	FORMATO INFORME DE PRESTACION DE SERVICIOS	Código	Versión
		IPSE-CO-F73	6
		Fecha:	Paginas
		15/12/2021	1/23

CONTRATO DE PRESTACIÓN DE SERVICIOS No.:					**226**	Del Año:		**2023**	
CONTRATISTA:	**MANUEL HUMBERTO SANTANDER PELAEZ**				**C.C./ C.E. No.:**	**98.629.535**			
PERIODO DEL INFORME:	**Desde:**	**01**	**11**	**2023**	**Hasta:**	**30**	**11**	**2023**	
		Día	Mes	Año		Día	Mes	Año	

1. INFORMACIÓN GENERAL DEL CONTRATO

PRESTAR SERVICIOS PROFESIONALES PARA DEFINIR EL PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES – PETIC PARA EL HORIZONTE 2023-2026.								
Fecha de inicio	25	07	2023		**Fecha de terminación**	28	12	2023
	Día	Mes	Año			Día	Mes	Año

1.1. ANÁLISIS DE RIESGOS

1. Riesgos	2. Responsable	3. Materializado Si/No	4. Plan de acción
Se presenta cuando la definición de la necesidad y el objeto establecido en el estudio previo, no se ajusta.	IPSE	No	N/A
Se presenta cuando el contratista seleccionado no firma el contrato en el plazo establecido.	CONTRATISTA	No	N/A
Ocurre cuando se presentan retrasos o incumplimientos en la entrega de los informes y/o productos a cargo del contratista, o cuando los mismos no	CONTRATISTA	No	N/A
Ocurre cuando se presentan demoras por parte de la Entidad en las aprobaciones previas de los productos y/o informes desarrollados por el contratista.	IPSE	No	N/A
Se presenta por la expedición de normas que impongan nuevos tributos, impuestos o cargas parafiscales, que pueden afectar el equilibrio	IPSE CONTRATISTA	No	N/A

2. DETALLE DE LA EJECUCIÓN

CONTRATO DE PRESTACIÓN DE SERVICIOS No.:					226	Del Año:		2023
CONTRATISTA:	MANUEL HUMBERTO SANTANDER PELAEZ				C.C./ C.E. No.:	98.629.535		
PERIODO DEL INFORME:	Desde:	01	11	2023	Hasta:	31	11	2023
		Día	Mes	Año		Día	Mes	Año

No.	OBLIGACIÓN ESPECÍFICA	ACTIVIDADES EJECUTADAS	AVANCE/ ESTADO DE EJECUCIÓN
1.	Desarrollar e implementar, a través del documento respectivo, el marco de las políticas y procedimientos de seguridad de la información alineados con los objetivos y metas del PETIC para el IPSE.	**No se desarrollaron actividades en este período.**	**EN EJECUCIÓN**
2.	Diseñar, formular e implementar el Sistema de Gestión de Seguridad de la Información en el IPSE, conforme al documento maestro de seguridad y privacidad de la información (MSPI).	No se desarrollaron actividades en este período.	**EN EJECUCIÓN**
3.	Adelantar las evaluaciones periódicas de los riesgos de seguridad de la información y la actualización de los controles correspondientes en el IPSE, de acuerdo con las mejores prácticas y	No se desarrollaron actividades en este período.	**EN EJECUCIÓN**

CONTRATO DE PRESTACIÓN DE SERVICIOS No.:					226	Del Año:		2023
CONTRATISTA:	MANUEL HUMBERTO SANTANDER PELAEZ				C.C./ C.E. No.:	98.629.535		
PERIODO DEL INFORME:	Desde:	01	11	2023	Hasta:	31	11	2023
		Día	Mes	Año		Día	Mes	Año

	estándares internacionales.		
4.	Implementar para el IPSE los mecanismos de monitoreo y seguimiento para garantizar el cumplimiento de las políticas y controles establecidos en el SGSI.	No se desarrollaron actividades en este período.	**EN EJECUCIÓN**
5.	Participar en el proceso de elaboración de los planes de respuesta y continuidad de negocio cuando se generen en el IPSE incidentes de seguridad de la información.	No se desarrollaron actividades en este período.	**EN EJECUCIÓN**
6.	Realizar de auditorías internas correspondientes para evaluar la efectividad de SGSI y asegurar el cumplimiento de las regulaciones y normativas aplicables.	No se desarrollaron actividades en este período.	**EN EJECUCIÓN**
7.	Mantener y actualizar los registros y documentos relacionados con el SGSI, incluyendo	No se desarrollaron actividades en este período.	**EN EJECUCIÓN**

