Resolución Directoral Regional

Nº 0820 -2023-DRELM

Lima, 09 Jun. 2023

VISTOS: El expediente N.º 3240-2023-DRELM**,** el Informe N.° 0081-2023-MINEDU/VMGI-DRELM-OPP-ERMC, el Informe N.° 412-2023-MINEDU/VMGI-DRELM-OAJ-EGSA, y demás documentos que se adjuntan;

CONSIDERANDO:

Que, el artículo 191 del Reglamento de Organización y Funciones del Ministerio de Educación, aprobado por Decreto Supremo N.° 001-2015-MINEDU, señala entre otros aspectos, que la Dirección Regional de Educación de Lima Metropolitana es el órgano desconcentrado del Ministerio de Educación a través del Despacho Viceministerial de Gestión Institucional, responsable del servicio educativo y de los programas de atención integral en el ámbito de su jurisdicción así como de evaluar y supervisar a las Unidades de Gestión Educativa Local de Lima Metropolitana;

Que, el Manual de Operaciones de la Dirección Regional de Educación de Lima Metropolitana - MOP, aprobado por Resolución Ministerial N.° 215-2015-MINEDU y modificatoria, precisa que esta Dirección Regional tiene como objetivo, aplicar y gestionar en Lima Metropolitana, la política educativa nacional emitida por el MINEDU, actuando como instancia administrativa en los asuntos de su competencia;

Que, el artículo 3, literal h) del citado instrumento de gestión, señala que esta Dirección Regional tiene como una de sus funciones, promover la implementación de mecanismos de participación para garantizar una gestión transparente y equitativa;

Que, el literal f) del artículo 14 del MOP, establece como función de la Oficina de Planificación y Presupuesto, a través del Equipo de Tecnologías de la Información, el de, «B*rindar soporte técnico en materia de tecnologías de la Información a la DRELM, así como coordinar con el órgano competente del MINEDU, el asesoramiento en temas relacionados con las tecnologías de la información en las UGEL de Lima Metropolitana e Institutos y Escuelas de Educación Superior*»;

Que, con Resolución de Secretaría General N.° 101-2022-MINEDU, de fecha 16 de junio de 2022, se aprobó la Directiva denominada «Elaboración, aprobación y tramitación de actos resolutivos y documentos normativos del Ministerio de Educación», en adelante la Directiva, que tiene como objetivo, regular la elaboración, aprobación y trámite de actos resolutivos; así como la elaboración, aprobación y modificación de documentos normativos del MINEDU;

Que, el numeral 5, subnumeral 5.1 de la Directiva, señala que, *«Los órganos, unidades orgánicas, programas y proyectos del Ministerio de Educación pueden formular y proponer documentos normativos, en el marco de sus atribuciones y en concordancia con los documentos de gestión institucional correspondientes, teniendo la calidad de proponentes»;*

Que, sobre los documentos normativos, el numeral 7 de la Directiva establece que, *«Son aquellos documentos que tienen por objeto regular el cumplimiento de las funciones y disposiciones normativas sobre aspectos operativos o administrativos en los órganos, unidades orgánicas, órganos desconcentrados, programas y proyectos del MINEDU, así como de las demás instancias de gestión educativa descentralizada, cuando corresponda, clasificándose los mismos en: Lineamiento, Norma Técnica, Directiva, Manual»;*

Que, el subnumeral 7.4. del numeral 7 de la citada Directiva, sobre los Manuales, precisa que es un, *«Documento que explica de forma ordenada y sistemática, una materia con relación a aspectos educativos o de gestión, a fin de aclarar, entender o verificar una actividad o procedimiento (…) Se aprueba por Resolución Ministerial, Resolución Viceministerial, Resolución de Secretaría General, Resolución de Dirección Ejecutiva o Resolución Directoral, según corresponda»,* señalando a su vez la estructura que debe seguir, conforme al cuadro que adjunta;

Que, con Resolución Ministerial N.° 004-2016-PCM, de fecha 08 de enero de 2016, se aprobó el uso obligatorio de la Norma Técnica Peruana *«NTP-ISO/IEC 27001:2014 - Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición»,* en todas las entidades integrantes del Sistema Nacional de Informática que tiene por objeto especificar los requisitos para establecer, implementar, mantener, y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización;

Que, mediante Informe N.° 0063-2023-MINEDU/VMGI-DRELM-OPP-ETI, de fecha 11 de abril de 2023, el Equipo de Tecnologías de la Información de la Oficina de Planificación y Presupuesto de esta sede regional, solicitó la aprobación del Proyecto del *«Manual de Continuidad Informática de la Dirección Regional de Educación de Lima Metropolitana»,* el cual permitirá minimizar el tiempo de indisponibilidad de los servicios de la DRELM que son soportados por los servicios de Tecnologías de Información;

Que, con Informe N.° 0081-2023-MINEDU/VMGI-DRELM-OPP-ERMC, de fecha 17 de abril de 2023, el Equipo de Racionalización y Mejora Continua de la Oficina de Planificación y Presupuesto, emitió opinión favorable para la aprobación del *«Manual de Continuidad Informática de la Dirección Regional de Educación de Lima Metropolitana»,* por contribuir a la organización de actividades internas relacionadas al análisis de riesgo de la infraestructura informática de la DRELM y las acciones de prevención y atención de contingencias para garantizar la continuidad del servicio de las tecnologías de la Información en la DRELM, para lo cual adjunta el anexo correspondiente;

Que, a través del Informe N.º 412-2023-MINEDU/VMGI-DRELM-OAJ-EGSA, de fecha 02 de mayo de 2023, la Oficina de Asesoría Jurídica concluyó que, resulta legalmente viable aprobar el *«Manual de Continuidad Informática de la Dirección Regional de Educación de Lima Metropolitana»,* por encontrarse conforme a ley y según lo propuesto por el órgano técnico;

Que, conforme a la facultad establecida en el literal k) del artículo 8 del Manual de Operaciones de la Dirección Regional de Educación de Lima Metropolitana, aprobado por Resolución Ministerial N.° 215-2015-MINEDU y su modificatoria, corresponde emitir el acto resolutivo correspondiente;

Contando con el visado de la Oficina de Planificación y Presupuesto y la Oficina de Asesoría Jurídica de la Dirección Regional de Educación de Lima Metropolitana, y de conformidad con el Manual de Operaciones de la Dirección Regional de Educación de Lima Metropolitana y su modificatoria, aprobado por Resolución Ministerial N.°215-2015-MINEDU;

SE RESUELVE:

ARTÍCULO 1.- APROBAR el «Manual de Continuidad Informática de la Dirección Regional de Educación de Lima Metropolitana», conforme al Anexo que forma parte integrante de la presente resolución.

ARTÍCULO 2.- DISPONER, que el Equipo de Atención al Usuario y Gestión Documentaria de la Oficina de Atención al Usuario y Comunicaciones de esta sede regional notifique la presente resolución a todas las oficinas y unidades de la DRELM conforme a Ley.

ARTÍCULO 3.- DISPONER la publicación de la presente Resolución en el Portal de la Dirección Regional de Educación de Lima Metropolitana: www.drelm.gob.pe.

ARTÍCULO 4.- DISPONER que el Equipo de Archivo Documentario de la Oficina de Atención al Usuario y Comunicaciones archive los actuados adjuntos en el modo y forma de Ley.

Regístrese y Comuníquese,

Documento firmado digitalmente

LUIS ALBERTO QUINTANILLA GUTIÉRREZ
Director Regional de Educación de
Lima Metropolitana

LAQG/D.DRELM
MEFP/ J.OAJ
WJGM/ C. EGSA
KFCC/Abog.

Código : 020523515
Clave : 0D2C

MANUAL DE CONTINUIDAD INFORMÁTICA DE LA DIRECCIÓN REGIONAL DE EDUCACIÓN DE LIMA METROPOLITANA

Resolución de Aprobación			
Resolución Directoral N° -2023-DRELM			
Código	Versión	Páginas	Fecha de aprobación
MA-00X-01-DRELM	01		

Código : 100523296
Clave : 24E2

Control de Cambios		
Versión	**Sección / Ítem**	**Descripción del cambio:**
01	----	Nuevo

ESTADO FORMAL:

	Elaborado por:	**Revisado por:**
Nombre:	(Cargo): Especialista en Sistemas e Informática - Gerry Ax'l Vera Suasnábar	(Cargo): Responsable (e) del Equipo de Tecnologías de la Información - Julio Jesús Tello Barron
Fecha:	11/04/2023	11/04/2023

ÍNDICE

1. OBJETIVO

Los objetivos principales del presente documento son los siguientes:

- Contar con una estrategia planificada compuesta por un conjunto de procedimientos que garanticen la disponibilidad de una solución alterna que permita restituir rápidamente los sistemas de información de la Dirección Regional de Educación de Lima Metropolitana (DRELM) ante la eventual presencia de siniestros que paralicen parcial o totalmente los procesos.
- Recuperar la operatividad normal de los servicios críticos de redes y comunicaciones, sistemas de información, aplicaciones y bases de datos en el menor tiempo posible ante la ocurrencia de una falla.
- Asegurar la continuidad de los servicios, minimizando los daños a la DRELM mediante la protección y conservación de los activos ante las amenazas internas y externas.
- Establecer las secuencias que se han de seguir para organizar y ejecutar las acciones de control informático.
- Realizar mantenimientos preventivos a los equipos de cómputo y el centro de datos con el propósito de determinar las condiciones de operación y ampliar la vida útil de los mismos.

2. AMBITO DE APLICACIÓN

El presente Manuel es de observancia para la Dirección Regional de Educación de Lima Metropolitana.

3. BASE NORMATIVA

- Ley N° 29664, Ley que creó el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD)
- Ley N° 29733 – Ley de Protección de Datos Personales
- R.M 664-2018-MINEDU que aprobó la “Política General de Seguridad de la Información en el Ministerio de Educación”
- NTP 27001:2014 “Técnicas de seguridad. Sistemas de gestión de seguridad de la información: Requisitos”
- R.S.G 028-2019-MINEDU, que aprobó la directiva de “Verificación y validación de producto software de desarrollo externo”
- R.S.G 101-2022-MINEDU, que aprobó la “Elaboración, aprobación y tramitación de actos resolutivos y documentos normativos del Ministerio de Educación”

4. DEFINICIONES

- **Activo de Información:** Cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la entidad, pueden ser datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.
- **Acceso:** Es la lectura o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta una base de datos, los datos son primero accedidos y suministrados a la computadora y luego transmitidos a la pantalla del equipo.
- **Amenaza:** Cualquier evento que pueda interferir con el funcionamiento de un computador o causar la difusión no autorizada de información confiada a

un computador. Ejemplo: Fallas del suministro eléctrico, virus, saboteos o descuidos del usuario.

- **Aplicaciones:** Son los archivos y programas con sus correspondientes manuales de usuario y/o técnicos, desarrollados o adquiridos por la Entidad.
- **Base de Datos:** Es un conjunto de datos organizados, entre los cuales existe una correlación y que además están almacenados con criterios independientes de los programas que los utilizan. Entre sus principales características se encuentran brindar seguridad e integridad a los datos, proveer lenguajes de consulta, de captura y edición de los datos en forma interactiva, proveer independencia de los datos.
- **Ataque:** Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático o el intento de obtener de modo no autorizado la información confiada a un computador.
- **Incidente:** Cuando se produce un ataque o se materializa una amenaza se tiene un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de eliminación de un archivo protegido.
- **Integridad:** Los valores consignados en los datos se han de mantener de tal manera que representen la realidad y su modificación debe ser registrada en bitácoras del sistema que permitan la auditoría de los acontecimientos. Las técnicas de integridad sirven para prevenir el ingreso de valores errados en los datos sea esta situación provocada por el software de la Base de Datos, por fallas de los programas, del sistema, el hardware o, simplemente, por errores humanos.
- **Privacidad:** Se define como el derecho que tiene la DRELM para determinar, a quién, cuándo y qué información de su propiedad podrá ser difundida o transmitida a terceros.
- **Confidencialidad:** Propiedad de la información que hace que no esté disponible o que sea revelada a individuos o entidades no autorizados.
- **Control:** Medio para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la entidad que pueden ser de naturaleza administrativa, técnica, de gestión o legal.
- **Cortafuego (Firewall):** El Cortafuegos, es un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios y pueden ser implementados en hardware o software, o en una combinación de ambos.
- **Datos Personales:** Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados.
- **Manual de Continuidad Informático:** Manual definido y documentado que guían a la organización a responder, recuperar, reanudar los servicios de TI después de una interrupción.
- **Probabilidad:** Posibilidad que un evento determinado ocurra en un período de tiempo dado.
- **Riesgo:** El riesgo se define como la posibilidad que ocurra un evento adverso que afecte el logro de los objetivos de la entidad/dependencia.
- **Sistemas de Información:** Conjunto de elementos relacionados entre sí con un objetivo en común, en el cual se almacenan datos y se genera información

relacionada a un tema en particular, para ponerlos a disposición de sus usuarios. Pueden ser registros simples como archivos de Word/Excel, o pueden ser complejos como una aplicación de software con base de datos.

