PLAN DE RECUPERACIÓN DE TECNOLÓGICA – DRT

MINISTERIO DE EDUCACIÓN NACIONAL

UNIÓN TEMPORAL GESTIÓN INTEGRAL MEN

Enero 2022

Tabla de contenido

TABLA DE ILUSTRACIONES

TABLA DE TABLAS

1. Introducción

Contar con un Plan de Recuperación Tecnológico (DRT) reducirá el riesgo de detener operaciones y garantizar la continuidad de la Entidad ante alguna eventualidad que pueda causar daños a la infraestructura y afectar la disponibilidad e integridad de la información.

El presente documento comprende aspectos relevantes que orientan al Ministerio de Educación nacional (MEN) a recuperar los servicios críticos y la tecnología de apoyo que los soportan, frente una interrupción donde la alta disponibilidad implementada sea ineficiente.

Lo anterior con el fin de dar cumplimiento a lo establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) en la Resolución 500 de 2021, "por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital".

2. Glosario

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.[1]

Nivel de Criticidad: Descripción cualitativa usada para enfatizar la importancia de un recurso, proceso o función que debe estar disponible y operativa constantemente o disponible y operativa al menor tiempo posible después de que un incidente, emergencia o desastre ocurra.

Análisis de impacto al negocio (Business Impact Analysis, BIA). Proceso en el que se analiza el impacto de una interrupción conforme avanza el tiempo, en la organización. [Fuente: NTC– ISO 22301]

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

Interrupción (disruption). Incidente, bien sea esperado o no, que causa una alteración negativa y no planeada de la oferta esperada de los productos y servicios de acuerdo con los objetivos de la organización. [Fuente: NTC – ISO 22301]

Objetivo mínimo de continuidad de negocio (MBCO): Mínimo nivel de productos y/o servicios que es aceptable para que la organización alcance sus objetivos de negocio durante una interrupción.

[1] Ministerio de Tecnologías de la Información y las Comunicaciones. (2010). Guía 10 para la preparación de las TIC para la continuidad del negocio https://gobiernodigital.mintic.gov.co/portal/Categor-as/Seguridad-y-Privacidad-de-la-Informacion/150506:Guia-10-Continuidad-de-Negocio

Objetivo de recuperación (RTO). Tiempo Objetivo para Recuperar Sistemas y/o recursos que han sufrido una alteración.

Punto objetivo de recuperación de información (RPO). "Punto en el tiempo en el cual los datos deben ser recuperados después de que una interrupción ocurra." [1]

Máximos tiempos tolerables de interrupción (MTD). Periodo Máximo Tiempo de Inactividad que puede tolerar la Entidad sin entrar en colapso.

WRT (Work Recovery Time). Es el tiempo invertido en buscar datos perdidos y la realización de reparaciones. Se calcula como el tiempo entre la recuperación del sistema y la normalización de los procesos.

Disparador o detonante: Evento que hace que el sistema inicie una respuesta". [1]

3. Objetivos

- Definir las actividades a realizar en las diferentes etapas de recuperación tecnológica como son el antes, el durante y el después de una situación de contingencia y asignar los roles responsables de su ejecución.
- Establecer las actividades a realizar para diferentes escenarios de indisponibilidad, estrategias de recuperación y sus responsables.

4. Alcance

El presente Plan de Recuperación Tecnológica (DRT) aplica únicamente para los servicios críticos e infraestructura clave definidos en el Análisis de Impacto al Negocio (BIA) que soporta la OTSI para los diferentes procesos misionales y de apoyo del Ministerio de Educación Nacional. No contempla estrategias de recuperación de un DRP (Plan de Recuperación de Desastres), es decir para afectación general a las instalaciones de los centros de cómputo ni daños en los dispositivos que no cuentan con redundancia.

5. Contexto

La definición e implementación de un Plan de Recuperación de Tecnología (DRT) del Ministerio de Educación surge de la necesidad de contribuir con la gestión de la continuidad de sus procesos y servicios que se soportan en la Infraestructura tecnológica dando cumplimiento a lo establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) en la Resolución 500 de 2021, "por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital".

Las buenas prácticas profesionales para la gestión de continuidad del negocio del DRI INTERNATIONAL y de la norma técnica colombiana NTC ISO 22301 Sistemas de Gestión de Continuidad de Negocio, recomiendan igualmente documentar planes que puedan ser usados durante un incidente y que permitan a la Entidad seguir funcionando.

Además, el Ministerio de Educación Nacional cuenta con la Política de seguridad de la información en la continuidad de negocio (Ministerio de Educación Nacional de Colombia, 2020) la cual es tenida en cuenta dentro de las actividades de recuperación tecnológica de la OTSI[2]

[2] Ministerio de Educación Nacional. Política de seguridad de la información en la continuidad de negocio. https://sig.mineducacion.gov.co/lib/download.php?nivel1=a054VmZRbHVsejE2bHJsTHlMUUlEY3pIMDhCR0lBTkpFRDE5TmJWSFBaWTM2aTR1TUdKbEZKMEw2MGtxQ2YrbHpIYU9jU09JSjdzekhVZGErTmdNakE9PQ==&nivel2=Kzc2bmVCZWJSUzZGdldZRVhaak1HRklqcHB6dytzbW9udWVYTytlWHdRUnh3ZlJJRGIrZi9NRjl0bDdKc25MMw==

6. Condiciones normales de operación

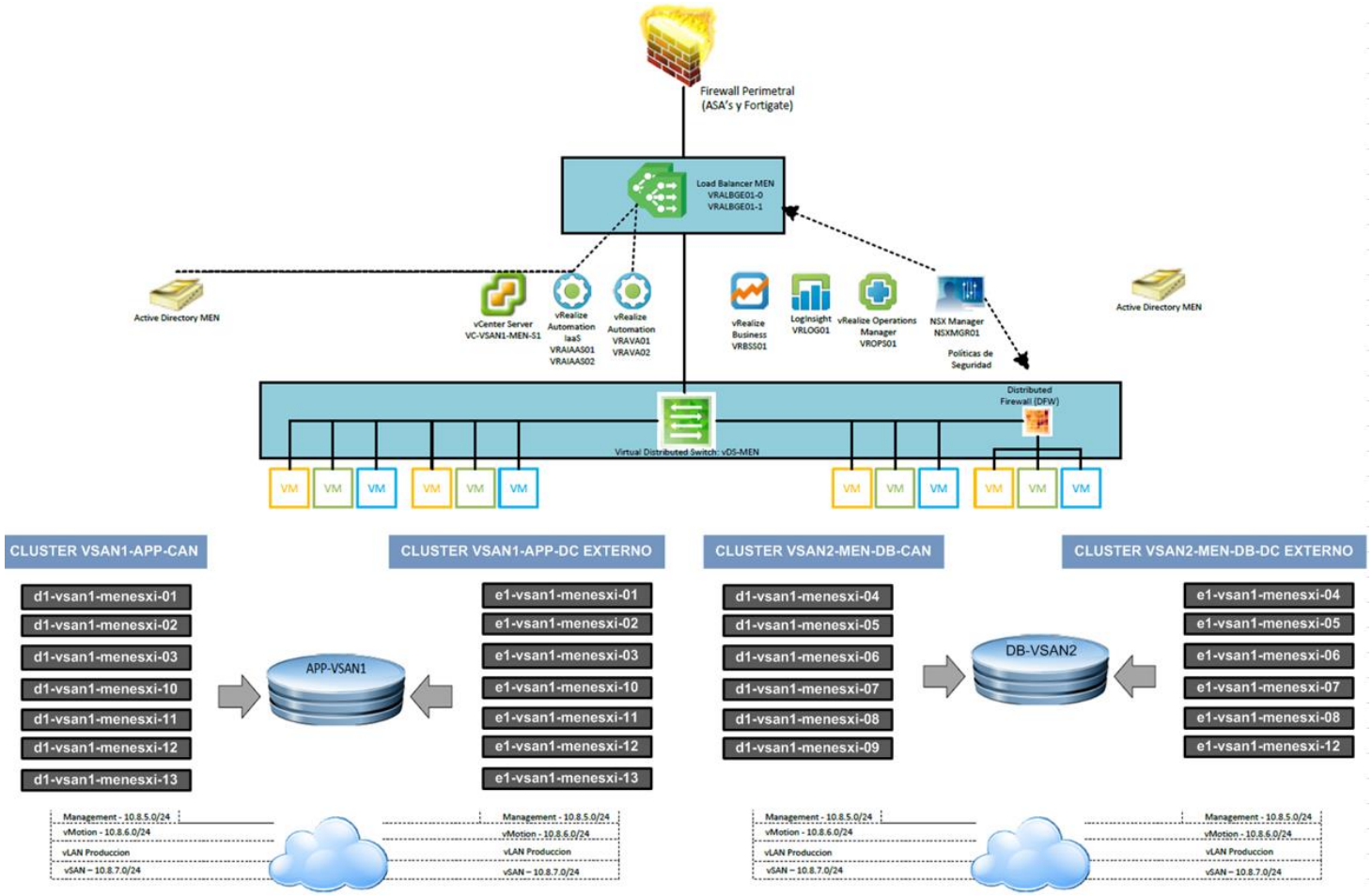
Actualmente la infraestructura de TI del Ministerio de Educación Nacional se encuentra implementada en un centro de datos principal ubicado en las instalaciones del Ministerio, en un centro de datos externo y en un centro adicional dedicado al proyecto E-learning de la Entidad, cada una con una conectividad dedicada monitoreada y controlada por la OTSI.