CONTRATO DE PRESTACIÓN DE SERVICIOS No.:					**226**	Del Año:		**2023**	
CONTRATISTA:	**MANUEL HUMBERTO SANTANDER PELAEZ**				**C.C./ C.E. No.:**	**98.629.535**			
PERIODO DEL INFORME:	**Desde:**	**01**	**11**	**2023**	**Hasta:**	**31**	**11**	**2023**	
		Día	Mes	Año		Día	Mes	Año	

	políticas, procedimientos, informes y evidencias de cumplimiento.		
8.	Capacitar y concientizar regularmente al personal del IPSE sobre los aspectos clave del SGSI, promoviendo la cultura de seguridad de la información en toda la organización.	No se desarrollaron actividades en este período.	**EN EJECUCIÓN**
9.	Colaborar y participar en el proceso de la evaluación y selección de proveedores y contratistas externos, en lo referente a la verificación de cumplimiento de los requisitos de seguridad de la información establecidos en el SGSI.	No se desarrollaron actividades en este período.	**EN EJECUCIÓN**
10.	Informar periódicamente al supervisor del contrato o a quien este delegue sobre el estado y avance del SGSI, señalando los	Elaboración del quinto informe de actividades	**EN EJECUCIÓN**

CONTRATO DE PRESTACIÓN DE SERVICIOS No.:					226	Del Año:		2023
CONTRATISTA:	MANUEL HUMBERTO SANTANDER PELAEZ				C.C./ C.E. No.:	98.629.535		
PERIODO DEL INFORME:	Desde:	01	11	2023	Hasta:	31	11	2023
		Día	Mes	Año		Día	Mes	Año

	logros, desafíos y áreas de mejora respectivas.		
11.	Participar en la revisión y actualización periódica del PETIC, al igual que en su adecuación con las políticas y estándares de seguridad de la información, garantizando una gestión integral y continua de la seguridad en el IPSE.	No se desarrollaron actividades en este período.	**EN EJECUCIÓN**
12.	Elaborar el documento de diagnóstico del modelo de seguridad y privacidad de la información del IPSE, siguiendo el formato establecido en la normativa aplicable.	No se desarrollaron actividades en este período.	**CERRADO**
13.	Elaborar el documento que contenga la hoja de ruta detallada para alcanzar las acciones establecidas en el segmento del anexo 3 del manual de Gobierno Digital.	No se desarrollaron actividades en este período.	**EN EJECUCIÓN**

CONTRATO DE PRESTACIÓN DE SERVICIOS No.:					226	Del Año:		2023
CONTRATISTA:	MANUEL HUMBERTO SANTANDER PELAEZ				C.C./ C.E. No.:	98.629.535		
PERIODO DEL INFORME:	Desde:	01	11	2023	Hasta:	31	11	2023
		Día	Mes	Año		Día	Mes	Año

14.	Elaborar el documento que describa los procesos de Inteligencia de Amenazas, Caza de Amenazas y Respuesta a Incidentes para el IPSE.	No se desarrollaron actividades en este período.	**CERRADO**
15.	Elaborar el plan de recuperación de desastres específico para la tecnología de la información del IPSE en el cual se definan las estrategias, acciones y recursos necesarios para restablecer los sistemas de información y las operaciones tecnológicas en caso de eventos catastróficos o interrupciones graves.	Al final del documento se relaciona el plan correspondiente.	**CERRADO**
16.	Participar en las reuniones y sesiones de trabajo solicitadas y/o requeridas en el desarrollo del objeto contractual.	No se desarrollaron actividades en este período.	**EN EJECUCIÓN**
17.	Desarrollar las demás actividades	No se desarrollaron actividades en este período.	**EN EJECUCIÓN**

	relacionadas con el objeto contractual que sean designadas por el supervisor del contrato.		

3. PRODUCTOS ENTREGADOS (En caso de haber sido pactados)

- Diagnóstico de seguridad de la información basado en la herramienta de diagnóstico del MSPI.
- Documento con proceso de caza de amenazas, threat modeling y respuesta a incidentes.

