Firma de Autorizaciones		
Elaboró	**Revisó**	**Aprobó**
Ingenieros Proceso Gestión Tecnológica OAP	Ingenieros Proceso Gestión Tecnológica OAP e Ingeniero a cargo del Sistema Integrado de Gestión	Jefe Oficina Asesora de Planeación

Control de Cambios	
Fecha	**Descripción**
Mayo de 2010	Actualización del Documento
Diciembre de 2013	Actualización del Documento
Julio de 2015	Actualización del Documento, de acuerdo a lo aprobado por el Comité Interno de Sistemas mediante Acta No. 03
Noviembre de 2017	Se incluyen anexo Nro. 1. Plan de contingencia al sistema de información administrativo y anexo Nro. 2 Plan de contingencia al sistema de información NÓMINA HUMANO, los cuales fueron aprobados en comité Interno de Sistemas mediante Acta Nro. 5
Marzo de 2018	Se actualiza el documento en cuanto a objetivo general, objetivos específicos, alcance del plan de contingencia de Tecnología, normatividad, se incluyen los sistemas de información existentes actualmente en el IDEP, se excluye información de diagnóstico y recomendaciones que no aplican al plan de contingencia actual. Se incluye información de tipos de incidentes que se pueden presentar.
Diciembre de 2018	Se incluye anexo 3: Contingencia para la recuperación recursos de red carpetas z y de oficina y anexo 4 contingencia para el apagado de hiperconvergencia. Se incluyen definiciones de hiperconvergencia, máquina virtual, sistema de información, Snapshots de almacenamiento. Se ajusta al numeral 7.2 incluyendo descripción de los Backus realizados y su periodicidad de ejecución.
Febrero de 2019	Se actualiza el numeral 7.2 del plan.
Mayo 2019	Se agregan los anexos 5, 6, 7, 8. Se actualiza el Anexo 4 PLAN DE CONTINGENCIA HYPERCONVERGENCIA actualizándose a la fecha, con las máquinas virtuales actuales. De igual forma se actualiza el Anexo 3. RECUPERACIÓN INFORMACIÓN RECURSOS DE RED. CARPETAS Z Y DE OFICINA, ajustándola a la nueva

	normativa del IDEP, que refiere a las Tablas de Retención Documental TRD. Se ajustó la tabla de contenido. Se hacen ajustes al ANEXO 5. PLAN DE ACCIÓN HIPERCONVERGENCIA.
Septiembre 2019	Se incluye los pasos para realizar el BACKUP Y RECUPERACIÓN DE LA CONFIGURACIÓN DEL SWITCHES HIPERCONVERGENCIA Y SWITHCES CISCO, ROUTER.
Mayo de 2020	Se actualiza el documento incluyendo la sección 8 que contempla el plan de contingencia de los seis sistemas de información. Se incluye la sección 9 donde se agrupan los otros planes de contingencia de sistemas como firewall, antivirus, hiperconvergencia y hardware en general. Se actualiza el documento de acuerdo a los contratos actuales en los sistemas de información y el antivirus. Se omiten los Backus a las carpetas "Z" las cuales ya no se utilizan y a cambio se realizan los Backus a las carpetas de las TRD... Se incluye la definición de Plan de Contingencia y Plan de continuidad del negocio donde se indica la diferencia entre estos dos planes. Se adiciona, en relación con las plataformas tecnológicas, bases de datos e infraestructura web, el ANEXO 15. SERVIDOR CONTINGENCIA WEB - ENTRADA Y SALIDA DE PRODUCCIÓN Se actualiza la sección de normatividad, Se incluye las definiciones de SSH y Cliente SSH. Se actualizan el ítem 3 SISTEMAS DE INFORMACIÓN PLATAFORMAS TECNOLÓGICAS, BASES DE DATOS E INFRAESTRUCTURA WEB DEL IDEP en donde se agregan las bases de datos. Se actualiza el Anexo 14. Se actualiza el ítem 7.2. PROCEDIMIENTO DE BACKUP O COPIA DE SEGURIDAD Se actualiza la tabla de contenido.
Junio 2021	Reestructuración del documento. De acuerdo a las observaciones que se han realizado en las auditorías se reestructuro el documento de la siguiente forma: Se incluye la sección 3 – Análisis de Impacto al Negocio BIA. Se incluye la sección 4 – Controles preventivos Se reestructura el punto 5 – Estrategia de contingencia Se incluye la sección 6- Mantenimiento al plan de contingencia

	Las secciones 4 y 5 de la versión 11 pasan a ser las secciones 7 y 8 respectivamente. En ambas secciones se realizan ajustes, se incluye nueva información. La sección 3 de la versión 11 pasa a ser la sección 9 de este documento en la cual se incluyen 7 numerales que consolidan las actividades generales del plan de contingencia. Los anexos pasan de 15 a 10, se reestructuran agrupando los que comparten las mismas actividades y tiempos. Las actividades iniciales de los anexos se trasladas a los 7 numerales del punto 9.
Octubre de 2022	Se da continuidad a la actualización del plan de contingencia en la especificación del análisis de impacto al negocio BIA. Se realizan cambios de redacción y actualización en los ítems 3.1, ANEXO 5 y otros. Se agregó el ANEXO 11. Se identifican los servicios y sistemas de información para dejarlos diferenciados.
Septiembre de 2023	Atendiendo la recomendación de la auditoría se crea la tabla con la interrelación entre los riesgos, activos de información y el plan de acción para cada contingencia. Se adicionan ANEXO 12 PLAN DE ACCIÓN BACKUP Y RECUPERACIÓN DEL SERVICIO WEB, ANEXO 13 PLAN DE ACCIÓN RECUPERACIÓN DEL CORREO ELECTRÓNICO y ANEXO 14 PLAN DE ACCIÓN RECUPERACIÓN DEL BIOMÉTRICO. Se agrega la tabla donde se indican las contingencias efectuadas desde 2019 a 2023, en lo que va corrido del año, estas hacen parte del plan de mantenimiento y monitoreo. Estas contingencias son tenidas en cuenta para las actualizaciones, mantenimientos y compras que realiza el IDEP en cuanto a tecnología. Se incluyó el numeral No. 12, Recomendaciones para las Oficinas y Dependencias del IDEP.

TABLA DE CONTENIDO

INTRODUCCIÓN

Para el Instituto para la Investigación Educativa y el Desarrollo Pedagógico IDEP es muy importante asegurar la operación y continuidad del negocio, por tal motivo ha decidido planear, implementar y mejorar un Plan de Contingencia Tecnológica IDEP, en adelante BCP, para identificar la infraestructura física, tecnológica, procesos críticos y sobre todo los riesgos de tipo catastróficos y así definir estrategias a fin de reducir los tiempos de recuperación, garantizando la continuidad de las operaciones y la gestión de los riesgos que pudieran afectar la continuidad del IDEP.

El BCP en el IDEP, permite que se realice la identificación de los riesgos que afecten la continuidad de la Institución, priorización de procesos de acuerdo con su criticidad, definición de estrategias de recuperación y el retorno de los procesos en el menor tiempo posible, identificación y asignación de recursos humanos y financieros y la definición de un plan de pruebas para el mantenimiento y mejora del BCP. Al establecer las medidas de mitigación, el IDEP, habilita los mecanismos que le permitan cumplir con los siguientes propósitos:

- Reducir el impacto generado frente a incidentes sobre la operación de las funciones críticas.

- Proteger la imagen, los intereses y el buen nombre de la Entidad.

- Disminuir las pérdidas de información.

- Obtener formación frente a incidentes de tal manera la protección de la integridad de las personas y bienes de la Entidad en forma adecuada, realizando una buena administración de la crisis.

1. OBJETIVO

1.1. Objetivo General

Proporcionar al Instituto para la Investigación Educativa y el Desarrollo Pedagógico IDEP un plan para contar con estrategias que permitan mitigar los riesgos, las causas y consecuencias asociadas a la infraestructura tecnológica, de manera que se pueda generar confianza a todos los interesados en cuanto al funcionamiento y rápida recuperación de los sistemas de información y servicios tecnológicos ante las posibles fallas que interrumpan la operación normal de los mismos.

1.2. Objetivos específicos

- Garantizar la continuidad del negocio controlando los componentes y elementos considerados como críticos en la operación diaria.

- Definir las acciones preventivas y correctivas, que permitan prevenir las eventualidades en las operaciones de los sistemas de información del IDEP y corregir en forma oportuna cualquier anormalidad que afecte su correcto funcionamiento.

- Implementar actividades preventivas y controles necesarios que permitan mantener en correcto funcionamiento la infraestructura tecnológica de la Entidad.

- Determinar mediante un análisis de una manera precisa cuales son los riesgos informáticos a los que se encuentra expuesto el Instituto.

- Reevaluar los controles existentes que sean considerados poco efectivos o no sean aplicables.

- Presentar recomendaciones que permitan disminuir la probabilidad de ocurrencia de una eventualidad y definir los procedimientos preventivos resultantes de estas recomendaciones.

- Mitigar las posibles fallas que se pueden presentar en el funcionamiento del hardware y software que conforman la plataforma estratégica del IDEP.

- Definir los lineamientos a seguir en caso de una eventual falla de la infraestructura o de los sistemas de información.

2. ALCANCE DEL PLAN DE CONTINGENCIA

El Plan de Contingencia del IDEP se orienta al proceso establecido como crítico dentro de la matriz de análisis de impacto del negocio (BIA), el cual es Gestión de las Tecnologías de la Información y las Comunicaciones y sus activos de información como proceso crítico. Dicho proceso es importante para que la Entidad continúe operando.

Éste alcance estará sujeto a las actualizaciones requeridas por la Alta Dirección y actividades de la Entidad.

3. ANÁLISIS DE IMPACTO AL NEGOCIO - BIA (Business Impact Analysis)

La fase de Análisis de Impacto del Negocio BIA (Business Impact Analysis) por sus siglas en inglés), permite identificar los procesos misionales y analizar el nivel de impacto que traería sobre estos las fallas que puedan presentarse en los servicios y sistemas de información que lo soportan. Esta sección contiene el análisis de impacto al negocio para el área de tecnología del IDEP, por lo tanto hace parte de la identificación y gestión de los sistemas y servicios de misión crítica en la Entidad.

Propósito del Análisis BIA y etapas:

El análisis de impacto del negocio como parte del plan de continuidad del negocio, debe entenderse como un marco conceptual sobre el cual las entidades deben planear integralmente los alcances y objetivos, que permiten proteger la información, en todas sus áreas críticas.

Las entidades deben establecer un análisis de impacto del negocio, que este alineado con el Plan General de Continuidad del Negocio de la Entidad; este debe tener una estrategia de continuidad de TI, que contenga los objetivos globales de la entidad, con respecto a las dimensiones de disponibilidad de datos, infraestructura tecnológica y recurso humano.

3.1. Identificación de funciones y procesos

En este paso se identifican las funciones del negocio útiles para apoyar la misión y los objetivos a alcanzar en el Sistema de Gestión de Seguridad de Información de

la Entidad. Este punto tiene como resultado generar un listado de roles y procesos, que sirven de análisis para el cumplimiento de los siguientes pasos del *BIA*.

Se identifican los servicios y sistemas de información con los cuales opera la entidad, así como los roles que desempeñan los diferentes actores frente a los mismos que inciden de alguna manera en la seguridad de la información.

Procesos (Servicios y Sistemas de Información)	Rol
Sistema de Información Cliente/Servidor: Goobi que interopera con el sistema de información Humano en modalidad fuera de línea.	Usuarios internos del Sistema. Soporte de primer nivel del sistema de información Goobi. Soporte de la infraestructura del IDEP. Proveedor del sistema Goobi. Soporte de especialistas del contrato de mantenimiento. Rol del Backup.
Sistema de Información web: Koha	Administradores de la plataforma Koha. Usuarios internos y externos del sistema. Soporte de la infraestructura del IDEP. Soporte de especialistas del contrato de mantenimiento. Rol del Backup.
Sistema de Información web: DSpace	Administradores de la plataforma DSpace. Usuarios internos y externos del sistema. Soporte de la infraestructura del IDEP. Soporte de especialistas del contrato de mantenimiento. Rol del Backup.

Sistema de Información web: OJS	Administradores de la plataforma OJS. Usuarios internos y externos del Sistema. Soporte de la infraestructura del IDEP. Soporte de especialistas del contrato de mantenimiento. Rol del Backup.
Sistema de Información web: VuFind	Administradores de la plataforma VuFind. Usuarios internos y externos del sistema. Soporte de la infraestructura del IDEP. Soporte de especialistas del contrato de mantenimiento. Rol del Backup.
Servicio de Correo electrónico	Administrador de la plataforma de correo. Usuarios internos del servicio. Proveedor del servicio Google. Rol del Backup.
Servicio de Internet	Contratista que presta el servicio. Usuarios internos del servicio. Soporte de la infraestructura del IDEP.
Servicio de Red (Cableado e inalámbrico)	Administrador del servicio de red. Usuarios internos y externos del servicio. Rol del Backup.
Sistema de Gestión de Aprendizaje (Moodle)	Administradores de la plataforma de Gestión de Aprendizaje Moodle. Usuarios internos y externos del servicio.

	Soporte de la infraestructura del IDEP. Rol del Backup.
Servicio de Base de Datos Oracle	Sistema de información Goobi. Proveedor Goobi SAS. Soporte de primer nivel de los sistemas de información Goobi y Humano. Soporte de la infraestructura del IDEP. Soporte de especialistas del contrato de mantenimiento.
Servicio de Base de Datos Mysql	Soporte de la infraestructura del IDEP. Soporte de especialistas del contrato de mantenimiento.
Servidores Físicos	Soporte de la infraestructura del IDEP. Soporte de especialistas del contrato de mantenimiento.
Sistema de Hipercovergencia	Servidores Virtuales Proveedor del sistema de hiperconvergencia (HP). Soporte de la infraestructura del IDEP. Soporte de especialistas del contrato de mantenimiento.
Servicio de Firewall	Usuarios internos del servicio de VPN. Proveedor del firewall. Soporte de la infraestructura del IDEP. Soporte de especialistas del contrato de mantenimiento.
Servicio de Antivirus	Administrador del Antivirus.

	Equipos de cómputo de uso del IDEP donde se instalaron las licencias de antivirus. Contratista que presta el servicio de soporte a las licencias Sophos. Rol del Backup
Servicio Mesa de Ayuda	Usuarios del IDEP de Mesa de Ayuda Agentes en la mesa de ayuda que dan soporte a los diferentes temas. Rol del Backup
Servicio página web Institucional	Administrador de la página web (webmaster) Usuarios internos y externos de la página.
Servicio de Aulas Virtuales.	Administrador del servicio Aulas Virtuales Proveedor del servicio de correos masivos
Servicio del Directorio Activo principal y secundario (Dominio)	Administrador del Directorio Activo Usuarios internos del servicio. Soporte de la infraestructura del IDEP.
Servicio de correos masivos	Administrador del servicio de correos masivos Proveedor del servicio de correos masivos
Servicio Zoom	Administrador del servicio Zoom Usuarios de la plataforma Zoom Proveedor del servicio
Servicio web Micrositios	Administrador de la página web (webmaster) Usuarios internos y externos de la página.
Otras Bases de Datos (MySql)	Administrador de Bases de Datos Soporte de la infraestructura del IDEP.

	Rol del Backup
Sistema de información Humano que interopera con el sistema de información Goobi en modalidad SAAS (fuera de línea).	Usuarios internos del Sistema. Soporte de primer nivel del sistema de información Humano. Contratista que provee el servicio en modalidad SAAS. Custodio del Backup.

3.2. Evaluación de impactos operacionales

Teniendo en cuenta los elementos operacionales de la organización, se requiere evaluar el nivel de impacto de una interrupción dentro de la Entidad.

El impacto operacional permite evaluar el nivel negativo de una interrupción en varios aspectos de las operaciones del negocio; el impacto se puede medir utilizando un esquema de valoración, con los siguientes **niveles: A, B o C.**

Nivel A: La operación es crítica para el negocio. Una operación es crítica cuando al no contar con ésta, la función del negocio no puede realizarse.
Nivel B: La operación es una parte integral del negocio, sin ésta el negocio no podría operar normalmente, pero la función no es crítica.
Nivel C: La operación no es una parte integral del negocio.