Dentro de su infraestructura hiperconvergente, la entidad reúne elementos de almacenamiento, recursos, red y gestión de esta en cuatro (4) clústers: dos de ellos destinados a gestionar aplicaciones y dos a gestionar bases de datos.

Con el objetivo de definir los escenarios, estrategias y actividades de recuperación se relacionan algunos diagramas que hacen parte de la infraestructura actual de TI de la entidad.

6.1.1 Diagrama de Arquitectura

Ilustración 1. Diagrama de Arquitectura Ministerio de Educación Nacional



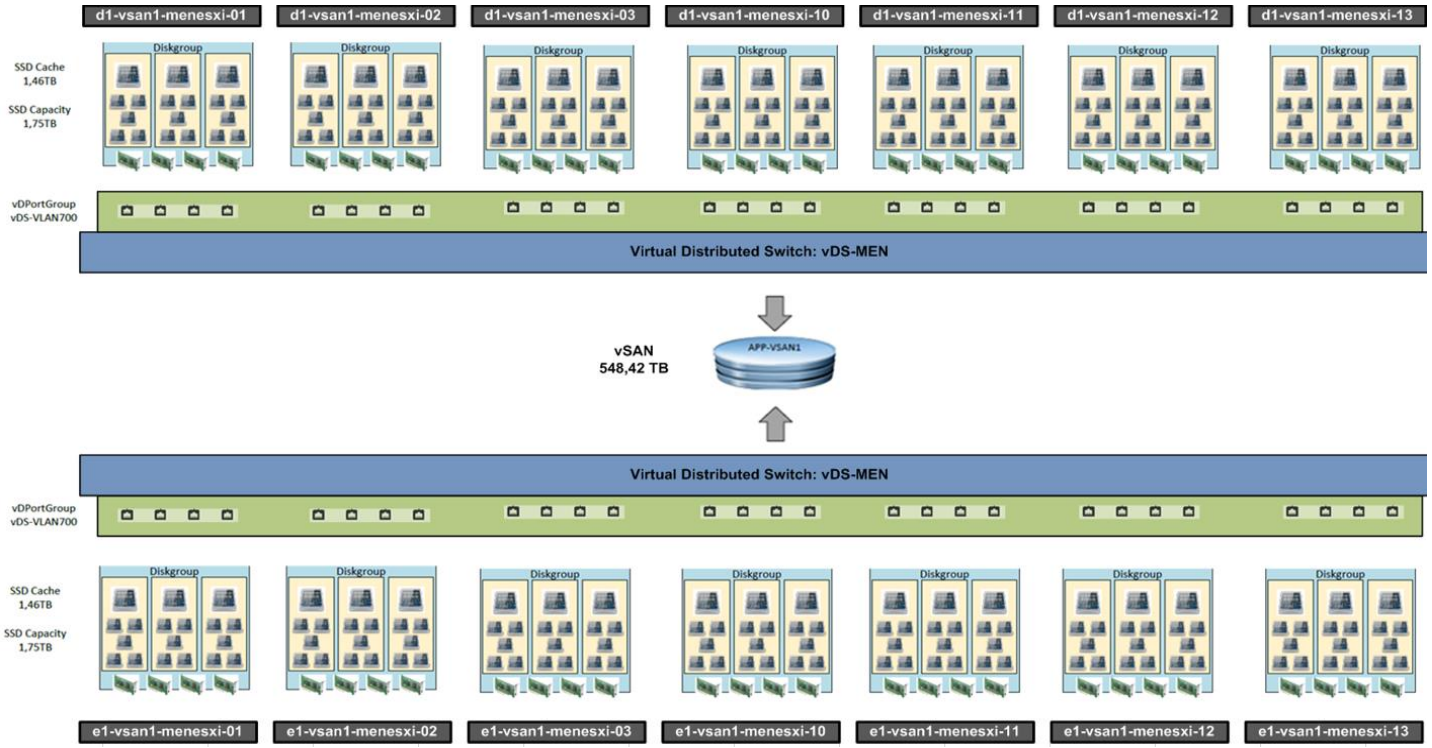
Recomendación: Para obtener mayor detalle de la infraestructura del MEN, se sugiere consultar el documento anexo denominado “Consolidado 3_Estado_Actual_Servicios_TIC 2020.xlsx”, que se encuentra en la siguiente ubicación: **Clic Aquí**

Nota: Para acceder a este documento se debe solicitar el permiso de acceso ya que no es información de carácter público.

6.1.2 Diagramas de Almacenamiento:

Diagrama de Almacenamiento de Aplicaciones: La distribución del manejo del almacenamiento de aplicaciones se realiza a través de 7 VDS (VMWARE, 2021) (VMware vSphere Distributed Switch[3]) en dos nodos:

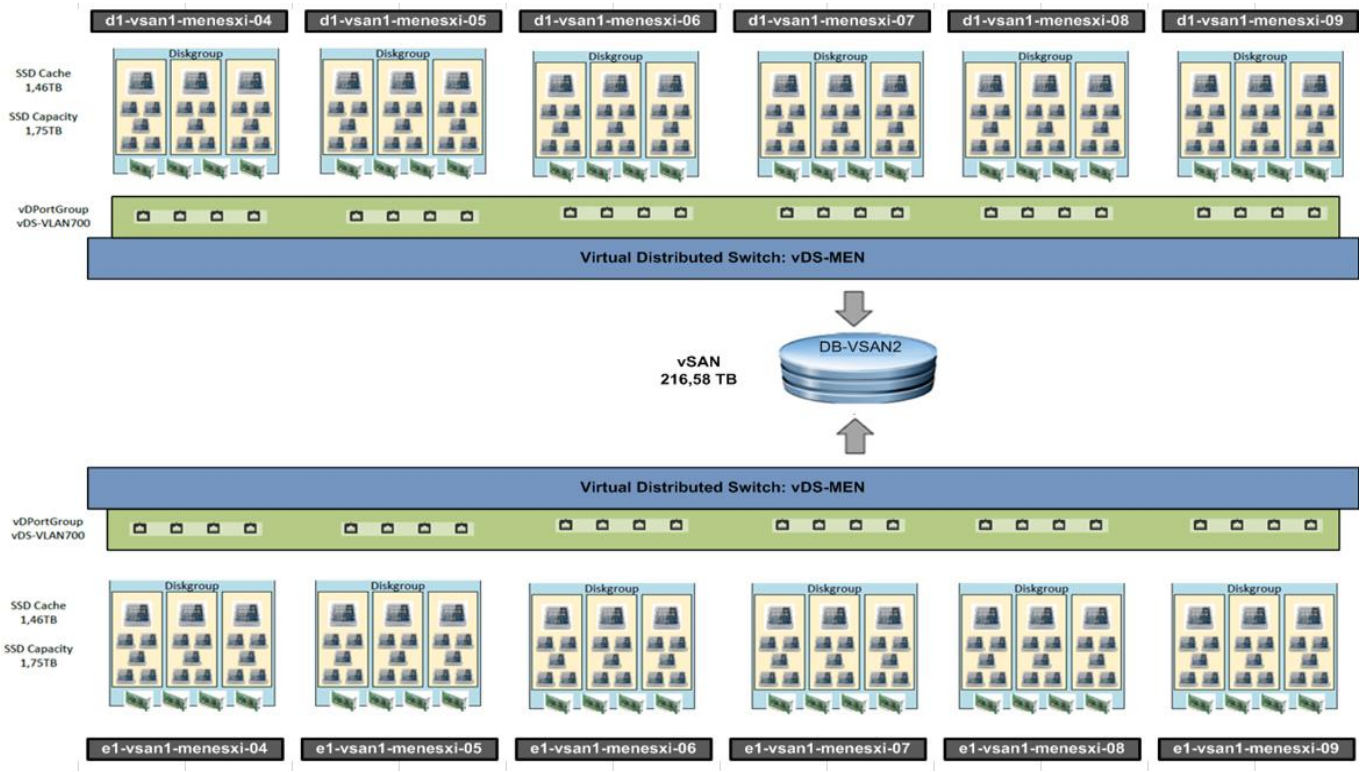
Ilustración 2. Diagrama de Almacenamiento Aplicaciones Ministerio de Educación Nacional



[3] Vmware (2021). vSphere Distributed Switch. https://www.vmware.com/co/products/vsphere/distributed-switch.html

Diagrama de Almacenamiento de Bases de Datos: La distribución del manejo del almacenamiento de aplicaciones de las bases de datos se realiza a través de 6 VDS (VMware vSphere Distributed Switch[4]) en dos nodos, de manera similar al manejo de aplicaciones:

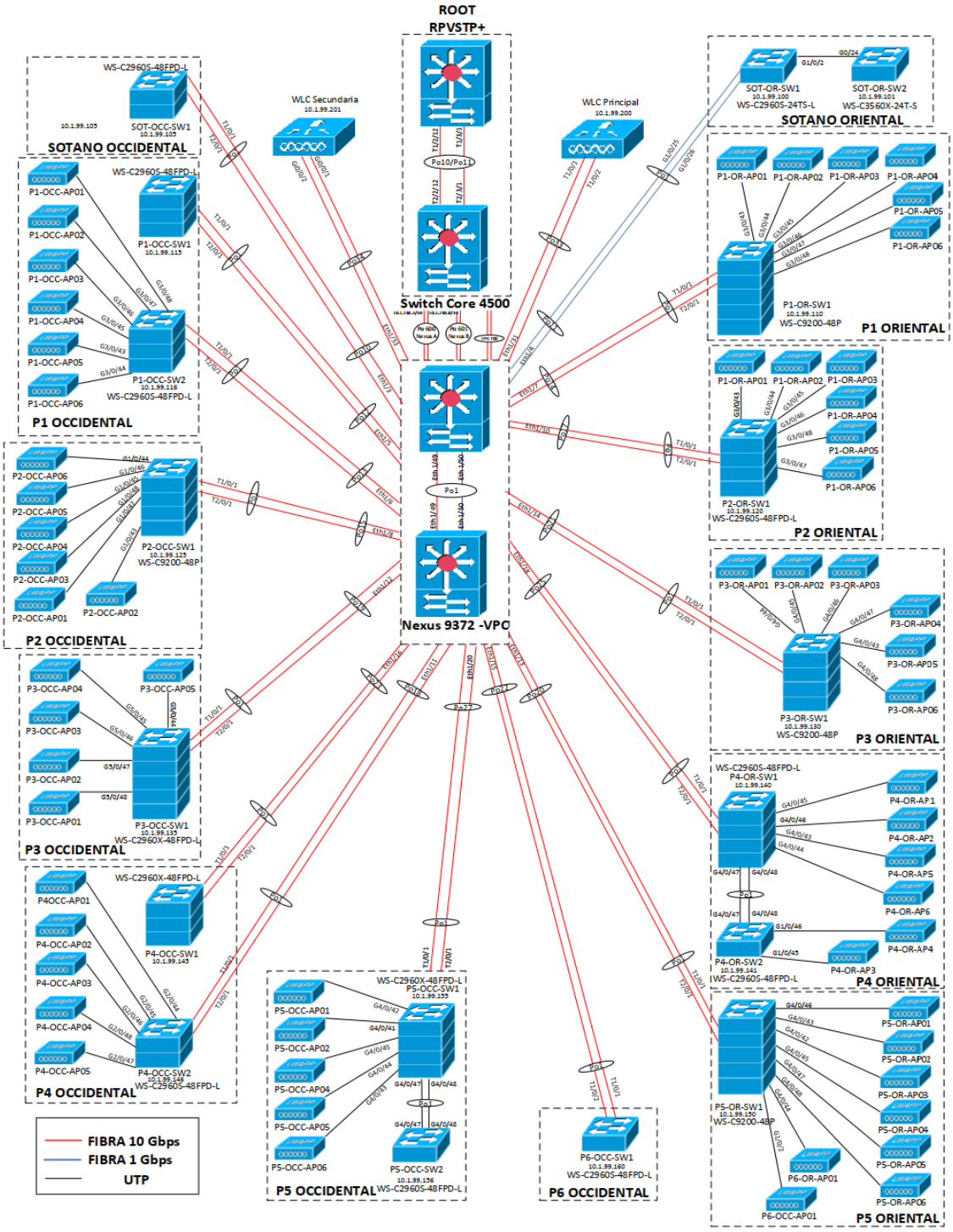
Ilustración 3. Diagrama de Almacenamiento Bases de Datos Ministerio de Educación Nacional



[4] Vmware (2021). vSphere Distributed Switch. https://www.vmware.com/co/products/vsphere/distributed-switch.html

6.1.3 Topología de red

Ilustración 4. Topología LAN Física del Ministerio de Educación Nacional



7. Relación de cumplimiento de la política de seguridad de la información en la continuidad de negocio

De acuerdo con el alcance establecido en la política de seguridad de la Información del Ministerio de Educación, código ST-GU-13, a continuación, se presenta la relación de cumplimiento a la misma a través del presente documento de DRT:

Control	Directrices	Observaciones
La organización deberá establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	Se debe contar con una estructura de gestión adecuada para prepararse, mitigar y responder a un evento perturbador usando personal con la autoridad, experiencia y competencia necesarias en el MEN. Se deben desarrollar y aprobar planes, procedimientos de respuesta y recuperación documentados, en los que se especifique en detalle como el MEN gestionará un evento perturbador y mantendrá su seguridad de la información en un límite predeterminado, con base en los objetivos de continuidad de seguridad de la información.	A través del presente documento de DRT, se proponen escenarios y estrategias de recuperación, así como la relación de las actividades a ejecutar en una situación de contingencia, además, también sirven para que dichos escenarios y estrategias se tomen como base para la realización de pruebas del DRT, las cuales se deben plasmar en el plan de pruebas cuya responsabilidad de asignación de esta gestión recae sobre el Jefe Oficina de Tecnología y Sistemas de Información. También, se establece en este documento los roles y responsabilidades para la gestión de actividades de recuperación.

Tabla 1. Control y directrices que se cumplen con el DRT

8. Relación del DRT con el Mapa de ruta de la arquitectura de seguridad

Dentro de las iniciativas que se contemplan en la Arquitectura de Seguridad (MEN, 2021) y de acuerdo al mapa de ruta establecido, se identifica que en la iniciativa numero 2 (INC02)[5], se describe lo que se debe implementar para cubrir las brechas identificadas entre el estado actual y el estado objetivo de la arquitectura de seguridad y como se puede observar el DRT es uno de los documentos en mención, a continuación, se muestra una tabla con la relación solo de la iniciativa número 2:

ID	BRECHA(S)	DESCRIPCIÓN	TIEMPO
INC02	BRE05 BRE06 BRE07 BRE08	Se debe implementar el DRT y realizar pruebas para verificar que los procedimientos permiten realizar la recuperación de la operación tecnológica, para ello se requiere como mínimo lo siguiente: - Divulgar el BIA. - Documentar, aprobar y divulgar el DRT. - Documentar, aprobar y divulgar una guía de pruebas de recuperación. - Realizar pruebas de continuidad tecnológica.	3 meses

Tabla 2. Iniciativa 2 del Modelo de Arquitectura de seguridad

ID	DESCRIPCIÓN	CAP	
BRE05	No se tiene un DRT aprobado y divulgado en la Entidad	**CSG07**	Continuidad de seguridad de la información
BRE06	No se han realizado pruebas de continuidad tecnológica donde se contemplen los controles de seguridad	**CSG07**	
BRE07	No se cuenta con una guía de ejecución de pruebas que contemple los procedimientos de recuperación	**CSG07**	
BRE08	No se ha divulgado el BIA en la Entidad	**CSG07**	

Tabla 3. Brechas que se cubren con la iniciativa 2 del Modelo de Arquitectura de Seguridad

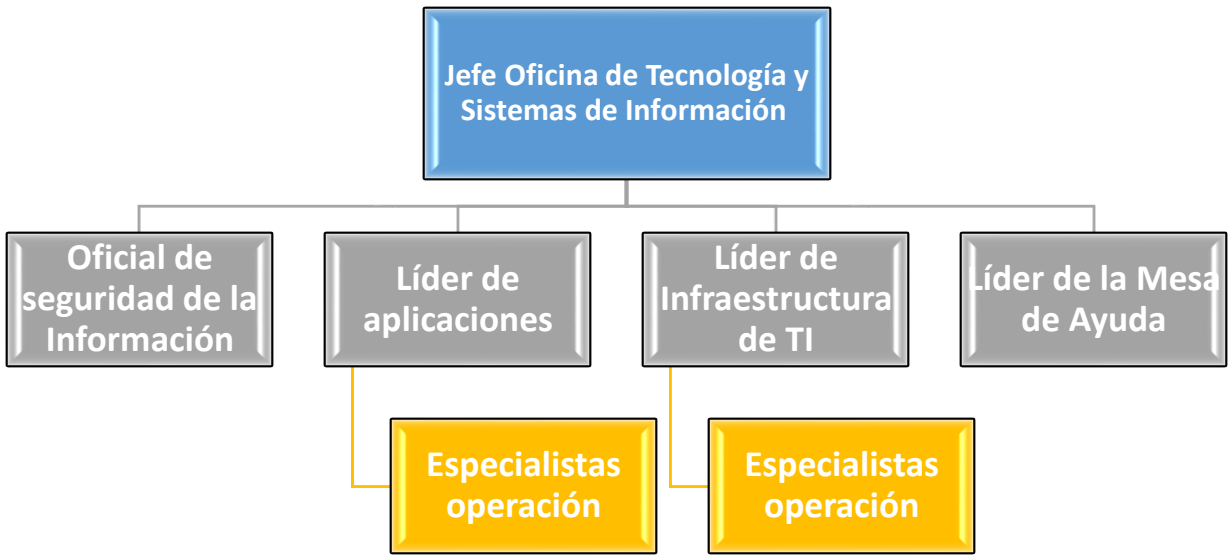
[5]UTGI – MEN (2021) Arquitectura de seguridad. Ministerio de Educación Nacional

9. Roles y Responsabilidades del Plan de Recuperación Tecnológica

Se considera el siguiente equipo mínimo de respuesta; el cual está conformado por personal clave necesario para la activación, recuperación y retorno a la normalidad; a través, de la gestión de diferentes actividades que se deben realizar en caso de una interrupción de la prestación de los Servicios Tecnológicos que soporta la OTSI, a fin de lograr el tiempo mínimo de recuperación (RTO) y la disponibilidad de los servicios, de acuerdo con los términos aprobados en el BIA:

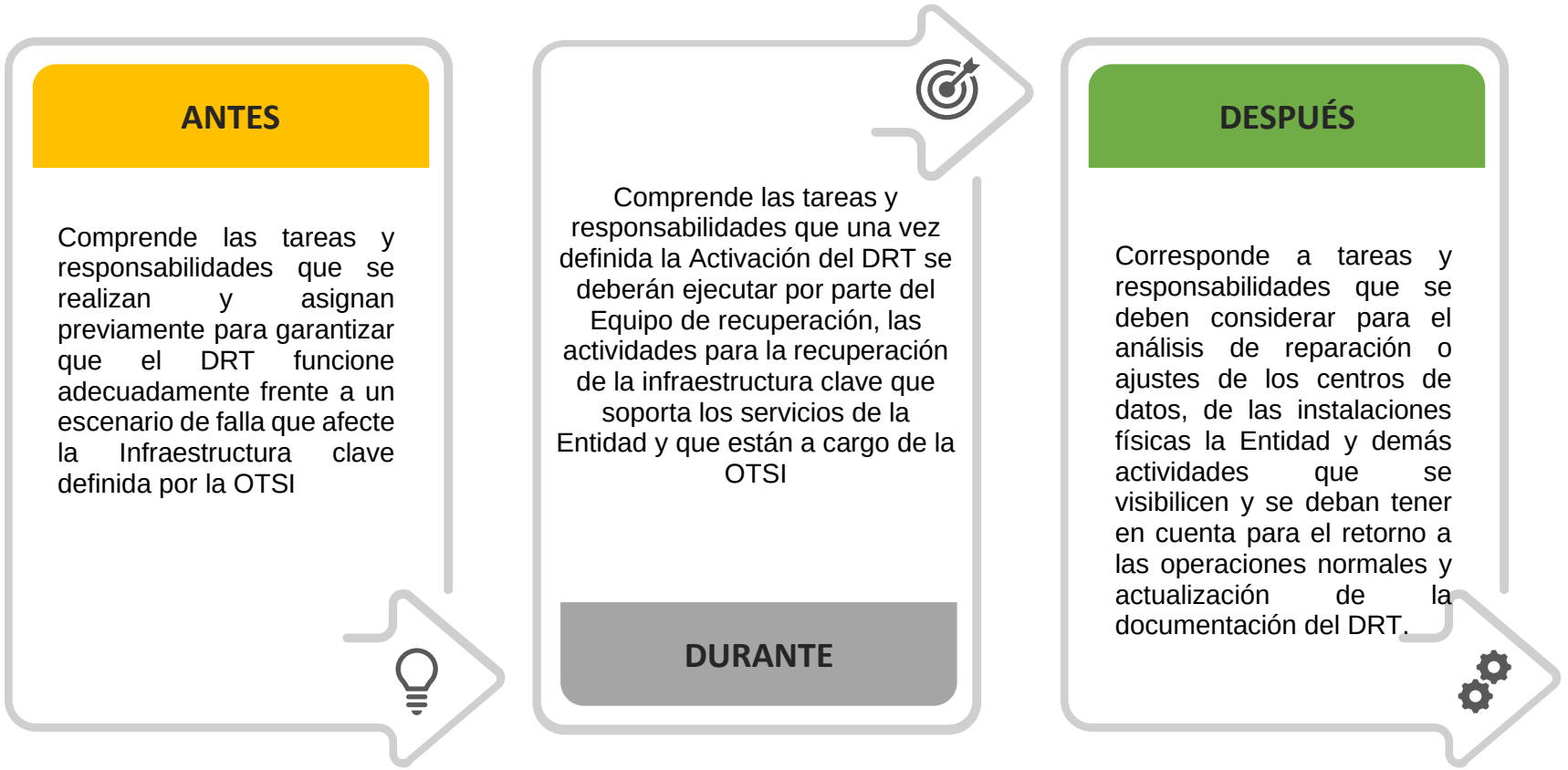
- Jefe Oficina de Tecnología y Sistemas de Información.
- Oficial de Seguridad de la información.
- Líder de infraestructura de TI.
- Líder de aplicaciones.
- Líder de la mesa de ayuda.
- Especialistas de Operación.

Ilustración 5. Roles DRT



9.1 Etapas del Plan de Recuperación Tecnológica

Ilustración 6. Etapas del DRT



Se establecen los siguientes roles y responsabilidades principales con las actividades mínimas a desarrollar en las 3 etapas del plan DRT:

Rol	Antes	Durante	Después
Jefe Oficina de Tecnología y Sistemas de Información	• Mantener actualizado el DRT. • Asignar la responsabilidad de actualización y documentación del DRT (información de contactos, inventario de activos, documentación en general) • Asignar la responsabilidad de coordinar las actividades de diseño e informe de pruebas del DRT. • Asignar la responsabilidad de Identificación de riesgos asociados al DRT. • Asignar la responsabilidad de revisión y análisis de informes de monitoreo a la infraestructura clave para la prestación de los servicios de la OTSI. • Coordinar con la oficina de control interno la realización de auditorías periódicas al DRT.	• Activar y desactivar el DRT y las estrategias de recuperación y contingencia. • Notificar a los proveedores clave la decisión de activar el DRT • Coordinar y trasladar personal al Centro de datos externo en caso de ser necesario. • Coordinar la comunicación para transmitir la situación de contingencia con la alta gerencia. • Establecer y determinar el impacto que se presenta en la operación y su afectación en la prestación del servicio. • Mantener comunicación constante con el equipo de recuperación. • Asignar la responsabilidad de realizar las acciones pertinentes para la redacción, producción y difusión de la información relacionada con las actividades del DRT.	• Analizar la información correspondiente a la activación, puesta en marcha y resultados del DRT. • Actualizar el DRT, de acuerdo con los inconvenientes y oportunidades de mejora encontrados. • Comunicar la actualización del DRT al equipo de respuesta y al personal del MEN que corresponda. • Asignar la responsabilidad de documentar y socializar las lecciones aprendidas del antes, durante y después de las actividades de recuperación. • Aginar la responsabilidad de gestionar el reporte de inconvenientes y oportunidades de mejora DRT. • Asignar la responsabilidad de documentar y socializar

Rol	Antes	Durante	Después
			las lecciones aprendidas durante la recuperación.
Líder de Infraestructura de TI y Líder de aplicaciones	• Participar en el análisis, desarrollo, implementación, pruebas y ejecución del DRT. • Mantener información actualizada sobre contratos de mantenimiento y garantías de proveedores y fabricantes. • Identificar los recursos requeridos para la operación del DRT	• Evaluar la interrupción o evento. • Coordinar el personal de soporte, especialistas y/o proveedores. • Iniciar la activación del DRT para la recuperación de los servicios teniendo en cuenta la prioridad definida en el Análisis de Impacto al Negocio. • Hacer seguimiento a las actividades de recuperación y Mantener informado Jefe Oficina de Tecnología y Sistemas de Información y a quien este designe sobre el avance de las mismas. • Gestionar la realización de pruebas básicas de los servicios de TI • Notificar sobre de recuperación de servicios de TI al grupo de recuperación de DRT	• Estimar fecha y hora para operar nuevamente en la Infraestructura principal. • Generar backups requeridos. • Notificar al equipo de DRT el fin de la contingencia. • Reportar los inconvenientes y oportunidades de mejora del DRT. • Documentar y socializar las lecciones aprendidas durante la recuperación.

Rol	Antes	Durante	Después
Oficial de Seguridad de la Información	• Apoyar las actividades de recuperación que se requieran. • Apoyar en la identificación de riesgos asociados a las estrategias del DRT. • Incluir actividades de entrenamiento, del DRT en los planes de concientización.	• Proveer información y soporte relacionado con la arquitectura de seguridad implementada en la entidad. • Hacer seguimiento a las actividades de recuperación y Mantener informado Jefe Oficina de Tecnología y Sistemas de Información o a quien este designe las responsabilidades del DRT sobre los riesgos de continuidad asociados a la disponibilidad e integridad de información.	• Reportar los inconvenientes y oportunidades de mejora del DRT relacionados con seguridad de la información.
Líder de la mesa de Servicio	• Comunicar necesidades de ajuste al DRT. • Participar en la ejecución de las pruebas del DRT.	• Evaluar el desastre, interrupción o incidente. • Monitorear y alertar el o los eventos que reportan las diferentes herramientas tecnológicas relacionados con el rendimiento de los servicios. • Verificar disponibilidad de los servicios con una frecuencia acordada con todo el equipo del DRT. • Comunicar al Líder de operación de la UT, al líder de Aplicaciones, al líder de infraestructura y al oficial de Seguridad de la	• Reportar los inconvenientes y oportunidades de mejora del DRT • Documentar y socializar las lecciones aprendidas durante la recuperación.

Rol	Antes	Durante	Después
		Información, la activación del DRT. • Solicitar la corrección del componente afectado y realizar seguimiento de la solución. • Estar atentos para dar una correcta información a las personas que lo requieran. • Mantener informado al equipo del DRT sobre el estado de los servicios afectados.	
Especialistas de operación	• Monitorear el comportamiento de la tecnología que soporta los sistemas de TI y realizar los reportes que correspondan. • Reportar situaciones fuera de lo común que ameriten toma de decisiones de alto nivel.	• Ejecutar los procedimientos o actividades de recuperación de los servicios de la OTSI.	• Documentar el o los incidentes (la causa raíz, las acciones ejecutadas y la solución) • Participar en la actualización del procedimiento para recuperar los servicios. • Recomendar y ejecutar acciones de mejora para evitar reincidencias del incidente. • Documentar y socializar las lecciones aprendidas durante la recuperación.

Tabla 4. Roles y responsabilidades del equipo mínimo de respuesta

10. Criterios de activación del DRT

La Mesa de Servicio debe atender los incidentes relacionados con la interrupción o indisponibilidad de los servicios de TI, así mismo debe gestionar el o los incidentes y determinar si se solicita al **Jefe Oficina de Tecnología y Sistemas de Información** activar el Plan de recuperación tecnológica, considerando los siguientes aspectos:

- El incidente tiene potencial de superar el RTO establecido.
- El incidente afecta un servicio crítico de manera considerable.
- Analizar si han sucedido eventos disruptivos en entidades similares al Ministerio de Educación Nacional que ameriten activar el DRT.
- Existencia situaciones adversas visiblemente identificadas que no permitan la operación normal.