- **Datos:** En general se consideran datos a todos aquellos elementos por medio de los cuales es posible la generación de información. Tales elementos pueden ser estructurados (base de datos) o no estructurados (correos electrónicos) y se presentan en forma de imágenes, sonidos o colección de bits.
- **Centro de Datos:** El centro de datos, es un centro de procesamiento para obtener información, en el cual se albergan los sistemas de información, hardware, componentes asociados, como telecomunicaciones y sistemas de almacenamiento.

5. SIGLAS

- **DRELM:** Dirección Regional de Educación de Lima Metropolitana
- **ETI:** Equipo de Tecnologías de la Información
- **MINEDU:** Ministerio de Educación
- **NTP:** Norma Técnica Peruana
- **OPP:** Oficina de Planificación y Presupuesto
- **SGSI:** Sistema de Gestión de la Seguridad de la Información

6. CONTENIDO

6.1 ANALISIS DE IMPACTO DE LA CONTINUIDAD DE LOS SERVICIOS DE TECNOLOGIAS DE INFORMACIÓN

En esta fase se procederá a la identificación de los procesos críticos, los recursos y el periodo máximo de recuperación de los servicios de tecnologías de la información, para los cuales se considerarán todos los elementos susceptibles de provocar eventos que conlleven a activar la contingencia.

6.1.1 Servicios de TI

Los procesos de la DRELM están soportados por los siguientes servicios de Tecnologías de la Información (TI)

N°	Servicio TI	Descripción	Crítico para operaciones internas	Crítico para operaciones externas
1	Internet Corporativo	El servicio de acceso a internet con flujo de carga (publicación) y descarga (navegación) en la Sede Central de la DRELM	Alta	Alta
2	Acceso a dominio	Servicio de autentificación en el dominio de la DRELM con el uso de credenciales institucionales (usuario y contraseña)	Alta	Baja
3	Telefonía IP	Servicio de comunicación telefónica por Red IP mediante el uso de teléfono físico	Baja	Media

N°	Servicio TI	Descripción	Crítico para operaciones internas	Crítico para operaciones externas
4	Correo Institucional	Servicio de mensajería de correo electrónico bajo el dominio @drelm.gob.pe	Alta	Media
5	Internet inalámbrico	Servicio de acceso a internet mediante conectividad WIFI	Medio	Baja
6	Almacenamiento en nube	El servicio de almacenamiento en nube habilita el mecanismo para resguardo de archivos y acceso desde cualquier lugar con conexión a internet	Medio	Medio
7	Videoconferencia	Servicio de videoconferencia, conferencia web y llamadas por internet	Media	Media
8	Microformas Digitales	Servicio de digitalización de documentos con valor legal	Media	Baja
9	Acceso a red	El servicio de acceso a red permite la conexión de un equipo de cómputo a la red de datos institucional	Alta	Baja
10	Almacenamiento de servidores	Servicio de repositorio digital de archivos generados en las aplicaciones y digitalización de documentos	Alta	Alta
11	Firma Digital	Servicio de firma digital mediante el uso de certificados digitales de RENIEC	Alta	Baja
12	Base de datos	Servicio de repositorio de información indexada en base de datos para aplicaciones y servidores del centro de datos	Alta	Alta
13	VPN	Servicio de conectividad remota segura para ejecutar trabajo remoto	Baja	Alta
14	Estaciones de trabajo	Equipamiento de cómputo como recurso para el procesamiento de información	Alta	Media
15	Sistemas de información Internos	Aplicaciones disponibles para acceso por personal administrativo de la DRELM	Alta	Media
16	Sistemas de información externos	Aplicaciones disponibles para acceso para público en general	Media	Alta
17	Personal crítico responsable de los procesos TI	Servicios profesionales críticos encargados de procesos de TI	Alta	Media
18	Centro de datos	Servicio de hosting y housing como infraestructura de soporte para los servicios de TI de la DRELM	Alta	Alta

N°	Servicio TI	Descripción	Crítico para operaciones internas	Crítico para operaciones externas
19	Transmisión de datos	El servicio de conectividad remota de la DRELM con MINEDU y UGELs	Media	Media

6.1.2 Priorización de restauración de servicios de TI

La priorización de la restauración de los servicios de tecnologías de información se realizará según la siguiente tabla:

Descripción	Prioridad de recuperación
Atención prioritaria: Sistemas de información y equipos que requieran alta disponibilidad de atención a clientes externos	1
Atención estándar: Sistemas de información y equipos no relacionados con la atención a los clientes externos	2
Atención baja: Sistemas de información de uso interno, uso poco frecuente y/o que manejan bajo volumen de información	3

Luego del análisis, considerando la criticidad, se determina de la siguiente manera la priorización de restauración de los servicios de tecnologías de la información:

N°	Servicios TI	Prioridad
1	Centro de datos	1
2	Acceso a red	1
3	Internet Corporativo	1
4	Almacenamiento de servidores	1
5	Base de datos	1
6	Estaciones de trabajo	1
7	Sistemas de información Internos	1
8	Sistemas de información Externos	1
9	Personal crítico responsable de los procesos TI	2
10	Acceso a dominio	2
11	Transmisión de datos	2
12	Correo Institucional	2
13	Firma Digital	2
14	Microformas Digitales	2
15	Almacenamiento en nube	2
16	VPN	2
17	Videoconferencia	2
18	Internet inalámbrico	3
19	Telefonía IP	3

6.2 EVALUACIÓN DE RIESGO

6.2.1 Identificación de Amenazas

Para determinar el riesgo asociado a cada servicio de TI procederemos a definir las amenazas y la frecuencia o probabilidad de falla o interrupción asociado a estos.

N°	Amenaza	Descripción	Tipo
1	Falla en equipos de telecomunicaciones	Equipos de telecomunicaciones sin mantenimiento	Tecnológico
2	Ciberataque	Ataque de virus a los equipos de cómputo	
3	Falla de hardware o software	Equipos de cómputo sin mantenimiento preventivo, actualización o sin antivirus.	
4	Falla de suministro eléctrico en el Centro de Datos y gabinetes de comunicaciones	Falla del fluido eléctrico en la institución	Físico y ambiental
5	Ausencia o no disponibilidad del personal critico de TI	No contar con personal especializado de Tecnologías de Información	Recurso Humano
6	Vandalismo	Daño a los equipos de cómputo y/o archivos por parte del personal interno y/o externo	
7	Accesos no autorizados	Acceso a información de personal no autorizado	
8	Pandemia y/o epidemia	Información física sin digitalizar y/o sistemas de información con funcionamiento in house	Ambiental
9	Sismo	Destrucción de equipos de cómputo y archivos por un medio de un terremoto	Siniestro Natural
10	Inundación y aniego en el centro de datos	Destrucción de equipos de cómputo y archivos por falla del aire acondicionado o inundación	
11	Incendio en el Centro de Datos	Destrucción de equipos de cómputo y archivos por medio del fuego	

6.2.2 Probabilidad de ocurrencia

Es la cuantificación de ocurrencia de que una amenaza se produzca realmente. Para el cálculo de probabilidad utilizaremos la siguiente tabla:

Probabilidad	Valor	Descripción
Baja	4	Se puede presentar al menos una vez en 5 años o más
Media	6	Se puede presentar al menos una vez en 3 años
Alta	8	Se puede presentar al menos una vez al año
Muy Alta	10	Se puede presentar más de 1 vez al año

A continuación, se muestra la probabilidad estimada de las amenazas a los servicios de TI:

N°	Amenaza (Evento)	Probabilidad de ocurrencia
1	Ciberataque	10
2	Falla de equipos de telecomunicaciones	6
3	Falla de hardware o software	10
4	Falla de suministro eléctrico en el Centro de datos y gabinetes de comunicaciones	8
5	Ausencia o no disponibilidad del personal crítico de TI	8
6	Vandalismo	4
7	Accesos no autorizados	8
8	Pandemia	4
9	Sismo	4
10	Inundación en el Centro de datos	4
11	Incendio en el Centro de datos y/o equipos de cómputo	4

6.2.3 Identificación de impacto

El impacto del riesgo mide la gravedad o magnitud del efecto adverso a causa de la ocurrencia de la amenaza. Es una calificación aplicada a la amenaza, para describir el grado de afectación. La medición puede ser cualitativa o cuantitativa.

Para nuestro caso la clasificación del impacto será en una escala 4 al 10 categorizando desde los niveles Bajo hasta Muy Alto, tal como se muestra la siguiente tabla:

Impacto	Valor	Descripción
Bajo	4	No representa un impacto importante. Se cuenta con controles suficientes que responden a un programa de mantenimiento (evaluados y mejorados), se evidencia que han respondido a acontecimiento ocurridos y ejercicios realizados, se puede prescindir del servicio por un tiempo limitado
Medio	6	El impacto sobre la confidencialidad, integridad y disponibilidad de la información es limitado en tiempo y alcance. Su efecto es para un proceso de soporte o actividad específica que puede subsanarse en corto plazo
Alto	8	Impacta en forma grave a un área o servicio específico, se puede llegar a comprometer documentos internos clasificados como confidenciales, paralizar o retrasar procesos claves por un tiempo considerable. Su efecto está limitado dentro de la DRELM
Muy Alto	10	Impacta en forma severa a todo la DRELM y su efecto no solo se limita a este. Compromete la confidencialidad o integridad de información crítica o la continuidad de las operaciones por paralización de los servicios más allá de los tiempos tolerables por la entidad.

6.2.4 Cálculo del nivel de Riesgo

Para determinar el Nivel de Riesgo de un servicio de TI de la DRELM, se ha considerado los controles existentes que mitigan la afectación de las

amenazas y/o el impacto descrito en el punto anterior. Para la identificación del Nivel de Riesgo se considera la siguiente matriz:

Probabilidad de ocurrencia	**Muy Alta**	**10**	40 (Medio)	60 (Alto)	80 (Muy Alto)	100 (Muy Alto)
	Alta	**8**	32 (Medio)	48 (Alto)	64 (Alto)	80 (Muy Alto)
	Media	**6**	24 (Bajo)	36 (Medio)	48 (Alto)	60 (Alto)
	Baja	**4**	16 (Bajo)	24 (Bajo)	32 (Medio)	40 (Medio)
Nivel De Riesgo (probabilidad de ocurrencia x impacto)			**4**	**6**	**8**	**10**
			Bajo	**Medio**	**Alto**	**Muy Alto**
			Impacto			

Interpretación de cada cuadrante de calor o nivel de riesgo de la amenaza en evaluación:

Muy Alto	Riesgo no aceptable, se requiere acción correctiva inmediata
Alto	Riesgo no aceptable, se requiere de una acción correctiva, pero se permite planificar plazos y compromisos
Medio	Riesgo aceptable con revisión de la dirección, y se evalúa tomar acciones
Bajo	Riesgo aceptable, sin revisión y no se requieren acciones

Listado de riesgos considerando las amenazas existentes a los servicios de TI.

