El gobierno de TI, gestiona y controla los riesgos, mide el desempeño de TI, busca optimizar las inversiones de TI y establecer un esquema de toma de decisiones de TI. El gobierno de TI, es parte del gobierno corporativo o empresarial.
- **Servicio Tecnológico**: Es un caso particular de un servicio de TI que consiste en una facilidad directamente derivada de los recursos de la plataforma tecnológica (hardware y software) de la institución. En este tipo de servicios los Acuerdos de Nivel de Servicio son críticos para garantizar algunos atributos de calidad como disponibilidad, seguridad, confiabilidad, etc.

9. MARCO NORMATIVO

La Oficina de Gestión TIC del de la empresa de servicios públicos EMPITALITO E.S.P., tiene agrupada la normatividad que lo rige en los siguientes grupos: institucional, de gobierno digital, relacionada con propiedad intelectual, seguridad de la información y otras normativas.

NORMATIVIDAD	DESCRIPCIÓN
DECRETO 1151 DE 2008	Lineamientos generales de la Estrategia de Gobierno Digital de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones.
LEY 1341 2009	Define principios y conceptos sobre la sociedad de la información y la organización de las TIC, se crea la Agencia Nacional de Espectro
DECRETO 2693 2012	Establece los lineamentos generales de la Estrategia de Gobierno en Linea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009, 1450 de 2011
DECRETO 2573 2014	Establece los lineamientos generales de la Estrategia de Gobierno Digital, se reglamenta parcialmente la Ley 1341 de 2009
LEY 1712 2014	Crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional

DECRETO 103 2015	Reglamenta parcialmente la Ley 1712 de 2014 (Gestión de la información pública)
RESOLUCIÓN 3564 2015	Reglamenta algunos artículos y parágrafos del Decreto número 1081 de 2015 (Lineamientos para publicación de la Información para discapacitados)
DECRETO 1078 2015	Expide el Decreto Único Reglamentario del Sector de las TIC
RESOLUCIÓN 2405 2016	Adopta el modelo del Sello de Excelencia Gobierno en Línea y se conforma su comité
DECRETO 728 2016	Actualiza el Decreto 1078 de 2015 con la implementación de zonas de acceso público a Internet inalámbrico
DECRETO 1413 DE 2017	Actualiza el Decreto Único Reglamentario del sector de las TIC, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales
DECRETO 1008 2018	Establece los lineamientos generales de la política de Gobierno Digital y actualizando el Decreto Único Reglamentario del sector de las TIC
COMPES 3975 2019	Política Nacional Para La Transformación Digital E Inteligencia Artificial
DIRECTIVA 02 2019	Moderniza el sector de las TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones
LEY 1955 2019	Simplificación de interacción digital los ciudadanos y el Estado
LEY 1978 DEL 2019	Plan de desarrollo 2018-2022. "pacto por Colombia, pacto por la equidad"
DECRETO 2106 DEL 2109	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública Cap. II Transformación Digital Para Una Gestión Publica Efectiva
DECRETO 620 MAYO 2020	Estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales"
GUÍA	Guía para la preparación de las TIC para la continuidad del negocio

Tabla1. Marco Normativo

10. DESCRIPCIÓN DEL PLAN DE CONTINGENCIA INFORMÁTICO

10.1. DIAGNOSTICO DE PROCESOS Y SERVICIOS

Principales Procesos de Software:

Aplicativos misionales y de apoyo definidos en la intranet de la Entidad:

- Software Integrado HAS SQL
- Sistema ORFEO Gestión Documental
- Sistema GLPI
- Software Ofimático

Principales servicios que deberán ser restablecidos Y/O recuperados

- Canales de Conectividad
- Bases de Datos
- Correo Electrónico
- Antivirus.
- Firewall
- Portal Web www.empitalito.gov.co

10.2. IDENTIFICACIÓN, ANÁLISIS Y EVALUACIÓN DE RIESGOS

Metodología aplicada:

Para la clasificación de los activos de las Tecnologías de Información de la empresa de servicios públicos domiciliarios de Pitalito EMPITALITO ESP, se han considerado tres criterios:

a) Grado de adversidad: Un evento se define con grado de adversidad (Leve, moderada, grave y muy severo).
b) Frecuencia del Evento: Nunca, aleatoria, periódico y continuo.
c) Impacto: El impacto de un evento puede ser (Leve, moderado, grave y muy severo).