Se anexa al presente informe los soportes de las actividades efectuadas:

DISASTER RECOVERY PLAN TI

IPSE

NOVIEMBRE 2023

CONTRATO DE PRESTACIÓN DE SERVICIOS No.:					226	Del Año:		2023
CONTRATISTA:	MANUEL HUMBERTO SANTANDER PELAEZ				C.C./ C.E. No.:	98.629.535		
PERIODO DEL INFORME:	Desde:	01	10	2023	Hasta:	31	10	2023
		Día	Mes	Año		Día	Mes	Año

TABLA DE CONTENIDO

1. Introducción 8

1.1 Objetivo del Plan 8
1.2 Alcance del Plan 8
1.3 Definición de Desastre en el Contexto del IPSE 9
1.4 Importancia del DRP en el Sector Eléctrico 9
1.5 Principios Rectores del DRP 10
1.6 Participantes y Responsabilidades 12
1.7 Estructura del Documento 12

2. Análisis de riesgo y evaluación de impacto en el negocio 12

2.1 Procesos corporativos del IPSE 12
2.2 Evaluación de los sistemas críticos de TI 14

3. ESTRATEGIAS DE RECUPERACIÓN 20

3.1 Sistema de gestión documental Orfeo 20
3.2 Sistema de información geográfica SIGIPSE..... 21
3.3 Página Web..... 22
3.4 Escritorios virtuales..... 23

Introducción

Objetivo del Plan

Este capítulo establece el marco y los objetivos del Plan de Recuperación de Desastres (DRP) específicamente diseñado para los activos tecnológicos críticos del IPSE. El objetivo principal es garantizar la continuidad del negocio y la integridad de los sistemas de información críticos en el caso de un desastre natural, ciberataque, falla técnica u otros incidentes disruptivos.

Alcance del Plan

El DRP abarca todos los aspectos críticos de las operaciones tecnológicas de la empresa, incluyendo infraestructura de red, sistemas de control industrial, bases de datos, aplicaciones de software, y hardware. Se consideran tanto los centros de datos principales como los secundarios y otros activos tecnológicos distribuidos.

CONTRATO DE PRESTACIÓN DE SERVICIOS No.:					226	Del Año:		2023
CONTRATISTA:	MANUEL HUMBERTO SANTANDER PELAEZ				C.C./ C.E. No.:	98.629.535		
PERIODO DEL INFORME:	Desde:	01	10	2023	Hasta:	31	10	2023
		Día	Mes	Año		Día	Mes	Año

Definición de Desastre en el Contexto del IPSE

Un desastre se define como cualquier evento que cause una interrupción significativa en las operaciones normales de la empresa, incluyendo pero no limitado a:

- Desastres naturales (tormentas, terremotos, inundaciones).
- Ataques cibernéticos (ransomware, intrusiones a la red).
- Fallas técnicas y errores humanos.

Importancia del DRP en el Sector Eléctrico

El sector eléctrico es fundamental para el funcionamiento de la sociedad moderna. La dependencia de la electricidad en todos los aspectos de la vida diaria y la economía convierte a la continuidad del servicio eléctrico en una necesidad primordial. En este contexto, el Plan de Recuperación de Desastres (DRP) juega un papel crucial:

- El IPSE tiene impacto en la Seguridad Nacional y la Infraestructura Crítica:
  - Infraestructura Crítica: El sector eléctrico es considerado una infraestructura crítica. Una interrupción prolongada puede desencadenar fallos en cascada en otros sectores vitales como el agua, la salud, el transporte y las comunicaciones.
  - Seguridad Nacional: La estabilidad del sector eléctrico es esencial para la seguridad nacional. Las interrupciones pueden afectar operaciones militares y de emergencia, así como la seguridad de datos críticos.
- Consecuencias Económicas
  - Impacto Económico Directo: Interrupciones en el suministro eléctrico pueden resultar en pérdidas económicas sustanciales para la empresa, incluyendo daños a equipos, pérdida de ingresos y penalizaciones por incumplimiento de contratos.
  - Impacto Económico Indirecto: Las empresas y consumidores dependen de la electricidad para sus operaciones. La falta de suministro puede causar pérdidas económicas significativas a nivel regional o nacional.
- Impacto en la Salud y Seguridad Pública
  - Servicios de Emergencia: Los hospitales y servicios de emergencia dependen de la electricidad para operar. Una interrupción puede poner en riesgo vidas y la prestación de servicios críticos de salud.