N°	Amenaza	Riesgo	Probabilidad	Impacto	Nivel de riesgo
1	Ciberataque	Daño o perdida de equipo, unidades de almacenamiento, etc	10	6	60
2	Ciberataque	Imposibilidad de acceso a los recursos informáticos, sean estos por cambios voluntarios o involuntarios, tales como cambio de claves de acceso, eliminación de los archivos o proceso de información no deseado	10	8	80
3	Ciberataque	Exposición de información por suplantación de identidad a través de técnicas de ingeniería social	10	8	80
4	Ciberataque	Alteraciones de la información por manejo inadecuado de contraseñas (inseguras, compartidas)	10	6	60

N°	Amenaza	Riesgo	Probabilidad	Impacto	Nivel de riesgo
5	Ciberataque	Perdida o alteración de información institucional, por intromisión de agentes externos y/o inescrupulosos, los cuales pueden generar daño y perdida de información institucional	10	10	100
6	Ciberataque	Indisponibilidad de los sistemas por ataques de denegación de servicio (DDoS) a aplicaciones críticas	10	10	100
7	Falla en equipos de telecomunicaciones	Dificultad para acceder a los servicios de internet e intranet	6	8	48
8	Falla en equipos de telecomunicaciones	Saturación del servicio de red inalámbrica por acceso no autorizado	6	4	24
9	Falla en equipos de telecomunicaciones	Suplantación de identidad o acceso no autorizado por desprotección de equipos móviles corporativos	6	4	24
10	Falla de hardware o software	Indisponibilidad del acceso al dominio de DRELM por falla de hardware	6	10	60
11	Falla de hardware o software	Exposición de información por acceso electrónico no autorizado a sistemas internos	6	8	48
12	Falla de hardware o software	Exposición de información por acceso electrónico no autorizado a sistemas externos	6	6	36
13	Falla de hardware o software	Indisponibilidad del servicio de firma digital	6	6	36
14	Falla de hardware o software	Falta de actualización de software y hardware (procesos y recursos)	6	8	48
15	Falla de hardware o software	Daño físico por cableado de red expuesta o en mal estado en las instalaciones de la institución	6	6	36
16	Falla de hardware o software	Pérdida de información por uso de software sin soporte del fabricante	6	8	48
17	Falla de suministro eléctrico en el Centro de Datos y gabinetes de comunicaciones	Daño en los discos duros o componentes de los servidores, controladores de red, equipamiento de infraestructura, etc	8	8	64
18	Falla de suministro eléctrico en el Centro de Datos y gabinetes de comunicaciones	Daño en el equipamiento del Centro de Datos por corte no programado de energía	8	8	64

N°	Amenaza	Riesgo	Probabilidad	Impacto	Nivel de riesgo
19	Ausencia o no disponibilidad del personal crítico de TI	Perdida de datos por error de personal no especializado	8	6	48
20	Ausencia o no disponibilidad del personal crítico de TI	Indisponibilidad de los sistemas de información por error en la ejecución de procedimientos no documentados	8	6	48
21	Ausencia o no disponibilidad del personal crítico de TI	Perdida de información por falta de traslado de copias de seguridad hacia el servicio de custodia	8	8	64
22	Vandalismo	Daño físico o lógico de los equipos de cómputo de la DRELM	4	6	24
23	Vandalismo	Eliminación de información por parte del personal de la DRELM	4	8	32
24	Accesos no autorizados	Robo de información por parte de personal no autorizado	8	8	64
25	Pandemia y/o epidemia	Indisponibilidad de los servicios por falta de personal técnico	4	6	24
26	Sismo	Perdida de información en el centro de datos inhouse	4	10	40
27	Sismo	Daño de los equipos de cómputo de la DRELM	4	6	24
28	Inundación y aniego en el Centro de Datos	Indisponibilidad del centro de datos por inundación o aniego en las instalaciones de la DRELM	4	10	40
29	Inundación y aniego en el Centro de Datos	Daño del centro de datos por falla en el equipo de aire acondicionado o ventilación del centro de datos	4	8	32
30	Incendio en el Centro de datos y/o equipos de cómputo	Daño del centro de datos por un corto circuito	4	10	40
31	Incendio en el Centro de datos y/o equipos de cómputo	Daño de los equipos de cómputo de la DRELM por una mala conexión eléctrica	4	6	24

6.2.5 Identificación de controles existentes

La identificación de controles existentes, permiten conocer que tan protegidos están los servicios de TI de la DRELM frente a cada amenaza.

Los controles existentes son:

N°	Amenaza	Riesgo	Control
1	Ciberataque	Daño o perdida de equipo, unidades de almacenamiento, etc	• Software antivirus instalado en los servidores de red y equipos de cómputo DRELM • Mantenimiento preventivo de servidores y equipos de cómputo

N°	Amenaza	Riesgo	Control
			• Restricciones de acceso a páginas web sospechosas • Restricciones de acceso a puertos periféricos en los equipos de cómputo • Respaldo de copias de seguridad de la información en el servidor de backup
2	Ciberataque	Imposibilidad de acceso a los recursos informáticos, sean estos por cambios voluntarios o involuntarios, tales como cambio de claves de acceso, eliminación de los archivos o proceso de información no deseado	• Respaldo de copias de seguridad de la información (carpetas compartidas) en el servidor de backup
3	Ciberataque	Exposición de información por suplantación de identidad a través de técnicas de ingeniería social	• Solución antivirus instalada en los servidores de red y equipos de cómputo DRELM • Acceso a los equipos de cómputo y/o sistemas de información de la DRELM mediante clave fuerte la cual tiene que contener, mínimo 8 dígitos (mayúsculas, minúsculas, números y caracteres alfanuméricos)
4	Ciberataque	Alteraciones de la información por manejo inadecuado de contraseñas (inseguras, compartidas)	• Acceso a la institución mediante registro en el reloj biométrico y/o personal de seguridad • Acceso a los equipos de cómputo y/o sistemas de información de la DRELM mediante clave fuerte la cual tiene que contener, mínimo 8 dígitos (mayúsculas, minúsculas, números y caracteres alfanuméricos)
5	Ciberataque	Perdida o alteración de información institucional, por intromisión de agentes externos y/o inescrupulosos, los cuales pueden generar daño y perdida de información institucional	• Respaldo de copias de seguridad de la información (carpetas compartidas) en el servidor de backup • Seguridad perimetral • Acceso a la institución mediante registro en el reloj biométrico y/o personal de seguridad • Solución antivirus instalada en los servidores de red y equipos de cómputo DRELM
6	Ciberataque	Indisponibilidad de los sistemas por ataques de denegación de servicio (DDoS) a aplicaciones críticas	• Solución antivirus instalada en los servidores de red y equipos de cómputo DRELM • Seguridad perimetral
7	Falla en equipos de telecomunicaciones	Dificultad para acceder a los servicios de internet e intranet	• Restricciones de acceso a páginas web sospechosas • Acuerdos de niveles de servicio con proveedor de servicio de internet

N°	Amenaza	Riesgo	Control
8	Falla en equipos de telecomunicaciones	Saturación del servicio de red inalámbrica por acceso no autorizado	• Seguridad perimetral • Acuerdos de niveles de servicio con proveedor de servicio de internet
9	Falla en equipos de telecomunicaciones	Suplantación de identidad o acceso no autorizado por desprotección de equipos computo corporativos	• Acceso a la institución mediante registro en el reloj biométrico y/o personal de seguridad • Software antivirus instalado en los servidores de red y equipos de cómputo DRELM
10	Falla de hardware o software	Indisponibilidad del acceso al dominio de DRELM por falla de hardware	• Actualización de parches de seguridad de sistemas operativos en servidores y equipos de cómputo • Mantenimiento preventivo de servidores y equipos de cómputo
11	Falla de hardware o software	Exposición de información por acceso electrónico no autorizado a sistemas internos	• Solución antivirus instalada en los servidores de red y equipos de cómputo DRELM • Acceso a los equipos de cómputo y/o sistemas de información de la DRELM mediante clave fuerte la cual tiene que contener, mínimo 8 dígitos (mayúsculas, minúsculas, números y caracteres alfanuméricos)
12	Falla de hardware o software	Exposición de información por acceso electrónico no autorizado a sistemas externos	• Solución antivirus instalada en los servidores de red y equipos de cómputo DRELM • Acceso a los equipos de cómputo y/o sistemas de información de la DRELM mediante clave fuerte la cual tiene que contener, mínimo 8 dígitos (mayúsculas, minúsculas, números y caracteres alfanuméricos)
13	Falla de hardware o software	Indisponibilidad del servicio de firma digital	• Acuerdos de niveles de servicio con proveedor de servicio de internet y servicio de firma • Actualización de parches de seguridad de sistemas operativos en servidores y equipos de cómputo
14	Falla de hardware o software	Falta de actualización de software y hardware (procesos y recursos)	• Actualización de parches de seguridad de sistemas operativos en servidores y equipos de cómputo • Mantenimiento preventivo de servidores y equipos de cómputo
15	Falla de hardware o software	Daño físico por cableado de red expuesta o en mal estado en las instalaciones de la institución	• Seguridad perimetral • Mantenimiento preventivo del cableado estructurado

N°	Amenaza	Riesgo	Control
16	Falla de hardware o software	Pérdida de información por uso de software sin soporte del fabricante	• Respaldo de copias de seguridad de la información (carpetas compartidas) en el servidor de backup • Instalación de software licenciado
17	Falla de suministro eléctrico en el Centro de Datos y gabinetes de comunicaciones	Daño en los discos duros o componentes de los servidores, controladores de red, equipamiento de infraestructura, etc	• Respaldo de copias de seguridad de la información (carpetas compartidas) en el servidor de backup • Mantenimiento preventivo de servidores y equipos de cómputo
18	Falla de suministro eléctrico en el Centro de Datos y gabinetes de comunicaciones	Daño en el equipamiento del Centro de Datos por corte no programado de energía	• Mantenimiento preventivo de Tableros eléctrico y UPS.
19	Ausencia o no disponibilidad del personal crítico de TI	Perdida de datos por error de personal no especializado	• Cámaras de vigilancia en el interior del Centro de Datos • Sistema de control biométrico de acceso al Centro de Datos • Capacitación al personal de ETI
20	Ausencia o no disponibilidad del personal crítico de TI	Indisponibilidad de los sistemas de información por error en la ejecución de procedimientos no documentados	• Capacitación al personal de ETI
21	Ausencia o no disponibilidad del personal crítico de TI	Perdida de información por falta de traslado de copias de seguridad hacia el servicio de custodia	• Cámaras de vigilancia en el interior del Centro de Datos • Sistema de control biométrico de acceso al Centro de Datos • Respaldo de copias de seguridad de la información (carpetas compartidas) en el servidor de backup
22	Vandalismo	Daño físico o lógico de los equipos de cómputo de la DRELM	• Cámaras de vigilancia en el interior del Centro de Datos • Respaldo de copias de seguridad de la información (carpetas compartidas) en el servidor de backup • Mantenimiento preventivo de servidores y equipos de cómputo

N°	Amenaza	Riesgo	Control
			• Acceso a la institución mediante registro en el reloj biométrico y/o personal de seguridad
23	Vandalismo	Eliminación de información por parte del personal de la DRELM	• Respaldo de copias de seguridad de la información (carpetas compartidas) en el servidor de backup • Acceso a los equipos de cómputo y/o sistemas de información de la DRELM mediante clave fuerte la cual tiene que contener, mínimo 8 dígitos (mayúsculas, minúsculas, números y caracteres alfanuméricos)
24	Accesos no autorizados	Robo de información por parte de personal no autorizado	• Acceso a los equipos de cómputo y/o sistemas de información de la DRELM mediante clave fuerte la cual tiene que contener, mínimo 8 dígitos (mayúsculas, minúsculas, números y caracteres alfanuméricos) • Acceso a la institución mediante registro en el reloj biométrico y/o personal de seguridad • Acceso a los equipos de cómputo y/o sistemas de información de la DRELM mediante clave fuerte la cual tiene que contener, mínimo 8 dígitos (mayúsculas, minúsculas, números y caracteres alfanuméricos) • Solución antivirus instalada en los servidores de red y equipos de cómputo DRELM • Acceso a la institución mediante registro en el reloj biométrico y/o personal de seguridad
25	Pandemia y/o epidemia	Indisponibilidad de los servicios por falta de personal técnico	• Respaldo de personal y/o capacitación sobre las actividades realizadas por cada uno
26	Sismo	Perdida de información en el centro de datos inhouse	• Respaldo de copias de seguridad de la información (carpetas compartidas) en el servidor de backup
27	Sismo	Daño de los equipos de cómputo de la DRELM	• Respaldo de copias de seguridad de la información (carpetas compartidas) en el servidor de backup
28	Inundación y aniego en el Centro de Datos	Indisponibilidad del centro de datos por inundación o aniego en las instalaciones de la DRELM	• Cámaras de vigilancia en el interior del Centro de Datos
29	Inundación y aniego en el	Daño del centro de datos por falla en el equipo de aire acondicionado o ventilación del centro de datos	• Cámaras de vigilancia en el interior del Centro de Datos