Aspectos de procedimiento y consideración:

a) **Plan de Contingencia:** Son procedimientos que definen cómo una entidad continuará o recuperará sus funciones críticas en caso de una interrupción no planeada. Los sistemas son vulnerables a diversas interrupciones, que se pueden clasificar en:

   - ✓ Leves (Caídas de energía de corta duración, fallas en disco duro, etc.)
   - ✓ Severas (Destrucción de equipos, incendios, etc.)

b) **Riesgo:** Es la vulnerabilidad de un Activo o bien, ante un posible o potencial perjuicio o daño. Existen distintos tipos de riesgo:

- ✓ Riesgos Naturales: tales como mal tiempo, terremotos, etc.
- ✓ Riesgos Tecnológicos: tales como incendios eléctricos, fallas de energía, ataques informáticos.
- ✓ Riesgos Sociales: como actos terroristas y desordenes.

Para realizar un análisis de todos los elementos de riesgos a los cuales está expuesto el conjunto de equipos informáticos y la información procesada de la entidad iniciaremos describiendo los activos que se pueden encontrar dentro de las tecnologías de información de la entidad:

a) **Activos susceptibles de daño:**

- ✓ Personal
- ✓ Servidores
- ✓ Software
- ✓ Información
- ✓ Energía eléctrica
- ✓ Equipos de Seguridad Perimetral
- ✓ Equipos activos
- ✓ Ups
- ✓ Aires Acondicionados

b) **Posibles Daños:**

- ✓ No se cuenta con acceso físico a las instalaciones debido a protestas, desastres naturales, fallas sistema control de acceso.
- ✓ Imposibilidad de acceso a los recursos informáticos, sean estos por cambios involuntarios o intencionales, tales como cambios de claves de acceso, eliminación o borrado físico/lógico de información clave, proceso de información no deseado

c) **Fuentes de daño:**

- ✓ Acceso físico no autorizado
- ✓ Desastres Naturales (Movimientos telúricos, Inundaciones, Fallas en los equipos de soporte causadas por el ambiente, la red de energía eléctrica o el no acondicionamiento atmosférico necesario.

- ✓ Fallas de Personal Clave (Enfermedad, Accidentes, Renuncias, Abandono de sus puestos de trabajo y Otros).
- ✓ Fallas de Hardware (Falla en los Servidores o Falla en el hardware de Red, Switches, cableado de la Red, Router, Firewall).
- ✓ Ataques Informáticos

d) **Clases de Riesgos:**

- ✓ Incendio o Fuego.
- ✓ Falla en los equipos.
- ✓ Equivocaciones.
- ✓ Acción virus informático.
- ✓ Fenómenos naturales.
- ✓ Accesos no autorizados.
- ✓ Ausencia del personal de sistemas.
- ✓ Ataques Informáticos

10.3. PLAN DE RESPALDO - ANTES

Describe las contramedidas preventivas que se deben realizar para evitar la materialización de la amenaza, de acuerdo a la identificación de los tipos de riesgos y análisis de afectación al buen funcionamiento de las operaciones de la entidad, resultado obtenido en el numeral 5.2 "Identificación, análisis y evaluación del riesgo".

Y contramedidas correctivas en los casos de revisión periódica acordada o después de presentada la incidencia, con el fin de evaluar si las acciones propuestas para mitigar el riesgo fueron eficaces, ineficaces o no estaban prevista, lo cual obliga a realizar un nuevo análisis de riesgo para mejor el plan de contingencia propuesto.

10.3.1. Actividades previas al desastre

Se considera las actividades de resguardo de la información, en busca de un proceso de recuperación con el menor costo posible para la Entidad, de acuerdo a los lineamientos contemplados en los soportes físicos y lógicos de la infraestructura tecnológica de la entidad y en la realización de copias de seguridad. Se establece los procedimientos relativos a:

- ✓ **Sistemas e Información:** La Entidad cuenta con Sistemas de Información, tanto los de desarrollo propio, como los desarrollados por empresas externas.