11. Plan de Comunicación

11.1 Notificación del Evento

El líder de la mesa de servicio deberá:

- Comunicar la situación que se presente al **Jefe Oficina de Tecnología y Sistemas de Información**, al líder de Aplicaciones, al líder de infraestructura y al oficial de Seguridad de la Información y solicitar la autorización de activación del DRT.
- Estar atento para dar una correcta información a las personas que lo requieran, en los intervalos de reporte que se definan.
- Mantener informado al equipo mínimo de respuesta del estado del servicio afectado.

11.2 Notificaciones externas

- El **Jefe Oficina de Tecnología y Sistemas de Información** deberá coordinar toda comunicación que se realice con los medios externos de prensa, clientes, proveedores y otras entidades, generando comunicados, notas de prensa y/o entrevistas con redacción correcta e información oportuna, produciendo y difundiendo los mismos.

11.3 Notificaciones de Emergencia a Usuario Final

- El líder de la mesa de servicio deberá gestionar que se contacten con los usuarios finales que han sido o serán afectados; a través de los canales de comunicación internos del Ministerio de Educación Nacional. La comunicación será de manera clara y precisa de los hechos ocurridos, sus consecuencias y la fecha y hora estimada para que el servicio sea restablecido.

11.4 Manejo de Crisis

- El líder de la mesa de servicio deberá gestionar la crisis mediante los diferentes recursos disponibles en el momento de la situación, en busca de minimizar el impacto que esto pueda ocasionar al MEN y para ello debe considerar analizar los siguientes aspectos:
    - Servicios afectados.
    - Tiempo estimado para normalización de la prestación del servicio.
    - Riesgos a los que estaría expuesto el MEN por la Activación del Plan.

12. Análisis de Estrategias de continuidad y planteamiento de escenarios de indisponibilidad

En el siguiente vinculo “Análisis de estrategias de continuidad.xls” se encuentra el documento con el mismo nombre, donde se ha relacionado las infraestructuras, tecnologías y proveedores Claves identificados en el análisis de impacto de negocios – BIA realizado sobre los servicios que presta la OTSI, además se plantean posibles escenarios de indisponibilidad o falla, posibles estrategias de recuperación, analizando si se encuentra implementada o no la estrategia para el escenario relacionado y además, se documenta un análisis de conveniencia; este análisis se realizó teniendo en cuenta los RTO establecidos en el ejercicio BIA para cada uno de los servicios tecnológicos.

Para un mejor entendimiento de la información mencionada anteriormente del Análisis de estrategias de continuidad, se debe tener en cuenta la siguiente relación:

Ilustración 7. Relación uno o varios activos a uno o varios escenarios

En la anterior imagen, se observa que la relación puede ser uno a muchos o muchos a muchos, sin embargo, en el planteamiento que se propone en este documento de DRT entre escenario y estrategia es una relación de uno a uno, es decir que para un escenario debe existir una estrategia de recuperación:

Ilustración 8. Relación uno a uno entre Escenario y Estrategia

Escala de evaluación de la estrategia

Basados en la siguiente escala se realiza la evaluación de implementación de la estrategia:

Valores	Datos	Descripción
-	No implementada	Estrategia que no ha sido implementada
50	Definida no implementada	Estrategia que se ha definido debe implementarse
75	Implementada parcialmente	Estrategia implementada parcialmente
100	Implementada completamente	Estrategia implementada totalmente y con documentación establecida

Tabla 5. Escala de evaluación de implementación de estrategia

Las estrategias implementadas o implementadas parcialmente son las que cuentan con actividades de recuperación, en este mismo vinculo "Análisis de estrategias de continuidad.xls" se puede visualizar un nivel más detallado de los resultados que se presentan a continuación:

12.1 Planteamiento de escenarios y estrategias para Instalación/Equipos Clave

Activos	Escenarios	Estrategia	Implementada	Valor cualitativo de la implementación de la estrategia	Servicio	Priorización de recuperación	RTO
Instalación/Equipos Clave	1. No disponibilidad de sistema de respaldo en equipos de comunicaciones	1. Activar el servicio de red en el centro de datos alterno	SI	Implementada completamente	Red	1	2 horas
	2. No disponibilidad total o parcial de los Servicios Tecnológicos de Infraestructura	2. Activar los procesos o procedimientos Alternos (Seguridad)	SI	Implementada completamente	Catálogo de Servicio	3	4 horas
	3. Indisponibilidad de la información	3. Restablecer un Backup de la última configuración buena conocida	SI	Implementada completamente	backup	3	4 horas
	4. No disponibilidad del servicio de conectividad a internet	4. Activar el router de contingencia	SI	Implementada completamente	Red	1	2 horas
	5. No disponibilidad de mecanismos de monitoreo	5. Activar sistema de monitoreo de respaldo	NO	No implementada	Monitoreo	2	12 horas
	6. Falta de disponibilidad en la redundancia de las aplicaciones	6. Activar los servicios de aplicaciones en el sitio alterno	NO	No implementada	Sistemas de Información	1	2 horas
	7. Falta de Disponibilidad en la redundancia de los servidores	7. Reemplazar Equipos Servidores (host de virtualización)	SI	Implementada parcialmente	Virtualización	1	>2 horas

Activos	Escenarios	Estrategia	Implementada	Valor cualitativo de la implementación de la estrategia	Servicio	Priorización de recuperación	RTO
	8. Ausencia de comunicación con el sitio alterno	8. Contar con proveedores de servicios alternos	NO	No implementada	Red	1	2 horas

Tabla 6. Escenarios, Estrategias vs Priorización para Instalación/Equipos Clave

12.2 Planteamiento de escenarios y estrategias para Tecnología Clave

Activos	Escenarios	Estrategia	Implementada	Valor cualitativo de la implementación de la estrategia	SERVICIO	Priorización de recuperación	RTO
Tecnología clave	1. Indisponibilidad de la información	1. Restablecer un Backup de la última configuración buena conocida	SI	Implementada completamente	Backup	3	4 horas
	2. No Acceso al Servicio de Correo Electrónico	2.1 Activar el servicio de correo en el sitio alterno	NO	No implementada	Correo Electrónico	1	> 2 horas
		2.2 Establecer un SLA con Microsoft	SI	Implementada completamente	Correo Electrónico	1	> 2 horas
	3. No acceso a la Información de OneDrive	3. Restablecer un backup de la información de los usuarios	SI	Implementada completamente	One Drive	3	2 horas
	4. No Disponibilidad	4. Activar el sistema de	SI	Implementada completamente	Virtualización	1	> 2 horas

Activos	Escenarios	Estrategia	Implementada	Valor cualitativo de la implementación de la estrategia	SERVICIO	Priorización de recuperación	RTO
	total o parcial de las máquinas virtuales	virtualización en el centro de datos alterno					
	5. Indisponibilidad del sistema de control de acceso a redes	5. Activar el servicio de control acceso a redes en el centro de datos alterno	SI	Implementada completamente	Seguridad	1	2 horas
	6. No disponibilidad de mecanismos de obtención de direccionamiento IP	6. Activar el servicio de DHCP en el centro de datos alterno	NO	No implementada	Sistemas Operativos	1	12 horas

Tabla 7. Escenarios, Estrategias vs Priorización para tecnología clave

12.3 Planteamiento de escenarios y estrategias para Proveedores / Suministro o Servicio Claves

Activos	Escenarios	Estrategia	Implementada	Valor cualitativo de la implementación de la estrategia	SERVICIO	Priorización de recuperación	RTO
Proveedores/ Suministro o Servicio Claves	**1.** Ausencia del Personal de Operación de infraestructura tecnológica	1.1 Documentar procesos y procedimientos de operación	SI	Implementada parcialmente	Catálogo de Servicio	3	4 horas
		1.2 Capacitar personal de backup	SI	Implementada completamente	Catálogo de Servicio	3	4 horas
	2. Indisponibilidad de información	2. 1 Realizar backup de la Información	SI	Implementada completamente	Backup	3	4 horas
		2.2 Recuperación de la base de datos a partir del último backup consistente	SI	Implementada completamente	Backup	3	4 horas

Activos	Escenarios	Estrategia	Implementada	Valor cualitativo de la implementación de la estrategia	SERVICIO	Priorización de recuperación	RTO
		2.3 Recuperación de información con equipo experto	SI	Implementada completamente	Backup	3	4 horas
	3. No disponibilidad de repuestos o partes de equipos de comunicaciones e infraestructura	3. Reemplazo de partes de servidores físicos	SI	Implementada completamente	Préstamos	5	2 horas
	4. No disponibilidad del Servicio de Mesa de Ayuda	4. Activar el servicio de mesa de servicio, en el centro de datos alterno	SI	Implementada parcialmente	Sistemas Operativos	1	12 horas
	5. Indisponibilidad total o parcial de servicios tecnológicos por fallas en los servidores	5. Activar servicios tecnológicos en el centro de datos alterno	SI	Implementada parcialmente	Catálogo de Servicio	3	4 horas
	6. Indisponibilidad total o parcial de los sistemas de Información	6. Activar los sistemas de información	SI	Implementada parcialmente	Sistemas de Información	1	>12 Horas
	7. No disponibilidad del Servicio de Internet	7. Activar el canal de internet de contingencia	NO	No implementada	Red	1	2 horas

Tabla 8. Escenarios, Estrategias vs Priorización para proveedores/suministros o servicios clave

13. Actividades de Recuperación ante una disrupción para los servicios identificados como críticos en el BIA

De acuerdo con las tablas: Tabla 6. Escenarios, Estrategias vs Priorización para Instalación/Equipos Clave, Tabla 7. Escenarios, Estrategias vs Priorización para tecnología clave y Tabla 8. Escenarios, Estrategias vs Priorización para proveedores/suministros o servicios clave se plantean actividades de recuperación para las estrategias que han sido implementadas completa o parcialmente, para que orienten a los responsables con el que hacer a fin de recuperar y garantizar la prestación de los servicios tecnológicos, sobre 4 escenarios y se documentaron 4 estrategias con alto nivel de detalle y para los demás se documenta una propuesta inicial de las estrategias que se debe continuar detallando como parte del fortalecimiento del DRT, a continuación se presentan los 4 escenarios:

1. No disponibilidad de sistema de respaldo en equipos de comunicaciones
2. No disponibilidad total o parcial de los Servicios Tecnológicos de Infraestructura
3. Indisponibilidad de la información
4. Indisponibilidad total o parcial de los sistemas de Información críticos

13.1 No disponibilidad de sistema de respaldo en equipos de comunicaciones

13.1.1 Activar el servicio de red en el centro de datos alterno

Descripción general de los procedimientos aplicados en cada ambiente/equipo, este se encuentra incluido en cada uno de los cuadros relacionados de cada equipo o sistema.

