Firma de Autorizaciones		
Elaboró	**Revisó**	**Aprobó**
Contratista Sistemas Oficina Asesora de Planeación	Contratistas Sistemas Oficina Asesora de Planeación	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 NOMINA 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 numeral 7.2 incluyendo descripción de los backups 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 actualizándola 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.

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 backups a las carpetas “Z” las cuales ya no se utilizan y a cambio se realizan los Backup 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.

TABLA DE CONTENIDO

INTRODUCCIÓN 6

1. OBJETIVO 6

1.1. Objetivo General 6

1.2. Objetivos específicos 7

2. ALCANCE DEL PLAN DE CONTINGENCIA 7

3. ANÁLISIS DE IMPACTO AL NEGOCIO - BIA (Business Impact Analysis) 8

3.1. Identificación de los procesos misionales y criticidad de recuperación: 8

3.2. Identificación los requerimientos de recursos 13

3.3. Identificar las prioridades de recuperación de servicios y sistemas de información 14

4. CONTROLES PREVENTIVOS 15

4.1. Capacidad de las UPS 15

4.2. Capacidad de los sistemas de refrigeración 15

4.3. Sistema de extinción de incendio 15

4.4. Sistemas de monitoreo capacidad de los servidores 16

4.5. Sistemas de monitoreo de aplicaciones 16

4.6. Sistemas de monitoreo de bases de datos 16

4.7. Toma de copias de respaldo y Periodicidad 16

4.8. Sistemas de almacenamiento de copias de respaldo 17

4.9. Sistemas de protección de la seguridad de la información 17

4.10. Realizar simulacros y pruebas a los backups realizados 18

4.11. Contar con servidores alternos para la restauración de los sistemas de información 18

5. ESTRATEGIAS DE CONTINGENCIA 18

5.1. Empresas de Servicio o Proveedores de Servicios Externos 18

5.2. Identificación de Incidentes que se pueden presentar 19

6. MANTENIMIENTO AL PLAN DE CONTINGENCIA 19

6.1. Revisión y actualización del plan 19

7. REFERENCIAS NORMATIVAS 20

8. GLOSARIO DE TÉRMINOS 21

9. PLAN DE CONTINGENCIA PARA LOS SISTEMAS DE INFORMACIÓN 24

9.1.1. FASES DEL PLAN 25

9.1.1. Fase de Notificación del incidente 25

9.1.2. Fase Evaluación del Incidente 25

9.1.3. Establecer el origen de la falla y la posible solución 25

9.1.4. Activar el plan de contingencia y notificar 26

9.1.5. Llevar a cabo las acciones para restablecer el servicio 26

9.1.6. Validar el resultado de las acciones realizadas 26

9.1.7. Presentar el informe resultado de las acciones realizadas 26

ANEXO 1. PLAN DE ACCIÓN PARA LOS APLICATIVOS WEB KOHA, OJS, DSPACE, VUFIND, CAJA DE HERRAMIENTAS y HUMANO 27

ANEXO 2. PLAN DE ACCIÓN AL SISTEMA DE INFORMACIÓN ADMINISTRATIVO Y FINANCIERO. 28

ANEXO 3. PLAN DE ACCIÓN AL SISTEMA DE INFORMACIÓN NÓMINA HUMANO. 30

ANEXO 4. PLAN DE ACCIÓN PARA LA RECUPERACIÓN INFORMACIÓN RECURSOS DE RED TABLAS DE RETENCIÓN DOCUMENTAL TRD 31

ANEXO 5. PLAN DE ACCIÓN HIPERCONVERGENCIA. 33

ANEXO 6. PLAN DE ACCIÓN FALLOS EN LA CONFIGURACIÓN DEL FIREWALL 35

ANEXO 7. PLAN DE ACCIÓN FALLO TOTAL EN UNO DE LOS COMPONENTES DEL HARDWARE DEL O DEL FIREWALL. 38

ANEXO 8. PLAN DE ACCIÓN FALLO EN LA CONSOLA DE ADMINISTRACIÓN DEL ANTIVIRUS. 41

ANEXO 9. PLAN DE ACCIÓN BACKUP Y RECUPERACIÓN DE LA CONFIGURACIÓN DE LA PLATAFORMA TECNOLÓGICA DE SWITCHES DE HIPERCONVERGENCIA Y SWITCHES CISCO, ROUTER 43