N°	Amenaza	Riesgo	Control
	Centro de Datos		• Mantenimiento preventivo para equipos de aire acondicionado.
30	Incendio en el Centro de datos y/o equipos de cómputo	Daño del centro de datos por un corto circuito	• Cámaras de vigilancia en el interior del Centro de Datos • Mantenimiento preventivo de Tableros eléctrico y UPS. • Alarma contra incendios en el Centro de Datos
31	Incendio en el Centro de datos y/o equipos de cómputo	Daño de los equipos de cómputo de la DRELM por una mala conexión eléctrica	• Mantenimiento preventivo de Tableros eléctrico y UPS. • Alarma contra incendios en el Centro de Datos

6.3 ESCENARIOS DE RIESGO

Considerando los servicios de TI, y luego de realizar el análisis de riesgos, se han determinado los siguientes escenarios de riesgo:

N°	Escenario	Descripción
A	Destrucción e indisponibilidad del Centro de Datos	En este escenario se considera que los recursos informáticos alojados en el Centro de Datos se encuentran indisponibles a causa de la destrucción originada por un sismo, inundación, incendio, vandalismo, ataque terrorista o intento de denegación de servicios.
B	Indisponibilidad de servicios críticos por falla de hardware o software	En este escenario se considera la indisponibilidad de los servicios críticos causados por una falla física o lógica de los servidores, debido a su obsolescencia tecnológica.
C	Indisponibilidad en los servicios críticos por la ocurrencia de un ciberataque	En este escenario se considera la indisponibilidad de los sistemas y robo de información como resultado de un ciberataque.
D	Indisponibilidad en los servicios críticos por falla en la energía eléctrica en el Centro de Datos	En este escenario se considera que el suministro de energía eléctrica del centro de Datos se encuentre indisponible ocasionando la indisponibilidad de los servicios de tecnologías de la información y pérdida de comunicación en los equipos que conforman la infraestructura tecnológica.
E	Indisponibilidad de los servicios críticos por ausencia o indisponibilidad del personal critico	En este escenario se considera que no se encuentra disponible el personal necesario para la administración y gestión de la infraestructura tecnológica y servicios de tecnología, lo cual puede traer como consecuencia la indisponibilidad de los mismos
F	Indisponibilidad de los servicios críticos por	En este escenario se considera que los equipos de redes y comunicaciones se encuentren indisponibles como resultado de una falla física o

	falla en los equipos de comunicaciones	lógica, lo cual trae como consecuencia la caída de servicios informáticos y perdida de comunicación en los equipos que conforman la infraestructura tecnológica

6.4 ESTRATEGIAS DE RECUPERACIÓN

Se proponen las posibles soluciones de recuperación de los escenarios de riesgos, incluyendo estrategias preventivas y correctivas.

Se han seleccionado alternativas para los escenarios de amenaza identificados que cumplen con los tiempos de recuperación.

A continuación, se indican las posibles estrategias de recuperación:

a) Destrucción de los recursos informáticos alojados en el centro de datos como resultado de un sismo, inundación o incendio

- Implementar un Centro de Datos de contingencia en las instalaciones de un proveedor en la nube, además que en caso se presente un escenario de sismo, el proveedor también pueda proporcionar servicios de comunicaciones para el restablecimiento de los servicios críticos.
- Virtualizar los servidores físicos para mejorar los tiempos de recuperación en caso de falla de hardware de los servidores.
- Realizar copias de respaldo de instaladores de las aplicaciones, de software base, sistema operativo, utilitarios, etc
- Almacenar las copias de respaldo diarias en un ambiente separado del Centro de Datos
- Recomendar contratar el servicio de almacenamiento de las copias de respaldo a cargo de proveedor externo, con un periodo mínimo semanal de retiro de copias de respaldo hacia las instalaciones externas
- Asegurarse de contar con enlaces redundantes con el Centro de Datos de contingencia.
- Contar con switches de respaldo que como mínimo sean de capa 3 modelo OSI para uso de Core y Distribución
- Implementar sistema de extinción contra incendio en el Centro de Datos
- Eliminar todo material inflamable del ambiente de Centro de Datos y cuarto de UPS
- Contratar un servicio de mantenimiento preventivo y correctivo para el UPS y banco de baterías

b) Indisponibilidad de servidores críticos por falla de hardware o software Implementar alta disponibilidad en los servidores virtualizados

- Virtualizar los servidores físicos para mejorar los tiempos de recuperación en caso de falla de hardware de los servidores
- Contar con Acuerdos de Niveles de Servicio (SLA) con los proveedores para que en caso sea necesario, puedan sustituir de manera inmediata los servidores físicos
- Programación de revisiones anuales de obsolescencia tecnológica de las partes internas de los servidores informáticos, para realizar la renovación de las mismas, en caso se requiera.

c) Indisponibilidad en los servicios críticos por la ocurrencia de un ciberataque

- Mantener actualizado los sistemas operativos de los servidores y estaciones de trabajo
- Mantener actualizado el software de protección antivirus en cada servidor y estación de trabajo
- Mantener controles de seguridad perimetral como Firewall, AntiDDoS, UTM gestionado
- Desarrollar planes y capacitaciones de sensibilización en materia de seguridad de la información y buenas prácticas en el uso de los sistemas informáticos
- Mantener el monitoreo del rendimiento y consumo de los recursos en los servidores
- Realizar pruebas anuales de Hacking Ético de terceros especializados

d) Indisponibilidad en los servicios críticos por falla en la energía eléctrica en el Centro de Datos

- Contratar un servicio de mantenimiento preventivo y correctivo para el UPS, pozo a tierra y banco de baterías
- Implementar un tablero de transferencia automático (Bypass) en el centro de Datos para asegurar la continuidad eléctrica ante fallas del sistema de UPS
- Implementar un sistema de UPS redundante con circuitos independientes que alimenten a los servidores y equipos críticos del Centro de Datos
- Configurar el monitoreo remoto del UPS con alertas en caso de detectarse falla en el suministro eléctrico y/o banco de baterías
- Realizar el apagado de los equipos, mientras se cuente con energía del UPS
- Evaluar contar con un tablero de transferencia (Bypass) en el suministro eléctrico, para asegurar una mínima interrupción de energía ante trabajos de mantenimiento
- Evaluar la implementación de un generador eléctrico para proveer energía al Centro de Datos en casos de falla de la red eléctrica pública a cargo de servicio generales.

e) Indisponibilidad de los servicios críticos por ausencia o indisponibilidad del personal critico

- Eliminar la dependencia funcional de los puestos críticos, capacitando a un reemplazo para cada rol, de tal manera que pueda asumir las funciones en caso el personal principal se encuentre indispuesto
- Entrenar al personal de ETI en el proceso de recuperación de los servicios de TI. La capacitación debe ser planificada, estructurada y acorde con las exigencias de recuperación. El entrenamiento se debe evaluar para verificar que se ha logrado sus objetivos
- Elaborar un programa de vacaciones que garantice la presencia permanente del personal critico de los diferentes procesos de ETI, tales como soporte técnico, redes y comunicaciones, sistemas de información y bases de datos, así como seguridad de la información.

- Elaborar una base de datos de conocimiento, en caso el personal encargado de ciertos procedimientos, tanto principal, como de reemplazo se encuentren indispuestos.

f) Indisponibilidad de los servicios críticos por falla en los equipos de comunicaciones

- Contar con switches de respaldo que como mínimo seas de capa 3 de modelo OSI, almacenados en un ambiente separado del Centro de Datos
- Realizar copias de respaldo periódicas de la configuración de los equipos de comunicaciones
- Mantener los Acuerdos de Niveles de Servicio (SLA) con los proveedores para que en caso sea necesario, puedan sustituir de manera inmediata los equipos de comunicaciones del Centro de datos

Asimismo se precisa que para la contratación de los bienes y servicios que se requiera para la implementación del presente plan, el requerimiento del bien o servicio (adjuntando las especificaciones técnicas o términos de referencia, según sea el caso) deben ser remitidos a la Oficina de Administración, para que la Unidad de Logística continúe con el proceso de contratación correspondiente, de conformidad a la Ley N° 30225, Ley de Contrataciones del Estado (y modificatorias) y el Decreto Supremo N° 344-2018-EF, Reglamento de la Ley de contrataciones del Estado (y modificatorias)

6.5 PLAN DE RECUPERACIÓN

Una vez identificados los escenarios de riesgos, se desarrollan los Planes de Recuperación.

6.5.1 Invocación del plan

Esta sección define cuándo, cómo y por quien se pone en ejecución el proceso de recuperación de los servicios de TI que se encuentran en el Centro de Datos.

N°	Escenario	Detecta Situación	Estrategia	Ejecuta el plan	Autorizado para activar el plan
1	Destrucción e indisponibilidad del Centro de Datos	Personal de la DRELM	Activación del Manual de Continuidad Informática	Equipo de Tecnologías de información	Responsable de ETI
2	Indisponibilidad de servicios críticos por falla de hardware o software	Personal de la DRELM	Activación del Manual de Continuidad Informática	Equipo de Tecnologías de información	Responsable de ETI

3	Indisponibilidad en los servicios críticos por la ocurrencia de un ciberataque	Personal de la DRELM	Activación del Manual de Continuidad Informática	Equipo de Tecnologías de información	Responsable de ETI
4	Indisponibilidad en los servicios críticos por falla en la energía eléctrica en el Centro de Datos	Personal de la DRELM	Activación del Manual de Continuidad Informática	Equipo de Tecnologías de información	Responsable de ETI
5	Indisponibilidad de los servicios críticos por ausencia o indisponibilidad del personal critico	Personal de la DRELM	Activación del Manual de Continuidad Informática	Equipo de Tecnologías de información	Responsable de ETI
6	Indisponibilidad de los servicios críticos por falla en los equipos de comunicaciones	Personal de la DRELM	Activación del Manual de Continuidad Informática	Equipo de Tecnologías de información	Responsable de ETI

6.5.2 Notificación de Invocación del Manual

La notificación es responsabilidad del Responsable del Equipo de Tecnologías de Información de la DRELM, quien está autorizado para invocar el Manual e informar al personal de soporte de TI y Desarrollo de Software quienes encabezarán los grupos de recuperación que a su vez informarán a los miembros del grupo acerca del incidente y de las acciones a ser adoptadas. Así mismo se comunicará al Oficial de Seguridad de la Información o quien realice funciones similares, quien realizará el seguimiento de las acciones adoptadas y de su efectividad.