La misión del Instituto es la de fortalecer y gestionar la investigación y la innovación, así como el desarrollo pedagógico y profesional docente, con miras a producir conocimiento que aporte al cierre de las brechas socioeducativas, a la garantía del derecho a la educación, a la transformación pedagógica y al reconocimiento del saber docente, para aportar en la construcción de un nuevo contrato social y ambiental, para el logro de los objetivos perseguidos por la entidad se cuenta con sistemas de información web y servicios que están soportados por la infraestructura tecnológica y todo lo que esto conlleva para mantenerla operando en óptimas condiciones. Es así que en el siguiente cuadro se muestran los sistemas y servicios considerados como indispensable para la operación de la entidad:

Nombre del Servicio o Sistema de Información	Tiempo de interrupción no programada tolerable	Descripción del sistema o servicio	Impacto Operacional
Sistema de Información Cliente/Servidor:	De acuerdo a la importancia y criticidad el sistema Goobi no se	El sistema de información Goobi soporta la operación administrativa y financiera del	

Nombre del Servicio o Sistema de Información	Tiempo de interrupción no programada tolerable	Descripción del sistema o servicio	Impacto Operacional
Goobi que interopera con el sistema de información Humano en modalidad fuera de línea.	programa estar en indisponibilidad por más de 8 horas laborales.	IDEP, la radicación, contratación, almacén (bienes y publicaciones) y la contabilidad. Es un sistema de propiedad de la empresa Goobi SAS.	**A**
Sistema de Información web: Koha	El sistema Koha debe estar disponible los 7 días de la semana para consulta de las partes interesadas en cualquier momento. La indisponibilidad del sistema no afecta directamente la operación de la entidad, pero si la misionalidad.	El sistema Koha es una biblioteca digital que agrupa material bibliográfico dirigido a la comunidad educativa para consulta de los usuarios autorizados. En el buscador bibliográfico podrá realizar búsquedas específicas de acuerdo al criterio que seleccione como título, Autor, Tema, ISBN, ISSN, series y signatura. Es una herramienta de código abierto.	**B**
Sistema de Información web: DSpace	El sistema DSpace debe estar disponible los 7 días de la semana para consulta de las partes interesadas en cualquier momento. La indisponibilidad del sistema no afecta directamente la operación de la entidad, pero si la misionalidad.	El sistema DSpace es una biblioteca digital que agrupa colecciones digitales, y comúnmente es usada como solución de repositorio bibliográfico institucional. Soporta una gran variedad de datos, incluyendo libros, tesis, fotografías, filmes, video, datos de investigación y otras formas de contenido. Los datos son organizados como ítems que pertenecen a una colección; cada colección pertenece a una comunidad. Es una herramienta de código abierto.	**B**
Sistema de Información web: OJS	El sistema OJS debe estar disponible los 7 días de la semana para consulta de las partes interesadas en cualquier momento. La indisponibilidad del sistema no afecta	Esta herramienta OJS es el portal de revistas del IDEP. Es una herramienta de código abierto.	**B**

Nombre del Servicio o Sistema de Información	Tiempo de interrupción no programada tolerable	Descripción del sistema o servicio	Impacto Operacional
	directamente la operación de la entidad, pero si la misionalidad.		
Sistema de Información web: VuFind	El sistema Vufind debe estar disponible los 7 días de la semana para consulta de las partes interesadas en cualquier momento. La indisponibilidad del sistema no afecta directamente la operación de la entidad, pero si la misionalidad.	El objetivo de VuFind es permitir a los usuarios buscar y navegar a través de todos los recursos de la biblioteca digital. Es una herramienta de código abierto.	**B**
Servicio de Correo electrónico que integra la herramienta meet	El tiempo de indisponibilidad tolerable debe ser 1 hora	Medio de contacto institucional que integra otras funcionalidades colaborativas.	**A**
Servicio de Internet	Según los acuerdos de niveles de servicio firmados en el contrato, el tiempo de indisponibilidad debe ser menor o igual a 0,4% del año.	Canal dedicado a Internet, reuso 1:1 de 80 Mbps.	**A**
Servicio de Red inalámbrica (Internet wifi)	El tiempo de indisponibilidad tolerable debe ser no mayor a 24 horas	Elementos de red para brindar internet a dispositivos móviles	**B**
Sistema de Gestión de Aprendizaje (Moodle)	El tiempo de indisponibilidad tolerable debe ser no mayor a 8 horas	Herramienta para la gestión de aulas virtuales.	**B**
Base de Datos Oracle	De acuerdo a la importancia y criticidad la indisponibilidad será máximo 8 horas.	Motor de Base de Datos Oracle 12C que se usa en los sistemas de información del IDEP.	**A**
Sistema de Hipercovergencia	El sistema de hiperconvergencia debe estar disponible 24 horas al día los 7 días de la semana para permitir la consulta por parte de los ciudadanos y grupos de interés en cualquier momento.	La hiperconvergencia es un sistema compuesto por dos nodos o servidores, 2 switchs de capa tres cada uno de 24 puertos instalado en stack. Tiene puertos de fibra óptica para conectar los nodos. El último componente de la hiperconvergencia es el	**A**

Nombre del Servicio o Sistema de Información	Tiempo de interrupción no programada tolerable	Descripción del sistema o servicio	Impacto Operacional
	La indisponibilidad del sistema no afecta directamente la operación de la entidad, pero si la misionalidad.	software de virtualización VMWare (VCenter y VSphere).	
Firewall	El firewall debe estar disponible las 24 horas del día los 7 días de la semana para brindar la seguridad perimetral de la entidad, así como en este momento coyuntural, brindar acceso remota la red LAN a través del servicio de Red Privada Virtual (VPN). La indisponibilidad del sistema puede afectar directamente la operación de la entidad por la afectación de seguridad en la información.	Es un equipo de seguridad perimetral que tiene los servicios de Antivirus, prevención de intrusos y amenazas de ataque virtual, Control de Acceso a aplicaciones, a sitios Web e IPS. Brinda el servicio de VPN.	**A**
Servicio de Antivirus	Su indisponibilidad tolerable no debe ser mayor a 48 horas.	Aplicación que realiza tareas como la revisión de amenazas de seguridad en los equipos de la entidad.	**B**
Servicio de Mesa de Ayuda	El tiempo de indisponibilidad máximo de 12 horas. Las solicitudes podrán realizarse también por otros medios en caso de falla, sin afectar la operación.	Servicio que permite el registro de los casos de soporte tanto de los sistemas de información como técnicos.	**C**
Servicio de página web Institucional	El tiempo de indisponibilidad máximo de 8 horas, es un servicio de vital importancia para la operación.	Página web institucional donde se encuentran los accesos a los diferentes sistemas web y las publicaciones, documentos y eventos que realiza el instituto como parte integral de la operación.	**A**

Nombre del Servicio o Sistema de Información	Tiempo de interrupción no programada tolerable	Descripción del sistema o servicio	Impacto Operacional
Servicio del Directorio Activo principal y secundario (Dominio)	El tiempo de indisponibilidad máximo de 1 hora, es un servicio de vital importancia para la operación	Elementos de red que soportan la conectividad del cableado estructurado, brindando los recursos de internet y servicios compartidos y conectividad interna.	**A**
Servicio de correos masivos	El tiempo de indisponibilidad máximo de 72 horas. Se puede utilizar el servicio de correo electrónico para el envío de mensajes de alta prioridad, limitando el alcance de los grupos objetivos.	Servicio para el envío de correos electrónicos a listas con gran de contactos.	**C**
Servicio de Video Conferencia	El tiempo de indisponibilidad máximo de 72 horas. Se puede utilizar el servicio de video conferencia de Google, limitando la posibilidad de transmitir en Facebook life.	Servicio multimedia que permite la interacción entre distintas personas o grupos de trabajo para la realización y o transmisión de eventos, reuniones, charlas, cursos, entre otros, usando dispositivos como teléfonos inteligentes, tabletas, computadoras, entre otros.	**C**
Servicio web Micrositios	El tiempo de indisponibilidad máximo de 12 horas. Las solicitudes podrán realizarse también por otros medios en caso de falla, sin afectar la operación.	Servicio de información misional publicada en espacios Web.	**C**
Otras Bases de Datos (MySql)	El tiempo de indisponibilidad máximo de 8 horas, es un servicio de vital importancia para la operación	Servicio de bases de datos que soportan o son la persistencia de sitios Web.	**A**

Sistemas de información Externos soportados por el Servicio de Internet del IDEP.

Nombre del Servicio o Sistema de Información	Descripción del sistema o servicio	Impacto Operacional
Sistema de información Humano que interopera con el sistema de información Goobien modalidad fuera de línea.	El sistema de información HUMANO permite la liquidación mensual de la nómina con lo que esto conlleva, registro de novedades, conceptos de provisiones y aportes a la seguridad social.	**B**

3.3. Identificación de procesos críticos

La identificación de los procesos críticos del negocio se da con base en la clasificación de los impactos operacionales de las organizaciones.

Para este caso tomamos los procesos del cuadro del punto B y seleccionamos los procesos que se identificaron como críticos:

Nombre del Servicio o Sistema de Información	Descripción del sistema o servicio
Sistema de Información Cliente/Servidor: Goobi que interopera con el sistema de información Humano en modalidad fuera de línea.	El sistema de información Goobi soporta la operación administrativa y financiera del IDEP, la radicación, contratación, almacén (bienes y publicaciones) y la contabilidad. Es un sistema de propiedad de la empresa Goobi SAS.
Servicio de Correo electrónico que integra la herramienta meet	Medio de contacto institucional que integra otras funcionalidades colaborativas como el meet.
Servicio de Internet	Canal dedicado a Internet, reuso 1:1 de 80 Mbps.
Servidor Repositorio Digital.	Servidor Virtual LAMP (Linux, Apache, MySql y PHP) Debian versión 14.
Servidor Aula Virtual.	Servidor Virtual LAMP (Linux, Apache, MySql y PHP) Ubuntu 20.
Servidor de Bases de Datos	Servidor Virtual LAMP (Linux, Apache, MySql - PosgreSQL). Ubuntu 20.
Base de Datos Oracle	Motor de Base de Datos Oracle 12C que se usa en los sistemas de información del IDEP.
Sistema de Hipercovergencia	La hiperconvergencia es un sistema compuesto por dos nodos o servidores, 2 switchs de capa tres cada uno de 24 puertos instalado en stack. Tanto los nodos y los switch diponen de puertos de fibra óptica para si inteconexión. El último componente de la hiperconvergencia es el software de virtualización VMWare (VCenter y VSphere). Sobre esta plataforma están instaladas máquinas virtuales o servidores.
Firewall	Es un equipo de seguridad perimetral Fortinet que tiene los servicios de Antivirus, prevención de intrusos y amenazas de ataque virtual, Control de Acceso a

Nombre del Servicio o Sistema de Información	Descripción del sistema o servicio
	aplicaciones, a sitios Web e IPS. Brinda el servicio de VPN.
Servicio de red LAN	Compuesta por los equipos activos y cableado estructurado que conforman la red de la entidad, facilitando acceso a recursos compartidos, internet y conectividad interna.
Página web Institucional	Página web institucional donde se encuentran los accesos a los diferentes sistemas web y las publicaciones, documentos y eventos que realiza el instituto como parte integral de la operación.

Es de anotar que algunos servicios, a raíz de la pandemia, se convirtieron en servicios indispensables para la operación del Instituto, es así que el firewall cobra una relevancia importante en los servicios prestados por la entidad a diferencia de años anteriores, esto ocurre por la necesidad que se creó del trabajo remoto desde cualquier ubicación. Así mismo los servicios de correo electrónico y las herramientas para videoconferencias, que permiten el trabajo colaborativo a través de las sesiones virtuales, cobran igual relevancia en los procesos de la entidad.

3.4. Establecimiento de tiempos de recuperación

Una vez identificados los procesos críticos del negocio, se deben establecer los tiempos de recuperación que son una serie de componentes correspondientes al tiempo disponible para recuperarse de una alteración o falla de los servicios; el entendimiento de estos componentes es fundamental para comprender el BIA. Los tiempos de recuperación de describen a continuación:

Tiempo de Recuperación	Descripción
RPO	Magnitud de la pérdida de datos medida en términos de un periodo de tiempo que puede tolerar un proceso de negocio.
RTO	Tiempo Disponible para Recuperar Sistemas y/o recursos que han sufrido una alteración.
WRT	Tiempo Disponible para Recuperar Datos Perdidos una vez que los sistemas están reparados. Tiempo de Recuperación de Trabajo.
MTD	Periodo Máximo Tiempo de Inactividad que puede tolerar la Entidad sin entrar en colapso.

La tabla a continuación muestra los servicios y sistemas críticos de la entidad y el periodo de tiempo máximo de inactividad.

Nombre del Servicio o Sistema de Información	MTD
Sistema de Información Cliente/Servidor: Goobi que interopera con el sistema de información Humano en modalidad fuera de línea.	8 horas laborales
Servicio de Correo electrónico que integra la herramienta meet	1 hora laboral
Servicio de Internet	1 hora laboral
Servidor Repositorio Digital.	8 horas
Base de Datos Oracle	8 horas laborales
Sistema de Hipercovergencia	4 horas laborales
Firewall	1 hora laboral
Servicio de red LAN	1 hora laboral
Página web Institucional	8 horas

3.5. Identificación de recursos

Las diferentes actividades contempladas en la función crítica del negocio deben considerarse de vital importancia cuando apoyan los procesos críticos del negocio; por lo tanto es clave en este punto, la identificación de recursos críticos de Sistemas de Tecnología de Información que permitan tomar acciones para medir el impacto del negocio de las Entidades.

La lista a continuación muestra los recursos físicos con que cuenta el Instituto para mantener la infraestructura tecnológica en funcionamiento:

Los detalles de los servidores se especifican en documento anexo confidencial.

Recurso Tecnológico	Servicios
Servidor Apolo.	Directorio Activo principal de la Entidad.
Servidor Apolo.	Está alojado el sistema de información Goobi que provee el servicio centralizado a los usuarios del sistema. Este recurso cuenta con varias carpetas que son requeridas para el funcionamiento del sistema de información Goobi.
Nodo 1 - Hiperconvergencia HPG9	Servidores Virtuales
Nodo 2 - Hiperconvergencia HPG9	Servidores Virtuales

	DNS Alternativo Koha OJS Repositorio Digital VuFind Moodle
Servidor HP DL380 G7	Página web Mesa de ayuda
Servidor HP DL380 G7	Base de datos Oracle Pruebas
Servidor HP DL380 G7	Base de datos Oracle producción
Firewall	Fortigate

3.6. Disposición de los RTO/RPO (Recovery Time Objective/Recovery Point Objective)

RTO: Tiempo de Recuperación Objetivo: Asociado con la restauración de los recursos que han sido alterados de las Tecnologías de la Información; comprende el tiempo disponible para recuperar recursos alterados.

Adicionalmente, se aplica el WRT, es decir el tiempo que es requerido para completar el trabajo que ha estado interrumpido con el propósito de volverlo a la normalidad.

Servicio	RTO
Sistemas web: OJS Koha Dspace VUfind Caja de herramientas	12 horas
Goobi	5 horas y 15 minutos
Humano	6 horas
Tablas de retención documental	13 horas
Hiperconvergencia	1 hora
Firewall - Configuración	3 horas
Firewall -Fallo total	25,5 horas
Consola Antivirus	9 horas
Switches y routers	2 horas
Página web – Alistar servidor de contingencia	43 minutos

3.7. Identificación de procesos alternos

La identificación de procesos alternos hace posible que los procesos del negocio puedan continuar operando en caso de presentarse una interrupción; para ello es oportuno que las

Entidades tengan métodos alternativos de manera temporal que ayuden a superar la crisis que ha generado una interrupción; por lo tanto para cada proceso crítico que se establezca (en los servicios), se debe poseer un procedimiento manual de continuidad del servicio.

El IDEP actualmente cuenta con un servidor alterno para el sistema Goobi junto con la base de datos, esto también se encuentra implementado para las fallas en la página web para lo cual también se cuenta con un servidor alterno.

3.7.1. Identificación de las prioridades de recuperación de servicios y sistemas de información

Ante las fallas de los sistemas de información y/o servicios tecnológicos que se prestan a los usuarios del IDEP, se priorizan de acuerdo al impacto que la caída de los mismos pueda generar en la operación diaria del Instituto:

#	Sistema de Información o Servicio	Prioridad
1	Sistema Goobi	Alta
2	Sistema de información Humano	Alta
3	Sistema de Información web: Koha	Alta
4	Sistema de Información web: DSpace	Alta
5	Sistema de Información web: OJS	Media
6	Sistema de Información web: VuFind	Media
7	Servicio de Correo electrónico	Media
8	Servicio de Internet	Media
9	Servicio Web y Micrositios.	Media
10	Servicio de Bases de Datos	Media
11	Servicio de Aulas Virtuales.	Media
12	Base de Datos Oracle	Alta
13	Sistema de Hiperconvergencia	Alta
14	Servicio Firewall	Alta
15	Servicio Antivirus	Alta
16	Servicio de WIFI	Baja
17	Servicio de Red LAN	Alta

3.7.2. Identificación de los procesos misionales y criticidad de recuperación:

Para formular el BIA el IDEP realizó un inventario de activos de información donde se clasificaron los sistemas y servicios como críticos.