  - Bienestar Público: La falta de electricidad afecta el bienestar general, especialmente en condiciones extremas de temperatura o durante emergencias naturales.
- Repercusiones Sociales y Comunitarias
  - Calidad de Vida: La electricidad es esencial para la calidad de vida moderna, impactando todo, desde la calefacción y refrigeración doméstica hasta las comunicaciones y el entretenimiento.
  - Confianza Pública: La capacidad de proveer un servicio eléctrico confiable y seguro es fundamental para mantener la confianza pública en la empresa y en el gobierno.
- Desafíos Únicos del Sector
  - Complejidad Técnica: El sector eléctrico se caracteriza por su alta complejidad técnica, con redes interconectadas y sistemas de control industrial que requieren una atención especial en el DRP.
  - Ciberseguridad: Dada la creciente amenaza de ataques cibernéticos, el DRP debe abordar la protección de infraestructuras críticas contra tales riesgos.

Principios Rectores del DRP

El Plan de Recuperación de Desastres (DRP) en el IPSE se rige por una serie de principios fundamentales que garantizan su efectividad y relevancia. Estos principios son esenciales para diseñar un plan robusto y resiliente que pueda responder adecuadamente a diversas situaciones de emergencia:

- Resiliencia
  - Fortalecimiento de Infraestructura: El DRP debe enfocarse en fortalecer la infraestructura contra posibles desastres, lo que implica una inversión continua en tecnologías más resistentes y sistemas redundantes.
  - Capacidad de Adaptación: La resiliencia también implica la capacidad de adaptar y modificar rápidamente los sistemas y procesos en respuesta a desastres inesperados o cambios en el entorno de amenazas.
- Recuperación Rápida
  - Tiempo de Recuperación Objetivo (RTO): Establecimiento de objetivos claros para el tiempo de recuperación de servicios críticos, minimizando así el impacto de las interrupciones.

- Priorización de Activos Críticos: Identificación y priorización de los sistemas y procesos más críticos para el funcionamiento de la empresa, asegurando su rápida recuperación.

- Redundancia
  - Sistemas Duplicados: Implementación de sistemas duplicados para los componentes críticos del sistema eléctrico y de TI, asegurando que la falla de un componente no cause una interrupción total.
  - Centros de Datos y Operaciones de Respaldo: Mantenimiento de centros de datos y operaciones de respaldo que puedan asumir las funciones críticas en caso de fallo del sistema principal.
- Revisión y Actualización Continua
  - Adaptación a Nuevas Tecnologías y Amenazas: El DRP debe ser un documento vivo, regularmente actualizado para reflejar los cambios en tecnología y el paisaje de amenazas.
  - Feedback y Aprendizaje Continuo: Incorporación de lecciones aprendidas de ejercicios de prueba y experiencias reales de desastres para mejorar continuamente el plan.
- Enfoque Integral
  - Integración con la Gestión de Riesgos y Seguridad: El DRP debe estar alineado con la gestión de riesgos más amplia de la empresa y los planes de seguridad para crear un enfoque cohesivo.
  - Participación de Stakeholders: Involucrar a todas las partes interesadas, incluyendo personal de TI, operaciones, seguridad, y la alta dirección, para garantizar una visión integral y el compromiso con el plan.
- Formación y Concienciación
  - Capacitación del Personal: La formación regular del personal en procedimientos de recuperación de desastres es esencial para asegurar una respuesta rápida y efectiva durante un incidente.
  - Simulacros y Pruebas: Realización periódica de simulacros y pruebas del DRP para garantizar que todos los involucrados estén familiarizados con sus roles y responsabilidades en caso de un desastre.

Estos principios no solo guían la creación y mantenimiento del DRP, sino que también aseguran que la empresa del sector eléctrico esté preparada para enfrentar y recuperarse de desastres de manera efectiva, protegiendo así sus operaciones, clientes y la infraestructura crítica a la que sirve.

Participantes y Responsabilidades

Las actividades descritas en este plan serán ejecutadas por el equipo de TI. Se involucra al área de comunicaciones externas para coordinar la comunicación con las distintas partes interesadas de la entidad.

Estructura del Documento

El DRP se divide en varias secciones, cada una abordando diferentes aspectos de la recuperación de desastres:

- Análisis de Riesgo y Evaluación de Impacto en el Negocio (BIA)
- Estrategias de Recuperación.
- Planes de Implementación.
- Pruebas y Mantenimiento del Plan.

Análisis de riesgo y evaluación de impacto en el negocio

El Análisis de Impacto en el Negocio (BIA) es un componente crítico del Plan de Recuperación de Desastres (DRP) del IPSE. Su propósito es identificar y evaluar los impactos de interrupciones en los sistemas de tecnología de la información (TI) sobre las operaciones de la empresa.