6.5.3 Plan de Contingencia y Recuperación de Servicios de TIC

El Manual de Recuperación de los servicios de Tecnología de la Información está alineado a los escenarios de mayor nivel de riesgo, identificados en la Matriz de Riesgos, los cuales serán abordados en planes independientes, tal como se indica en el siguiente cuadro:

N°	Escenario	Nivel de Riesgo	Plan de Recuperación
1	Destrucción e indisponibilidad del Centro de Datos	Alto	PR-01
2	Indisponibilidad de servicios críticos por falla de hardware o software	Alto	PR-02

3	Indisponibilidad en los servicios críticos por la ocurrencia de un ciberataque	Alto	PR-03
4	Indisponibilidad en los servicios críticos por falla en la energía eléctrica en el Centro de Datos	Alto	PR-04
5	Indisponibilidad de los servicios críticos por ausencia o indisponibilidad del personal critico	Alto	PR-05
6	Indisponibilidad de los servicios críticos por falla en los equipos de comunicaciones	Alto	PR-06

Los planes de recuperación se encuentran en el **Anexo 01.**

6.6 PLAN DE PRUEBAS

6.6.1 Propósito y alcance

El propósito del Plan de Pruebas es validar las actividades del Manual de Continuidad Informática, las capacidades del personal de TI en la ejecución del manual y verificar que el desarrollo de las actividades sea correcto.
El alcance de las pruebas del Manual de Continuidad Informática es probar el restablecimiento de la operatividad de los recursos que forman parte de los escenarios de riesgo.

6.6.2 Escenarios y estrategias

Los escenarios de pruebas deben simular la inhabilitación de las operaciones en el Centro de Datos con el fin de realizar una prueba que contemple la ejecución de los planes de acción descritos en Manual de Continuidad Informática, es importante que estas pruebas se coordinen con las áreas usuarias.

En la etapa de planificación de las pruebas se especifica los aspectos que debe cubrir cada escenario:

Prueba:	Prueba de Conocimiento del Manual de Continuidad Informática
Responsable	Oficial de Seguridad de Información o quién realice funciones similares
Periodicidad	Anual
Descripción de la Prueba	
Este escenario consiste en evaluar mediante un test escrito el nivel de conocimiento del equipo sobre el Manual de Continuidad Informática, así como sus responsabilidades. **Anexo 02** **Post de la prueba** El responsable debe elaborar un informe de los resultados obtenidos que contenga los siguientes puntos: • Tipo de prueba:	

- Día:
- Duración:
- Participantes:
- Resultados:
- Acciones Correctivas:

De ser necesario se deben actualizar el Manual de Continuidad Informática con las lecciones aprendidas de esta prueba.

Prueba:	Prueba de Contingencia de los servicios informáticos
Responsable	Técnico en Redes y Comunicaciones Oficial de Seguridad de Información o quién realice funciones similares
Periodicidad	Anual

Descripción de la Prueba

Este escenario consiste en simular la caída de los servidores poniendo en marcha la activación de servidores de contingencia (máquinas virtuales o hosting alterno)

Pre de la prueba

- Informar a las áreas usuarias los horarios y fecha de indisponibilidad de los servicios de TI relacionados con los servidores involucrados
- Solicitar la participación de los servidores civiles de las oficinas para realizar pruebas en el escenario de contingencia
- Coordinar con proveedores de servidores o hosting, la fecha de realización de la prueba
- Realizar copias de respaldo de las máquinas virtuales alojadas en el Storage principal

El día de la prueba

- Confirmar la asistencia del personal de TI
- Descargar los sistemas informáticos de la plataforma virtualizada
- Apagar / desconectar el servidor de base de datos (SQL Server y/o MySQL
- Apagar los servidores involucrados
- Realizar la actividad descrita en el Manual de Contingencia Informático
- Realizar pruebas de conectividad de los sistemas, así como al servidor de archivos, acceso a internet y correo electrónico
- Documentar todos los problemas identificados. Usar el Anexo 03

Post de la prueba

Los responsables deben elaborar un informe de los resultados obtenidos en el Anexo 03 que contenga los siguientes puntos:

- Tipo de prueba:
- Día:
- Duración:
- Participantes:
- Resultados:
- Acciones Correctivas:

De ser necesario se deben actualizar el Manual de Continuidad Informático con las lecciones aprendidas de esta prueba.

Prueba:	Prueba de falta de suministro eléctrico al Centro de Datos
Responsable	Técnico en Redes y Comunicaciones Oficial de Seguridad de Información o quién realice funciones similares
Periodicidad	Anual
Descripción de la Prueba	
Este escenario consiste en simular la falta de energía eléctrica en el Centro de Datos. Pre de la prueba • Informar a las áreas usuarias la fecha y ventanas horarias de indisponibilidad de los servicios de TI • Solicitar la participación de los servidores civiles de las oficinas para realizar pruebas en el escenario de contingencia • Informar a la Unidad de Logística la fecha de realización de la prueba • Validar la existencia de copias de respaldo de las máquinas virtuales, equipos de comunicaciones y equipos de seguridad perimetral. El día de la prueba • Confirmar la asistencia del personal de TI • Baja del suministro eléctrico en el tablero principal del Centro de Datos • Supervisión el estado de carga de UPS • Apagado progresivo de servidores y equipamiento de comunicaciones • Validar el apagado total de los equipos de Centro de Datos • Realizar las actividades descritas en el Plan de recuperación PR-05 del presente Manual de Contingencia Informática • Realizar pruebas de conectividad de los sistemas, así como al servidor de archivos, acceso a internet y correo electrónico • Documentar todos los problemas identificados. Usar el Anexo 03. Post de la prueba Los responsables deben elaborar un informe de los resultados obtenidos en el Anexo 03 que contenga los siguientes puntos: • Tipo de prueba: • Día • Duración • Participantes: • Resultados: • Acciones Correctivas: De ser necesario se deben actualizar el Manual de Continuidad Informático con las lecciones aprendidas de esta prueba	

6.7 PLAN DE COMUNICACIÓN Y CAPACITACIÓN

Las previsiones para las situaciones de contingencia no pueden considerarse fiables hasta que se hayan ejercitado. La comunicación y sensibilización hacia el personal de la DRELM ayudará a mantener y mejorar las acciones de respuesta ante eventos que generen indisponibilidad de los servicios de TI o aplicaciones tecnológicas de mayor criticidad para la DRELM.

Para la comunicación y capacitación se consideran los siguientes aspectos:

PERSONAL:

- Los especialistas del Equipo de Tecnologías de Información
- El personal clave que hace uso de los sistemas de información (Servidores Civiles DRELM)

TEMAS:

- Responsabilidades en el Manual de Continuidad Informática
- Procedimientos de recuperación
- Pruebas de recuperación
- Mejora continua del Manual de Continuidad Informática

Las capacitaciones deberán ser ejecutadas en grupos diferentes, considerando en una de ellos al personal de ETI y en el otro grupo al personal clave (Servidores Civiles DRELM) de las aplicaciones y/o servicios informáticos.

La DRELM ha establecido las siguientes actividades como parte del plan de comunicación y capacitación, las mismas que deben ejecutarse por lo menos una vez al año debiendo difundir las actualizaciones del Manual de Continuidad informático y responsabilidades del personal sobre reactivar las operaciones en caso de interrupción:

Actividad	Descripción
Capacitación	Preparar una presentación que resuma el Manual de Continuidad Informática a) Imprimir copias o compartirlas virtualmente el manual para que sean distribuidas durante la capacitación b) Convocar al personal mencionado para revisar el Manual de Continuidad Informática c) Desarrollar la capacitación al personal de ETI y personal clave (Servidores Civiles DRELM) d) Con la retroalimentación obtenida, evaluar la modificación del Manual de Continuidad Informática
Evaluación	a) Preparar una evaluación escrita de conocimiento para cada persona del equipo del Manual de Continuidad Informática para verificar las responsabilidades que tienen b) Con la retroalimentación obtenida, evaluar la modificación del Manual de Continuidad Informática

7. ANEXOS

7.1 Anexo N°01 – Planes de recuperación
7.2 Anexo N°02 – Formato para la evaluación de conocimiento del Plan de Contingencia
7.3 Anexo N°03 – Formato de control de certificaciones de las pruebas

ANEXO 01: PLANES DE RECUPERACIÓN

Plan de Recuperación	PR-01
Escenario	En este escenario se considera que los recursos informáticos alojados en el Centro de Datos no se encuentran disponibles a causa de la destrucción originada por un incendio, sismo o inundación.
Estrategia	1. Implementar un centro de datos de contingencia en las instalaciones de un proveedor con servicios en la nube o de una institución educativa perteneciente a la DRELM, además que en caso se presente un escenario de contingencia, el proveedor también pueda proporcionar servicios de comunicaciones para el restablecimiento de los servicios críticos. 2. Virtualizar los servidores físicos para mejorar los tiempos de recuperación en caso de falla de hardware de los servidores. 3. Realización de copias de seguridad de instaladores de las aplicaciones, software base, sistema operativo, utilitarios, etc. 4. Implementar enlaces redundantes con el Centro de Datos alterno. 5. Contar con switches de respaldo, de preferencia sean como mínimo de capa 3 del modelo OSI
Servicios TI	Analizando el escenario de riesgo y considerando la lista de servicios y activos, se determina que los servicios de TI a recuperar se pueden agrupar y recuperar en el siguiente orden de prioridad: 1. Red de datos (Equipo de comunicaciones) 2. Internet y seguridad perimetral 3. Servicio de Autenticación de Red 4. Sistema de almacenamiento (Storage) 5. Servidores Físicos 6. Sistema de Virtualización (Hipervisor) 7. Servidores Virtuales 8. Base de datos y aplicativos informáticos

1. PLAN DE ACCIÓN – Red de Datos (Equipo de comunicaciones)

Componentes:

- Switch Core, Switch de distribución
- Enlace de datos con proveedor en la nube

Etapas:

a) Antes de la Contingencia

Ejecutante	Actividad
Responsable de ETI Técnico en Redes y Comunicaciones	1. Contratar servicios de enlace de datos y servicio de enlace de contingencia hacia el Centro de Datos de un proveedor de hosting, donde se recuperarán los servicios críticos.
Técnico en Redes y Comunicaciones	2. Realizar copias de respaldo mensuales de la configuración de los equipos de comunicación
Técnico en Redes y Comunicaciones	3. Mantener actualizado el diagrama de conexiones físicas y las ubicaciones de los equipos
Técnico en Redes y Comunicaciones	4. Mantener un switch administrable de contingencia, que mínimo sea de capa 3 del modelo OSI
Responsable de ETI	5. Revisar el cumplimiento de las copias de respaldo y operatividad del equipo de contingencia.

b) Durante la Contingencia

Ejecutante	Actividad
Técnico en Redes y Comunicaciones	1. Revisar la operatividad del Switch Core y equipos de comunicación del Centro de Datos. En caso de estar inoperativos realizar el punto 2, caso contrario ir al punto 3.
Técnico en Redes y Comunicaciones	2. Realizar las configuraciones de red en el Switch capa 3 de contingencia
Técnico en Redes y Comunicaciones	3. Verificar la conectividad con el Centro de Datos de contingencia.

c) Después de la Contingencia

Ejecutante	Actividad
Técnico en Redes y Comunicaciones	1. Gestionar con el proveedor correspondiente la reposición de los recursos afectados.
Técnico en Redes y Comunicaciones	2. Configurar el hardware nuevo o reparado
Responsable de ETI	3. Verificar el cumplimiento del procedimiento de recuperación

2. PLAN DE ACCIÓN – Internet y Seguridad perimetral

Componentes:

- UTM (parte del servicio de Internet y Seguridad Perimetral)

Etapas:

a) Antes de la Contingencia

Ejecutante	Actividad
Técnico en Redes y Comunicaciones	1. Supervisar que el proveedor del servicio de internet este realizando respaldos periódicos de la configuración de los equipos UTM
Técnico en Redes y Comunicaciones	2. Mantener actualizado un diagrama de conexiones de los equipos que estén en el Centro de Datos y la documentación con la relación de políticas implementadas
Responsable de ETI	3. Revisar que se ejecute el respaldo de información

b) Durante la Contingencia

Ejecutante	Actividad
Técnico en Redes y Comunicaciones	1. Reportar al proveedor del servicio de internet y Seguridad Perimetral la falla en el servicio
Técnico en Redes y Comunicaciones	2. Revisar el correcto funcionamiento de las políticas de navegación en el servicio de Internet de Contingencia
Técnico en Redes y Comunicaciones	3. Verificar la comunicación vía Internet hacia los servicios publicados

c) Después de la Contingencia

Ejecutante	Actividad
Técnico en Redes y Comunicaciones	1. Gestionar con el proveedor del servicio de internet correspondiente la reposición de los recursos afectados
Técnico en Redes y Comunicaciones	2. Revisar el correcto funcionamiento del servicio de internet
Técnico en Redes y Comunicaciones	3. Verificar la comunicación desde Internet hacia los servicios publicados.