Nombre del Servicio o Sistema de Información	Periodicidad de Uso en el IDEP	Tiempo de interrupción no programada tolerable	Descripción del sistema o servicio
Sistema de Información Cliente/Servidor: Goobi que	El sistema se utiliza en modalidad 5 x 8 y eventualmente se	De acuerdo a la importancia y criticidad el sistema Goobi no se	El sistema de información Goobi soporta la operación administrativa y

Nombre del Servicio o Sistema de Información	Periodicidad de Uso en el IDEP	Tiempo de interrupción no programada tolerable	Descripción del sistema o servicio
interopera con el sistema de información Humano en modalidad fuera de línea.	requiere los fines de semana y festivos.	programa estar en indisponibilidad por más de 8 horas laborales.	financiera del IDEP, la radicación, contratación, almacén (bienes y publicaciones) y la contabilidad. Es un sistema de propiedad de la empresa Goobi SAS.
Sistema de Información web: Koha	El sistema Koha está disponible en la página web para consulta permanente de las partes interesadas a través del link de la página del Idep.	El sistema Koha debe estar disponible los 7 días de la semana para consulta de las partes interesadas en cualquier momento. La indisponibilidad del sistema no afecta directamente la operación de la entidad, pero si la misionalidad.	El sistema Koha es una biblioteca digital que agrupa material bibliográfico dirigido a la comunidad educativa para consulta de los usuarios autorizados. En el buscador bibliográfico podrá realizar búsquedas específicas de acuerdo al criterio que seleccione como título, Autor, Tema, ISBN, ISSN, series y signatura. Es una herramienta de código abierto.
Sistema de Información web: DSpace	El sistema DSpace está disponible en la página web para consulta permanente de las partes interesadas a través del link de la página del Idep.	El sistema DSpace debe estar disponible los 7 días de la semana para consulta de las partes interesadas en cualquier momento. La indisponibilidad del sistema no afecta directamente la operación de la entidad, pero si la misionalidad.	El sistema DSpace es una biblioteca digital que agrupa colecciones digitales, y comúnmente es usada como solución de repositorio bibliográfico institucional. Soporta una gran variedad de datos, incluyendo libros, tesis, fotografías, filmes, video, datos de investigación y otras formas de contenido.

Nombre del Servicio o Sistema de Información	Periodicidad de Uso en el IDEP	Tiempo de interrupción no programada tolerable	Descripción del sistema o servicio
			Los datos son organizados como ítems que pertenecen a una colección; cada colección pertenece a una comunidad. Es una herramienta de código abierto.
Sistema de Información web: OJS	El sistema OJS está disponible en la página web para consulta permanente de las partes interesadas a través del link de la página del Idep.	El sistema OJS debe estar disponible los 7 días de la semana para consulta de las partes interesadas en cualquier momento. La indisponibilidad del sistema no afecta directamente la operación de la entidad, pero si la misionalidad.	Esta herramienta OJS es el portal de revistas del IDEP. Es una herramienta de código abierto.
Sistema de Información web: VuFind	El sistema Vufind está disponible en la página web para consulta permanente de las partes interesadas a través del link de la página del Idep.	El sistema Vufind debe estar disponible los 7 días de la semana para consulta de las partes interesadas en cualquier momento. La indisponibilidad del sistema no afecta directamente la operación de la entidad, pero si la misionalidad.	El objetivo de VuFind es permitir a los usuarios buscar y navegar a través de todos los recursos de la biblioteca digital. Es una herramienta de código abierto.
Servicio de Correo electrónico	El sistema se usa 7 días a la semana las 24 horas del día.	Según los acuerdos de niveles de servicio del proveedor, aunque suele ser muy estable.	Medio de contacto institucional que integra otras funcionalidades colaborativas.
Servicio de Internet	El canal debe estar en funcionamiento 7 días a	Según los acuerdos de niveles de servicio firmados en	Canal dedicado a Internet, reuso 1:1 de 80 Mbps.

Nombre del Servicio o Sistema de Información	Periodicidad de Uso en el IDEP	Tiempo de interrupción no programada tolerable	Descripción del sistema o servicio
	la semana las 24 horas del día.	el contrato, el tiempo de indisponibilidad debe ser menor o igual a 0,4% del año.	
Servidor Repositorio Digital.	El servidor debe estar en funcionamiento 7 días a la semana las 24 horas del día.	El tiempo de indisponibilidad tolerable debe ser no mayor a 8 horas	Servidor LAMP (Linux, Apache, MySql y PHP) Debian versión 14.
Base de Datos Oracle	Se utiliza en modalidad 5 x 8 y eventualmente se requiere los fines de semana y festivos.	De acuerdo a la importancia y criticidad la indisponibilidad será máximo 8 horas.	Motor de Base de Datos Oracle 12C que se usa en los sistemas de información del IDEP.
Sistema de Hipercovergencia	El sistema se usa 7 días a la semana las 24 horas del día. Aunque existe redundancia de nodos, es crucial mantenerlo en total disponibilidad.	El sistema de hiperconvergencia debe estar disponible 24 horas al día los 7 días de la semana para permitir la consulta por parte de los ciudadanos y grupos de interés en cualquier momento. La indisponibilidad del sistema no afecta directamente la operación de la entidad, pero si la misionalidad.	La hiperconvergencia es un sistema compuesto por dos nodos o servidores, 2 switchs de capa tres cada uno de 24 puertos instalado en stack. Tiene puertos de fibra óptica para conectar los nodos. El último componente de la hiperconvergencia es el software de virtualización VMWare (VCenter y VSphere).
Firewall	Se usa 7 días a la semana las 24 horas del día.	El firewall debe estar disponible las 24 horas del día los 7 días de la semana para brindar la seguridad perimetral de la entidad, así como en este momento coyuntural, brindar acceso remoto a la red LAN a través del servicio de Red Privada Virtual (VPN).	Es un equipo de seguridad perimetral que tiene los servicios de Antivirus, prevención de intrusos y amenazas de ataque virtual, Control de Acceso a aplicaciones, a sitios Web e IPS. Brinda el servicio de VPN.

Nombre del Servicio o Sistema de Información	Periodicidad de Uso en el IDEP	Tiempo de interrupción no programada tolerable	Descripción del sistema o servicio
		La indisponibilidad del sistema puede afectar directamente la operación de la entidad por la afectación de seguridad en la información.	
Antivirus	Su uso está limitado al tiempo	Su indisponibilidad tolerable no debe ser mayor a 48 horas.	Aplicación que realiza tareas como la revisión de amenazas de seguridad en los equipos de la entidad.
Servicio de WIFI	El servicio se utiliza en modalidad 5 x 8.	El tiempo de indisponibilidad tolerable debe ser no mayor a 24 horas	Elementos de red para brindar internet a dispositivos móviles
Servicio de red LAN	Los servicios son necesarios 7 días a la semana las 24 horas del día	El tiempo de indisponibilidad máximo de 1 hora, es un servicio de vital importancia para la operación	Elementos de red que soportan la conectividad del cableado estructurado, brindando los recursos de internet y servicios compartidos y conectividad interna.

4. CONTROLES PREVENTIVOS

Esta sección identifica y detalla los controles preventivos que se realizan como parte de las actividades de los planes de seguridad y privacidad de la información, plan de tratamiento de riesgos y plan de mantenimiento y monitoreo que tienen como propósito la realización de tareas y el establecimiento de controles tanto preventivos como correctivos para evitar las fallas de los sistemas de información y de los servicios informáticos que presta la Oficina Asesora de Planeación a la entidad a través del Grupo de Tecnología del IDEP.

4.1. Capacidad de las UPS

Ups de 10Kva para las oficinas del cuarto piso y el Data Center, y UPS de 6Kva para las oficinas del octavo piso.

El tiempo máximo a full carga según el fabricante es de 10 min, hay que tener en cuenta que las UPS están diseñadas en dar el tiempo suficiente para el apagado controlado de los equipos de computación (PCs y Servidores) y equipos de comunicaciones.

4.2. Capacidad de los sistemas de refrigeración

La unidad de Aire Acondicionado es de 24000 Btu suficiente para mover y refrigerar el Data Center.

4.3. Sistema de extinción de incendio

El IDEP está protegido con un extintor clase C (equipos eléctricos energizados) para el datacenter, así mismo se suspendieron los aspersores en este sitio y se cuenta con un sensor de humo.

Así mismo el Centro Empresarial arrecife donde están ubicadas las oficinas del IDEP cuenta con los elementos para atender este tipo de situaciones.

4.4. Sistemas de monitoreo capacidad de los servidores

Los servidores se monitorean directamente cada fin de semana y se revisan los logs generados para validar las situaciones que se están presentando y tomar acciones correctivas y preventivas. Y cada 15 días se valida si existen actualizaciones del sistema operativo para realizarlas.

4.5. Sistemas de monitoreo de aplicaciones

El sistema de información administrativo y financiero Goobi se monitorea a diario en horario laboral determinando que se encuentre en funcionamiento.

El funcionamiento de la página web se realiza diariamente donde se toma un backup y se actualiza el sistema alterno de contingencia, esta actividad es realizada todos los días.

El sistema de hiperconvergencia que aloja las aplicaciones web es monitoreado a diario para validar el estado de los servidores virtuales.

El IDEP no cuenta con herramientas de monitoreo por lo tanto estas actividades se realizan de forma directa sobre las máquinas a través de los sistemas propios.

4.6. Sistemas de monitoreo de bases de datos

La base de datos Oracle que sostiene el aplicativo Goobi es monitoreada a diario en la toma del backup.

4.7. Toma de copias de respaldo y Periodicidad

La Oficina Asesora de Planeación – Sistemas quien se encarga del proceso de las copias de seguridad de los computadores y servidores que se encuentran en producción del IDEP, realiza esta actividad con el único objetivo de respaldo en caso de presentarse una emergencia; esto incluye las bases de datos de cada uno de los sistemas existentes y las carpetas TRD que fueron creadas en el 2019 como parte del proceso de Gestión Documental de la Entidad.

El Técnico Operativo – 314 de la Oficina Asesora de Planeación realiza Backups diarios a los registros de las bases de datos con los que funcionan los diferentes aplicativos con los que cuenta el IDEP (Base de datos Oracle, CEDOC, Página Web, entre otros); semanales a los documentos y archivos de los aplicativos (Documentos escaneados GOOBI, Centro de Documentación, Humano y KOHA).

Los servidores Poseidón (Página Web), idep-koha (revistas, catálogo, repositorio, caja-herramientas, cuentan con scripts que realizan la copias de respaldo de las aplicaciones, archivos instaladas en estos servidores, así como las bases de datos que los soportan.

Los Backups realizados se registran en el formato FT-GT-12-16 Control Back Ups y revisión de servidores.

Listado de Backups que se realizan con periodicidad para atender las contingencias:

Sistema o Servicio respaldado	Periodicidad	Objetos que se respaldan	Tiempo de recuperación
WEB	Diario/Semanal	Archivos de la sitios / Bases de Datos MySql	1 Hora
WEB-KOHA	Diario	Base de datos My SQL de la plataforma	1 Hora
WEB-KOHA	Semanal	Objetos de la aplicación WEB-KOHA	1 Hora
WEB OJS	Diario	Base de datos MySQL de la plataforma	1 Hora
WEB OJS	Semanal	Objetos de la aplicación WEB-OJS	1 Hora
WEB DSPACE	Diario	Base de datos POSTGRESQL	1 Hora
WEB DSPACE	Semanal	Objetos de la aplicación WEB-DSPACE	1 Hora
GOOBI	Diario	Base de datos ORACLE	1 Hora
GOOBI	Semanal	Objetos de la aplicación Goobi	1 Hora
TRDs	Semanal	Documentos finales catalogados en las TRD y guardados en la carpeta compartida	1 Hora
HUMANO	Mensual	Base de datos ORACLE son recibidas por parte del proveedor para almacenar	1 Hora

4.8. Sistemas de almacenamiento de copias de respaldo

Se almacenan semanalmente los backups (copias de respaldo o de seguridad) en un disco duro, que queda en caja fuerte en custodia en la tesorería del IDEP.

Se almacenan trimestralmente los backups en un disco, que queda en caja fuerte en custodia de la oficina externa del IDEP ubicada en la Secretaría de Educación Distrital SED.

4.9. Sistemas de protección de la seguridad de la información

La información de las tablas TRD está protegida a través de las reglas del Directorio Activo que restringen los accesos a las carpetas de cada una de las oficinas. Así mismo estas carpetas solo pueden accederse con una conexión autorizada a la red del IDEP a través del usuario y clave asignados. Si se realiza por conexión remota esta es validada y asignadaa través del usuario y clave proporcionado para el uso de la VPN y controlado a su vez porel firewall del Instituto.

Se cuenta además con el software antivirus instalado en todas las máquinas del IDEP.

La base de datos de los sistemas de información se encuentran protegidas en servidores a los cuales únicamente se tiene acceso el grupo de Ingenieros del área. Se cuenta con grupos en el directorio activo y reglas que restringen los accesos por lo que solo las personas autorizadas podrán tener acceso a los servidores que alojan las bases de datos.

Las ips de los servidores que alojan las bases de datos y las claves de acceso directo a las mismas solo son conocidas por los Ingenieros del área y solo se puedan acceder a través de los usuarios autenticados.

4.10. Realizar simulacros y pruebas a los backups realizados

En el 2021 se realizó el simulacro de restauración de los backups de base de datos de los sistemas de información Goobi y Humano. Estos simulacros hacen parte de las actividades que se programan en los planes anuales de Gobierno Digital y Seguridad digital.

4.11. Contar con servidores alternos para la restauración de los sistemas de información

Se cuenta actualmente con un servidor virtual alterno, cuya función es administrar la base de datos Oracle, se encuentra instalado en el sistema de hiperconvergencia y cumple la función de administrar las bases de datos de Oracle en ambiente de pruebas.

Se cuenta con una instancia de base de datos Oracle en un servidor independiente en la cual se restablecen los backups para realizar pruebas o en caso de contingencia.

5. ESTRATEGIAS DE CONTINGENCIA

Para que exista continuidad del negocio en el IDEP, se deben tener presentes los planes de contingencia definidos con cada uno de los proveedores de servicios como también las estrategias definidas al interior de la entidad.

5.1. Empresas de Servicio o Proveedores de Servicios Externos

El IDEP actualmente cuenta con el respaldo de los Terceros que proveen el soporte a los sistemas de información Goobi y Humano con quienes se tienen acuerdos para brindar el soporte que se requiera a los planes de contingencia en el IDEP. El sistema de información Humano se encuentra en la web en modalidad SAS, por lo que en este momento el proveedor es el encargado de garantizar la disponibilidad de la herramienta y de llevar a cabo los planes de contingencia en caso de requerirse.

Se cuenta con el contrato de mantenimiento a la infraestructura lógica del IDEP mediante el cual se tiene previsto tener disponibilidad el apoyo técnico de Ingenieros y expertos en los diversos temas y plataformas que maneja la entidad a fin de brindar el soporte requeridoen caso de contingencia.

5.2. Identificación de Incidentes que se pueden presentar

- Para incidentes que se presenten en relación de operadores de servicios públicos como luz, agua, gas y otros, que afecten la operación de interna del IDEP los mecanismos de recuperación y contingencia están sujetas a los ANS de dichos proveedores.
- Cualquier incidente interno que pudiera potencialmente causar o afectar la interrupción de las operaciones de los sistemas de información, como son la falla en los servidores o puntos de conexión.
- Cualquier incidente o incorrecta manipulación de los sistemas de información que ocasione desviaciones o pérdida de información.
- Inundación del datacenter.
- Apagado de los servidores por una descarga eléctrica.
- Fallas en el sistema de aire acondicionado que genere recalentamiento en los equipos del Data Center.
- Interrupción total de las operaciones del Centro de Cómputo debido a daños en hardware y/o software de los equipos servidores o pérdida de conectividad.

6. MANTENIMIENTO AL PLAN DE CONTINGENCIA

6.1. Revisión y actualización del plan

Se tiene previsto realizar una revisión y actualización al plan de contingencia al menos una vez al año. La revisión del plan de contingencia es una de las actividades que se debe incluir en la revisión del Sistema Integrado de gestión del IDEP.

Los aspectos que se deben tener en cuenta para realizar las actualizaciones al plan son las siguientes:

- Resultados de auditorías al cumplimiento del plan de contingencia
- Retroalimentación de partes interesadas como Comisión Distrital de Sistemas, Secretaria de Hacienda, proveedores relacionados con el plan de contingencia, oficina de control interno entre otros.

7. REFERENCIAS NORMATIVAS

Resolución 305 de 2008: "Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espacialesy Software Libre."