Procesos corporativos del IPSE

- Gestión de supervisión, interventoría y seguimiento: Su objetivo es realizar supervisión, interventoría o seguimiento a los proyectos relacionados con infraestructura energética o de prestación del servicio de energía eléctrica verificando que las obligaciones contractuales se cumplan.
- Gestión de proyectos: Su objetivo es estructurar, viabilizar y promocionar proyectos que permitan entregar soluciones energéticas sostenibles y eficientes a las comunidades de las ZNI.
- Gestión de telemetría y monitoreo: Su objetivo es generar información oportuna, validada y confiable de prestación del servicio de energía en las ZNI, a través de la disponibilidad de la infraestructura de telemetría y aplicando metodologías documentadas.

CONTRATO DE PRESTACIÓN DE SERVICIOS No.:					226	Del Año:		2023
CONTRATISTA:	MANUEL HUMBERTO SANTANDER PELAEZ				C.C./ C.E. No.:	98.629.535		
PERIODO DEL INFORME:	Desde:	01	10	2023	Hasta:	31	10	2023
		Día	Mes	Año		Día	Mes	Año

- Gestión auditorías: Su objetivo es dar cumplimiento a las actividades establecidas en la realización de las Auditorías de Gestión teniendo en cuenta la normatividad vigente, procurando la mejora continua en el desempeño institucional.
- Planeación institucional: Su objetivo es establecer los lineamientos de la planificación institucional a partir del Plan Nacional de Desarrollo y el Plan Sectorial, para dar cumplimiento a la misión, visión y objetivos de la entidad, siguiendo las directrices del Modelo Integrado de Planeación y Gestión, orientado en la programación y el seguimiento de la ejecución del presupuesto.
- Mejoramiento: Su objetivo es realizar el seguimiento a la medición y análisis de los procesos del Sistema de Gestión Integrado, adicionalmente, evaluar su desempeño a partir de los instrumentos establecidos para el mejoramiento continuo de los procesos.
- Gestión de talento humano: Su objetivo es gestionar las actividades requeridas para la permanencia, compensación y desarrollo del talento humano desde su vinculación hasta su retiro, seleccionando al personal de acuerdo con sus competencias y buscando mejorarlas para lograr el cumplimiento de los objetivos institucionales.
- Gestión SGSST: Su objetivo es contribuir al mejoramiento de las condiciones de trabajo seguro, saludable y de bienestar de los servidores públicos del IPSE y las partes interesadas, previniendo los peligros, controlando los riesgos de seguridad y salud en el trabajo y favoreciendo el clima laboral, con la normatividad legal aplicable.
- Gestión de infraestructura: Su objetivo es suministrar, mantener y salvaguardar los recursos de infraestructura (bienes y servicios) necesarios para el cumplimiento de los objetivos institucionales garantizando la oportunidad y satisfacción de las partes interesadas.
- Gestión financiera: Su objetivo es registrar y analizar los hechos económicos para presentar razonable y oportunamente la información financiera.
- Gestión de TI: Su objetivo es gestionar estratégicamente las necesidades de innovación en tecnología, seguridad y operatividad que requieran las partes interesadas, con el fin de apoyar el cumplimiento de los objetivos institucionales en el marco de la estrategia de Gobierno Digital.
- Gestión jurídica: Su objetivo es representar al IPSE en los asuntos judiciales y extrajudiciales a través de asistencia jurídica especializada, proveer por la

prevención del daño antijurídico y asesorar al Instituto en la aplicación de la normatividad vigente.

- Gestión de contratación: Su objetivo es realizar el proceso de contratación de manera eficaz, eficiente y efectiva, en armonía con los objetivos institucionales y las normas legales vigentes para coadyuvar en el cumplimiento de la misión institucional
- Gestión documental: Su objetivo es gestionar la documentación institucional a través del Sistema de Gestión Documental, desarrollando eficientemente las actividades de creación, recepción, ubicación, acceso, custodia, trazabilidad, recuperación y preservación de los documentos, cumpliendo la legislación vigente y las normas técnicas correspondientes.

Evaluación de los sistemas críticos de TI

Para efectos de la evaluación de riesgos, se utilizarán las definiciones de probabilidad e impacto de acuerdo con las figuras 1 y 2.