ANEXO 10. PLAN DE ACCIÓN SERVIDOR CONTINGENCIA WEB - ENTRADA Y SALIDA DE PRODUCCIÓN 44

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 Investigación Educativa y el Desarrollo Pedagógico 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 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

- Realizar las actividades preventivas y controles necesarios que permitan mantener en correcto funcionamiento la infraestructura tecnológica de la Entidad.
- 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.
- 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 ó no sean aplicables.
- Presentar recomendaciones que permitan disminuir la probabilidad de ocurrencia de una eventualidad y definir los procedimientos preventivos resultantes de estas recomendaciones.
- Listar 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.

Propósito del Análisis BIA:

A. Identificar los procesos misionales y criticidad de recuperación:

Se identifican los sistemas y servicios más importantes y los cuales deben ser recuperados con prioridad sobre los demás. El plan de contingencia contempla la recuperación de los sistemas y servicios de criticidad alta.

B. Identificar los requerimientos de recursos

La identificación de los esfuerzos necesarios para recuperar los sistemas implica una evaluación detallada de los recursos necesarios para reactivar los procesos misionales y la identificación de las interdependencias entre recursos y sistemas. Algunos de los elementos que se deben considerar incluyen: talento humano, instalaciones, equipos, software, archivos de datos y componentes de los sistemas.

C. Identificar las prioridades de recuperación de servicios y sistemas de información

Se identifican los sistemas y servicios que sean prioritarios de recuperar ante eventuales fallas.

3.1. 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
1	Sistema de Información Cliente/Servidor: Goobi que interopera con el sistema de información Humano en	El sistema se utiliza en modalidad 5 x 8 y eventualmente se requiere los fines de semana y festivos.	De acuerdo a la importancia y criticidad el sistema Goobi no se programa estar en indisponibilidad por más de 8 horas laborales.	El sistema de información Goobi soporta la operación administrativa y financiera del IDEP, la radicación, contratación, almacén (bienes 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
	modalidad fuera de línea.			publicaciones) y la contabilidad. Es un sistema de propiedad de la empresa Goobi SAS.
2	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.
3	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. Los datos son organizados como ítems que pertenecen a una colección; cada

#	Nombre del Servicio o Sistema de Información	Periodicidad de Uso en el IDEP	Tiempo de interrupción no programada tolerable	Descripción del sistema o servicio
				colección pertenece a una comunidad. Es una herramienta de código abierto.
4	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.
5	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.
6	Servicio de Correo electrónico	El sistema se usa 7 días a la semana las 24 horas del día.		Medio de contacto institucional que integra otras funcionalidades colaborativas.
7	Servicio de Internet	El canal debe estar en funcionamiento 7 días a la semana las 24 horas del día.	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 60 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
8	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.
9	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.
10	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).
11	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 remota la red LAN a través del servicio de Red Privada Virtual (VPN). La indisponibilidad del sistema puede afectar directamente la operación de la	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
			entidad por la afectación de seguridad en la información.	
12	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.
13	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
14	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.

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

#	Nombre del Servicio o Sistema de Información	Periodicidad de Uso en el IDEP	Tiempo de interrupción no programada tolerable	Descripción del sistema o servicio
1	Sistema de información Humano que interopera con el sistema de información Goobi en modalidad fuera de línea.	El sistema se utiliza para la liquidación mensual de la Nómina del IDEP y opera bajo modalidad SAS.	De acuerdo a la importancia y criticidad el sistema Humano no se programa estar en indisponibilidad por más de 8 horas laborales.	El sistema de información HUMANO permite la liquidación mensual de la nómina con lo que esto conlleva, registro de novedades, conceptos de provisiones 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
				aportes a la seguridad social.