- ✓ **Equipos de Cómputo:** Se debe tener en cuenta el registro de Hardware, impresoras, scanner, switches, y otros, detallando su ubicación (software que usa, ubicación y nivel de uso institucional). Se debe emplear los siguientes criterios sobre identificación y protección de equipos:
  - Pólizas de seguros comerciales, como parte de la protección de los activos institucionales y considerando una restitución por equipos de mayor potencia, teniendo en cuenta la depreciación tecnológica.
  - Mantenimiento actualizado del inventario de los equipos de cómputo requerido como mínimo para el funcionamiento permanente de cada sistema en la institución.

- ✓ **Obtención y almacenamiento de los Respaldos de Información (BACKUPS):** Se debe contar con procedimientos para la obtención de las copias de seguridad de todos los elementos de software y datos necesarios para asegurar la correcta ejecución de los sistemas en la institución. Las copias de seguridad son las siguientes:
  - Backup del Sistema Operativo: Todas las versiones de sistema operativo instalados en la Red. (Periodicidad – Semestral).
  - Backups de los datos (Base de datos, passsword y todo archivo necesario para la correcta ejecución del software aplicativos de la institución). (Periodicidad – Mensual).

10.3.2. MEDICIÓN Y PREVENCIÓN DE LAS CLASES DE RIESGO

Teniendo en cuenta lo anterior, corresponde al presente Plan de Contingencia minimizar estos índices con medidas preventivas y correctivas sobre cada caso de Riesgo:

INCENDIO O FUEGO	
Grado de Adversidad:	Muy Severo
Frecuencia de Evento:	Aleatorio
Grado de Impacto:	Alto

Situación Presentada	Acción Definida
En el Centro de Cómputo donde están ubicados los servidores, equipos de comunicación y conectividad, está dotado de un sistema contra incendios y se cuenta con extintores ubicados estratégicamente para cualquier eventualidad.	Se cumple.
A los servidores se les realizan backups de la información generada periódicamente, pero no existe ninguna otra copia de respaldo en el exterior.	Después de realizar backups de los servidores de forma semanal, se debe almacenar en discos duros externos y buscar la manera de vincular este

	proceso con la extracción segura de la Entidad con algún servicio de Bodegaje y/o almacenamiento seguro.
La oficina donde están ubicados los servidores cuenta con un extintor cargado, ubicado muy cerca a esta oficina. De igual forma cada piso cuenta con un extintor debidamente cargado.	Se cumple.
Adquirir servicios en las nubes para los servidores de HAS SQL, ORFEO, GLPI para tener un sitio alterno donde se publicaran aplicativos de la Entidad permitiendo así tener redundancia en los diferentes servicios que están ubicados en el Centro de Datos.	Proponer el proyecto de adquisición de servicios en la nube y solicitar su asignación presupuestal.

ROBO DE EQUIPOS Y ARCHIVOS	
Grado de Adversidad:	Muy Severo
Frecuencia de Evento:	Aleatorio
Grado de Impacto:	Alto

Situación Presentada	Acción Definida
Se cuenta con servicio de vigilante y las personas particulares que ingresan a la entidad, no son registradas.	Recomendar a la administración un servicio de vigilancia con funciones de registro y control de activos fijos de la Institución.
Autorización escrita firmada por el responsable de almacén y funcionario responsable, para la salida de equipos de la Entidad.	Definir formato de entrada y salida de elementos y equipos de la entidad.

FALLA EN LOS EQUIPOS	
Grado de Adversidad:	Grave
Frecuencia de Evento:	Aleatorio
Grado de Impacto:	Grave

Situación Presentada	Acción Definida
La falla en los equipos muchas veces se debe a falta de mantenimiento y limpieza.	Realizar mantenimiento preventivo de equipos por lo menos dos veces al año.

La falla en el hardware de los equipos requiere de remplazo de repuestos de forma inmediata.	Contar con proveedores en caso de requerir remplazo de piezas y de ser posible contar con repuestos de equipos en desuso o que sean declarados para dar de baja.
Cada área funcional se une a la Red de datos a través del cableado estructurado que se centraliza en el Centro de Datos principal, la falta de energía en el Centro de Datos, originaria la ausencia de uso de los servicios de red.	Se cuenta con un sistema de UPS's que soportan el servicio eléctrico en caso de falla eléctrica.
Falla switch de Core	Contar con redundancia o sistema de alta disponibilidad, que cumpla con las funciones del equipo principal en caso de falla. Contar con la garantía y el soporte especializado sobre el equipo.
Falla Firewall	Contar con redundancia o sistema de alta disponibilidad, que cumpla con las funciones del equipo principal en caso de falla. Contar con la garantía y el soporte especializado sobre el equipo
Fallas Servidores de aplicaciones	Se debe contar con herramientas de respaldo que nos permitan recuperar el servidor afectado
Fallas Servidores de Bases de Datos	Se debe contar con mecanismos de respaldo que nos permitan recuperar la información y la configuración de estas máquinas en caso de presentarse fallas.