Decreto 1078 de 2015: "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

ARTÍCULO 2.2.17.4.3. Obligaciones comunes de los prestadores de servicios ciudadanos digitales. Los prestadores de servicios ciudadanos digitales deberán cumplir las siguientes obligaciones:

Numeral 7: Implementar sistemas de gestión de seguridad y controles que permitan disminuir y gestionar el riesgo asociado a la integridad, confidencialidad y disponibilidad de la información para lo cual adoptarán el cumplimiento de estándares de amplio reconocimiento nacionales o internacionales de acuerdo con los lineamientos del Modelo de seguridad y privacidad de la información de la política de Gobierno Digital.

Numeral 9: Contar con las herramientas suficientes y adecuadas para garantizar la disponibilidad de los servicios ciudadanos digitales.

Ley 1712 de 2014: "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones."

Decreto 1004 del 14 de junio de 2018. "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"

La Ley 1523 de 2012 adoptó la Política y el Sistema Nacional de Gestión del Riesgo de Desastres en Colombia. Con base en este análisis diseñarán e implementarán las medidas de reducción del riesgo y planes de emergencia y contingencia que serán de su obligatorio cumplimiento.

Artículo 42. Análisis específicos de riesgo y planes de contingencia. Todas las entidades públicas o privadas encargadas de la prestación de servicios públicos, que ejecuten obras civiles mayores o que desarrollen actividades industriales o de otro tipo que puedan significar riesgo de desastre para la sociedad, así como las que específicamente determine la Unidad Nacional para la Gestión del Riesgo de Desastres, deberán realizar un análisis específico de riesgo que considere los posibles efectos de eventos naturales sobre la infraestructura expuesta y aquellos que se deriven de los daños de la misma en su área de influencia, así como los que se deriven de su operación. Con base en este análisis diseñará e implementarán las medidas de reducción del riesgo y planes de emergencia y contingencia que serán de su obligatorio cumplimiento.

8. GLOSARIO DE TÉRMINOS

Caja de Herramientas: Es una aplicación WEB para potenciar el pensamiento crítico de estudiantes y docentes.

Copias de seguridad (Backup): una copia de seguridad o backup (su nombre en Inglés) en tecnología de la información o informática es una copia de seguridad - o el proceso de copia de seguridad - con el fin de que estas copias adicionales puedan utilizarse para restaurar el original después de una eventual pérdida de datos.

Cliente SSH: Aplicación que implementa el protocolo SSH para realizar acceso remoto a dispositivos de cómputo que dispongan de dicho servicio.

Disco duro: en informática, un disco duro o disco rígido (en inglés *Hard Disk Drive*, HDD) es un dispositivo de almacenamiento de datos no volátil que emplea un sistema degrabación magnética para almacenar datos digitales. Se compone de uno o más platos o discos rígidos, unidos por un mismo eje que gira a gran velocidad dentro de una caja metálica sellada. Sobre cada plato se sitúa un cabezal de lectura/escritura que flota sobre una delgada lámina de aire generada por la rotación de los discos.

DSPACE: es un software de código abierto para la creación de repositorios y bibliotecas digitales que provee herramientas para la administración de colecciones digitales. Este

sistema soporta una gran variedad de datos incluyendo libros, tesis, fotografías, videos, datos de investigación y otras formas de contenido.

Enrutador (router) : el enrutador (calco del inglés *router*), direccionador, ruteador o encaminador es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red). Un enrutador es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la mejor ruta que debe tomar el paquete de datos.

Gestión de continuidad de negocio (BCM): Proceso general de gestión holístico que identifica amenazas potenciales a una organización y el impacto que se podría causar a la operación de negocio que en caso de materializarse y el cual provee un marco de trabajo para la construcción de la resiliencia organizacional con la capacidad de una respuesta efectiva que salvaguarde los intereses de las partes interesadas claves, reputación, marca y actividades de creación de valor.[1]

Hardware: corresponde a todas las partes físicas y tangibles de una computadora: sus componentes eléctricos, electrónicos, electromecánicos y mecánicos, sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.

Hyperconvergencia: La hiperconvergencia es la combinación de componentes virtuales y físicos de una infraestructura, tales como servidores, redes y hardware de almacenamiento, resultando en un único dispositivo controlado por software. La hiperconvergencia permite simplificar las operaciones de TI desglosando los nichos tradicionales y permitiendo que el mismo hardware gestione el almacenamiento, el Procesamiento, las redes y lavirtualización.

Hub: Concentrador. Dispositivo capaz de enlazar físicamente varios ordenadores de forma pasiva, enviando los datos para todos los ordenadores que estén conectados, siendo éstos los encargados de discriminar la información.

KOHA: Koha es un sistema integrado de gestión de bibliotecas, que se ofrece como software libre.Koha tiene todas las características previstas en un programa integrado de gestión de bibliotecas.

LAN: (Local Area Network - Red de Área Local). Interconexión de computadoras y periféricos para formar una red dentro de una empresa u hogar, limitada generalmente a un edificio.

Máquina virtual: una máquina virtual es un software que simula un sistema de computación y puede ejecutar programas como si fuese una computadora real.

[1] Guía 10 MinTic – Seguridad y Privacidad de la Información – Continuidad del Negocio

Módem : Un **módem** es un dispositivo que sirve para enviar una señal llamada *moduladora* mediante otra señal llamada *portadora*. Se han usado módems desde los años 60, principalmente debido a que la transmisión directa de las señales electrónicas inteligibles, a largas distancias, no es eficiente, por ejemplo, para transmitir señales de audio por el aire, se requerirían antenas de gran tamaño (del orden de cientos de metros) para su correcta recepción. Es habitual encontrar en muchos módems de red conmutada la facilidad de respuesta y marcación automática, que les permiten conectarse cuando reciben una llamada de la RTPC (Red Telefónica Pública Conmutada) y proceder a la marcación de cualquier número previamente grabado por el usuario. Gracias a estas funciones se pueden realizar automáticamente todas las operaciones de establecimiento de la comunicación.

Plan de Contingencia: Conjunto de estrategias, acciones, procedimientos planificados y responsabilidades definidas para minimizar el impacto de una interrupción imprevista de las funciones críticas y conseguir la restauración de las mismas, dentro de unos límites de tiempo establecidos. Sin que sea una regla general, se suele aplicar al plan circunscrito a las actividades de los departamentos de Sistemas de Información.

OJS: Open Jornal System (OJS) es un sistema de administración y publicación de revistas y documentos periódicos (seriadas) en Internet, que permite un manejo eficiente y unificado del proceso editorial, con esto se busca acelerar el acceso a la difusión de contenidos e investigación producido por las universidades y centros de investigación.

Red: Una **red de computadoras**, también llamada **red de ordenadores** o **red informática**, es un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos para compartir información y recursos. Este término también engloba aquellos medios técnicos que permiten compartir la información.

Sitio alterno: Ubicación alterna de operaciones seleccionada para ser utilizada por una organización cuando las operaciones normales no pueden llevarse a cabo utilizando las instalaciones normales después de que se ha producido una interrupción.

Software: se conoce como **software** al equipamiento lógico o soporte lógico de una computadora digital; comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos del sistema, llamados hardware.

Servidores: una aplicación informática o programa que realiza algunas tareas en beneficio de otras aplicaciones llamadas clientes. Algunos servicios habituales son los servicios de archivos, que permiten a los usuarios almacenar y acceder a los archivos de una computadora y los servicios de aplicaciones, que realizan tareas en beneficio directo del usuario final. Este es el significado original del término. Es posible que un ordenador cumpla simultáneamente las funciones de cliente y de servidor.

S.O. (Sistema Operativo): un **Sistema operativo** (SO) es un software que actúa de interfaz entre los dispositivos de hardware y los programas de usuario o el usuario mismo

para utilizar un computador. Es responsable de gestionar, coordinar las actividades y llevar a cabo el intercambio de los recursos y actúa como intermediario para las aplicaciones que se ejecutan.

Sistema de información: Un sistema de información es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.

Snapshots de almacenamiento: Los Snapshots de almacenamiento son una forma cada vez más común de proteger los archivos y los sistemas de almacenamiento. Gracias a la tecnología de los snapshots podemos crear copias de nuestros sistemas de archivos en un momento en el tiempo y en un estado concreto, los Snapshots no son un sistema de recuperación de datos en si ya que dependen de la fuente principal para restaurar la información a un estado anterior.

SSH: (o Secure SHell) es el nombre de un protocolo y del programa que lo implementa cuya principal función es el acceso remoto a un servidor por medio de un canal seguro en el que toda la información está cifrada. Además de la conexión a otros dispositivos, SSH permite copiar datos de forma segura (tanto archivos sueltos como simular sesiones FTP cifradas), gestionar claves RSA para no escribir contraseñas al conectar a los dispositivos y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSHy también puede redirigir el tráfico del (Sistema de Ventanas X) para poder ejecutar programas gráficos remotamente. El puerto TCP asignado es el 22.

Telecomunicaciones: es una técnica consistente en transmitir un mensaje desde un punto a otro, normalmente con el atributo típico adicional de ser bidireccional. El término *telecomunicación* cubre todas las formas de comunicación a distancia, incluyendo radio, telegrafía, televisión, telefonía, transmisión de datos e interconexión de computadoras a nivel de enlace.

VPN: por las siglas en inglés de Virtual Private Network, o red privada virtual, es un túnel seguro entre su dispositivo y la internet. Las VPN protegen su tráfico en línea contra espías, interferencias y censura.

9. PLAN DE CONTINGENCIA PARA LOS SISTEMAS DE INFORMACIÓN

Un Plan de Contingencia consiste en restar el impacto financiero que puede acusar un «incidente» inesperado en la compañía dentro del marco de los procedimientos habituales de la empresa, este plan trabaja para recuperar a la compañía de los imprevistos especiales que se puedan dar, y que por su causa interrumpen el sistema de producción.

Un Plan de Continuidad está enfocado a asegurar la continuidad del negocio, cuando de repente ocurre un incidente inesperado. Este plan lo que intenta es no detener la

productividad de la empresa, e intentar que la situación que ha sucedido en ese momento nos afecte lo menos posible.

Muchas veces estos dos conceptos no se pueden desligar, un plan de contingencia puede estar dentro de un Plan de Continuidad, ya que lo que se busca con estas medidas es una rápida recuperación ante los desastres, para reanudar lo antes posible la cadena de producción.[2]

10. FASES DEL PLAN

10.1. Fase de Notificación del incidente

Los usuarios de los diferentes sistemas de información deben informar formalmente de la pérdida total o parcial de disponibilidad, integridad o autenticidad. Esto se debe realizar por medio de la Mesa de Ayuda seleccionado el sistema de información o servicio que presenta la falla.

10.2. Fase Evaluación del Incidente

Los Ingenieros a cargo del área de Sistemas evalúan el incidente teniendo en cuenta los aspectos a continuación:

Los incidentes ocurridos en los sistemas de información y/o servicios son escalados a través de la mesa de ayuda y clasificados de acuerdo a los Ingenieros asignados como soporte de primer nivel. En este caso la persona a cargo evalúa el incidente y determina qué tipo de incidente es

Si el incidente es de seguridad se deberá tomar en cuenta la Guía GU-GT-12-01 Guía para la gestión de incidentes de seguridad de la información y solicitar al usuario el diligenciamientos del el formato FT-GT-12-21 Reg Incidentes Seg Info V1.

En caso de que el incidente sea de un sistema de información para el cual se cuenta con servicio de soporte por parte del fabricante o desarrollador, se contactará el proveedor a fin de determinar el origen del mismo y determinar el impacto, tiempos y la solución.

En caso de que el incidente se trate de una falla técnica que deja sin funcionamiento una parte del hardware se contactará el proveedor del servicio de mantenimiento de la infraestructura del IDEP a fin de recibir el soporte requerido y el reemplazo o arreglo de las piezas que fallan.

[2] https://www.audea.com/plan-de-continuidad-y-plan-de-contingencia-una-forma-de-salvar-tu-negocio/

Los Ingenieros a cargo del área de Sistemas evalúan la situación y determinan si es necesario activar o no el plan de contingencia. Se notifica al proveedor del sistema o servicio sobre la falla y al Jefe de la Oficina de Planeación para que en conjunto se determine la activación del plan de contingencia.

Posterior a la evaluación se notifica a través de correo electrónico a las partes interesadas de los tiempos estimados en la recuperación del sistema o servicio.

10.3. Establecer el origen de la falla y la posible solución

En esta fase se determina que originó la falla y cuál es la solución a brindar para restablecer el servicio. Así mismo es necesario determinar los recursos, impactos y tiempos para restablecer el servicio. Se debe especificar los recursos humanos que intervienen en la solución y el rol que tiene cada uno frente a la solución que se dará.

Solo en caso de que la falla deje en indisponibilidad uno de los servicios críticos en horas laborales y que se determine que se tomará más de 4 horas en el restablecimiento de este se activará el plan de contingencia detallado en los anexos de este documento.

10.4. Activar el plan de contingencia y notificar

En esta fase se activa el plan de contingencia y se informa a los interesados el tiempo que tomará restablecerse el servicio.

10.5. Llevar a cabo las acciones para restablecer el servicio

En esta fase se llevan a cabo las actividades planteadas en los anexos de este documento para cada sistema o servicio que presente la falla.

10.6. Validar el resultado de las acciones realizadas

Una vez se surten las actividades definidas en cada uno de los planes individuales de acuerdo a la contingencia presentada, es necesario realizar las validaciones para verificar el estado de estas acciones. Así mismo después de que la contingencia sea superada es necesario realizar el respectivo seguimiento por un lapso de tiempo para poder determinar que la contingencia ha sido superada con éxito.

10.7. Presentar el informe resultado de las acciones realizadas

Toda vez que finalicen las actividades de los planes y una vez superada la contingencia es necesario presentar el respectivo informe que contenga la información suficiente para

permitir tomar acciones correctivas o preventivas a fin de que esta no vuelva a ocurrir. Por lo tanto se debe contar con datos como:

- Origen de la contingencia - Qué provocó la falla.
- Actividades realizadas para corregir la falla.
- Actividades realizadas para atender la contingencia y dar continuidad al negocio.

11. RELACIÓN ENTRE ACTIVOS CRÍTICOS, RIESGOS Y PLAN DE ACCIÓN

Riesgos

En el siguiente cuadro se relacionan el tratamiento de riesgos y los planes de continuidad, teniendo en cuenta la correlación entre activos – riesgos y planes de contingencia y continuidad (en elaboración), cuyos activos tienen una alta CRITICIDAD. Así las cosas, este plan se focaliza en los activos a cargo del proceso del Proceso de Gestión Tecnológica, por ende no de los servicios alojados en la infraestructura sobre la cual están operando.

Descripción del Riesgo	Activo de Información	Plan de Acción
Posibilidad de daño económico y reputacional por la no prestación de servicios tecnológicos a la entidad debido a Suspensión o interrupción de los servicios TI y daños de los equipos que hacen parte de la infraestructura.	- Hiperconvergencia Dos nodos HPE HC380 Cluster Node P9D74A. ● Nuevo Portal ● Micrositios ● Bases de Datos ● Campus EMMI ● Revistas ● Repositorio Digital ● Dominio Alterno Servidor HP - REF. DL380G7 ● Base de Datos Oracle (Pruebas y Producción) ● Base de Datos del Sistema Administrativo y Financiero- Goobi Servidor HP - REF. DL380G7	Los planes de acción diseñados para atender estos fallos se detallan en este documento en los anexos 1 al 14.