Actividad	Responsable	Documentación de Soporte
1. Realizar pruebas de comunicación. 2. Revisión de configuración de puertos. 3. Reestablecer configuración de acuerdo con el último	Especialista de Networking	En el siguiente vínculo se encuentra el documento: PROCEDIMIENTO PARA RECUPERAR SERVICIOS_ GT&SEG

Actividad	Responsable	Documentación de Soporte
Backups en caso de requerirse. (Opcional). 4. Realizar pruebas de comunicación y pruebas de integridad de servicio. 5- Pruebas de HA (Alta disponibilidad).		

13.2 No disponibilidad total o parcial de los Servicios Tecnológicos de Infraestructura

13.2.1 Activar los procesos o procedimientos Alternos (NetWorking)

Actividad	Responsable	Documentación de Soporte
Alta Disponibilidad de Switchs Nexus de Datacenter Cuando ocurre apagado de los switch Nexus 9372 se realizan los siguientes pasos para recuperar el servicio de conectividad: 1. Se verifica conectividad a nivel de ping y acceso a los switchs. 2. Se verifica que los equipos enciendan adecuadamente y reconozcan todos los puertos e interfaces asociadas. 3. Se realiza una verificación a nivel de logs y alarmas. 4. Se verifica que todos los puertos conectados estén es estado Up. 5. Se verifica el estado de todas las VLANs. 6. Verificación de la alta disponibilidad de los switch Nexus. 7. Se verifica que la fibra oscura conectada que interconecta los Data Center tenga operatividad.	Especialista de Networking	En el siguiente vínculo se encuentra el documento: Documento Maqueta Actividades de recuperación de infraestructura y comunicaciones.docx

8. En caso de daño del algún switch se procede a crear el caso con el fabricante Cisco para solicitar el respectivo RMA. 9. Cuando llegue el equipo a las instalaciones del MEN se procederá con las respectivas configuraciones y programación del respectivo cambio.		
Alta Disponibilidad de Switchs Core 4500 Cuando ocurre apagado de los switch Core se realizan los siguientes pasos para recuperar el servicio de conectividad. 1. Se verifica conectividad a nivel de ping y acceso a los switchs. 2. Se verifica que los equipos enciendan adecuadamente y reconozcan todos las tarjetas, componentes e interfaces asociadas. 3. Se realiza una verificación a nivel de logs y alarmas. 4. Se verifica que todos los puertos conectados estén en estado Up. 5. Se verifica el estado de todas las VLANs. 6. Verificación de la alta disponibilidad de los switchs 4500 conectados por medio de VSS. 7. Se verifica que la conectividad a los diferentes componentes de red de respuesta. 8. En caso de daño del algún componente de los switchs se procede a crear el caso con el fabricante Cisco para solicitar el respectivo RMA.	Especialista de Networking	En el siguiente vínculo se encuentra el documento: Documento Maqueta Actividades de recuperación de infraestructura y comunicaciones.docx

9. Cuando lleguen los componentes a las instalaciones del MEN se procederá con las respectivas configuraciones y programación del respectivo cambio.		
- **Equipo de Networking Balanceador** Cuando ocurre apagado de los balanceadores, se realizan los siguientes pasos para recuperar el servicio de conectividad. 1. Se verifica conectividad a nivel de ping y acceso a los equipos. 2. Se verifica que los equipos enciendan adecuadamente y reconozcan todos los puertos e interfaces asociadas. 3. Se realiza una verificación a nivel de logs y alarmas. 4. Verificación de funcionamiento de la alta disponibilidad en los balanceadores Fortinet 2000F en cada Data Center. 5. Se verifica que la conectividad a los diferentes componentes de red. 6. Se verifica que el estado de las diferentes políticas de balanceo. 7. Se realiza verificación de que las diferentes aplicaciones se encuentren operativas. 8. En caso de daño del algún equipo se procede a crear el caso con el fabricante	Especialista de Networking	En el siguiente vínculo se encuentra el documento: Documento Maqueta Actividades de recuperación de infraestructura y comunicaciones.docx

Fortinet para solicitar el respectivo RMA.		
- **Equipos de Networking Acceso** Cuando ocurre apagado de los switchs de acceso, se realizan los siguientes pasos para recuperar el servicio de conectividad. 1. Se verifica conectividad a nivel de ping y acceso a los switchs. 2. Se verifica que los equipos enciendan adecuadamente y reconozcan todos los puertos e interfaces asociadas. 3. Se realiza una verificación a nivel de logs y alarmas. 4. Verificación de la alta Disponibilidad de los diferentes Stack de switch de los diferentes pisos del MEN. 5. Se verifica la conectividad hacia los switchs de distribución Nexus. 6. Se verifica que el estado de todos los puertos conectados, estén es un estado normal Up/down. 7. Se verifica la conexión de los diferentes computadores de los usuarios a las respectivas VLAN. 8. En caso de daño del algún switch se procede a crear el caso con el fabricante Cisco para solicitar el respectivo RMA. 9. Cuando llegue el equipo a las instalaciones del MEN se procederá con las respectivas configuraciones y	Especialista de Networking	En el siguiente vínculo se encuentra el documento: Documento Maqueta Actividades de recuperación de infraestructura y comunicaciones.docx

programación del respectivo cambio.		

13.2.2 Activar los procesos o procedimientos Alternos (Seguridad)

Actividad	Responsable	Documentación de Soporte
1. Verificación de acceso a través de vpn en DC. 2. Validación y pruebas de conectividad hacia equipo de seguridad. 3. Verificación de estado de dispositivos de seguridad afectados. 4. Verificación y listado de servicios afectados según DC afectado. 5. En caso de falla parcial de uno de los equipos firewall del DC se procede a abrir caso con el fabricante y validar el reemplazo del equipo de ser necesario. 6. En caso de falla total los equipos del firewall datacenter, habría indisponibilidad hacia/desde Internet del datacenter. se procede a crear el caso con el fabricante y validar el reemplazo del equipo de ser necesario. 7. En caso de falla parcial de los dispositivos WAF, se procede a abrir caso con el fabricante y validar el reemplazo del equipo de ser necesario. 8. En caso de falla total de los dispositivos WAF, habría indisponibilidad de las publicaciones que soporte el clúster en el datacenter correspondiente. Se procede a crear el caso con el fabricante para solicitar el respectivo diagnóstico	Especialista Seguridad informática	En el siguiente vínculo se encuentra el documento: PROCEDIMIENTO PARA RECUPERAR SERVICIOS_ GT&SEG

y/o reemplazo de los equipos. 9. En caso de falla parcial de uno de los equipos DDoS, se procede a abrir caso con el fabricante y validar el reemplazo del equipo de ser necesario. 10. En caso de falla total del clúster de equipos DDoS, habría indisponibilidad hacia/desde Internet, se procede a crear el caso con el fabricante para solicitar el respectivo diagnóstico y/o reemplazo de los equipos. 11. En caso de falla parcial de uno de los equipos ESA, se procede a abrir caso con el fabricante y validar el reemplazo del equipo de ser necesario. 12. En caso de falla total de los equipos ESA, se debe ajustar el registro MX hacía Office365 para que los correos lleguen directamente a la nube mientras se restablece la operación de los ESA. 13. En caso de falla parcial de uno de los dispositivos ISE, Confirmación de apuntamiento a servidor radius desde los dispositivos de red LAN/WLAN al equipo que se encuentra activo. Posteriormente se debe reaprovisionar la máquina virtual a la versión de la máquina que presentó el fallo. 14. En caso de falla total de los dispositivos ISE, sería necesario eliminar la autenticación a nivel de red LAN/WLAN contra los dispositivos ISE mientras se realiza el reaprovisionamiento de las máquinas y su		

restablecimiento de configuración a partir de los backups de la solución.		