EQUIVOCACIONES EN EL MANEJO DEL SISTEMA	
Grado de Adversidad:	Moderado
Frecuencia de Evento:	Periódico
Grado de Impacto:	Moderado
Situación Presentada	**Acción Definida**
Equivocaciones que se producen de forma involuntaria, con respecto al manejo de información, software y equipos.	Realizar capacitación al ingreso sobre el manejo de los sistemas a cargo y generar documentación, manuales e instructivos.
El daño de equipos por fallas en la energía eléctrica, requiere contar con dispositivos que amplíen tiempo para apagar correctamente el equipo.	Es necesario que las estaciones de trabajo tengan un UPS individual que soporte los fallos de energía. Relativamente Se cumple algunos equipos.

Se presentan equivocaciones en el manejo de información debido a que, al momento de iniciar actividades en el cargo asignado, no se suministran manuales, o se hace entrega puntual de instrucciones o políticas de manejo y/o operación de las distintas plataformas, Sistemas Operativos y demás elementos de TI.	Definir políticas de informática claras y precisas, las cuales se deben comunicar a los funcionarios al ingresar a ocupar sus respectivos cargos o al cumplir con sus obligaciones contractuales, al igual que cualquier modificación a las mismas. Generar manuales y documentación de los diferentes sistemas.

ACCIÓN DE VIRUS INFORMÁTICO	
Grado de Adversidad:	Muy Severo
Frecuencia de Evento:	Continuo
Grado de Impacto:	Grave

Situación Presentada	Acción Definida
Se cuenta con un software antivirus para la entidad. (ESET Internet Security).	Se debe evitar que las licencias de antivirus expiren, se requiere renovación con anterioridad a la finalización del contrato
Se cuenta con privilegios de acceso a los servidores y segmentos de red diferentes para evitar la propagación de virus.	Se cumple.
Únicamente el área de sistemas es la encargada de realizar la instalación de software en cada uno de los equipos de acuerdo a su necesidad	Se cumple
Reconocimiento de malware a través de correos electrónicos recibidos	Crear un correo institucional para cada funcionario, de forma que únicamente se reciba información de importancia para la entidad. Se debe aprender a identificar por parte de los usuarios correos maliciosos. Capacitaciones por parte del área de sistemas a los funcionarios de la entidad para detectar posibles correos maliciosos.

FENÓMENOS NATURALES	
Grado de Adversidad:	Grave

Frecuencia de Evento:	Aleatorio
Grado de Impacto:	Grave

Situación Presentada	Acción Definida
En la última década no se han registrado urgencias por fenómenos naturales como terremotos o inundaciones.	Aunque la probabilidad de ocurrencia es baja se requiere tener en cuenta medidas de prevención.
Aunque existen épocas de lluvia fuertes, las instalaciones de EMPITALITO ESP están debidamente protegidas.	Tomar medidas de prevención.
Los servidores principales se encuentran en un ambiente libre de filtraciones	Ante la mínima filtración se debe informar de inmediato a la Dirección, para realizar el respectivo mantenimiento correctivo y preventivo.