	● Dominio ● Sistema Administrativo y Financiero- Goobi ● Carpetas Compartidas.	
Posibilidad de daño económico y reputacional por la no prestación de servicios tecnológicos a la entidad debido a la imposibilidad de normalizar el funcionamiento de los servicios e infraestructura tecnológica	- Hiperconvergencia Dos nodos HPE HC380 Cluster Node P9D74A. - Servidor HP - REF. DL380G7 - (RAI_IDEP_01) Base de Datos Oracle (Pruebas y Producción) ● Base de Datos del Sistema Administrativo y Financiero- Goobi - Servidor HP - REF. DL380G7 - (RAI_IDEP_01) ● Sistema Administrativo y Financiero- Goobi ● Carpetas Compartidas. - Firewall - Biométrico - Dos SWITCHES ARUBA 3810M 24G -Switch 3COM 4200G 48 puertos. - Switch CISCO 500D.	Los planes de acción diseñados para atender estos fallos se detallan en este documento en los anexos 1 al 14, esto de acuerdo al tipo de fallo presentado. Para los activos mencionados se realizan los planes de los anexos: 2- Recuperación del Sistema de Información Administrativo y Financiero (Goobi) y Base de datos Oracle 5- Recuperación Hiperconvergencia 14- Recuperación del Biométrico 6 - Recuperación del Firewall 9 - Recuperación de las configuraciones de switches y otros elementos
Posibilidad de daño económico y reputacional por pérdida o adulteración	Servidor Nuevo Portal Servidor Micrositios	Los planes de acción diseñados para atender estos fallos se detallan en este documentos en los

de la información y no continuidad en la prestación de servicios tecnológicos a la entidad debido a la inadecuada implementación de las Políticas de Seguridad y Privacidad de la Información, parametrizaciones y configuraciones de seguridad.	Servidor Bases de Datos Servidor Campus EMMI Servidor Revistas Servidor Dominio Alterno Sistema Sistema Administrativo y Financiero-Goobi Servicio de Carpetas Compartidas.	anexos: 2- Recuperación del Sistema de Información Administrativo y Financiero (Goobi) y Base de datos Oracle 4- Recuperación Backups de las TRD 10 y 11- Micrositios, 12- Servicios Web
Posibilidad de daño económico y reputacional por la Indisponibilidad de los servicios y operación sin licencias debido a falta de oportunidad en la identificación de las necesidades de la infraestructura tecnológica.	Licencias del servicio de Correo Electrónico. Licencias y Soporte Oracle. Licencias M-365 Licencias Antivirus Sistema Biométrico	Los planes de acción diseñados para atender estos fallos se detallan en este documentos en los anexos: 2- Recuperación del Sistema de Información Administrativo y Financiero (Goobi) y Base de datos Oracle Anexo 8 - Fallos en el Antivirus Anexo 13 - Recuperación del Correo Electrónico Anexo 14 - Recuperación del Biométrico

12. RECOMENDACIONES PARA LAS OFICINAS Y SUBDIRECCIONES DEL IDEP

Cualquier dispositivo que se encuentre conectado a una red LAN, y que ésta a su vez este conectada a Internet, o que también se encuentre conectado a Internet de forma directa, hace que sobre la información alojada en el dispositivo se enfrenta a riesgos inesperados al tener la probabilidad de ser víctima de ciberataques. Consciente de ello, el proceso de Gestión Tecnológica con el fin de minimizar riesgos de ataques o minimizar el impacto en caso de ser víctima de una ataque; realiza tareas y usa herramientas tecnológicas (en ambos casos acorde con los recursos disponibles) para respaldar la información, mantener

actualizados los dispositivos y aplicaciones, por citar algunos ejemplos; acorde con lo expresado en sus planes de Mantenimiento y Monitoreo, Seguridad y Privacidad de la Información, entre otros; en concordancia por lo expresado por Gobierno Digital[3].

La política de Gobierno Digital busca "*fortalecer la relación Ciudadano - Estado, mejorando la prestación de servicios por parte de las entidades, y generando confianza en las instituciones que conforman la administración pública y el Estado en general,*" siendo un objetivo transversal para todo el estado y sus instituciones, lo que hace que implícitamente su transversalidad aplique para el IDEP. Así las cosas, todas las Oficinas y subdirecciones del IDEP deben estar involucradas activamente en la implementación de ésta política al interior de las mismas.

Uno de los aspectos a tener en cuenta de Gobierno Digital está relacionado con lanecesidad de que cada oficina y subdirección cuenten con un Plan de Contingencia que explicite los diferentes riesgos y su materialización que se puedan presentar en el funcionamiento y desarrollo de sus procesos y procedimientos, el impacto que ellos tengan, la forma de prevenirlos y mitigarlos; de tal forma que permita continuar la operación de la entidad en el caso que por ejemplo, no se cuente con Infraestructura tecnológica. Esto implica la posterior normalización de las operaciones. Es importante resaltar que cada unode éstos Planes de Contingencia harán parte del Plan de Continuidad del Negocio, el cual está gestionado por la Alta Dirección.

Se recomienda que cada uno de los colaboradores del IDEP se documente, socialicen y apliquen la Política de Gobierno Digital, información que se encuentra en los siguientes link:

https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/ Manual de Gobierno Digital:

https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/

[3] https://gobiernodigital.mintic.gov.co/portal/

ANEXOS

ANEXO 1. PLAN DE ACCIÓN PARA LOS APLICATIVOS WEB KOHA, OJS, DSPACE, VUFIND

Objetivo General

Recuperación en la continuidad de las operaciones del Aplicativo Web que presenta la falla o indisponibilidad, para garantizar la disponibilidad, integridad y autenticidad de la información institucional hacia los usuarios de la entidad.

Objetivos Específicos

1. Surtir las etapas del plan de contingencia planteadas en este documento.
2. Llevar a cabo las actividades planeadas a fin de restablecer el servicio.
3. Garantizar la integridad y autenticidad de la información recuperada de los bakcups (copias de respaldo o de seguridad).
4. Solicitar la intervención del proveedor para restablecer el aplicativo.

Plan de acción

A continuación, se presentan las actividades, responsables y tiempos para el desarrollo de la implementación del presente plan de contingencia.

Las actividades planteadas se realizarán ante el peor escenario en el cual se ha perdido completamente el acceso al sistema de información o servicio prestado:

Actividad	Responsable	Tiempo Estimado
Instalación del motor de base de datos correspondiente en un servidor o computador ubicado en las instalaciones de la entidad, bien sea en su sede principal o en la oficina externa ubicada en la SED.	Ingenieros del área a cargo de la infraestructura	2 horas
Restauración del backup de la base de datos más recientes que se tengan de los discos guardados en las cajas fuertes de la entidad.	Ingenieros del área a cargo de la infraestructura	1 hora
Instalación del aplicativo sistema WEB en un servidor o computador ubicado en las instalaciones de la entidad, bien sea en su sede principal o en la oficina externa ubicada en la SED	Proveedor del sistema de información web	4 a 6 horas
Configuración de la conectividad entre la base de datos y el aplicativo sistema	Ingenieros del área a cargo de la infraestructura	1 hora
Restauración de los datos de la aplicación que reposan en los backups y que están relacionados con recursos que manejan estos aplicativos (videos, documentos, fotos, etc.)	Ingenieros del área a cargo de la infraestructura	2 horas

ANEXO 2. PLAN DE ACCIÓN AL SISTEMA DE INFORMACIÓN ADMINISTRATIVO Y FINANCIERO.

Objetivo General

Recuperación en la continuidad de las operaciones en el Sistemas de Información Administrativo y Financiero GOOBI que el IDEP tiene en producción, para garantizar la disponibilidad, integridad y autenticidad de la información institucional hacia los usuarios de la entidad.

Objetivos Específicos

1. Surtir las etapas del plan de contingencia planteadas en este documento.
2. Llevar a cabo las actividades planeadas a fin de restablecer el servicio.
3. Garantizar la integridad y autenticidad de la información recuperada de los backups (copias de respaldo o de seguridad).
4. Solicitar la intervención del proveedor para restablecer el aplicativo.

Plan de acción

A continuación, se presentan las actividades, responsables y tiempos para el desarrollo de la implementación del presente plan de contingencia.

Las actividades planteadas se realizarán ante el peor escenario en el cual se ha perdido completamente el acceso al sistema de información o servicio prestado

Actividad	Responsable	Tiempo Estimado
Subir el servidor de contingencia que administra el motor de la Base de Datos Oracle.	Ingenieros del área a cargo de la infraestructura	15 minutos
Ubicar y restaurar el backup del día anterior de la base de datos y del aplicativo SISTEMA DE INFORMACIÓN ADMINISTRATIVO Y FINANCIERO GOOBI en el servidor de contingencia.	Ingenieros del área a cargo de la infraestructura	1 Hora
En caso de no contar con el servidor de aplicativo de respaldo se debe: Instalar el aplicativo SISTEMA ADMINISTRATIVO Y FINANCIERO en un servidor o computador ubicado en las instalaciones de la entidad, bien sea en su sede principal o en la oficina externa ubicada en la SED.	Ingenieros del área a cargo de la infraestructura	1 hora

Este sistema está disponible en un servidor de pruebas.		
Configuración de la conectividad entre la base de datos y el aplicativo sistema	Ingenieros del área a cargo de la infraestructura	1 hora
Restauración de los datos de la aplicación que reposan en los backups y que están relacionados con recursos que manejan el sistema (Archivos PDF que corresponden a adjuntos en el sistema Goobi)	Ingenieros del área a cargo de la infraestructura	2 horas

ANEXO 3. PLAN DE ACCIÓN AL SISTEMA DE INFORMACIÓN NÓMINA HUMANO.

Objetivo General

Recuperación en la continuidad de las operaciones en el Sistemas de Información NÓMINA HUMANO que el IDEP tiene en nube como servicio de alojamiento y administración que presta el proveedor Soporte Lógico a partir del año 2020, para garantizar la disponibilidad, integridad y autenticidad de la información institucional hacia los usuarios de la entidad. El plan de contingencia del IDEP, se establece en el caso que falle el plan de contingencia del proveedor Soporte Lógico.

Los objetivos y actividades de este plan están enfocados en tener la capacidad de poner operativo el sistema de respaldo que se tiene como contingencia en la infraestructura del IDEP, el cual se adecuó entre el 2019 y 2020, y restablecer el sistema lo más pronto posible para dar continuidad al negocio.

Objetivos Específicos

1. Surtir las etapas del plan de contingencia planteadas en este documento.
2. Solicitar la intervención del proveedor para actualizar y restablecer el aplicativo.
3. Llevar a cabo las actividades planeadas a fin de restablecer el servicio.
4. Garantizar la integridad y autenticidad de la información recuperada de los backups (copias de respaldo o de seguridad).

Plan de acción

A continuación, se presentan las actividades, responsables y tiempos para el desarrollo de la implementación del presente plan de contingencia.

Actividad	Responsable	Tiempo Estimado
Subir el servidor de contingencia que administra la Base de Datos Oracle de contingencia.	Ingenieros del área a cargo de la infraestructura	15 minutos
Ubicar y restaurar el backups (copias de respaldo o de seguridad) disponible más recientes que se tenga en el servidor Oracle de contingencia.	Ingenieros del área a cargo de la infraestructura	1 a 2 horas
Realizar la configuración de la conectividad entre la base de datos y el aplicativo NÓMINA HUMANO, apoyado por el material (manuales o guías) suministrados por Soporte Lógico y en caso de requerirse, soporte vía osticket del proveedor.	Ingenieros del área a cargo de la infraestructura	20 minutos

Se requiere validar que la aplicación en el servidor de contingencia sea la versión más reciente de que disponga el proveedor.	Proveedor del sistema Humano	15 minutos
En caso de requerirse se solicita al proveedor la actualización del sistema HUMANO a la versión más reciente.	Proveedor del sistema Humano	3 - 4 horas

1. Plan De Acción Otros Recursos

El IDEP cuenta además de los sistemas de información con otros sistemas, servicios y repositorios que requieren se cuente con un plan de contingencia que atienda cualquier eventualidad de fallo que se presente. A continuación se presenta el listado de estos recursos y el plan de contingencia para cada uno:

SISTEMAS DE INFORMACIÓN		
ANEXO	**DESCRIPCIÓN**	**ESTADO**
4	Recursos de Red tablas de Retención Documental	BUENO
5	Sistema de Hiperconvergencia	BUENO
6	Sistema Firewall como aplicación	BUENO
7	Componentes Hardware relacionados con el Firewall	BUENO
8	Antivirus	BUENO
9	Backup y recuperación de la configuración del switches hiperconvergencia y switches cisco, router.	BUENO

ANEXO 4. PLAN DE ACCIÓN PARA LA RECUPERACIÓN INFORMACIÓN RECURSOS DE RED TABLAS DE RETENCIÓN DOCUMENTAL TRD

Objetivo general

Recuperación de la información que los funcionarios del IDEP almacenan en los recursos de red en las carpetas de las Tablas de Retención Documental TDR ante una incidencia de seguridad que cuyo alcance implique problemas de integridad y disponibilidad de esta información.

Objetivos específicos

- **a.** Respaldar y garantizar el correcto almacenamiento y recuperación de la información contenida en los recursos de red Tablas de Retención Documental TDR.
- **b.** Realizar pruebas de funcionamiento a los backups (copias de respaldo o de seguridad) de los recursos de red Tablas de Retención Documental TDR.
- **c.** Garantizar la continuidad de las operaciones administrativas y académicas derivadas de la información contenida en estas carpetas.
- **d.** Garantizar la integridad y autenticidad de la información recuperada de los bakcups (copias de respaldo o de seguridad)

Alcance

El Plan de Contingencia para la recuperación de información de los documentos almacenados en las carpetas de los documentos indicados en las Tablas de Retención Documental TDR**,** tiene como alcance la recuperación de dicha información sin identificar la importancia de estos documentos en la operación administrativa y académica del Instituto cuando se presente incidentes que afecte la prestación del servicio tecnológico al interior del IDEP bien sea por interrupción del servicio de energía o ataques informáticos.

Este plan identifica las actividades específicas que debe desarrollar, el personal técnico de sistemas del IDEP una vez detectada la incidencia y teniendo en cuenta la información suministrada por los funcionarios y contratistas.

Nota: La información a recuperar sólo podrá hacerse sobre las cuatro últimas copias de backups realizados.

Plan de acción

A continuación, se presentan las actividades, responsables y tiempos para el desarrollo de la implementación del presente plan de contingencia.

DESCRIPCIÓN	RESPONSABLE	TIEMPO ESTIMADO
Identificar la información a restaurar y la fecha de la misma a fin de obtener el disco de backup que lo contiene.	Técnico operativo OAP	1 Hora
Solicitar a Tesorería el disco duro custodiado que contenga la información a recuperar.	Técnico operativo Sistemas	Dentro de las siguientes 9 horas laborales después de recibida la solicitud de recuperación de información
Realizar la validación de los bacukps y proceder a la recuperación de la información solicitada cuando esta corresponda a la almacenada en las carpetas de las Tablas de Retención Documental TDR. Se hace partiendo del último backup realizado.	Técnico operativo Sistemas - IDEP	2 a 3 horas

ANEXO 5. PLAN DE ACCIÓN HIPERCONVERGENCIA.

Objetivo General

Recuperación en la continuidad del servicio de la Hiperconvergencia que el IDEP tiene en producción, para garantizar la disponibilidad, integridad y autenticidad de la información institucional hacia los usuarios de la entidad.

Objetivos Específicos

a. Respaldar los servicios informáticos almacenados en las máquinas virtuales de la Hiperconvergencia.
b. Realizar Snapshot semanalmente a cada una de las máquinas virtuales almacenadas en la Hiperconvergencia.
c. Garantizar la integridad y autenticidad de la información recuperada de los Snapshot (puntos de restauración).

Alcance

El Plan de Contingencia a la solución de Hiperconvergencia**,** está enmarcado dentro del PLAN DE CONTINGENCIA TECNOLÓGICA IDEP PL-GT-12-02, tiene como alcance la recuperación de la continuidad de los servicios informáticos de la entidad prestados a través de máquinas virtuales, cuando se presente pérdida total o parcial en la disponibilidad, integridad y/o autenticidad de estos servicios.

Este plan identifica las actividades específicas que deben desarrollar, el personal técnico del IDEP, con el apoyo de la empresa Hewllett Packard, quien es proveedor de la solución de Hiperconvergencia y presta el servicio de soporte a la misma. A la fecha se encuentra vigente el contrato de soporte con el fabricante lo cual brinda la posibilidad de atención por parte de expertos y una intervención rápida en caso de fallos.

Para el primer trimestre del año 2022, en la solución de Hiperconvergencia se encuentran incluidos los siguientes servidores virtualizados, que son objeto de este plan de contingencia:

- Servidor Web.
- Servidor Micrositios.
- Servidor Pensamiento Crítico.
- Servidor Gamificación.
- Servidor Campus EMMI.

- Servidor OJS
- Servidor Bases de Datos.
- Servidor KOHA.
- Servidor de Dominio Windows Server 2016 Standard.
- Servidor Secundario de Dominio Windows Server 2016 Standard, que incluye el sistema de información de nómina (Humano) de contingencia, y la consola de administración del Antivirus.
- Servidor Oracle Manager para la gestión del OracleVM (Virtualizador de Oracle). Oracle VM está instalado en un servidor físico G7 donde se encuentra la máquina virtual en la cual está instalado el servidor Oracle Linux, que a su vez tiene instalado el Motor de Base de Datos Oracle 12C. El Oracle VM .
- Extensible a todas las máquinas virtuales, que se instalen en la Hiperconvergencia.

Plan de acción

A continuación, se presentan las actividades, responsables y tiempos para el desarrollo de la implementación del presente plan de contingencia.

DESCRIPCIÓN	RESPONSABLE	TIEMPO ESTIMADO
1. Ingresar al VMware Vcenter / iESX.	Técnico operativo SISTEMAS - IDEP Ingenieros contratistas de sistemas Oficina Asesora de Planeación Ingeniero proveedor de la hiperconvergencia	15 minutos por cada máquina virtual afectada.
2. Identificar la máquina virtual o máquinas virtuales que presentan falta parcial o total de disponibilidad.	Técnico operativo SISTEMAS - IDEP Ingenieros contratistas de sistemas Oficina Asesora de Planeación Ingeniero proveedor de la hiperconvergencia	15 minutos por cada máquina virtual afectada.
3. Apagar la máquina virtual y restaurar el Snapshot.	Técnico operativo SISTEMAS - IDEP	15 minutos por cada máquina virtual afectada.