3. PLAN DE ACCIÓN – Servicio de Autenticación de Red

Componentes:

- Servidor virtual del directorio activo (Dominio Principal y secundario)
- Sistema de almacenamiento (Storage)

Etapas:

a) Antes de la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Responsable de ETI	1. Cumplir con el procedimiento de respaldo de la información
Especialista en Sistemas e Informática Responsable de ETI	2. Guardar una copia de respaldo en un servidor local y enviar una copia el lugar de custodia
Responsable de ETI	3. Revisar que se ejecute el respaldo de la información

b) Durante la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Responsable de ETI	1. Restablecer la copia de respaldo del servidor de directorio activo
Técnico en Redes y Comunicaciones	2. Configurar parámetros de red y verificar
Especialista en Sistemas e Informática Responsable de ETI	3. Realizar pruebas sobre el servicio de directorio activo

c) Después de la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Responsable de ETI	1. Gestionar con el proveedor correspondiente la reposición de los recursos afectados
Especialista en Sistemas e Informática Responsable de ETI	2. Realizar una copia de respaldo del Directorio Activo de Contingencia
Especialista en Sistemas e Informática Responsable de ETI	3. Restaurar el Directorio Activo de Contingencia en el Directorio Activo de producción recuperado
Responsable de ETI	4. Verificar el cumplimiento del procedimiento de recuperación

4. PLAN DE ACCIÓN – Sistema de almacenamiento (Storage)

Componentes:

- Sistema de almacenamiento (Storage)

Etapas:

a) Antes de la Contingencia

Ejecutante	Actividad
Técnico en Redes y Comunicaciones Responsable de ETI	1. Mantener copias de respaldo de la configuración del sistema de almacenamiento
Técnico en Redes y Comunicaciones Responsable de ETI	2. Cumplir con el Respaldo de la Información
Técnico en Redes y Comunicaciones Responsable de ETI	3. Mantener actualizada la copia en el sistema de almacenamiento de contingencia (Storage de contingencia en Hosting)
Técnico en Redes y Comunicaciones	4. Mantener actualizado el diagrama de la configuración y conexiones del sistema de almacenamiento
Responsable de ETI	5. Revisar que se ejecute el respaldo de la información

b) Durante la Contingencia

Ejecutante	Actividad
Técnico en Redes y Comunicaciones Responsable de ETI	1. Revisar la operatividad del sistema almacenamiento de contingencia (Storage) y promoverlo como sistema de almacenamiento principal
Técnico en Redes y Comunicaciones	2. Configurar parámetros de red y verificar
Técnico en Redes y Comunicaciones Responsable de ETI	3. Verificar la comunicación desde los servidores
Responsable de ETI	4. Realizar pruebas de los sistemas de información

c) Después de la Contingencia

Ejecutante	Actividad
Técnico en Redes y Comunicaciones Responsable de ETI	1. Gestionar con el proveedor correspondiente la reposición de los recursos afectados
Técnico en Redes y Comunicaciones Responsable de ETI	2. Configurar el hardware y software de los recursos afectados

Técnico en Redes y Comunicaciones Responsable de ETI	3. Actualizar las configuraciones del Sistema de almacenamiento (Storage)
Responsable de ETI	4. Realizar pruebas sobre las aplicaciones involucradas
Responsable de ETI	5. Verificar el cumplimiento del procedimiento de recuperación

5. PLAN DE ACCIÓN – Servidores Físicos

Componentes:

- Respaldo de información
- Licencias de sistemas operativos de servidores
- Conexión al sistema de almacenamiento (Storage)

Etapas:

a) Antes de la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Responsable de ETI	1. Cumplir con el respaldo de la información
Especialista en Sistemas e Informática Responsable de ETI	2. Almacenar una copia de respaldo en un servidor local y/o enviar una copia de respaldo al proveedor (en caso se contrate) de custodia
Responsable de ETI	3. Revisar que se ejecute el respaldo de la información

b) Durante la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Responsable de ETI	1. Realizar la restauración del servidor físico en un servidor virtual
Técnico en Redes y Comunicaciones	2. Configurar parámetros de red y verificación
Especialista en Sistemas e Informática Responsable de ETI	3. Realizar pruebas de los servicios en el servidor virtual
Responsable de ETI	4. Verificar el cumplimiento del procedimiento de recuperación

c) Después de la Contingencia

Ejecutante	Actividad
Técnico en Redes y Comunicaciones Responsable de ETI	1. Gestionar con el proveedor correspondiente la reposición de los recursos afectados

Especialista en Sistemas e Informática Responsable de ETI	2. Coordinar con el dueño del proceso soportado por el sistema de información recuperado, para identificar la información no recuperada posterior al último respaldo de información
Especialista en Sistemas e Informática Responsable de ETI	3. En caso soliciten, ejecutar el pase a producción para actualización de información
Responsable de ETI	4. Realizar pruebas sobre los servicios del servidor virtual
Responsable de ETI	5. Verificar el cumplimiento del procedimiento de recuperación

6. PLAN DE ACCIÓN – Sistema de Virtualización (Hipervisor)

Componentes:

- Servidores Host
- Hipervisor: VmWare vSphere Client
- Conexión al Sistema de almacenamiento (Storage)

Etapas:

a) Antes de la Contingencia

Ejecutante	Actividad
Responsable de ETI	1. Contratar servicio de hosting bajo demanda, asegurando la disponibilidad de máquinas virtuales para ser activadas en un escenario de contingencia
Especialista en Sistemas e Informática Responsable de ETI	2. Cumplir con el respaldo de la información
Especialista en Sistemas e Informática Responsable de ETI	3. Guardar una copia de respaldo en un servidor local y enviar otra copia al lugar de custodia
Responsable de ETI	4. Revisar que se ejecute el respaldo de la información

b) Durante la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Responsable de ETI	1. Comunicar a proveedor de hosting la activación de la contingencia y solicitar el aprovisionamiento de los recursos para las máquinas virtuales necesarias

Técnico en Redes y Comunicaciones	2. Verificar la conectividad con el sistema de almacenamiento (Storage)
Especialista en Sistemas e Informática Responsable de ETI	3. Configurar la plataforma de Virtualización VmWare vSphere Client (Hipervisor)
Técnico en Redes y Comunicaciones	4. Verificar la comunicación a nivel de red de cada Hipervisor
Responsable de ETI	5. Verificar el cumplimiento del procedimiento de recuperación

c) Después de la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Responsable de ETI	1. Gestionar con el proveedor correspondiente la reposición de los recursos afectados
Especialista en Sistemas e Informática Técnico en Redes y Comunicaciones Responsable de ETI	2. Configurar la plataforma de Virtualización en el recurso nuevo o reparado
Técnico en Redes y Comunicaciones Responsable de ETI	3. Actualizar las configuraciones de red de cada Hipervisor
Responsable de ETI	4. Verificar el cumplimiento del procedimiento de recuperación

7. PLAN DE ACCIÓN – Servidores Virtuales

Componentes:

- Máquinas virtuales
- Licencias de sistemas operativos de servidores
- Conexión al Sistema de almacenamiento (Storage)

Etapas:

a) Antes de la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Responsable de ETI	1. Cumplir con el Respaldo de la Información
Especialista en Sistemas e Informática Responsable de ETI	2. Almacenar una copia de respaldo en un servidor local y/o enviar una copia de respaldo al proveedor (en caso se contrate) de custodia
Responsable de ETI	3. Revisar que se ejecute el Respaldo de Información

b) Durante la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Responsable de ETI	1. Realizar la restauración del servidor virtual
Técnico en Redes y Comunicaciones	2. Configurar parámetros de red y verificación
Especialista en Sistemas e Informática Responsable de ETI	3. Realizar pruebas de los servicios del servidor virtual
Responsable de ETI	4. Verificar el cumplimiento del procedimiento de recuperación

c) Después de la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Responsable de ETI	1. Coordinar con el dueño del proceso soportado por el sistema de información recuperado, para identificar la información no recuperada posterior al último respaldo de información
Especialista en Sistemas e Informática Responsable de ETI	2. Ejecutar el pase a producción para actualización de información
Especialista en Sistemas e Informática Responsable de ETI	3. Realizar pruebas sobre los servicios del servidor virtual
Responsable de ETI	4. Verificar el cumplimiento del procedimiento de recuperación

8. PLAN DE ACCIÓN – Base de datos

Componentes:

- Servidor
- Conexión al Sistema de almacenamiento (Storage)

Etapas:

a) Antes de la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Especialista en Sistemas de Información Analista de Sistemas Analista Programador	1. Cumplir con el procedimiento de respaldo de la información
Especialista en Sistemas e Informática	2. Monitorear el correcto funcionamiento del motor de base de datos

Especialista en Sistemas de Información Analista de Sistemas Analista Programador	
Especialista en Sistemas e Informática Especialista en Sistemas de Información Analista de Sistemas Analista Programador	3. Guardar una copia de respaldo en un servidor local y enviar una copia el lugar de custodia
Responsable de ETI	4. Revisar que se ejecute el respaldo de la información

b) Durante la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Especialista en Sistemas de Información Analista de Sistemas Analista Programador	1. Activar una máquina virtual como parte del hosting, restaurar la base de datos y sistemas web
Especialista en Sistemas e Informática Especialista en Sistemas de Información Analista de Sistemas Analista Programador	2. Validar que la información puede ser consultada
Responsable de ETI	3. Verificar el cumplimiento del procedimiento de recuperación

c) Después de la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Técnico en Redes y Comunicaciones	1. Gestionar con el proveedor correspondiente la reposición de los recursos afectados
Especialista en Sistemas e Informática Especialista en Sistemas de Información Analista de Sistemas Analista Programador	2. Instalar recursos afectados
Especialista en Sistemas e Informática Especialista en Sistemas de Información Analista de Sistemas Analista Programador	3. Configurar la base de datos y sistemas web

Especialista en Sistemas e Informática Especialista en Sistemas de Información Analista de Sistemas Analista Programador	4. Validar que la información puede ser consultada en el hardware nuevo o reparado
Responsable de ETI	5. Verificar el cumplimiento del procedimiento de recuperación

Plan de Recuperación	**PR-02**
Escenario	En este escenario se considera la indisponibilidad de los servicios críticos causados por una falla física o lógica de los servidores.
Estrategia	1. Virtualizar los servidores físicos para mejorar los tiempos de recuperación en caso de falla de hardware. 2. Contar con Acuerdos de Niveles de Servicio (SLA) con los proveedores para que en caso sea necesario, puedan sustituir de manera inmediata los servidores físicos y central telefónica. 3. Implementar un procedimiento de respaldos 4. Programación de dos revisiones anuales de obsolescencia tecnológica de las partes internas de los servidores informáticos, para realizar la renovación de las mismas, en caso se requiera.
Servicios TI	1. Servidores Físicos

1. PLAN DE ACCIÓN – Servidores Físicos

Componentes:

- Servidores
- Copias de Respaldo de información
- Licencias de sistemas operativos de servidores
- Conexión al Sistema de almacenamiento (Storage)

Etapas:

a) Antes de la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Técnico en Redes y Comunicaciones Responsable de TI	1. Cumplir con el procedimiento de respaldo de la información
Especialista en Sistemas e Informática Técnico en Redes y Comunicaciones	2. Almacenar una copia de respaldo en un servidor local y enviar una copia de respaldo al proveedor de custodia