ACCESOS NO AUTORIZADOS	
Grado de Adversidad:	Grave
Frecuencia de Evento:	Aleatorio
Grado de Impacto:	Grave

Situación Presentada	Acción Definida
Se controla el acceso al sistema de red mediante Directorio Activo, en donde se permite el uso de servicios de red con un usuario y con su respectiva clave.	Se cumple.
La asignación de usuario se realiza de acuerdo a los parámetros y políticas establecidas por la Dirección y se solicita en forma virtual a través de los medios designados de acuerdo al Procedimiento para la gestión de servicios de tecnologías de la información y las comunicaciones.	Se debe solicitar por escrito (E-mail) a la Mesa de Servicios la creación de usuarios y los permisos que se requiere sean asignados, o cualquier cambio referente a los mismos.
La oficina Gestión del talento humano no comunica con celeridad a la oficina de sistemas, cuando un funcionario ingresa a la empresa, sale a vacaciones o se retira de la entidad a fin de desactivar ese usuario.	Se debe informar a la oficina TIC, que funcionario ingresa, sale a vacaciones o se retira de la entidad para así bloquear el respectivo usuario por el tiempo de ausencia, igualmente en caso de retiro definitivo.

Se acostumbra a confiar la clave de acceso (uso personal) a compañeros de área, sin medir la implicación en el caso de acceso no autorizado.	Capacitar al personal sobre la confidencialidad de sus contraseñas, recalcando la responsabilidad e importancia que ello implica, sobre todo para el manejo de software. Se debe habilitar en todos los sistemas de información utilizados en la Entidad, la funcionalidad de solicitar de manera obligatoria el cambio de contraseña en los periodos de tiempo que indique el manual de políticas de uso y seguridad de la información, con el fin de fortalecer la cultura de manejo de contraseñas de manera responsable.
Se cuenta con perfiles de navegación para restringir y proteger a la Entidad de páginas maliciosas y optimizar los recursos de red.	Se tiene un firewall con políticas de bloqueo de páginas maliciosas. Se cumple
No se cancelan los usuarios del personal que se retira de la entidad de forma inmediata, recurriendo en algunos casos a utilizar la contraseña del funcionario ausente.	Tan pronto se informe que un funcionario se retira definitivamente se debe cancelar este usuario.

AUSENCIA DEL PERSONAL A CARGO DE LAS LABORES ADMINISTRATIVAS DE TI	
Grado de Adversidad:	Grave
Frecuencia de Evento:	Aleatorio
Grado de Impacto:	Grave
Situación Presentada	**Acción Definida**
En la empresa, la planta de personal del área de tecnología es reducido, se cuenta con un funcionario para el manejo de toda la infraestructura TI (Base de datos, Sistemas de Información, Servidores, redes, etc.)	Es importante reforzar el personal del área de sistemas con personal capacitado que tenga el conocimiento y la experiencia como backup de las personas que tienen a cargo al acceso y manejo de los diferentes sistemas, Bases de Datos, Directorio Activo, Redes, Servidores, Equipos activos y de seguridad perimetral.

El funcionario de Sistemas de Información, es la única persona con claves de acceso al sistema, conocedor del manejo de la red y los sistemas de información.	Se debe generar politicas de manejo de contraseñas y copias de respaldo de las contraseñas utilizadas para los sistemas más importantes del área.
Aunque se ha diagramado un esquema general de la Red de Datos de la Entidad, en caso de fallas en la red y ausencia del funcionario de sistemas encargado, no existe un diagrama lógico completo en el cual se definan las conexiones de red existentes, de forma que agilice la labor de recuperación del sistema.	Realizar el diagrama lógico de la red y revisar la demarcación de cada uno de los puntos de red físicos para que en caso de falla se agilice el trabajo de inspección y por ende la recuperación del sistema, para el centro de datos.

10.4. PLAN DE EMERGENCIA - DURANTE

Considera las contramedidas que se deben aplicar durante la materialización de la amenaza, para mitigar las consecuencias generadas por el siniestro.

Cuando se materializa un riesgo, este puede producir un Evento, por tanto, a continuación, se describen los eventos a considerar dentro del Plan de Contingencia.

RIESGO	EVENTO	MEDIDA APLICADA	RECURSO DE CONTINGENCIA
FALLAS DE RED GENERAL	No hay comunicación con aplicaciones y servicios de red	-Requerimiento del usuario reportando la falla. - Validación de primer nivel equipos de comunicaciones (ping). - Validación física de los leds (indicadores) alarmados. - Reportar al proveedor la falla presentada.	- Soporte especializado proveedor de conectividad -Diagrama Lógico de la red -Cables de fibra -Cables Utp
FALLA DE RED USUARIO	No hay comunicación entre el usuario y los diferentes servicios de red.	-Requerimiento del usuario reportando la falla. -Validación de primer nivel por parte del encargado de dar soporte de mesa de servicios. - Validar si tarjeta de red linkea - Si no está linkenado solicitar validar estado del punto de red en el centro de datos. - Si el punto de red está funcionando correctamente validar si existe problema en la	-Cables Utp -Tarjetas de Red -Equipo Activo -Soporte equipos activos