	Ingenieros contratistas de sistemas Oficina Asesora de Planeación Ingeniero proveedor de la hiperconvergencia	
4. Verificar el correcto funcionamiento del servicio o sitios Web que fueron afectado.	Técnico operativo SISTEMAS - IDEP Ingenieros contratistas de sistemas Oficina Asesora de Planeación Ingeniero proveedor de la hiperconvergencia	15 minutos por cada máquina virtual afectada.

ANEXO 6. PLAN DE ACCIÓN FALLOS EN LA CONFIGURACIÓN DEL FIREWALL.

Objetivo General

Recuperación en la continuidad del servicio del equipo de seguridad perimetral tipo Firewall que el IDEP tiene en producción, para garantizar la disponibilidad, integridad y autenticidad de la información institucional, así como salvaguardar la infraestructura tecnológica de hardware y servicios ubicada en las instalaciones del IDEP.

Objetivos Específicos

a. Respaldar la configuración del equipo de seguridad perimetral tipo Firewall.
b. Copiar el archivo de configuración en la unidad para su copia de respaldo.
c. Restaurar la configuración del equipo de seguridad perimetral tipo Firewall para garantizar la continuidad del funcionamiento del mismo.

Alcance

El Plan de Contingencia al equipo de seguridad perimetral tipo Firewall**,** está enmarcado dentro del PLAN DE CONTINGENCIA TECNOLÓGICA IDEP PL-GT-12-02, tiene como alcance la recuperación de la continuidad de los servicios informáticos de la entidad prestados que requieren el uso del Firewall, cuando se presente pérdida total o parcial en la configuración de éste, que impacten en disponibilidad, integridad y/o autenticidad de estos servicios en el IDEP, que requieran de conexiones seguras a internet.

Este plan identifica las actividades específicas que deben desarrollar, el personal técnico del IDEP, con el apoyo de la empresa ITSellcon SAS, quien es proveedor de la solución de seguridad perimetral y presta el servicio de soporte a la misma, o en su defecto con el fabricante de la misma, en este caso FORTINET.

Para finales del año 2018, se renovaron las licencias y el soporte por tres (3) años con el fabricante. Además se contrataron diez (10) horas de soporte con el proveedor.

Plan de acción

A continuación, se presentan las actividades, responsables y tiempos para el desarrollo de la implementación del presente plan de contingencia.

DESCRIPCIÓN	REQUERIMIENTO	TIEMPO ESTIMADO
Se requiere el documento IN-GTH 12-09 INSTRUCTIVO RESTAURACIÓN ARCHIVO DE LA CONFIGURACIÓN DEL FIREWALL 1. Ingresar mediante un navegador a la URL de la consola de administración del firewall (https://192.168.X.X). 2. Revisar las gráficas de funcionamiento de la memoria, del procesador, uso de disco, el ancho de banda de la interfaz LAN y WAN. 3. Revisar los logs. 4. Si se identifica problemas en la configuración proceder a restaurar la copia de respaldo del archivo de configuración más reciente. 5. Reiniciar el Firewall.	- IN-GTH 12-09 INSTRUCTIVO RESTAURACIÓN ARCHIVO DE LA CONFIGURACIÓN DEL FIREWALL. - Computadores de escritorio o portátiles. - Acceso a través de escritorio remoto de Windows. - Ingresar a la dirección de la consola del firewall.	30 minutos - 1 hora.
Los Ingenieros contratistas de sistemas Oficina Asesora de Planeación y el Técnico Operativo realizan pruebas de conexión a red y navegación en internet, para verificar el correcto funcionamiento de la restauración de la configuración del firewall y se valide la disponibilidad, integridad y autenticidad de la información. Se informa a los usuarios mediante correo electrónico los resultados de las pruebas realizadas con la descripción de los posibles eventos o incidentes detectados o con la conformidad en la recuperación del servicio e información y se anuncia la normalización de los servicios.	Computadores con acceso a la red LAN	1 hora.
Los Ingenieros contratista sistemas – OAP, Técnico operativo OAP realizan la actualización de la Base de datos de Activos Información Software, Hardware y Servicios, registrando la labor realizada. En caso de no presentarse observaciones continúa con las actividades generales del plan	Computadores con acceso a los servicios informáticos la Base de datos de Activos Información Software, Hardware y Servicios	1 día.

ANEXO 7. PLAN DE ACCIÓN FALLO TOTAL EN UNO DE LOS COMPONENTES DEL HARDWARE DEL O DEL FIREWALL.

Objetivo General

Recuperación en la continuidad del servicio del equipo de seguridad perimetral tipo Firewall que el IDEP tiene en producción, para garantizar la disponibilidad, integridad y autenticidad de la información institucional, así como salvaguardar la infraestructura tecnológica de hardware y servicios ubicada en las instalaciones del IDEP.

Objetivos Específicos

a. Reparar o reemplazar el equipo de seguridad seguridad perimetral tipo Firewall/FWaaS.
b. Restaurar el servicio de seguridad perimetral tipo firewall.

Alcance

El Plan de Contingencia al equipo de seguridad perimetral tipo Firewall**,** está enmarcado dentro del PLAN DE CONTINGENCIA TECNOLÓGICA IDEP PL-GT-12-02, tiene como alcance la recuperación de la continuidad de los servicios informáticos de la entidad prestados que requieren el uso del Firewall, cuando se presente una falla total o parcial en la hardware, que impacten en la disponibilidad, integridad y/o autenticidad de estos servicios en el IDEP, que requieran de conexiones seguras a internet.

Este plan identifica las actividades específicas que deben desarrollar el personal técnico del IDEP, con el apoyo de la empresa ITSellcon SAS, quien es proveedor de la solución de seguridad perimetral y presta el servicio de soporte a la misma, o en su defecto con el fabricante, en este caso FORTINET.

Para finales del año 2018, se renovaron las licencias con una vigencia de tres (3) años, que incluyen la garantía sobre el equipo en caso de fallo, para su reemplazo por un equipo temporal, mientras se recibe el equipo nuevo de reemplazo; además se contrataron diez (10) horas de soporte.

En el año 2021 se realizó la renovación de la licencia por un año, la cual está vigente hasta el año 2022. En esta ocasión no se incluyeron horas de soporte por parte del proveedor, dado que se incluyeron en el contrato de mantenimiento.

Plan de acción

A continuación, se presentan las actividades, responsables y tiempos para el desarrollo de la implementación del presente plan de contingencia.

DESCRIPCIÓN	REQUERIMIENTO	TIEMPO ESTIMADO
Los ingenieros de sistemas de la Oficina Asesora de Planeación detectan una anomalía en el funcionamiento del firewall al encontrar testigos de alarma encendidos o no enciende el dispositivo. De igual forma los usuarios pueden reportar problemas en el acceso a los servicios de red o de navegación.	Solicitud de los usuarios de la infraestructura tecnológica o identificación por parte de los ingenieros de sistemas de la Oficina Asesora de Planeación.	Por demanda
Los ingenieros de sistemas de la Oficina Asesora de Planeación validan lo indicado por el usuario en la solicitud o reporte del evento o incidente relacionado con problemas de acceso a sitios web o dificultad para navegar en internet y/o el acceso a alguno de los sistemas descritos en elalcance de esta contingencia. Se realiza la revisión de manuales y se procede a una revisión física del equipo.	Equipos de Cómputo o acceso al centro de datos para inspección visual del firewall.	Inmediato
1. Ingresar mediante un navegador a la URL de la consola de administración del firewall (https://192.168.X.X:2xx). 2. Revisar los logs. 3. Si se verifican e identifican los testigos encendidos. 4. Se verifica la conexión de potencia eléctrica.	Computadores de escritorio o portátiles. Acceso a través de escritorio remoto de Windows. Ingresar a la dirección de la consola del firewall.	30 minutos.
Los Ingenieros contratistas de sistemas Oficina Asesora de Planeación y el Técnico Operativo contactan con el proveedor a los canales indicados en el contrato, para abrir un caso o ticket. De ser posible la conexión, el proveedor accede al equipo para realizar el diagnóstico.	Dispositivo de seguridad perimetral. Conexión a Internet.	30 minutos.
Los Ingenieros contratistas de sistemas Oficina Asesora de Planeación y el Técnico Operativo contactan con el proveedor para solicitar el equipo de respaldo exigido en el contrato y a los acuerdos de niveles de servicio.	Trámites administrativos para el ingreso del equipo de seguridad perimetral de reemplazo. Cambio de equipo de seguridad perimetral tipo firewall	4 - 8 horas

El proveedor realiza la instalación y configuración del equipo temporal de reemplazo.	Acceso al centro de datos. Equipo de cómputo. Acceso a la Red.	2 horas
Una vez realizada la configuración e instalación del equipo temporal de reemplazo, los usuarios podrán acceder a los servicios de acceso a internet y conexión a todos los equipos de red. Se solicita a los usuarios, que realicen la verificación del estado de los servicios.	Equipo de temporal de reemplazo de firewall.	30 minutos.
Los Ingenieros contratista sistemas – OAP, Técnico operativo OAP realizan la actualización de la Base de datos de Activos Información Software, Hardware y Servicios, registrando la labor realizada. En caso de no presentarse observaciones continúa con la siguiente acción	Computadores con acceso a los servicios informáticos la Base de datos de Activos Información Software, Hardware y Servicios	1 día.

ANEXO 8. PLAN DE ACCIÓN FALLO EN EL ENDPOINT PROTECTION Y SERVER PROTECTION DEL ANTIVIRUS SOPHOS INTERCEPT X ADVANCED.

Objetivo General

Recuperación en la continuidad del servicio de la consola de administración del antivirus que el IDEP tiene en producción, para garantizar la disponibilidad, integridad y autenticidad de la información institucional, así como salvaguardar la infraestructura tecnológica de hardware y servicios ubicada en las instalaciones del IDEP.

Objetivos Específicos

a. Ingresar a la consola Sophos Central para verificar las alertas.
b. Permitir la administración de los agentes y antivirus instalados del antivirus Sophos instalados en los equipos de cómputo del IDEP.

Alcance

El Plan de Contingencia para el fallo en el funcionamiento de la consola de administración del antivirus**,** está enmarcado dentro del PLAN DE CONTINGENCIA TECNOLÓGICA IDEP PL-GT-12-02, y tiene como alcance la recuperación de la continuidad de los servicios informáticos de la entidad que brindan las funcionalidades del antivirus cuando se presente una pérdida total o parcial en la consola de administración del antivirus, que impacten en el monitoreo de los agentes y actualizaciones de los clientes del antivirus instalados en los equipos del IDEP, afectando la seguridad de la información, aumentando el riesgo de la disponibilidad, integridad y/o autenticidad de la información institucional alojada en los equipos de la entidad.

Este plan identifica las actividades específicas que deben desarrollar, el personal técnico del IDEP, con el apoyo de la empresa ITSEC SAS, quien es proveedor de la solución de Antivirus Sophos y presta el servicio de soporte a la misma, o en su defecto con el fabricante de la misma (SOPHOS).

Para finales del año 2019, el IDEP adquirió la actualización de consola de administración y ochenta (80) licencias para los equipos (Windows y MAC) y servidores, con una vigencia por (1) un año. Además se Contrató un año de servicio de soporte el cual se brindará cada tres meses y el servicio de actualización, migración y depuración de la consola de administración de Kaspersky.

En marzo de 2020, se realizó la actualización, migración y depuración de la consola de Kaspersky y se actualizaron las licencias del agente y antivirus a las máquinas locales (PC y portátiles) conectadas a la consola.

El 26 de agosto de 2023 se instala un nuevo antivirus SOPHOS en el instituto teniendo en cuenta de tener una administración centralizada de equipos activos de red y de seguridad con el antivirus.

Este servicio de soporte y actualización se realizará cada tres meses y durante un año, contados a partir de la primera actualización.

Plan de acción

A continuación, se presentan las actividades, responsables y tiempos para el desarrollo de la implementación del presente plan de contingencia.

DESCRIPCIÓN	REQUERIMIENTO	TIEMPO ESTIMADO
Los ingenieros de sistemas de la Oficina Asesora de Planeación o el TécnicoOperativo no pueden acceder a la consola de administración o detectan una anomalía en el funcionamiento de la consola, como puede ser que se cierra sin intervención alguna, o no está realizando las actualizaciones de los equipos mediante la interacción con los agentes.	Equipo de cómputo. Conexión a la red.	Por demanda.
Nota: Verificar previo a la llamada, la disponibilidad de horas con el proveedor/fabricante. Los ingenieros de sistemas de la Oficina Asesora de Planeación o el Técnico Operativo, contactan con el proveedor /fabricante por los canales de comunicación descritos en la documentación que hace parte del contrato y se abre un ticket por el fallo detectado.	Equipo de Cómputo. Conexión a Internet. Servicio Telefónico.	Inmediato
1. Se brinda acceso remoto o se recibe en las instalaciones del IDEP, al ingeniero certificado en Sophos enviado por el proveedor/fabricante. 2. Ingresa al servidor de dominio principal, donde se encuentra la Consola de Administración. 3. El proveedor/fabricante realiza la revisión y configuración pertinente.	Computadores de escritorio o portátiles. Acceso a través de escritorio remoto de Windows. Ingresar a la dirección de la consola del antivirus.	4 – 8 horas.
Los Ingenieros contratistas de sistemas Oficina Asesora de Planeación y el Técnico Operativo realizan la inspección de funcionamiento de la consola.	Computadores con acceso a la red LAN	1 hora.

Se realiza una inspección del funcionamiento del antivirus en los equipos de sistemas de la Oficina Asesora de Planeación. Se recibe y verifica el informe presentado por el Proveedor/fabricante, de las tareas realizadas.		

ANEXO 9. PLAN DE ACCIÓN BACKUP Y RECUPERACIÓN DE LA CONFIGURACIÓN DE LA PLATAFORMA TECNOLÓGICA DE SWITCHES DE HIPERCONVERGENCIA Y SWITCHES CISCO, ROUTER

Objetivo General

Recuperación en la continuidad del servicio de la recuperación de la configuración del switches hiperconvergencia y switches Cisco, router.

Objetivos Específicos

a. Restaurar la configuración de los switches hiperconvergencia
b. Restaurar Switches Cisco
c. Restaurar Router

Alcance

El Plan de Contingencia para el fallo en el funcionamiento de la consola de administración del antivirus**,** está enmarcado dentro del PLAN DE CONTINGENCIA TECNOLÓGICA IDEP PL-GT-12-02, y tiene como alcance la recuperación de la continuidad de los servicios informáticos de la entidad que brindan las funcionalidades de la recuperación de la configuración de los switches de la hiperconvergencia y switches Cisco, router.

Este plan identifica las actividades específicas que deben desarrollar, el personal técnico del IDEP.

Plan de acción

A continuación, se presentan las actividades, responsables y tiempos para el desarrollo de la implementación del presente plan de contingencia.

DESCRIPCIÓN	REQUERIMIENTO	TIEMPO ESTIMADO
Ingresa a la configuración de cada switch o router mediante Cliente SSH o la consola de administración. Para ello se requiere digitar el usuario y la clave	Equipo de cómputo. Conexión a la Red LAN Cliente SSH	3 minutos.
Esta actividad se debe realizar cada vez que se cambie la configuración del switch o router	Equipo de cómputo. Conexión a la Red LAN Cliente SSH	150 minutos.

En caso de que se requiera recuperar una configuración previa, se debe restaurar el backup de configuración del switch o router correspondiente. El Técnico Operativo ingresa a la dirección IP y digitando usuario y clave a través del software que provee cada fabricante.	Equipo de cómputo. Conexión a la Red LAN Cliente SSH	20 minutos.

ANEXO 10. PLAN DE ACCIÓN SERVIDOR CONTINGENCIA MICROSITIOS - ENTRADA Y SALIDA DE PRODUCCIÓN

Objetivo General

Recuperación en la continuidad del servicio Micrositios ante el fallo o no funcionamiento del servidor Web de producción, incluyendo bases de datos e infraestructura web.

Objetivos Específicos

a. Realizar cambios en la configuración de los servidores Web Virtual de producción Poseidón y alterno físico, para el relevo del servicio.
b. Restablecer el servicio Web y los micrositios en caso de fallos o no funcionamiento del servidor Web de producción Virtualizado, iniciando la contingencia con el servidor Web físico alterno.
c. Retornar a producción el servidor Web Virtualizado

Alcance

El Plan de Contingencia para el fallo en el funcionamiento del servidor web virtualizado o falla en el servicio de la hiperconvergencia que afecte el funcionamiento de las máquinas virtuales, que comprometa el funcionamiento total del Portal y Micrositios del IDEP**,** está enmarcado dentro del PLAN DE CONTINGENCIA TECNOLÓGICA IDEP PL-GT-12-02 y tiene como alcance la recuperación de la continuidad de los servicios informáticos de la entidad que brindan las funcionalidades de la recuperación de la asociadas a la entrada en producción del servidor Web Alterno y el cambio al estado original antes de la contingencia. Este plan identifica las actividades específicas que deben desarrollar, el personal técnico del IDEP.