Nivel	Descriptor	Descripción	Frecuencia
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	Posible	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	Improbable	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

Figura 1: Tabla probabilidad metodología de riesgos IPSE

CONTRATO DE PRESTACIÓN DE SERVICIOS No.:					226	Del Año:		2023
CONTRATISTA:	MANUEL HUMBERTO SANTANDER PELAEZ				C.C./ C.E. No.:	98.629.535		
PERIODO DEL INFORME:	Desde:	01	10	2023	Hasta:	31	10	2023
		Día	Mes	Año		Día	Mes	Año

Nivel	Impacto Consecuencias Cuantitativo	Impacto Consecuencias Cualitativo
Catastrófico	Impacto que afecte la ejecución presupuestal en un valor ≥50%. Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%. Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50%. Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad. Impacto que afecte la ejecución presupuestal en un valor ≥20%. Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%.	Interrupción de las operaciones de la entidad por más de cinco (5) días. Intervención por parte de un ente de control u otro ente regulador. **Pérdida de información crítica para la entidad que no se puede recuperar.** **Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal.** **Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.** **Interrupción de las operaciones de la entidad por más de dos (2) días.** **Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta.**

CONTRATO DE PRESTACIÓN DE SERVICIOS No.:					226	Del Año:		2023
CONTRATISTA:	MANUEL HUMBERTO SANTANDER PELAEZ				C.C./ C.E. No.:	98.629.535		
PERIODO DEL INFORME:	Desde:	01	10	2023	Hasta:	31	10	2023
		Día	Mes	Año		Día	Mes	Año

Mayor	Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20%. Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad. Impacto que afecte la ejecución presupuestal en un valor ≥5%.	**Sanción por parte del ente de control u otro ente regulador.** **Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno.** **Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.** **Interrupción de las operaciones de la entidad por un (1) día.**

CONTRATO DE PRESTACIÓN DE SERVICIOS No.:					226	Del Año:		2023
CONTRATISTA:	MANUEL HUMBERTO SANTANDER PELAEZ				C.C./ C.E. No.:	98.629.535		
PERIODO DEL INFORME:	Desde:	01	10	2023	Hasta:	31	10	2023
		Día	Mes	Año		Día	Mes	Año

Moderado	Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%. Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥5%. Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad. Impacto que afecte la ejecución presupuestal en un valor ≥1%. Pérdida de cobertura en la prestación de los servicios de la entidad ≥5%.	**Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad.** **Inoportunidad en la información, ocasionando retrasos en la atención a los usuarios.** **Reproceso de actividades y aumento de carga operativa.** **Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos.** **Investigaciones penales, fiscales o disciplinarias.** **Interrupción de las operaciones de la entidad por algunas horas.**

CONTRATO DE PRESTACIÓN DE SERVICIOS No.:					226	Del Año:		2023
CONTRATISTA:	MANUEL HUMBERTO SANTANDER PELAEZ				C.C./ C.E. No.:	98.629.535		
PERIODO DEL INFORME:	Desde:	01	10	2023	Hasta:	31	10	2023
		Día	Mes	Año		Día	Mes	Año

Menor	Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥1%. Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥1% del presupuesto general de la entidad. Impacto que afecte la ejecución presupuestal en un valor ≥0,5%. Pérdida de cobertura en la prestación de los servicios de la entidad ≥1%.	**Reclamaciones o quejas de los usuarios, que implican investigaciones internas disciplinarias.** **Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.** **No hay interrupción de las operaciones dela entidad.**
Insignificante	Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥0,5%. Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5% del presupuesto general de la entidad.	**No se generan sanciones económicas o administrativas.** **No se afecta la imagen institucional de forma significativa.**

Figura 2: Tabla impacto metodología de riesgos IPSE

Los activos tecnológicos objeto del plan de recuperación de desastres de TI son las siguientes:

CONTRATO DE PRESTACIÓN DE SERVICIOS No.:					226	Del Año:		2023
CONTRATISTA:	MANUEL HUMBERTO SANTANDER PELAEZ				C.C./ C.E. No.:	98.629.535		
PERIODO DEL INFORME:	Desde:	01	10	2023	Hasta:	31	10	2023
		Día	Mes	Año		Día	Mes	Año