		tarjeta de red, en caso de afirmativo realizar cambio o arreglo de la misma -Validar estado patch cord. Si persiste la falla Validar por parte del segundo nivel -Que el punto de red del usuario esté conectado en el centro de datos. -Validar estado del punto de red en el equipo activo. -Probar el cable UTP. Si existe daño, realizar el cambio del cable -Validar cable de red desde patch panel a equipo activo. -Revisar estado de la interfaz equipo activo.	
FALLAS SERVIDOR	No hay acceso a aplicativos o Información	-Validación de segundo nivel de la falla presentada -Validar fallas en componentes de hardware, disco duro, memorias, fuentes, ventilador, procesador.	-Stock repuestos servidor Backup periódico de la información. -Mantenimiento preventivo servidores. -Backup máquinas virtuales para restauración de los servicios.
FALLAS UPS	Daño de equipos, perdida de información	-Validación estado de los ups. - Validación estado de las baterias. -Mantenimientos preventivos.	-Mantenimiento preventivo Ups
VIRUS	Perdida de información	-Validación de primer nivel en sitio. -Validar que tenga cliente de antivirus instalado. -Validar que el cliente de antivirus este activo. -Correr el cliente de antivirus para escanear el equipo en busca del virus. Validación de segundo nivel -Revisar consola de antivirus para generar reportes de virus.	-Mantenimiento software antivirus

		-Actualizar desde la consola las listas de virus reportados. -Mandar actualizaciones a los clientes.	
CORTE GENERAL DE FLUIDO ELECTRICO	No hay acceso a aplicativos o Información	-Revisar funcionamiento de las UPS mientras entra en servicio la planta eléctrica de respaldo. -Activar planta eléctrica para mantener el servicio.	-UPS -Planta Eléctrica -Mantenimiento Ups
FALTA DE PERSONAL	Demoras en respuesta a solicitudes y nuevos proyectos	-Diagrama de servicios administrador por funcionario. -Definir funcionario de respaldo para los procesos críticos de infraestructura. -Implementar metodología para el manejo de contraseñas de acceso a los diferentes recursos de T.I	-Soporte para los procesos críticos de la Entidad (Bases de Datos, Equipos activos, Servidores) -Soporte especializado en el grupo de mesa de servicios. -Manual de funciones del área
FALLAS EQUIPOS DE COMUNICACIÓN	No hay acceso a aplicativos, internet o Información	-Pruebas de primer nivel hacia los diferentes equipos de comunicación para detectar cual está fallando (Router, Core, switch de borde, firewall) - Si el problema está en el Router se revisa en sitio para validar alertas en los leds -Reportar al proveedor de servicios de comunicación la falla presentada. Si el problema está en el Core, se activa equipo de respaldo, y se solicita servicio a la empresa de mantenimiento pata restaurar el principal. Si el problema está en el firewall se activa equipo secundario para mantener los servicios y se solicita el soporte a la empresa para revisar la falla en el equipo principal y restaurar.	-Contrato proveedor de servicios de conectividad. -Implementación de servicios de redundancia en el core, firewall -Mantenimiento equipos activos -Mantenimiento equipos de seguridad perimetral

INCENDIO, TERREMOTO	Indisponibilidad del centro de datos	-Implementar sistemas de control de incendios especializado para datacenter. -Realizar inventario de los servicios implementados en el datacenter -Realizar backup de la información y de los servidores que se encuentran en el datacenter. -Evaluar el daño -Restablecer o instalar nuevo centro de datos de acuerdo al daño presentado -Remplazar equipos afectados -Restaurar los backups -Restaurar servicios	-Mantenimiento preventivo sistema control de incendios. -Contratar servicios de nube que permitan restablecer los servicios que se tienen implementados en el datacenter principal. -Diagrama de servicios de la entidad que están alojados en el datacenter -Implementar servicios de almacenaje de los backups en lugar externo a la Entidad.