Este procedimiento incluye a las siguientes bases de datos del portal Web y los micrositios:
Base de datos Mysql

- mysql
- performance_schema
- information_schema

Bases de Datos Portal Institucional

- drupalweb

Bases de Datos Micrositios

- acompanamientoinsitu

- centrovirtual_wp
- ciidep
- colaboratorio
- culturademocratica
- desafiosdelaescuela
- encuesta
- encuestas
- esunanota
- helpdesk
- herram_virtual_db
- idep_moodle
- idep_transmedia
- idepcontigo
- innovaciones
- innovaidep
- maestrosinvestigadores
- moodleidep
- procesosymediaciones
- seminario
- sitiopremio
- ssped_wp
- testsisped
- uaque

Plan de acción

A continuación, se presentan las actividades, responsables y tiempos para el desarrollo de la implementación del presente plan de contingencia.

DESCRIPCIÓN	REQUERIMIENTO	TIEMPO ESTIMADO
Ingresar al sitio web del IDEP www.idep.edu.co y a los micrositios sisped.idep.edu.co,	Equipo de cómputo. Conexión a la Red LAN Internet Navegador.	5 minutos.

transmedia.idep.edu.co para corroborar el funcionamiento de los mismos. Identificar una caída del servicio de la Hiperconvergencia que afectó el funcionamiento del servidor Web.		
Realizar la conexión al servidor de contingencia con IP 192.168.X.X mediante un cliente SSH	Equipo de cómputo. Conexión a la Red LAN Cliente SSH	3 minutos.
Nota: Para este paso, se debe verificar que el servidor Web Virtualizado está apagado, con la interfaz de red abajo o una dirección IP diferente, Ingresar a la configuración de la tarjeta de red del servidor de contingencia y cambiar la dirección IP por 192.168.X.X. Iniciar el servicio de red o reiniciar el servidor.	Equipo de cómputo. Conexión a la Red LAN Cliente SSH	10 minutos.
Ingresar al sitio web del IDEP www.idep.edu.co y a los micrositios sisped.idep.edu.co, transmedia.idep.edu.co para corroborar el funcionamiento de los mismos.	Equipo de cómputo Navegador.	3 minutos.
Una vez restablecido el servidor de Producción Poseidón o el servicio de Hiperconvergencia, mantener la interfaz de red apagada o no iniciar la máquina virtual.	Equipo de cómputo Navegador.	3 minutos.
Realizar la conexión al servidor 192.168.X.X mediante un cliente SSH	Equipo de cómputo. Conexión a la Red LAN Cliente SSH	3 minutos.
Nota: Para este paso, se debe verificar que el servidor Web Virtualizado está apagado, con la interfaz de red abajo o una dirección IP diferente, Ingresar a la configuración de la tarjeta de red del servidor y cambiar la dirección IP por 192.168.X.X. Iniciar el servicio de red o reiniciar el servidor.	Equipo de cómputo. Conexión a la Red LAN Cliente SSH	10 minutos.
Encender la interfaz de red o iniciar la máquina virtual, según sea el caso.	Equipo de cómputo y acceso al interfaz de administración de la Hiperconvergencia.	3 minutos.
Ingresar al sitio web del IDEP www.idep.edu.co y a los micrositios	Equipo de cómputo Navegador.	3 minutos.

sisped.idep.edu.co, transmedia.idep.edu.co para corroborar el funcionamiento de los mismos.		
En caso que se requiera, realizar la sincronización de los servidores, para actualizarlos.	Equipo de cómputo. Conexión a la Red LAN Cliente SSH	10 minutos.

ANEXO 11. PLAN DE ACCIÓN BACKUP Y RECUPERACIÓN MICROSITIOS

Objetivo General

Recuperación en la continuidad de los micrositios alojados en el servidor Web Poseidón.

Objetivos Específicos

a. Restaurar el servicio de la plataforma Govimentum, según sea el grado de afectación.
b. Restaurar el servicio de los micrositios Wordpress, según sea el grado de afectación.

Alcance

El Plan de Contingencia para el fallo en la recuperación del servicio web y micrositios alojados en el servidor virtual Poseidon**,** está enmarcado dentro del PLAN DE CONTINGENCIA TECNOLÓGICA IDEP PL-GT-12-02, y tiene como alcance la recuperación de la continuidad de los servicios informáticos de la entidad que brindan las funcionalidades de la recuperación de los archivos y bases de datos de las aplicaciones Drupal y Wordpress, para normalizar su funcionamiento, con la menor pérdida de información posible.

Este plan identifica las actividades específicas que deben desarrollar, el personal técnico del IDEP.

Plan de acción

A continuación, se presentan las actividades, responsables y tiempos para el desarrollo de la implementación del presente plan de contingencia.

DESCRIPCIÓN	REQUERIMIENTO	TIEMPO ESTIMADO
Como parte del ejercicio de mantener la información institucional, se desarrollaron scripts que automatizan la copia de los archivos de las aplicaciones y bases de datos, objeto de este proceso. Ingresar al servidor Poseidón 192.168.X.X mediante un cliente SSH. Para ello se requiere digitar el usuario y la clave.	Equipo de cómputo. Conexión a la Red LAN Cliente SSH	3 minutos.
Esta actividad se realiza de forma periódica, para descargar los archivos generados por los scripts. Se graban en los dispositivos dispuestos para el almacenamiento de las copias de respaldo (NAS y	Equipo de cómputo. Conexión a la Red LAN Cliente SSH NAS	30 minutos.

Discos duros que se almacenan en la caja fuerte y en el sitio alterno).	Discos Duros	
En caso de fallo en el servicio web o micrositios, se identifica cuál o cuáles presentan fallo en el funcionamiento. Si ocurre fallo total del sitio web, se ejecuta el PLAN DE ACCIÓN SERVIDOR CONTINGENCIA WEB - ENTRADA Y SALIDA DE PRODUCCIÓN	Equipo de cómputo. Conexión a la Red LAN NAS Discos Duros	30 minutos.
Se identifica el archivo con la copia de respaldo más reciente y se copia en el servidor de producción (según el fallo reportado puede estar o no en funcionamiento el servicio web). Ingresar al servidor Poseidón 192.168.X.X mediante un cliente SSH. Para ello se requiere digitar el usuario y la clave.	Equipo de cómputo. Conexión a la Red LAN Cliente SSH Archivo copia de respaldo reciente.	20 minutos.
Realizar la descompresión y desempaquetado del archivo de copia de respaldo en una carpeta temporal. Dependiendo la intervención, se pueda usar todo el contenido (carpetas y archivos de los sitios y de las bases de datos). En caso contrario ubicar las carpetas y archivos base de datos específicos para restaurar.	Equipo de cómputo. Conexión a la Red LAN Cliente SSH	20 minutos.
En caso de requerir, detener servicios apache y mysql. Se hace por evitar posibles daños en los archivos, especialmente los de las bases de datos.	Equipo de cómputo. Conexión a la Red LAN Cliente SSH	5 minutos.
Realizar la sincronización de carpetas y archivos. Para el caso de MySQL se puede utilizar la CLI (recomendado) para cargar el script de las bases de datos respectivas o un cliente gráfico.	Equipo de cómputo. Conexión a la Red LAN Cliente SSH	20 minutos.
Iniciar servicios apache y MySql. Revisar el correcto funcionamiento de los servicios web afectados.	Equipo de cómputo. Conexión a la Red LAN Cliente SSH	5 minutos.

ANEXO 12. PLAN DE ACCIÓN BACKUP Y RECUPERACIÓN DEL SERVICIO WEB

Objetivo General

Recuperación en la continuidad del servicio web alojado en el servidor virtual Oporto creado en la solución hiperconvergente.

Objetivos Específicos

a. Restaurar el servicio de la plataforma Drupal, según sea el grado de afectación.
b. Normalizar el canal de comunicación en doble vía y el acceso a la información institucional, publicados en el Portal Web Institucional.

Alcance

El Plan de Contingencia para el fallo en la recuperación del servicio web y micrositios alojados en el servidor virtual Poseidon**,** está enmarcado dentro del PLAN DE CONTINGENCIA TECNOLÓGICA IDEP PL-GT-12-02, y tiene como alcance la recuperación de la continuidad de los servicios informáticos de la entidad que brindan las funcionalidades de la recuperación de los archivos y bases de datos de las aplicaciones Drupal 9, para normalizar su funcionamiento, con la menor pérdida de información posible.

Este plan identifica las actividades específicas que deben desarrollar, el personal técnico del IDEP.

Plan de acción

A continuación, se presentan las actividades, responsables y tiempos para el desarrollo de la implementación del presente plan de contingencia.

DESCRIPCIÓN	REQUERIMIENTO	TIEMPO ESTIMADO
Como parte del ejercicio de mantener la información institucional, se desarrollaron scripts que automatizan la copia de los archivos de las carpetas más importantes para el funcionamiento del servidor Oporto Ingresar al servidor 192.168.X.X mediante un cliente SSH.	Equipo de cómputo. Conexión a la Red LAN Cliente SSH	3 minutos.
Esta actividad se realiza de forma periódica, para descargar los archivos generados por los scripts. Se graban en los dispositivos dispuestos para el almacenamiento de las copias de respaldo	Equipo de cómputo. Conexión a la Red LAN Cliente SSH NAS Discos Duros	30 minutos.

(NAS y Discos duros que se almacenan en la caja fuerte y en el sitio alterno).		
Ingresar al sitio web del IDEP www.idep.edu.co para corroborar el funcionamiento del mismo. Identificar una caída del servicio de la Hiperconvergencia que afectó el funcionamiento del servidor Web.	Equipo de cómputo. Conexión a la Red LAN Internet Navegador.	10 minutos.
Ubicar el archivo de copia de respaldo más reciente realizado de dicho servidor.	Equipo de cómputo. Conexión a la Red LAN	2 horas.
Ingresar al sitio web del IDEP www.idep.edu.co para corroborar el funcionamiento del mismo.	Equipo de cómputo Navegador.	3 minutos.

ANEXO 13. PLAN DE ACCIÓN RECUPERACIÓN DEL CORREO ELECTRÓNICO

Objetivo General

Recuperación en la continuidad del servicio de correo electrónico institucional.

Objetivos Específicos

a. Crear cuenta de correo alterno con otro proveedor diferente al que se tiene la cuenta principal.
b. Realizar backup de la cuenta alterna al restablecerse el servicio del correo principal.
c. Transferir los correos de la cuenta alterna a la cuenta principal.

Alcance

El Plan de Contingencia para el fallo en la prestación del servicio de correo institucional**,** está enmarcado dentro del PLAN DE CONTINGENCIA TECNOLÓGICA IDEP PL-GT-12-02, y tiene como alcance la continuidad del servicio de correo electrónico para los puestos críticos mientras se restablece el servicio por parte del proveedor y su posterior envío de los correos a las cuentas principales.

Este plan identifica las actividades específicas que deben desarrollar, el personal técnico del IDEP.

Plan de acción

A continuación, se presentan las actividades, responsables y tiempos para el desarrollo de la implementación del presente plan de contingencia.

DESCRIPCIÓN	REQUERIMIENTO	TIEMPO ESTIMADO
Llamar al proveedor para avisar y recibir información del inconveniente presentado. Crear el respectivo ticket de servicio ante el proveedor.	Llamada telefónica. Conexión a Internet.	30 minutos.
Crear cuenta de correo alterno con otro proveedor diferente al que se tiene la cuenta principal para los jefes de oficina y los procesos que así lo requiera.	Conexión a Internet.	30 minutos.
Estar en contacto con el proveedor hasta que se restablezca el servicio de correo electrónico.	Proveedor.	determinado por el proveedor.
Una vez restablecido el servicio de correo electrónico institucional se procede a hacer el acompañamiento para realizar el backup a la cuenta de correo alterna.	Equipo de cómputo. Conexión a Internet.	30 minutos.
Se procede a copiar los correos del backup a la cuenta de correo principal de cada cuenta de correo.	Equipo de cómputo. Conexión a Internet.	60 minutos.

ANEXO 14. PLAN DE ACCIÓN RECUPERACIÓN DEL BIOMÉTRICO

Objetivo General

Recuperación para la continuidad del servicio del sistema Biométrico.

Objetivos Específicos

a. Determinar el inconveniente presentado.
b. Restaurar el último backup al sistema Biométrico.

Alcance

El Plan de Contingencia para la continuidad del servicio del sistema Biométrico**,** está enmarcado dentro del PLAN DE CONTINGENCIA TECNOLÓGICA IDEP PL-GT-12-02, y tiene como alcance la recuperación de la continuidad de los servicios de seguridad física de la entidad para permitir el acceso autorizado a las instalaciones del IDEP.

Este plan identifica las actividades específicas que deben desarrollar, el personal técnico del IDEP.

Plan de acción

A continuación, se presentan las actividades, responsables y tiempos para el desarrollo de la implementación del presente plan de contingencia.

DESCRIPCIÓN	REQUERIMIENTO	TIEMPO ESTIMADO
Determinar el inconveniente presentado si es por error de lectura de huella o por que la cuenta de usuario presenta fallos.	Equipo de cómputo. Conexión a la Red LAN.	5 minutos.
Si el problema es por error de lectura de huella, se puede hacer apertura remota a través del aplicativo ZKAccess.	Equipo de cómputo. Conexión a la Red LAN Conexión a VPN (si lo requiere).	5 minutos.
Para evitar el fallo por energía el sistema biométrico se encuentra conectado a toma de energía regulada bajo UPS.	Toma de corriente regulada.	0 minutos.

Si es porque la cuenta de usuario presenta fallos se procede a restaurar el último backup ó solicitar al usuario que se acerque para volver a tomar las huellas.	Equipo de cómputo. Conexión a la Red LAN.	20 minutos.

ATENCIÓN DE INCIDENTES DE SEGURIDAD Y FALLOS EN LAS MÁQUINAS

Los incidentes de seguridad y los fallos en las máquinas por cualquier motivo, son atendidos en el momento en que ocurren aplicando los planes de acción descritos en cada uno de los anexos, según apliquen.

Para fortalecer las acciones de los planes se diligencia en la sección respectiva del plan de mantenimiento y monitoreo las contingencias atendidas, la fecha en que se atiende, el Ingeniero que resuelve y las acciones realizadas, estas situaciones son el insumo para fortalecer los planes de acción aquí descritos.