Responsable de TI	
Responsable de ETI	3. Revisar que se ejecute el respaldo de la información

b) Durante la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Técnico en Redes y Comunicaciones Responsable de TI	1. Realizar la restauración del servidor físico en un servidor virtual
Técnico en Redes y Comunicaciones	2. Configurar parámetros de red y verificación
Especialista en Sistemas e Informática Técnico en Redes y Comunicaciones Responsable de TI	3. Realizar pruebas de los servicios en el servidor virtual
Especialista en Sistemas e Informática Responsable de TI	4. Revisar la seguridad de la información en la etapa de contingencia

c) Después de la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Técnico en Redes y Comunicaciones Responsable de TI	1. Gestionar ante con el proveedor correspondiente la reposición de los recursos afectados
Especialista en Sistemas e Informática Técnico en Redes y Comunicaciones Responsable de TI	2. Coordinar con el dueño del proceso soportado por el sistema de información recuperado, para identificar la información no recuperada posterior al último respaldo de información
Especialista en Sistemas e Informática Responsable de TI	3. En caso lo soliciten, ejecutar el pase a producción para actualización de información
Especialista en Sistemas e Informática Responsable de TI	4. Realizar pruebas sobre los servicios del servidor virtual
Responsable de ETI	5. Verificar el cumplimiento del procedimiento de recuperación

Plan de Recuperación	PR-03
Escenario	Indisponibilidad en los servicios críticos por la ocurrencia de un ciberataque
Estrategia	1. Mantener actualizado los sistemas operativos de los servidores y estaciones de trabajo 2. Mantener actualizado el software de protección antivirus en cada servidor y estación de trabajo 3. Mantener controles de seguridad perimetral como Firewall, AntiDDoS, UTM 4. Desarrollar planes de sensibilización en materia de seguridad de la información y buenas prácticas en el uso de los sistemas informáticos 5. Realizar el monitoreo del rendimiento y consumo de los recursos en los servidores 6. Realizar pruebas anuales de Hacking Éticos de terceros especializados
Servicios TI	Analizando el escenario de riesgo y considerando la lista de servicios y activos, se determina el orden de recuperación de los siguientes servicios de TI: 1. Sistema de Almacenamiento (Storage) 2. Bases de Datos 3. Sistemas de Información

1. PLAN DE ACCIÓN – Sistema de Almacenamiento (Storage)

Componentes:

- Servidores
- Sistema de almacenamiento (Storage)

Etapas:

a) Antes de la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Responsable de TI	1. Mantener la copia de respaldo del sistema de almacenamiento
Especialista en Sistemas e Informática Técnico en Redes y Comunicaciones Responsable de TI	2. Mantener actualizada la copia en el sistema de almacenamiento de contingencia (Storage de contingencia en Hosting)
Responsable de ETI	3. Supervisar el cumplimiento de las copias de respaldo

b) Durante la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Técnico en Redes y Comunicaciones Responsable de TI	1. Aislar los sistemas de almacenamiento
Especialista en Sistemas e Informática Técnico en Redes y Comunicaciones Responsable de TI	2. Comunicar al proveedor del servicio de seguridad gestionada sobre el suceso para que identifique la fuente y otros posibles equipos comprometidos
Especialista en Sistemas e Informática Técnico en Redes y Comunicaciones Responsable de TI	3. Revisar el estado del sistema de almacenamiento de contingencia y en caso no se encuentre comprometido será promovido como sistema de almacenamiento principal en cuanto el proveedor de software antivirus y/o de seguridad gestionada hayan aislado la fuente del ataque
Especialista en Sistemas e Informática Responsable de TI	4. En caso ambos sistemas de almacenamiento se encuentren comprometidos se deberá restaurar la última copia de respaldo en uno de los sistemas de almacenamiento
Especialista en Sistemas e Informática Técnico en Redes y Comunicaciones Responsable de TI	5. Validar con el proveedor antimalware y/o proveedor de seguridad gestionada sobre la factibilidad de habilitación del sistema de almacenamiento
Técnico en Redes y Comunicaciones Responsable de TI	6. Realizar la habilitación de la comunicación hacia el sistema de almacenamiento
Especialista en Sistemas e Informática Técnico en Redes y Comunicaciones Responsable de TI	7. Gestionar las pruebas con los usuarios principales de los sistemas de información
Técnico en Redes y Comunicaciones Responsable de TI	8. Gestionar las pruebas sobre las unidades de red
Responsable de TI	9. Revisar los controles principales de seguridad configurados para la contingencia

c) Después de la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Técnico en Redes y Comunicaciones Responsable de TI	1. Realizar la configuración del sistema de almacenamiento de contingencia (replicación)
Especialista en Sistemas e Informática Técnico en Redes y Comunicaciones Responsable de TI	2. Actualizar las configuraciones del Sistema de almacenamiento (Storage)

2. PLAN DE ACCIÓN – Base de Datos

Componentes:
Servidor de base de datos
Conexión al Sistema de almacenamiento (Storage)

Etapas:

a) Antes de la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Especialista en Sistemas de Información Analista en Sistemas Analista Programador	1. Cumplir con el procedimiento de respaldo de información (base de datos y sistemas web)
Especialista en Sistemas e Informática Especialista en Sistemas de Información	2. Mantener actualizado los parches de seguridad en los servidores
Especialista en Sistemas e Informática Responsable de TI	3. Guardar una copia de respaldo en un servidor local y enviar otra copia al proveedor de custodia
Responsable de ETI	4. Supervisar el cumplimiento de las actividades 1, 2 y 3 establecidas en esta etapa “Antes de la contingencia”

b) Durante la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Especialista en Sistemas de Información	1. Aislar el servidor de base de datos afectado

Técnico en Redes y Comunicaciones Responsable de TI	2. Comunicar al proveedor del Servicio Antimalware y/o al proveedor del Servicio de Seguridad Gestionada sobre el suceso para que identifique la fuente y otros posibles equipos comprometidos
Especialista en Sistemas e Informática Especialista en Sistemas de Información	3. Evaluar el nivel de compromiso en el servidor y posibilidad de restablecerlo
Especialista en Sistemas e Informática Especialista en Sistemas de Información	4. Para el caso donde el servidor no pueda restablecerse, deberá reinstalarse
Especialista en Sistemas e Informática Especialista en Sistemas de Información	5. Levantar la copia de respaldo en el servidor de base de datos reinstalado
Especialista en Sistemas e Informática Especialista en Sistemas de Información Técnico en Redes y Comunicaciones Responsable de TI	6. Realizar las configuraciones necesarias para la comunicación entre la base de datos y storage
Especialista en Sistemas e Informática Especialista en Sistemas de Información Analista de Sistemas Analista Programador	7. Gestionar las pruebas con los usuarios principales de los sistemas de información
Responsable de ETI	8. Supervisar el cumplimiento de las actividades durante la contingencia
Especialista en Sistemas e Informática Responsable de ETI	9. Revisar los controles principales de seguridad para la configuración en contingencia

c) Después de la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Especialista en Sistemas de Información	1. Revisar el funcionamiento, para identificar si existen cambios que no han sido recuperados porque no se encontraban configurados en la copia de respaldo y solicitar el pase a producción de base de datos en caso corresponda
Especialista en Sistemas e Informática	2. Ejecutar el pase a producción con los cambios solicitados

Especialista en Sistemas de Información Analista de Sistemas Analista Programador	
Especialista en Sistemas e Informática Especialista en Sistemas de Información Analista de Sistemas Analista Programador	3. Validar que la información puede ser consultada en el servidor configurado
Especialista en Sistemas e Informática Especialista en Sistemas de Información Analista de Sistemas Analista Programador	4. Gestionar las pruebas con los usuarios principales de los sistemas de información
Responsable de ETI	5. Supervisar el cumplimiento de las actividades 2,3 y 4
Especialista en Sistemas e Informática Responsable de ETI	6. Revisar el restablecimiento de los controles de seguridad

3. PLAN DE ACCIÓN – Sistemas de información

Componentes:
Código fuente de aplicaciones
Conexión al Sistema de almacenamiento (Storage)

Etapas:

a) Antes de la Contingencia

Ejecutante	Actividad
Especialista en Sistemas de Información Analista de Sistemas Analista Programador	1. Mantener el registro de cambios y versiones del código fuente de las aplicaciones
Especialista en Sistemas e Informática Especialista en Sistemas de Información Analista de Sistemas Analista Programador	2. Cumplir con el respaldo de información (servidores de aplicaciones, códigos fuente de las aplicaciones)
Especialista en Sistemas e Informática Especialista en Sistemas de Información Analista de Sistemas Analista Programador	3. Revisar que el antimalware instalado en los servidores se encuentre actualizado

Especialista en Sistemas e Informática Especialista en Sistemas de Información Analista de Sistemas Analista Programador	4. Mantener actualizado los parches de seguridad en servidores
Responsable de ETI	5. Supervisar el cumplimiento de las actividades 1, 2, 3 y 4 establecidas en esta etapa “Antes de la Contingencia”

b) Durante la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Técnico en Redes y Comunicaciones Responsable de ETI	1. Aislar el servidor afectado
Especialista en Sistemas e Informática Técnico en Redes y Comunicaciones Responsable de ETI	2. Comunicar al proveedor del servicio antimalware y/o proveedor del servicio de seguridad gestionada sobre el suceso para que identifique la fuente y otros posibles equipos comprometidos
Especialista en Sistemas e Informática Técnico en Redes y Comunicaciones Responsable de ETI	3. Validar con el proveedor antimalware y/o proveedor de seguridad gestionada sobre la factibilidad de recuperación del equipo(s) o servicio(s) comprometido(s)
Especialista en Sistemas e Informática Responsable de ETI	4. Para el caso donde el servicio o equipo comprometido no pueda restablecerse, se deberán levantar las copias de respaldo de los servidores más recientes
Especialista en Sistemas e Informática Especialista en Sistemas de Información Técnico en Redes y Comunicaciones Responsable de TI	5. Realizar las configuraciones necesarias para la comunicación con la base de datos y storage
Especialista en Sistemas e Informática Especialista en Sistemas de Información Analista de Sistemas Analista Programador	6. Gestionar las pruebas con los usuarios principales de los sistemas de información

Especialista en Sistemas e Informática Responsable de ETI	7. Revisar los controles principales de seguridad para la configuración de contingencia

c) Después de la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Especialista en Sistemas de Información	1. Coordinar con el dueño del proceso soportado por el sistema de información, para identificar si existen cambios que no han sido recuperados porque no se encontraban configurados en la copia de respaldo
Especialista en Sistemas e Informática Especialista en Sistemas de Información Analista de Sistemas Analista Programador	2. En caso lo soliciten, ejecutar el pase a producción para actualización de información
Especialista en Sistemas e Informática Especialista en Sistemas de Información Analista de Sistemas Analista Programador	3. Realizar pruebas sobre la aplicación
Responsable de ETI	4. Supervisar el cumplimiento de la actividad 1, 2 y 3

Plan de Recuperación	**PR-04**
Escenario	En este escenario se considera que el suministro de energía eléctrica del Centro de Datos se encuentre indisponible ocasionando la indisponibilidad de los servicios de tecnologías de la información y pérdida de comunicación en los equipos que conforman la infraestructura tecnológica
Estrategia	1. Contratar un servicio de mantenimiento preventivo y correctivo para el UPS y banco de baterías 2. Implementar un tablero de transferencia automático (Bypass) en el Centro de Datos para asegurar la continuidad eléctrica ante fallas del sistema de UPS 3. Implementar un sistema de UPS redundante con circuitos independientes que alimenten a los servidores y equipos críticos del Centro de Datos 4. Configurar el monitoreo remoto del UPS con alertas en caso de detectarse falla en el suministro eléctrico y/o banco de baterías 5. Realizar el apagado de los equipos en forma ordenada 6. Implementar un tablero de transferencia (Bypass) en el suministro eléctrico, para asegurar una mínima interrupción de energía ante trabajos de mantenimiento. 7. Evaluar e implementar un generador eléctrico para proveer energía al Centro de Datos en casos de falla de la red eléctrica publica
Servicios TI	Analizando el escenario de riesgo, mientras se cuenta con energía del UPS, se debe realizar el apagado de los equipos. Una vez que retorne la energía eléctrica se realizara el encendido de los equipos en el siguiente orden: 1. Red de datos (Equipos de comunicaciones) 2. Internet y Seguridad Perimetral 3. Sistema de almacenamiento (Storage) 4. Sistema de Virtualización (Hipervisor) 5. Servicio de Autenticación de Red 6. Base de datos 7. Servidores Virtuales 8. Servidores Físicos