3.2. Identificación los requerimientos de recursos

Con el propósito de realizar la recuperación de los sistemas de información y servicios tecnológicos que presta el IDEP se requiere de una serie de recursos tecnológicos y humanos para llevarlo a cabo.

#	Nombre del Servicio o Sistema de Información	Recursos
1	Sistema de Información Cliente/Servidor: Goobi que interopera con el sistema de información Humano en modalidad fuera de línea.	El servicio de Soporte que presta el proveedor Goobi SAS dueño del sistema. El servicio de mantenimiento de la infraestructura lógica y física del IDEP para la administración de la base de datos Oracle. El soporte de Primer Nivel prestado por el Ingeniero a cargo de los sistemas de Información. El soporte de Primer Nivel es prestado por el Ingeniero a cargo de los sistemas de Información.
2	Sistema de información Humano que interopera con el sistema de información Goobi en modalidad fuera de línea.	El servicio de Soporte que presta el proveedor Soporte Lógico dueño del sistema. El soporte de Primer Nivel es prestado por el Ingeniero a cargo de los sistemas de Información.
3	Sistema de Información web: Koha	El servicio de mantenimiento de la infraestructura lógica y física del IDEP. El soporte de primer nivel es prestado por los Ingenieros del área.
4	Sistema de Información web: DSpace	El servicio de mantenimiento de la infraestructura lógica y física del IDEP. El soporte de primer nivel es prestado por los Ingenieros del área.
5	Sistema de Información web: OJS	El servicio de mantenimiento de la infraestructura lógica y física del IDEP. El soporte de primer nivel es prestado por los Ingenieros del área.
6	Sistema de Información web: VuFind	El servicio de mantenimiento de la infraestructura lógica y física del IDEP. El soporte de primer nivel es prestado por los Ingenieros del área.

#	Nombre del Servicio o Sistema de Información	Recursos
7	Servicio de Correo electrónico	El servicio de soporte de los niveles 2,3,4..n lo presta la empresa proveedor del servicio. El soporte de primer nivel es prestado por los Ingenieros del área.
8	Servicio de Internet	El servicio de soporte de los niveles 2,3,4..n lo presta la empresa proveedor del servicio. El soporte de primer nivel es prestado por los Ingenieros del área.
9	Servidor Web	El soporte al servidor Web del IDEP es prestado por los Ingenieros del área.
10	Base de Datos Oracle	El servicio de soporte de niveles superiores se realiza con el contrato de mantenimiento a la infraestructura tecnológica. El soporte de primer nivel es prestado por los Ingenieros del área.
11	Sistema de Hiperconvergencia	El servicio de soporte de los niveles 2,3,4..n lo presta la empresa proveedor del servicio. El soporte de primer nivel a la infraestructura del IDEP prestado por los Ingenieros del área.
12	Firewall	El servicio de soporte de los niveles 2,3,4..n lo presta la empresa proveedor del servicio. El soporte de primer nivel es prestado por los Ingenieros del área.
13	Antivirus	El servicio de soporte que presta la empresa proveedora. El soporte de primer nivel es prestado por los Ingenieros del área.
14	Servicio de WIFI	El soporte de primer nivel es prestado por los Ingenieros del área.
15	Servicio de Red LAN	El servicio de soporte de niveles superior es prestado con el contrato de mantenimiento de la infraestructura del IDEP. El soporte de primer nivel prestado por los Ingenieros del área.

3.3. Identificar 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	Servidor Web.	Media
10	Base de Datos Oracle	Alta
11	Sistema de Hiperconvergencia	Alta
12	Firewall	Alta
13	Antivirus	Alta
14	Servicio de WIFI	Baja
15	Servicio de Red LAN	Alta

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 My SQL 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 asignada a través del usuario y clave proporcionado para el uso de la VPN y controlado a su vez por el firewall del Instituto.