A continuación se incluye el link que da acceso al Plan de Mantenimiento y Monitoreo y también la tabla que se viene trabajando durante estos años como insumo para las mejoras a realizar a los planes de acción:

https://docs.google.com/spreadsheets/d/1uzdZQiXoqDD3pnB6DMchqA3JB9vIP7jq/edit?usp=sharing&ouid=115541243112431525010&rtpof=true&sd=true

Bitácora Contingencias Ejecutadas 2023:

No.	Fecha	Nombre Contingencia	Acciones Ejecutadas	Responsable de la Acción	Observaciones	Riesgo Materializado Matriz de Riesgos
1	30/01/2023	Apagado infraestructura de TI no controlada				Indisponibilidad
2	27/02/2023	Apagado infraestructura de TI controlada	Debido a un fuerte aguacero se filtró agua al interior de la casa IDEP, Sede San Luis lo que puso en riesgo la infraestructura tecnológica del IDEP ya que el agua caía sobre algunos PC y sobre la toma corriente de uno de los elementos de tecnología. Esta situación podría ocasionar un corto o daño	Técnico Operativo de la OAP y contratistas.	Se toman evidencias en fotos donde se observa la afectación y los equipos que fueron protegidos con sombrillas para evitar una afectación.	Indisponibilidad de los sistemas y servicios tecnológicos del IDEP

			permanente en la infraestructura por lo tanto se procedió a apagar todos los servidores y se solicitó a los Colaboradores del IDEP apagar los equipos y protegerlos del agua. Para poder prender de nuevo los equipos y retomar las actividades una vez la lluvia pasó se identificó el breaker de la toma afectada por la lluvia y se procedió a bajarlo, así mismo la toma se secó con un trapo para evitar un cortocircuito. Por instrucciones de la alta Dirección se procedió a encender las máquinas una vez se controló el riesgo.			
3	7,8,9,10 y 11 marzo/2023	Encendido gradual de infraestructura	Luego de haber realizado las revisiones a la instalación de la infraestructura y elementos en el centro de datos, se inicia el proceso de ubicación de los servidores y elementos de comunicaciones, en los diferentes racks o muebles.	Técnico Operativo de la OAP y contratistas.	Se habilitan los servicios web (Portal, Micrositios, aulas virtuales, que se encontraban alojados en los servidores, se reestablece el servicio de acceso remoto y	

			De igual forma se realizó la conexión de los mismos y del cableado de red, para el posterior encendido de los mismos.			
4	09/06/2023	Caída del servicio de Internet	Interrupción total del servicio de internet	Técnico Operativo de la OAP y contratistas.	Desde las 7:30 am hasta las 12 m, se presentó una interrupción total en el servicio de internet.	Indisponibilidad
5	26/06/2023	Intermitencia en el servicio de Internet	Interrupción del servicio de internet generando intermitencia	Técnico Operativo de la OAP y contratistas.		Indisponibilidad
6	05/09/2023	Caída en el servicio de Internet	Interrupción total del servicio de internet	Técnico Operativo de la OAP y contratistas.		Indisponibilidad
7	06/09/2023	Intermitencia en el servicio de Internet	Interrupción del servicio de internet generando intermitencia	Técnico Operativo de la OAP y contratistas.		Indisponibilidad

Bitácora Contingencias Ejecutadas 2022:

No.	Fecha	Nombre Contingencia	Acciones Ejecutadas	Responsable de la Acción	Observaciones	RIESGO MATERIALIZADO EN MATRIZ DE RIESGO
1	28/04/2022	Caída de todos los equipos del Data Center	1. Corte inesperado en el fluido eléctrico en el sector 2. Se apagaron abruptamente todos los Servidores y equipos de comunicación del Instituto al igual que los PCs en Casa IDEP. 3. Se determinó que una de las dos fases de la casa no tenía energía y por ende no podían operar con normalidad las UPSs. 4.	Contratistas TI	Por falta de fluido eléctrico se cayeron todos los Servidores y equipos de Comunicación del Data Center.	Indisponibilidad de los servicios
2	06/06/2022	Caída de servicios Web alojados en la hipeconvergencia.	Se llena el espacio de almacenamiento de la hiperonvergencia, por la no reclamación de espacio de esta, procedimiento que se informa por parte del fabricante durante este soporte , debe ser realizado frecuentemente teniendo en cuenta que la solución no borra completamente la información siendo necesario hacerla mediante la ejecución de comandos, para "reclamarlo". A partir de este momento, se inicia la ejecución periódica de los	Contratista TI y Fabricante HPE, mediante el contrato xyz de 2022.	No se realizaba la ejecución del comando " esxcli storage vmfs unmap -l <nombre_data_store>"	Indisponibilidad de los servicios

			comandos indicados por HPE en los espacios de almacenamiento definidos de la hiperconvergencia. Se adelanta el proceso de adecuación de un disparador automático (cron), para realizar dicha tarea de forma automática periódicamente.			
3	09/06/2022	Caída sitio Profes en Acción (gamificación)	Como consecuencia de la caída de la hiperconvergencia, el sitio de gamificación produjo un error en el sistema operativo, por lo que fue necesario realizar un procedimiento de chequeo del disco para solventarlo.	Contratistas TI	Servicio normalizado, no fue necesario recurrir a las instantáneas, dado que eran del mes de marzo, lo que podría generar pérdida de información subida durante los primeros días de junio.	Indisponibilidad de los servicios
4	24/10/2022 y 25/10/2022	Apagado infraestructura de TI	Como consecuencia del fallo en una fase de las tres que brinda electricidad a la casa, se hizo necesario realizar un apagado controlado de toda la infraestructura de TI del IDEP.	Contratistas TI	Durante el proceso de normalización de los servicios, no se presentaron problemas, daños en equipos o servidores o infraestructura ni tampoco de información.	Indisponibilidad de los servicios
5	20/11/2022 y 21/11/2022	Apagado infraestructura de TI parcialmente controlada	Hubo fallo del fluido eléctrico por fallas en el sector la energía de las UPS permitió apagar de manera controlada solo la hiperconvergencia. El resto de equipos se apagaron de forma no controlada. El ejercicio encendido controlado, no generó fallos o problemas	Contratistas TI	Durante el restablecimiento de los servicios se presentaron: 1. Dificultad para subir la Base de Datos Oracle (Sistema Goobi) 2. Posterior a la falla se han detectado equipos con errores en discos y fallas en los técnicas	Indisponibilidad de los servicios

			reportados tanto en infraestructura como en servicios.			
6	17/12/2022 - 19/12/2022	Apagado infraestructura de TI no controlada	Por fallos en el fluido eléctrico el 17/12/2022 se agotan las baterías de la UPS lo que produjo un apagado abrupto de toda la infraestructura de TI. Dicho corte fue notificado en el CHAT la Subdirección Administrativa y Financiera. El 18/12/2022 en horas de la tarde el prestador de servicio ENEL inicia labores de restablecimiento del servicio, aunque ese mismo día se produce un segundo corte en horas de la noche y se encuentra un número no determinado de lámparas o luminarias dañadas, con lo que se toma la decisión de no encender la infraestructura de TI hasta la Subdirección Administrativa y Financiera gestione con FAMOG la visita técnica para determinar el correcto funcionamiento del fluido eléctrico en la			Indisponibilidad de los servicios

			casa. Una vez normalizado el servicio de fluido eléctrico y con el visto bueno de FAMOC DE PANEL se realizó un encendido controlado de toda la infraestructura, con actividades de revisión y corrección de errores a los servidores, en especial a los nodos de la hiperconvergencia. Durante este proceso se corrigen los posibles errores tanto en hardware como software. Finalizado ésto se normalizan los servicios el 19/12/2022. Al 20 de diciembre de 2022 no se han identificado o reportado fallos en el funcionamiento de los servicios. Luego de la normalización tanto del fluido eléctrico como del funcionamiento de la infraestructura de TI y los servicio asociados, se identifican daños en una placa base (board), 2 discos duros, y 1 teclado. Se encuentra en revisión para su diagnóstico 2 equipos y 3 discos duros.			

Bitácora de contingencias ejecutadas 2019-2020:

Fecha	Nombre Contingencia	Acciones Ejecutadas	Responsable de la Acción	Observaciones
19/06/2019	Caída del servidor de dominio principal.	1. Se realizó una actualización del dominio Windows Server 2016 virtualizado, que generó un error, que trajo como consecuencia que el sistema operativo no iniciara. 2. Se probó reiniciar varias veces la máquina virtual pero el resultado fue el mismo del punto 1. 3. Se contactó con el soporte de Microsoft Colombia, indicando que para poder brindar el soporte de acuerdo al contrato que se tenía era indispensable permitir el acceso remoto al servidor, lo cual era prácticamente imposible, por lo indicado en el punto 1. 4. Por lo indiado en el punto 3, se procedió a realizar una nueva instalación desde cero del servidor, aplicando las actualizaciones liberadas por Microsoft a la fecha de realizada la actualización. Vale la pena resaltar, que se realizó un Snapshot de la máquina virtual previo a la aplicación de las actualizaciones. 5. Por último se realizó la promoción como servidor de dominio. Se verificó que quedara correctamente funcionando, así como sincronizadas las reglas y configuraciones. 6. Se realiza la correcta promoción como Controlador de Dominio Principal (Windows Server 2016) y Controlador de Dominio Secundario (Windows Server 2008), eliminando los controladores de dominio inactivos o inexistentes.	Ing. Oscar Lozano Técnico Operativo	En ningún caso hubo interrupción del servicio, dado que se tiene un servidor de dominio de respaldo, instalado con Windows Server 2018.

08/05/2019	Bloqueo al aplicativo Goobi	1. Al ingreso al aplicativo el sistema generaba un mensaje y no permitía el ingreso. 2. Se informó inmediatamente por correo y telefónicamente al proveedor. 3. Se aplicó la contingencia, se restableció el backup del mismo día y del día anterior para validar si la falla se encontraba en estos días y ocurrió lo mismo. 4. El proveedor respondió en el término de unas horas y se soluciona el problema.	Contratista TI y Técnico Operativo	El proveedor IT-GOP había colocado un control que impidió el acceso a la aplicación. Fue corregido por el proveedor ya que al restablecer el backup de dos días anteriores, el problema se presentaba.
11/06/2019	Bloqueo Hiperconvergencia	1. Se sigue el proceso de contingencia. 2. Se solicita al proveedor SUMIMAS soporte técnico, este soporte requiere diligenciar un formato lo que toma tiempo. 3. Debido a la urgencia se contacta telefónicamente al servicio de HP. 5. HP responde con conexión remota, soluciona el problema y da algunas recomendaciones. 6. Esta solución se documenta y se ajustan los documentos asociados.	Jaime Acosta Oscar Lozano Juliett Yaver	Al realizar los snapshots se evidencia que el sistema de hiperconvergencia esta lento y se bloquea. En un momento se inhabilita la opción de Power On quedando sin servicio el servidor virtual Poseidon.
04/07/2019	Caída Hiperconvergencia	1. Corte inesperado en el fluido eléctrico a las 6:00 am 2. Al llegar a la oficina el sistema estaba prendido, es decir tenía corriente pero no tenía activos los servicios. 3. Se siguió el proceso de contingencia, se llamó al servicio de soporte y a la empresa SUMIMAS 4. El Servicio de soporte de HP atendió la solicitud en un par de horas y con las indicaciones se logró subir el sistema de Hiperconvergencia. 5. Dos días después llegó el soporte de SUMIMAS y realizó algunas recomendaciones.	Jaime Acosta Juliett Yaver	Por falta de fluido eléctrico durante más de una hora, se cayó el sistema de hiperconvergencia.

04/07/2019	Caída de sitios web, micrositios y revistas.	1. Con la caída de la hiperconvergencia, el portal Web, los micrositios y revistas, dejan de operar. 2. Se realiza la configuración de red del servidor de respaldo, dejándolo con la dirección IP del servidor de producción. 3. Se inician los servicios apache y mysql. 4. Reinicio del servidor de respaldo, entrando como sustituto del de producción. 5. Subida de los sitios web, micrositios y revistas.	Oscar Lozano	El procedimiento permitió tener fuera de servicio el portal web, los micrositios y revistas, por un periodo no mayor a 20 minutos. Una vez restablecida la hiperconvergencia, se realiza el cambio de configuración del servidor de pruebas, se detienen los servicios Apache y Mysql. Se realiza la sincronización entre el servidor de pruebas y el servidor de producción para actualizar los cambios realizados, restableciendo los servicios de portal, micrositios y revistas.
11/07/2019	Bloqueo al aplicativo Goobi	1. El proveedor realizó una actualización no controlada al sistema, la cual dejó fuera de servicio el aplicativo. 2. Se comunicó inmediatamente al proveedor vía telefónica y se inició el plan de contingencia. 3. El proveedor indica que una vez revisado no encuentra errores. 4. Se verifican los logs del antivirus y se detecta que al cambio del ejecutable el antivirus bloquea la ejecución ya que no reconoce el ejecutable como un software permitido. 5. Se levanta la restricción del antivirus y esto permitió el funcionamiento del software. Esto toma 3 horas.	Jaime Acosta Juliett Yaver	Hubo interrupción del servicio por 3 horas. Se inició el plan de contingencia para este caso y no funcionó porque el problema estaba en el bloqueo del antivirus, esto permitió buscar la causa real del problema, identificarlo y resolverlo.

23/09/2019	Bloqueo Hiperconvergencia	1. El domingo 22 de septiembre al realizar el borrado del snapshot de la máquina virtual idep-koha se degrada la máquina y bloquea el proceso por horas teniendo que cancelarlo. 2. El sistema genera una alerta donde indica que se debe realizar el proceso de consolidación. 3. Se realiza el proceso de consolidación llegando al 46% y generando un mensaje de error. 4. Se detiene el proceso y genera errores al intentar ejecutarlo nuevamente. 5. Se da inicio al plan de contingencia donde se contacta al proveedor de HP. 6. El proveedor tarda varias horas en lograr habilitar la máquina y dejarla productiva. 7. El soporte termina el día 24 de septiembre con la habilitación y estabilización de la hiperconvergencia. 8. El Ingeniero Experto sugiere no utilizar los snapshots como mecanismos de Backup ya que estos degradan la máquina.	Oscar Lozano Juliett Yaver	Al realizar el borrado del snapshot de la máquina virtual idep-koha, este proceso ralentiza la máquina y toma más de 9 horas sin terminar, permaneciendo estático en el 77% por cerca de 6 horas. Se procede a cancelar la tarea de remoción de snapshot la cual se demora cerca de 1 hora 30 minutos en finalizar al parecer sin novedad. Después se genera un mensaje en el cual se indica que se debe realizar un consolidate de la máquina, se lleva a cabo el procedimiento el cual alcanza el 46% y luego genera un error indicando que hay un proceso en ejecución. Lo que puede indicar que la cancelación no dejó la máquina estable. El soporte de HP apoya la actividad la cual toma casi todo el día para logar levantar la máquina.

28/02/2020	Caída Hiperconvergencia	El día 28 de febrero a las 2 pm se presentó un corte en el fluido eléctrico que duró alrededor de 1 hora y 30 minutos por problemas con la cafetera ubicada en la cocina de la oficina 402B, que hizo que se saltara el taco/braker de la oficina 402B que protege la línea de fluido eléctrico que alimenta entre otros elementos a la UPS, que a su vez afectó el taco/braker designado para dicha oficina en el cuarto eléctrico del piso 4 del edificio; provocando el apagado de la UPS (que estuvo encendida por alrededor de 15 minutos), produciendo como consecuencia el apagado abrupto e incorrecto de la Hiperconvergencia y demás equipos alojados en el Centro de Datos. Se procedió a solicitar a la administración del edificio, para que permitiera el acceso al cuarto eléctrico del piso 4, para proceder a activar habilitar el taco/braker y así restablecer el servicio de fluido eléctrico (que tomó de 1 hora y 30 minutos aproximadamente). Afectación Este corte afectó los siguientes equipos: 1. Servidor HPE G7 - Web Alterno. 2. Servidor HPE G7 – Dominio Alterno y Tablas de Retención Documental 3. Servidor HPE G7 - Oracle VM/Oracle Linux/Oracle12c 4. Router proveedor servicio de Internet 5. Firewall 6. Switch de Red Cisco 7. Servidor G4 - Base de Datos Oracle 8. Switchs Aruba - Hiperconvergencia	Oscar Lozano Cesar Linares	Consecuencias. Al restablecerse el fluido eléctrico se procede al encendido de los equipos afectados, la mayoría de los cuales encendieron correctamente y los servicios allí alojados se restablecieron sin novedad alguna, exceptuando los servicios alojados en la Hiperconvergencia, que dada su naturaleza tuvo problemas al encender, dejando por fuera varios servicios del IDEP. Acciones. Se contacta con el proveedor del soporte (HPE) de la Hiperconvergencia que abre un caso, y se pasa a producción el equipo físico G7 de respaldo que se tiene pare el sitio Web, el cual se toma alrededor de 5 minutos en iniciar, restableciendo el servicio del portal y micrositios. Hasta las 7 pm, se recibe la respuesta del hp, que mediante acceso remoto realiza la restauración del servicio de Hiperconvergencia, quedando éste normalizado. Se procede a apagar el servidor web de respaldo y el enciende el servidor virtual, restaurando el servidor virtual de producción.

		9. Servidores HPE G9 - Nodos Hiperconvergencia 10. Servidor HPE G5 - "Tercer Nodo" Hiperconvergencia		
11/09/2020	Nodo Apagado Hiperconvergencia	Se detecta que un nodo de la hipeconvergencia se apaga, y requiere que sea encendido físicamente. El segundo nodo muestra alerta por RAM y espacio en discos. Se contacta con el soporte del fabricante HPE, para verificar lo sucedido. En ningún momento hubo interrupción de los servicios alojados en la hipercongergencia. (Repositorio Digital, Web, servidor de dominio secundario.	Oscar Lozano	Cesar Linares se acerca a las instalaciones del IDEP y enciende el nodo apagado. En relación con las alarmas HPE indica que hacen parte del funcionamiento normal de la solución, que de acuerdo a los algoritmos de balanceo de carga, ella determinará en qué momento distribuir el uso de recursos disponibles, por lo que la alarma continuará hasta que la solución haga los cambios. Se aprovecha, para la realizar la recuperación de espacio de almacenamiento usado de las máquinas virtuales. Se realizó la migración de dos máquinas virtuales, de forma manual. [root@HPE-HC-CZ37431VN1:~] esxcli storage vmfs unmap -l Koha_DSpace

				[root@HPE-HC-CZ37431VN1:~] esxcli storage vmfs unmap -l Poseidon [root@HPE-HC-CZ37431VN1:~] esxcli storage vmfs unmap -l Windows [root@HPE-HC-CZ37431VN1:~] esxcli storage vmfs unmap -l Templates
11/10/2021	Caída del servidor apolo	El servidor apolo se cayó, en este se encuentra instalado el sistema de información Goobi.	César Linares	