13.3 Indisponibilidad de la información

13.3.1 Restablecer un Backup de la última configuración buena conocida

Actividad	Responsable	Documentación de Soporte
1. Recepción de Solicitud de Información para restauración 2. Validación de la información solicitada para restaurar. 3. Ubicación en la base de datos de la herramienta día y cinta de la última información. 4. Solicitud de la cinta a custodia si no se encuentra en la librería. 5. Colocar la cinta para recuperación. 6. Solicitud de ubicación para restauración. 7. Programación de la restauración. 8. Seguimiento de la restauración.	Administrador de Backup	Instructivo del fabricante: https://www.veritas.com/content/support/en_US/doc/130076143-140940382-0/v53900350-140940382

13.4 Indisponibilidad total o parcial de los sistemas de Información críticos

13.4.1 Activar los sistemas de información

Actividad	Responsable	Documentación de Soporte
Consideración especial para Bases de Datos en caso perdida de comunicación: • Disponibilidad de los servidores • Validar acceso a los servidores • Subir servicios de BD	Gestor de aplicaciones	En los siguientes vínculos se encuentran los documentos: Documento Maqueta Actividades de Recuperación CEBYM-CONVALIDA-NEC-DOCENTE-SGDEA-RRHH

• Verificar los listener de las BD afectadas • Verificación del alert log de la BD • Realizar test de conexiones por medio del developer Consideración especial para Bases de Datos en caso perdida de data: • Infraestructura debe garantizar la disponibilidad del servidor • Realizar restore de la BD con el ultimo backup tomado • Subir servicios de BD • Verificar los listener de las BD afectadas • Verificación del alert log de la BD • Realizar test de conexiones por medio del developer Consideración especial para Aplicaciones en caso de pérdida de comunicación: • Infraestructura debe asegurar que los servidores se encuentren disponibles • Las bases de datos deben estar disponibles • Validar acceso a los servidores • Validar los clústeres asociados a cada servidor • Subir servicios de capa media • Validar conexión hacia la BD		Documento Maqueta Actividades de Recuperación CNE-SUPERATE-LEGALIZACIONES Documento Maqueta Actividades de Recuperación SINEB-SISMA-SSDIPI4 Documento Maqueta Actividades de Recuperación SIMAT-SIPI-SIMPADE-SIUCE-SIA3-SIGAA-SIFSE NVO-SINEB PLANTAS-SIPTA2-NUEVO SIGCE ACTIVIDADES PARA RECUPERAR SERVICIOS DE APLICACIONES – WEBLOGIC ACTIVIDADES PARA RECUPERAR SERVICIOS DE APLICACIONES – TOMCAT ACTIVIDADES PARA RECUPERAR SERVICIOS DE APLICACIONES – JBOSS ACTIVIDADES PARA RECUPERAR SERVICIOS DE APLICACIONES – IIS

• Validación de logs a nivel de capa media • Cargue de URL's • Pruebas de login fallido • Consideración especial para Aplicaciones en caso de pérdida de data: • Solicitar restore del ultimo backup realizado según políticas • Infraestructura debe asegurar que los servidores se encuentren disponibles y accesible • Las bases de datos deben estar disponibles ➢ Validar acceso a los servidores • Validar los clúster asociados a cada servidor • Subir servicios de capa media • Validar conexión hacia la BD • Validación de logs a nivel de capa media • Cargue de URL's • Pruebas de login fallido		ACTIVIDADES PARA RECUPERAR SERVICIOS DE APLICACIONES - APACHE Documento Maqueta Actividades de Recuperación de BD oracle Documento Maqueta Actividades de Recuperación de BD SQL

13.5 No disponibilidad del servicio de conectividad a internet

13.5.1 Activar el router de contingencia

Actividad	Responsable	Documentación de Soporte
• Reemplazo de equipos router en DC. • Personal de campo reestableciendo la fibra. • Configuración S.O del router en caso de daño, a la misma configuración establecida.	Especialista de Networking	En el siguiente vínculo se encuentra el documento: CERTIFICACIÓN DE IDONEIDAD DEL PLAN DE CONTINUIDAD DEL NEGOCIO DE MEDIA COMMERCE

13.6 Falta de Disponibilidad en la redundancia de los servidores

13.6.1 Reemplazar Equipos Servidores (host de virtualización)

Actividad	Responsable	Documentación de Soporte
Reemplazar servidores físicos En caso falla sobre algún servidor físico de Hiperconvergencia que aloja el ambiente virtualizado se ejecutan las siguientes actividades: 1. Verificación de acceso a herramienta vCenter 2. Dado que es un clúster, se tiene tolerancia a fallo de 3 servidores físicos en la VSAN de Aplicaciones y fallo 2 servidores físicos de la VSAN de Bases de datos, se valida el servidor afectado. 3. Se coloca en mantenimiento el servidor. 4. Se realiza sincronización de la data. 5. Se escala a fabricante (HPE o CISCO) la falla tipo Hardware	Administrador de VMware	En el siguiente vínculo se encuentra el documento: PROCEDIMIENTO PARA RECUPERAR SERVICIOS GT&SEG

6. Se programa cambio de piezas 7. Se reemplazan piezas defectuosas 8. Se agrega el host nuevamente al clúster.		

13.7 No Acceso al Servicio de Correo Electrónico

13.7.1 Establecer un SLA con Microsoft

Actividad	Responsable	Documentación de Soporte
Gravedad A (crítica) No se puede obtener acceso a uno o varios servicios o éstos no se pueden utilizar. Los plazos de producción, operaciones o desarrollo se ven afectados gravemente o se producirá un grave impacto en la producción o rentabilidad. Se ven afectados varios usuarios o servicios. **Disponible: 24/74** **Tiempo de respuesta: una hora** **Gravedad B (alta)** El servicio se puede utilizar, pero de forma limitada. La situación tiene un impacto moderado en el negocio y se puede tratar durante el horario comercial. Un solo usuario, cliente o servicio se ve afectado parcialmente. **Disponible: 24/74** **Tiempo de respuesta: 2 hora** **Gravedad C (no crítica)** La situación genera un mínimo impacto en el negocio. El problema es	Administrador Microsoft Office 365	https://docs.microsoft.com/es-es/office365/servicedescriptions/office-365-platform-service-description/support

importante pero no genera un impacto significativo en la productividad o el servicio actual para el cliente. Un solo usuario sufre una interrupción parcial, pero existe una solución alternativa aceptable. **Disponible: 24/74** **Tiempo de respuesta: 4 horas**		

13.8 No acceso a la Información de OneDrive

13.8.1 Restablecer un backup de la información de los usuarios

Actividad	Responsable	Documentación de Soporte
• Validar en la nube. • Validar en la papelera de reciclaje de One Drive. • Escalar al equipo de office 365	Administrador Microsoft Office 365	https://docs.microsoft.com/es-es/office365/servicedescriptions/office-365-platform-service-description/support

13.9 No Disponibilidad total o parcial de las máquinas virtuales

13.9.1 Activar el sistema de virtualización en el centro de datos alterno

Actividad	Responsable	Documentación de Soporte
Actualmente se dispone de dos sites en los cuales existe un clúster extendido, la disponibilidad total o parcial de las máquinas virtuales depende exclusivamente de la configuración propia que tenga cada servicio. Dicho lo anterior, la solución Hiperconvergencia es la capa que provee los recursos necesarios para que las máquinas virtuales no generen fallas, dado que se tiene redundancia a nivel de centro	Administrador VMware	No Aplica

de datos y redundancia de datos en la VSAN ya que está implementando un RAID 5 sobre un RAID 1, tiene tolerancia a dos fallos de máquinas físicas y aun así las máquinas virtuales no se verán afectadas.		

13.10 Indisponibilidad del sistema de control de acceso a redes

13.10.1 Activar el servicio de control acceso a redes en el centro de datos alterno

Actividad	Responsable	Documentación de Soporte
Esta solución se encuentra compuesta por un clúster de dos dispositivos virtuales en modo Activo/Activo, en caso de falla parcial de los equipos ISE, se debe realizar Confirmación de apuntamiento a servidor radius desde los dispositivos de red LAN/WLAN al equipo que se encuentra activo. Posteriormente se debe reaprovisionar la máquina virtual a la versión de la máquina que presentó el fallo y realizar el cargue del backup para posterior validación del clúster y prueba de autenticación de la red LAN/WLAN. En caso de falla total de los dispositivos de control de identidades, Sería necesario eliminar la autenticación a nivel de red LAN/WLAN contra los dispositivos ISE mientras se realiza el reaprovisionamiento de las máquinas y su restablecimiento de configuración a partir de los	Especialista de Seguridad informática	No Aplica

backups de la solución. Sería necesario hacer un reimage de la máquina virtual a la versión de las máquinas virtuales y con ello cargar sobre estos el backup realizado para posterior validación del clúster y prueba de autenticación de la red LAN/WLAN.		

13.11 Ausencia del Personal de Operación de infraestructura tecnológica

13.11.1 Documentar procesos y procedimientos de operación

Actividad	Responsable	Documentación de Soporte
1. Identificar los roles críticos para la continuidad de la operación. 2. Establecer una estrategia de backup a partir de redundancia de conocimiento. 3. Asegurar los recursos tecnológicos para cada uno de los profesionales relacionados en los roles críticos. 4. Contar con el directorio de contactos. 5. Apoyo de personal experto en caso de requerirse.	Gerente de proyecto	En el siguiente vínculo se encuentra el documento: Documento Maqueta Actividades de Recuperación RRHH

13.11.2 Capacitar personal de backup

Actividad	Responsable	Documentación de Soporte
1. Entrega de políticas de backup 2. Entrega de inventario de cintas de backup. 3. Ingresos a la plataforma de backup 4. Procesos de ejecución de la plataforma de backup. 5. Actas de transferencia de conocimiento.	Administrador de backup	Link de acceso a documentación del fabricante https://www.veritas.com/content/support/en_US/doc/130076143-140940382-0/v53900350-140940382

13.12 Indisponibilidad de información

13.12.1 Recuperación de la base de datos a partir del último backup consistente

Actividad	Responsable	Documentación de Soporte
Consideración especial para Bases de Datos en caso perdida de comunicación: • Disponibilidad de los servidores • Validar acceso a los servidores • Subir servicios de BD • Verificar los listener de las BD afectadas • Verificación del alert log de la BD • Realizar test de conexiones por medio del developer	DBA Oracle	En el siguiente vínculo se encuentra el documento: Documento Maqueta Actividades de Recuperación de BD_oracle