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

Las 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 requerido en 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 ocasiones 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 Espaciales y 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 de grabación 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 la virtualización.

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.

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

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

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 SSH y 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]

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

9.1.1. FASES DEL PLAN

9.1.1. 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.

9.1.2. 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.

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.

9.1.3. 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.

9.1.4. 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 en restablecerse el servicio.

9.1.5. 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.

9.1.6. 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.

9.1.7. 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.

ANEXO 1. PLAN DE ACCIÓN PARA LOS APLICATIVOS WEB KOHA, OJS, DSPACE, VUFIND, CAJA DE HERRAMIENTAS y HUMANO

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 dato 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. Este sistema esta disponible en un servidor de pruebas.	Ingenieros del área a cargo de la infraestructura	1 hora

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

10. 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.

Para el primer trimestre del año 2019, en la solución de Hiperconvergencia se encuentran incluidos los siguientes servidores virtualizados, que son objeto de este plan de contingencia:

- Servidor Web que incluye los servicios de página WEB institucional y Micrositios.
- Servidor Pensamiento Crítico.
- Servidor Gamificación.
- Servidor KOHA con el servicio de Biblioteca virtual.
- Servidor DSPACE con el repositorio de experiencias docentes - SED.
- Servidor de Dominio Windows Server 2019.
- Servidor NÓMINA HUMANO de contingencia, que incluye la consola de administración del Antivirus.
- Servidor Oracle VM, servidor Linux Oracle que contiene el sistema virtualizado del Orcale para la administración del Motor de Base de Datos Oracle 12C, este último alojado en un servidor físico G7.
- 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 por acceso remoto al VMware Vcenter. 2. Identificar la máquina virtual o máquinas virtuales que presentan falta parcial o total de disponibilidad. 3. Apagar la máquina virtual y restaurar el Snapshot.	Técnico operativo SISTEMAS - IDEP Ingenieros contratistas de sistemas Oficina Asesora de Planeación Ingeniero proveedor de la hiperconvergencia	1 hora, 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.

2. 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://192.168.1.1xx:2xxxx). 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.
- **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.

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 el alcance 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://192.168.1.199:2xxxx). 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 LA CONSOLA DE ADMINISTRACIÓN DEL ANTIVIRUS.

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.** Restaurar o reinstalar la consola de administración del Antivirus Kaspersky.
- **b.** Permitir la administración de los agentes y antivirus instalados del antivirus Kaspersky 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 Kaspersky y presta el servicio de soporte a la misma, o en su defecto con el fabricante de la misma (Kaspersky Lab).

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.

Este servicio de soporte, actualización y verificación de la consola, 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 Técnico Operativo 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 kaspersky 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. 4. En caso de requerirlo, instala la consola nuevamente, y restaura todos los servicios.	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. 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.	Computadores con acceso a la red LAN	1 hora.

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 del 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.	3 minutos.
Esta actividad se debe realizar cada vez que se cambie la configuración del switch o router	Equipo de cómputo.	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.	20 minutos.

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

Objetivo General

Recuperación en la continuidad del servicio Portal Web del IDEP 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, 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.	Equipo de cómputo con navegador.	5 minutos.
Realizar la conexión al servidor 192.168.1.245 mediante un cliente SSH	Equipo de cómputo y 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 192.168.1.250. Iniciar el servicio de red o reiniciar el servidor.	Equipo de cómputo y 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 y 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 y navegador.	3 minutos.
Realizar la conexión al servidor 192.168.1.250 mediante un cliente SSH	Equipo de cómputo y 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 192.168.1.245. Iniciar el servicio de red o reiniciar el servidor.	Equipo de cómputo y 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 sisped.idep.edu.co, transmedia.idep.edu.co para corroborar el funcionamiento de los mismos.	Equipo de cómputo y navegador.	3 minutos.
En caso que se requiera, realizar la sincronización de los servidores, para actualizarlos.	Equipo de cómputo y cliente SSH.	10 minutos.