- Sistema de información geográfica del IPSE – SIGIPSE: Este sistema ofrece varias herramientas de información estandarizada y georreferenciada sobre información de soluciones energéticas del IPSE, caracterización de las Zonas No Interconectadas y datos de contexto a escala nacional, departamental y municipal. Esta información está representada en mapas interactivos y georreferenciados a través de vinculación de sistemas de información especializados cartografía-geografía. Adicionalmente se encuentra información detallada de las entidades del sector en forma de catálogo de datos. Este sistema es usado por los procesos de gestión de supervisión, interventoría y seguimiento, gestión de proyectos y gestión de telemetría y monitoreo. Su criticidad con base en la tabla de impacto de la metodología de riesgos es mayor. Al ser un sistema con información crítico, no es aceptable pérdida de información por lo que su RPO es 0. Luego de 1 hora la organización empieza a sufrir impactos relevantes, motivo por el cual su RTO es de máximo 1 hora.
- Sistema de gestión documental ORFEO: El instituto tiene dentro de sus deberes garantizar el normal funcionamiento de sus aplicaciones lo cual conlleva a la necesidad de ofrecer un servicio óptimo y eficiente para garantizar la preservación, gestión y visualización de la información que se administra, se produce y divulga de la institución. Se cuenta con un sistema de gestión documental llamado ORFEO el cual es una herramienta que apoya a las actividades administrativas, técnicas, de planificación, manejo y organización de la documentación producida y recibida por las entidades desde su origen hasta su destino final, esto con el fin de facilitar, controlar y conservar la documentación dando buenas prácticas en el cumplimiento de normatividad archivística. Todos los procesos descritos en el numeral 2.1 lo usan. Su criticidad con base en la tabla de impacto de la metodología de riesgos es catastrófica. Luego de 2 horas los impactos de la organización son relevantes, motivo por el cual la RTO es de dos horas.
- Página Web: El IPSE cuenta un portal web institucional https://ipse.gov.co/ reposa toda la información referente a su misionalidad como entidad estatal, los contenidos se administran a través de WordPress multisite. Es de vital importancia garantizar su optimo funcionamiento y acceso para los diferentes actores (procesos internos y visitantes). Todos los procesos descritos en el numeral 2.1 lo usan. Su criticidad con base en la tabla de impacto de la metodología de riesgos es mayor. Luego de 2 horas

los impactos de la organización son relevantes, motivo por el cual la RTO es de dos horas.

- Thin Client: El IPSE cuenta con terminales de usuario Thin Client, con su respectivo software y licencias para uso de ambiente de virtualización de escritorios VMware Horizon, contamos con enlaces de comunicación entre las 3 sedes del IPSE, con capacidades y velocidades limitadas, por lo cual se requiere mejorar estas capacidades ampliando, descentralizando los recursos de infraestructura para seguir con un crecimiento, respaldo, rendimiento y protección de aplicaciones en diversos entornos. Todos los procesos descritos en el numeral 2.1 lo usan. Su criticidad con base en la tabla de impacto de la metodología de riesgos es catastrófica. Al tratarse de la información de los usuarios que se utiliza día a día, no es posible aceptar pérdida de información por lo que su RPO es 0. Al ser el sistema utilizado por los usuarios para la ejecución de sus actividades diarias, se acepta un RTO máximo de dos horas para que la organización no sufra impactos relevantes.

Los riesgos de interrupción a los cuales pueden verse expuestos estos sistemas son:

- Interrupción de la continuidad de los sistemas tecnológicos: Esto puede ocasionarse por ataque cibernético, fallos en la alimentación de energía, errores humanos, sabotaje, problemas de la red o los enlaces de comunicaciones, desastre físico en el sitio donde se encuentran localizados (terremotos, incendio, inundación, entre otros) o daño físico de los componentes involucrados. La valoración en probabilidad es probable y la valoración en impacto es mayor.
- Pérdida de información: Esto puede ocasionarse por ataque cibernético, fallo en la alimentación de energía, error humano, sabotaje, daño físico de los componentes involucrados o problemas de ejecución de las copias de seguridad o replicación en los ambientes de procesamiento alterno. La valoración en probabilidad es probable y la valoración en impacto es mayor.

ESTRATEGIAS DE RECUPERACIÓN

Sistema de gestión documental Orfeo

- Se establecerán dos ambientes: principal y alterno.
    - El ambiente principal estará ubicado en azure.

- El ambiente alterno será on-premise.