La presente etapa incluye las actividades a realizar durante el desastre o siniestros, se debe tener en cuenta la probabilidad de su ocurrencia durante: el día, noche o madrugada. Este plan debe incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre el siniestro, descritas a continuación:

a) Buscar Ayuda de Otros Entes

Es de tener en cuenta que solo se debe realizar acciones de resguardo de equipos en los casos en que no se pone en riesgo la vida de personas. Normalmente durante la acción del siniestro es difícil que las personas puedan afrontar esta situación, debido a que no están preparadas o no cuentan con los elementos de seguridad, por lo que las actividades para esta etapa del proyecto de prevención de desastres deben estar dedicados a buscar ayuda inmediatamente para evitar que las acciones del siniestro causen más daños o destrucciones.

- ✓ Se tiene en las dependencias correspondientes los números de teléfono y direcciones de organismos e instituciones de ayuda.
- ✓ Todo el personal debe conocer la localización de vías de Escape o Salida: Deben estar señalizadas las vías de escape o salida.

- ✓ Instruir al personal de la entidad respecto a evacuación ante sismos, a través de simulacros, esto se realiza acorde a los programas de seguridad organizadas por la oficina de SST de la entidad u otros entes como las organizadas por el municipio y entes como bomberos, defensa civil entre otros.
- ✓ Ubicar y señalizar los elementos contra el siniestro: tales como extintores, zonas de seguridad (ubicadas normalmente en las columnas), donde el símbolo se muestra en color blanco con fondo verde.
- ✓ Secuencia de llamadas en caso de siniestro: tener a la mano elementos de iluminación, lista de teléfonos de instituciones como: Compañía de Bomberos, Hospitales, Centros de Salud, Ambulancias, Seguridad.

b) Formación de Equipos

Se debe establecer los equipos de trabajo, con funciones claramente definidas que deberán realizar en caso de desastre. En caso de que el siniestro lo permita (al estar en un inicio o estar en un área cercana, etc.), se debe formar 02 equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y el otro para salvamento de los equipos informáticos, teniendo en cuenta la clasificación de prioridades.

c) Entrenamiento

Se debe establecer un programa de prácticas periódicas con la participación de todo el personal en la lucha contra los diferentes tipos de siniestro, de acuerdo a los roles que se hayan asignado en los planes de evacuación del personal o equipos, para minimizar costos se pueden realizar recarga de extintores, charlas de los proveedores, etc. Es importante lograr que el personal tome conciencia de que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) pueden realmente ocurrir; y tomen con seriedad y responsabilidad estos entrenamientos; para estos efectos es conveniente que participen los Directivos, dando el ejemplo de la importancia que la Alta Dirección otorga a la Seguridad Institucional.

10.5. PLAN DE RECUPERACION - DESPUES

Comprende las contramedidas que se deben ejecutar después de materializada y controlada la amenaza, para restaurar los elementos informáticos, tecnológicos, y reanudar los servicios de la entidad.

- ❖ Evaluación de daños.
- ❖ Traslado de datos desde la ubicación de emergencia a la habitual.
- ❖ Reanudación de la actividad.

- Desactivación del precontrato de alquiler.
- Reclamaciones a la compañía de seguros.

El paso inicial en el desarrollo del plan contra desastres, es la identificación de las personas que serán las responsables de la ejecución del Plan de contingencia. Por tanto, se definen los siguientes responsables:

- **Administrador(es) de Infraestructura**: Sera responsable de llevar a cabo las acciones correctivas definidas anteriormente a fin de minimizar los riesgos establecidos.

- **Dirección de Tecnologías e Información**: Verificara la labor realizada por el (los) Administrador(es) de Infraestructura.

10.5.1. Actividades después del desastre

Estas actividades se deben realizar inmediatamente después de ocurrido el siniestro, son las siguientes:

a) Evaluación de daños

El objetivo es evaluar la magnitud del daño producido, es decir, que sistemas se están afectando, que equipos han quedado inoperativos, cuales se pueden recuperar y en cuanto tiempo. En el caso de la empresa de servicios públicos domiciliarios de Pitalito se debe atender los procesos de la:

- Dirección Comercial (Ventanilla PQR, Facturación, Matriculas, Cartera),
- Dirección Administrativa y Financiera (Contabilidad, Presupuesto, Tesorería, Talento Humano, Almacen, Archivo),
- Tecnologías e Información
- y demás primordiales para el funcionamiento de la Entidad, por la importancia estratégica.