Consideración especial para Bases de Datos en caso perdida de data: • Infraestructura debe garantizar la disponibilidad del servidor • Realizar restore de la BD con el ultimo backup tomado • Subir servicios de BD • Verificar los listener de las BD afectadas • Verificación del alert log de la BD • Realizar test de conexiones por medio del developer • Consideración especial para Aplicaciones en caso de pérdida de data: • Solicitar restore del ultimo backup realizado según políticas • Infraestructura debe asegurar que los servidores se encuentren disponibles y accesible		

13.12.2 Recuperación de información con equipo experto

Actividad	Responsable	Documentación de Soporte
1. Contactar a los expertos 2. Contar con soporte por parte del proveedor de la base de datos. 3. Tener conectividad a internet 4. Tener conectividad con los recursos de la organización 5. Disponibilidad del equipo de infraestructura 6. Contar con la autorización por parte del MEN para los expertos que apoyaran en la actividad.	Gerente de proyecto	En el siguiente vínculo se encuentra el documento: Directorio

13.13 No disponibilidad de repuestos o partes de equipos de comunicaciones e infraestructura

13.13.1 Reemplazo de partes de servidores físicos

Actividad	Responsable	Documentación de Soporte
Remplazo de partes de servidores físicos. En caso falla sobre algún servidor físico de Hiperconvergencia que aloja el ambiente virtualizado se ejecutan las siguientes actividades: 1. Verificación de acceso a herramienta vCenter. 2. Dado que es un clúster, se tiene tolerancia a fallo de 3 servidores físicos en la VSAN de Aplicaciones y fallo 2 servidores físicos de la VSAN de Bases de datos, se valida el servidor afectado. 3. Se coloca en mantenimiento el servidor.	Administrador WMware	No Aplica

4. Si es daño total se retira del clúster que corresponda. 5. Se realiza sincronización de la data. 6. Se escala a fabricante (HPE o CISCO) la falla tipo Hardware, cada contrato de soporte tiene SLA en tiempos de respuesta con el Ministerio de educación. Se programa cambio de piezas o servidor físico. 7. Se reemplazan piezas defectuosas o servidor físico. 8. Se agrega el host nuevamente al clúster de Hiperconvergencia.		

13.14 No disponibilidad del Servicio de Mesa de Ayuda

13.14.1 Activar el servicio de mesa de servicio, en el centro de datos alterno

Actividad	Responsable	Documentación de Soporte
En caso de no haber disponibilidad de servicio de mesa de ayuda, el personal cuenta con las siguientes herramientas para realizar sus actividades: 1. VPN 2. Equipo portátil. 3. Diadema 4. Teclado. 5. Router Wifi con Sim Card. 6. Mouse. 7. Acceso a internet. En caso de persistir el inconveniente los analistas pueden trabajar desde su casa como segunda alternativa porque tienen configurado	Coordinador de la Mesa de Servicio TI	No aplica

acceso remoto a las aplicaciones y a Avaya - CMS Supervisor (ingreso y salida de llamadas).		

13.15 Indisponibilidad total o parcial de servicios tecnológicos por fallas en los servidores

13.15.1 Activar servicios tecnológicos en el centro de datos alterno

Actividad	Responsable	Documentación de Soporte
actualmente se dispone de dos sites en los cuales existe un clúster extendido, la disponibilidad total o parcial de las máquinas virtuales depende exclusivamente de la configuración propia que tenga cada servicio. Dicho lo anterior, la solución Hiperconvergencia es la capa que provee los recursos necesarios para que las máquinas virtuales no generen fallas, dado que se tiene redundancia a nivel de centro de datos y redundancia de datos en la VSAN ya que está implementando un RAID 5 sobre un RAID 1, tiene tolerancia a dos fallos de máquinas físicas y aun así las máquinas virtuales no se verán afectadas.	Administrador VMware	En el siguiente vínculo se encuentra el documento: PROCEDIMIENTO PARA RECUPERAR SERVICIOS GT&SEG

14. Anexos

1. Análisis de estrategias de Continuidad.xls
2. Análisis de Impacto del Negocio.pdf
3. Consolidado 3_Estado_Actual_Servicios_TIC 2020.xlsx
4. Directorio.xls
5. ACTIVIDADES PARA RECUPERAR SERVICIOS DE APLICACIONES – APACHE
6. ACTIVIDADES PARA RECUPERAR SERVICIOS DE APLICACIONES – IIS
7. ACTIVIDADES PARA RECUPERAR SERVICIOS DE APLICACIONES – JBOSS
8. ACTIVIDADES PARA RECUPERAR SERVICIOS DE APLICACIONES – TOMCAT
9. ACTIVIDADES PARA RECUPERAR SERVICIOS DE APLICACIONES – WEBLOGIC
10. Documento Maqueta Actividades de Recuperación CEBYM-CONVALIDA-NEC-DOCENTE-SGDEA-RRHH
11. Documento Maqueta Actividades de Recuperación CNE-SUPERATE-LEGALIZACIONES
12. Documento Maqueta Actividades de Recuperación de BD SQL
13. Documento Maqueta Actividades de Recuperación de BD_oracle
14. Documento Maqueta Actividades de recuperación de infraestructura y comunicaciones
15. Documento Maqueta Actividades de Recuperación RRHH
16. Documento Maqueta Actividades de Recuperación SIMAT-SIPI-SIMPADE-SIUCE-SIA3-SIGAA-SIFSE NVO-SINEB PLANTAS-SIPTA2-NUEVO SIGCE
17. Documento Maqueta Actividades de Recuperación SINEB-SISMA-SSDIPI4
18. PROCEDIMIENTO PARA RECUPERAR SERVICIOS_ GT&SEG
19. CERTIFICACIÓN DE IDONEIDAD DEL PLAN DE CONTINUIDAD DEL NEGOCIO DE MEDIA COMMERCE

15. Referencias

- Ministerio de Tecnologías de la Información y las Comunicaciones. (Diciembre de 2010). *Guía para la preparación de las TIC para la continuidad del negocio (Guía No 10).* Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G10_Continuidad_Negocio.pdf

MEN, U. . (2021). *Arquitectura de seguridad.* Bogotá, Colombia: Contrato CO1.PCCNTR.1989604.

Ministerio de Educación Nacional de Colombia. (2020). Obtenido de Política de seguridad de la información en la continuidad de negocio: https://sig.mineducacion.gov.co/lib/download.php?nivel1=a054VmZRbHVsejE2bHJsTHlMUUlEY3pIMDhCR0lBTkpFRDE5TmJWSFBaWTM2aTR1TUdKbEZKMEw2MGtxQ2YrbHpIYU9jU09JSjdzekhVZGErTmdNakE9PQ==&nivel2=Kzc2bmVCZWJSUzZGdldZRVhaak1HRklqcHB6dytzbW9udWVYTytlWHdRUnh3ZlJJRGIrZi9

Presidencia de la Republica – DAPRE. (Enero de 2021). *Plan de tecnologías de información y comunicaciones para la continuidad de negocio.* Obtenido de https://dapre.presidencia.gov.co/dapre/DocumentosPlaneacion/D-TI-26-Plan-de-Tecnologias-de-Informacion-y-Comunicaciones-para-la-Continuidad-del-Negocio_V3.pdf

SHAREPOINT MINISTERIO DE EDUCACIÓN. (2021). *PROYECTO UTGI MEN*. Obtenido de https://mineducaciongovco.sharepoint.com/:x:/r/sites/Proyecto_UTGI_MEN/Documentos%20compartidos/PROYECTO_UTGI_MEN/3.%20Operaci%C3%B3n%20Servicios%20TI/3.2%20Gesti%C3%B3n%20T%C3%A9cnica/3.2.6.%20Bit%C3%A1cora%20consumo%20recursos%20-%20HC/Consolidado%203_E

Superintendencia de Sociedades. (Diciembre de 2011). *Guía: Plan de recuperación ante desastres – DRP.* Obtenido de https://www.supersociedades.gov.co/nuestra_entidad/Planeacion/SistemaIntegradode%20Gestion/Documentos%20Infraestructura/documentos/ginf-g-010%20Guia_%20PLAN DE RECUPERACIÓN DE DESASTRES TECNOLÓGICOS.pdf

VMWARE. (2021). Obtenido de vSphere Distributed Switch: https://www.vmware.com/co/products/vsphere/distributed-switch.html

Información Del Documento

Fecha	Versión	Responsable	Revisado por	Aprobado por
07/01/2022	9.0	Especialista de seguridad de la información	Líder Gestión Técnica y seguridad	

Control de cambios

Fecha	Versión	Causa Cambio	Aprobado por
19/04/2021	1.0	Creación del documento	
19/05/2021	2.0	Modificación de acuerdo con el comunicado INT-UT:COM-0421-222	
27/05/2021	3.0	Modificación de acuerdo con el comunicado INT-UT-COM-0521-286	
21/06/2021	4.0	Modificación de acuerdo con el comunicado INT-UT:COM-0621-307	
08/07/2021	5.0	Modificación de acuerdo con el comunicado INT-UT:COM-0621-307	
09/11/2021	6.0	Modificación de acuerdo con el comunicado INT-UT:COM-0721-354	
09/12/2021	7.0	Modificación de acuerdo con el comunicado INT-UT-COM-1121-694	
27/12/2021	8.0	Modificación de acuerdo con el comunicado INT-UT-COM-1221-790	
07/01/2022	9.0	Modificación de acuerdo con el comunicado INT-UT-COM-0122-839	