- Crear un registro DNS para Orfeo con duración de 300 segundos apuntando al ambiente principal del sistema.
- La base de datos sobre la que funciona Orfeo es postgresql. Se requiere configurar la replicación en línea desde el principal al alterno. La guía para configurar la replicación es https://kinsta.com/blog/postgresql-replication/#:~:text=PostgreSQL%20replication%20is%20defined%20as,as%20the%20“replica”%20server.
- En caso de desastre, se procede a switchear el ambiente cambiando el registro DNS al ambiente alterno que está on-premise. El tiempo de recuperación será de 5 minutos mientras el DNS refresca.
- Es importante efectuar pruebas de recuperación al menos mensuales para asegurar que el proceso de replicación funciona de forma adecuada.
- Se debe efectuar snapshot diarios de las máquinas en nube para asegurar recuperación del sistema principal en caso de alguna novedad. En caso de desastre en la nube, se procede con la restauración inmediata del snapshot para en un máximo de una hora poder tener servicio activo y funcionando.
- Se debe efectuar la copia de seguridad de las máquinas on-premise diarias para asegurar un punto adicional de recuperación. En caso que la restauración del ambiente de nube falle, se procede a restaurar las copias de seguridad de las máquinas on-premise, asegurando recuperación del servicio en un máximo de 12 horas.

Sistema de información geográfica SIGIPSE

- Se establecerán dos ambientes: principal y alterno.
  - El ambiente principal estará ubicado en azure.
  - El ambiente alterno será on-premise.
- Crear un registro DNS para SIGIPSE con duración de 300 segundos apuntando al ambiente principal del sistema.
- La base de datos sobre la que funciona SIGIPSE es postgresql. Se requiere configurar la replicación en línea desde el principal al alterno. La guía para configurar la replicación es https://kinsta.com/blog/postgresql-

replication/#:~:text=PostgreSQL%20replication%20is%20defined%20as,as%20the%20“replica”%20server.

- En caso de desastre, se procede a switchear el ambiente cambiando el registro DNS al ambiente alterno que está on-premise. El tiempo de recuperación será de 5 minutos mientras el DNS refresca.
- Es importante efectuar pruebas de recuperación al menos mensuales para asegurar que el proceso de replicación funciona de forma adecuada.
- Se debe efectuar snapshot diarios de las máquinas en nube para asegurar recuperación del sistema principal en caso de alguna novedad. En caso de desastre en la nube, se procede con la restauración inmediata del snapshot para en un máximo de una hora poder tener servicio activo y funcionando.
- Se debe efectuar la copia de seguridad de las máquinas on-premise diarias para asegurar un punto adicional de recuperación. En caso que la restauración del ambiente de nube falle, se procede a restaurar las copias de seguridad de las máquinas on-premise, asegurando recuperación del servicio en un máximo de 12 horas.

Página Web

- Se establecerán tres servidores redundantes, los cuales estarán ubicados en regiones distintas.
- El registro DNS del servidor web apuntará a un azure load balancer, el cual debe ser configurado para balancear las cargas entre los tres servidores.
- Debe contarse con un esquema de monitoreo de red para determinar cualquier falla en alguno de los servidores. En caso que ocurra, el servicio no se verá interrumpido y se hace necesario que TI del IPSE proceda a recuperar el servidor para asegurar que la continuidad permanece.
- Las máquinas deben replicarse de forma incremental del principal a los alternos utilizando la siguiente funcionalidad: https://learn.microsoft.com/es-es/azure/virtual-machines/disks-copy-incremental-snapshot-across-regions?tabs=azure-cli.
- Es importante efectuar pruebas de recuperación al menos mensuales para asegurar que el proceso de replicación funciona de forma adecuada.

CONTRATO DE PRESTACIÓN DE SERVICIOS No.:					226	Del Año:		2023
CONTRATISTA:	MANUEL HUMBERTO SANTANDER PELAEZ				C.C./ C.E. No.:	98.629.535		
PERIODO DEL INFORME:	Desde:	01	10	2023	Hasta:	31	10	2023
		Día	Mes	Año		Día	Mes	Año

Escritorios virtuales

- El IPSE cuenta con OneDrive donde todos los usuarios pueden trabajar para contar con una copia efectiva de seguridad de toda la información que plantean. Es indispensable asegurar que todos los usuarios trabajen sobre este ambiente para que la información permanezca.
- Los escritorios virtuales de azure deben contar con las imágenes que reflejen el mismo software instalado. Es importante actualizarla periódicamente para incluir los parches de seguridad que pudieran ser requeridos de acuerdo con las vulnerabilidades que sean evidenciadas.
- Si la plataforma de escritorios virtuales de azure tiene alguna novedad, los usuarios pueden switchearse a la que se encuentra on-premise y seguir trabajando con sus archivos desde onedrive.

En constancia de lo anterior, se firma el presente informe el (12) de (DICIEMBRE) de (2023).



Firma Contratista

Nombre: MANUEL HUMBERTO SANTANDER PELÁEZ



Vo.Bo. Supervisor y/o Interventor

Nombre: TANIA SIERRA HUERTAS