La recuperación y puesta en marcha de los servidores que alojan dichos sistemas, es prioritario.

b) Priorizar Actividades

La evaluación de los daños reales nos dará una lista de las actividades que debemos realizar, preponderando las actividades estratégicas y urgentes de nuestra institución. Las actividades comprenden la recuperación y puesta en marcha de los equipos de cómputo ponderado y los Sistemas de Información, compra de accesorios dañados, etc.

c) Ejecución de actividades

La ejecución de actividades implica la colaboración de todos los funcionarios, creando Equipos de Trabajo, asignando actividades. Cada uno de estos equipos deberá contar con un líder que deberá reportar el avance

de los trabajos de recuperación y en caso de producirse un problema, reportarlo de inmediato al Directivo, brindando posibles soluciones. Los trabajos de recuperación se iniciarán con la restauración del servicio usando los recursos de la institución, teniendo en cuenta que en la evaluación de daños se contempló y gestionó la adquisición de accesorios dañados. La segunda etapa es volver a contar con los recursos en las cantidades y lugares propios del Sistema de Información, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar la operatividad de la institución y el buen servicio de nuestro sistema e Imagen Institucional.

d) Evaluación de Resultados

Una vez concluidas las labores de Recuperación de los sistemas que fueron afectados por el siniestro, debemos de evaluar objetivamente, todas las actividades realizadas, con que eficacia se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades, como se comportaron los equipos de trabajo, etc. De la evaluación de resultados y del siniestro, deberían de obtenerse 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.

e) Retroalimentación de Actividades

Con la evaluación de resultados, podemos mejorar las actividades que tuvieron algún tipo de dificultad y reforzar los elementos que funcionaron adecuadamente.

11. CONCLUSIONES

El presente Plan de contingencia Informático de la Empresa de Servicios Públicos Domiciliarios de Pitalito EMPITALITO ESP, tiene como fundamental objetivo el salvaguardar la infraestructura de la Red y Sistemas de Información. Este Plan está sujeto a la infraestructura física y las funciones que realiza la oficina de Sistemas de la entidad.

Las principales actividades requeridas para la implementación del Plan de Contingencia Informático son: Identificación de riesgos, Minimización de riesgos, Identificación de posibles eventos para el Plan de Contingencia, Establecimiento del Plan de Recuperación y Respaldo, Plan de Emergencias y Verificación e implementación del plan.

No existe un plan único para todas las organizaciones, esto depende de la infraestructura física y las funciones que realiza en Centro de Procesamiento de Datos más conocido como Centro de Cómputo.

Lo único que realmente permite a la institución reaccionar adecuadamente ante procesos críticos, es mediante la elaboración, prueba y mantenimiento de un Plan de Contingencia.

12. RECOMENDACIONES

Hacer de conocimiento general el contenido del presente Plan de Contingencia Informático, con la finalidad de instruir adecuadamente al personal de la Empresa de Servicios Públicos Domiciliarios de Pitalito EMPITALITO ESP.

Adicionalmente al plan de contingencia Informático se deben desarrollar las acciones correctivas planteadas para minimizar los riesgos identificados. Es importante tener actualizados los contratos de garantía y licencias tanto de hardware como de software, así como pólizas de aseguramiento. Cuando los administradores de infraestructura se encuentren ausentes, se recomienda capacitar a una persona que pueda hacer lo mínimo indispensable para levantar todos los servicios, a fin de que la operación básica de la Entidad no se vea interrumpida.

CONTROL DE CAMBIOS:

VERSIÓN N°.	FECHA DE APROBACIÓN.	DESCRIPCIÓN DEL CAMBIO
1	02-10-2023	Se crea el Plan de contingencia informático y seguridad de la información

HENRY LISCANO PARRA
GERENTE

Elaboró: Jefersson Silva Losada	**Revisó:** Mónica Alexandra Lagos	**Aprobado:** Henry Liscano Parra
Cargo: Profesional de Sistemas	**Cargo:** Jefe Oficina de Planeación y Proyectos	**Cargo:** Gerente
Firma:	**Firma:**	**Firma:**

Aprobado mediante Resolución Administrativa N° 051 de 2023