1. PLAN DE ACCIÓN – Red de Datos (Equipos de comunicaciones)

Componentes:

Switches Core, Switches de Distribución
Enlace de datos con el servidor del proveedor

Etapas:

a) Antes de la Contingencia

Ejecutante	Actividad
Técnico en Redes y Comunicaciones	1. Realizar copias de respaldo mensuales de la configuración de los equipos de comunicación
Técnico en Redes y Comunicaciones	2. Mantener actualizado el diagrama de conexiones físicas y las ubicaciones de los equipos
Técnico en Redes y Comunicaciones	3. Mantener un switch administrable de contingencia, que mínimo sea de capa 3 del modelo OSI
Responsable de ETI	4. Revisar el cumplimiento de las copias de respaldo y de la operatividad del equipo de contingencia.

b) Durante la Contingencia

Ejecutante	Actividad
Técnico en Redes y Comunicaciones	1. Realizar el apagado de los equipos de comunicación

c) Después de la Contingencia

Ejecutante	Actividad
Técnico en Redes y Comunicaciones	1. Realizar el encendido de los equipos de comunicaciones
Responsable de ETI	2. Verificar el cumplimiento del procedimiento de recuperación

2. PLAN DE ACCIÓN – Internet y seguridad perimetral

Componentes:
UTM (parte del servicio de internet y seguridad perimetral)

Etapas:

a) Antes de la Contingencia

Ejecutante	Actividad
Técnico en Redes y Comunicaciones	1. Supervisar que el proveedor esté realizando respaldos periódicos de la configuración de los equipos UTM
Técnico en Redes y Comunicaciones	2. Mantener actualizado un diagrama de conexiones de los equipos que estén en el centro de datos y el documento con la relación de políticas implementadas
Responsable de ETI	3. Revisar que se ejecute el respaldo de información

b) Durante la Contingencia

Ejecutante	Actividad
Técnico en Redes y Comunicaciones	1. Reportar al proveedor de servicio de internet y seguridad perimetral el corte de energía eléctrica
Técnico en Redes y Comunicaciones	2. Realizar el apagado de los equipos del proveedor

c) Después de la Contingencia

Ejecutante	Actividad
Técnico en Redes y Comunicaciones	1. Realizar el encendido de los equipos
Técnico en Redes y Comunicaciones	2. Revisar el correcto funcionamiento del servicio de internet y políticas de navegación
Técnico en Redes y Comunicaciones Responsable de ETI	3. Verificar la comunicación desde Internet hacia los servicios publicados.

3. PLAN DE ACCIÓN – Sistema de almacenamiento (Storage)

Componentes:
Sistema de almacenamiento (Storage, Switch)

Etapas:

a) Antes de la Contingencia

Ejecutante	Actividad
Técnico en Redes y Comunicaciones	1. Mantener copias de respaldo de la configuración del sistema de almacenamiento
Técnico en Redes y Comunicaciones	2. Mantener copias de respaldo de la configuración de switch
Técnico en Redes y Comunicaciones	3. Cumplir con el respaldo de la información
Técnico en Redes y Comunicaciones	4. Mantener actualizada la copia en el sistema de almacenamiento de contingencia de contar con el hosting de redundante
Técnico en Redes y Comunicaciones	5. Mantener actualizado el diagrama de la configuración y conexiones del sistema de almacenamiento
Responsable de ETI	6. Revisar que se ejecute el respaldo de la información

b) Durante la Contingencia

Ejecutante	Actividad
Técnico en Redes y Comunicaciones	1. Realizar el apagado del sistema de almacenamiento (Storage)

c) Después de la Contingencia

Ejecutante	Actividad
Técnico en Redes y Comunicaciones	1. Realizar el encendido del storage
Especialista en Sistemas de Información	2. Realizar pruebas sobre las aplicaciones
Responsable de ETI	3. Verificar el cumplimiento del procedimiento de recuperación

4. PLAN DE ACCIÓN – Hipervisores de Virtualización

Componentes:
Servidores
Hipervisor: Hyper-V, VMware
Conexión al sistema de almacenamiento (Storage)

Etapas:

a) Antes de la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Especialista en Sistemas de Información Responsable de ETI	1. Cumplir con el respaldo de la información
Especialista en Sistemas e Informática Especialista en Sistemas de Información Responsable de ETI	2. Guardar una copia de respaldo en un servidor local y enviar otra copia al lugar de custodia
Responsable de ETI	3. Revisar que se ejecute el respaldo de la información

b) Durante la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Responsable de ETI	1. Realizar el apagado de los servidores de virtualización

c) Después de la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Responsable de ETI	1. Realizar el encendido de los servidores de virtualización
Especialista en Sistemas e Informática Responsable de ETI	2. Revisar el correcto funcionamiento del servicio de virtualización
Responsable de ETI	3. Verificar el cumplimiento del procedimiento de recuperación

5. PLAN DE ACCIÓN – Servicio de autenticación de red (Directorio Activo)

Componentes:
Servidor virtual del directorio activo (DC1 y DC2)
Sistema de almacenamiento (Storage)

Etapas:

a) Antes de la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Responsable de ETI	1. Cumplir con el procedimiento de respaldo de la información
Especialista en Sistemas e Informática Responsable de ETI	2. Guardar una copia de respaldo en un servidor local y enviar una copia al lugar de custodia
Responsable de ETI	3. Revisar que se ejecute el respaldo de la información

b) Durante la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Responsable de ETI	1. Realizar el apagado de los servidores de directorio activo

c) Después de la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Responsable de ETI	1. Realizar el encendido de la máquina virtual de directorio activo
Especialista en Sistemas e Informática Responsable de ETI	2. Revisar el correcto funcionamiento de las máquinas virtuales
Responsable de ETI	3. Verificar el cumplimiento del procedimiento de recuperación

6. PLAN DE ACCIÓN – Base de Datos (SQL Server - MySQL)

Componentes:
Servidor de base de datos
Conexión al Sistema de almacenamiento (Storage)

Etapas:

a) Antes de la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Especialista en Sistemas de Información Analista en Sistemas Analista Programador	1. Cumplir con el respaldo de la información
Especialista en Sistemas e Informática Especialista en Sistemas de Información Analista en Sistemas Analista Programador	2. Monitorear el correcto funcionamiento del SQL Server y MySQL
Especialista en Sistemas e Informática Especialista en Sistemas de Información Analista en Sistemas Analista Programador	3. Guardar una copia de respaldo en un servidor local y enviar copia al lugar de custodia
Responsable de ETI	4. Revisar que se ejecute el respaldo de la información

b) Durante la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Responsable de ETI	1. Realizar el apagado de la base de datos

c) Después de la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Responsable de ETI	1. Encender la base de datos
Especialista en Sistemas e Informática Especialista en Sistemas de Información Analista en Sistemas Analista Programador	2. Validar que la información puede ser consultada
Responsable de ETI	3. Verificar el cumplimiento del procedimiento de recuperación

7. PLAN DE ACCIÓN – Servidores Virtualizados

Componentes:
Máquinas virtuales
Licencias de sistemas operativos de servidores
Conexión al sistema de almacenamiento (Storage)

Etapas:

a) Antes de la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Responsable de ETI	1. Cumplir con el respaldo de la información
Especialista en Sistemas e Informática Responsable de ETI	2. Almacenar una copia de respaldo en un servidor local y enviar una copia de respaldo al proveedor de custodia
Responsable de ETI	3. Revisar que se ejecute el respaldo de la información

b) Durante la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Responsable de ETI	1. Realizar el apagado de la maquina virtual

c) Después de la Contingencia

Ejecutante	Actividad
Especialista en Sistemas e Informática Responsable de ETI	1. Encender la máquina virtual
Especialista en Sistemas e Informática Responsable de ETI	2. Realizar pruebas sobre los servicios del servidor virtual
Responsable de ETI	3. Verificar el cumplimiento del procedimiento de recuperación

8. PLAN DE ACCIÓN – Servidores Físicos

Componentes:
Servidor
Respaldo de información
Conexión al sistema de almacenamiento (Storage)

Etapas:

a) Antes de la Contingencia

Ejecutante	Actividad
Técnico en Redes y Comunicaciones Responsable de ETI	1. Cumplir con el respaldo de la información
Técnico en Redes y Comunicaciones Responsable de ETI	2. Almacenar una copia de respaldo en un servidor local y enviar una copia de respaldo al proveedor de custodia
Responsable de ETI	3. Revisar que se ejecute el respaldo de la información

b) Durante la Contingencia

Ejecutante	Actividad
Técnico en Redes y Comunicaciones Responsable de ETI	1. Realizar el apagado del servidor físico

c) Después de la Contingencia

Ejecutante	Actividad
Técnico en Redes y Comunicaciones Responsable de ETI	1. Encender el servidor físico
Técnico en Redes y Comunicaciones Responsable de ETI	2. Realizar pruebas sobre los servicios del servidor físico
Responsable de ETI	3. Verificar el cumplimiento del procedimiento de recuperación

Plan de Recuperación	PR-05
Escenario	En este escenario se considera que no se encuentra disponible el personal necesario para la administración y gestión de la infraestructura tecnológica y servicios de tecnología, lo cual puede traer como consecuencia la indisponibilidad de los mismos.
Estrategia	1. Eliminar la dependencia funcional de los puestos críticos, capacitando a un reemplazo para cada rol (personal alterno), de tal manera que pueda asumir las funciones en caso el personal principal se encuentre indispuesto 2. Entrenar al personal de ETI en el proceso de recuperación de todos los servicios de TI. La capacitación debe ser planificada, estructurada y acorde con las exigencias de recuperación. El entrenamiento se debe evaluar para verificar que se ha logrado sus objetivos. 3. Elaborar un programa de vacaciones que garantice la presencia permanente del personal crítico de las diferentes áreas y procesos de ETI, tales como soporte técnico, redes y comunicaciones, sistemas de información y bases de datos, así como seguridad de la información. 4. Elaborar instructivos y/o procedimientos, en caso el personal encargado de ciertos procedimientos, tanto principal como de reemplazo se encuentren indispuestos

1. PLAN DE ACCIÓN – Personal crítico de TI

Etapas:

a) Antes de la Contingencia

Ejecutante	Actividad
Responsable de ETI Especialista en Sistemas e Informática Especialista en Sistemas de Información Técnico en Redes y Comunicaciones Analista en Sistemas Analista Programador Soporte Técnico	1. Establecer instructivos y/o procedimientos para la administración de los servicios críticos
Especialista en Sistemas e Informática Técnico en Redes y Comunicaciones Soporte Técnico	2. Mantener los accesos remotos para que en caso se requiera se puedan administrar los servicios informáticos desde lugares externos

Responsable de ETI Especialista en Sistemas e Informática Especialista en Sistemas de Información Técnico en Redes y Comunicaciones Analista en Sistemas Analista Programador Soporte Técnico	3. Capacitar a personal alterno en la gestión y operación de los servicios críticos para garantizar la continuidad de la operación
Responsable de ETI	4. Revisar el cumplimiento de los puntos 1, 2 y 3

b) Durante la Contingencia

Ejecutante	Actividad
Responsable de ETI	1. Comunicar a la jefatura inmediata superior sobre la ausencia del personal especialista
Especialista en Sistemas e Informática Técnico en Redes y Comunicaciones Soporte Técnico	2. Coordinar la conexión remota a los equipos y sistemas, por parte del personal alterno

c) Después de la Contingencia

Ejecutante	Actividad
Responsable de ETI	1. Comunicar al personal reincorporado sobre las acciones tomadas en su ausencia
Responsable de ETI Especialista en Sistemas e Informática Especialista en Sistemas de Información Técnico en Redes y Comunicaciones Analista en Sistemas Analista Programador Soporte Técnico	2. Complementar los instructivos y/o procedimientos en caso sea necesario
Responsable de ETI	3. Revisar el cumplimiento de los puntos 1, 2

Plan de Recuperación	PR-06
Escenario	En este escenario se considera que los equipos de redes y comunicaciones se encuentren indisponibles como resultado de una falla física o lógica, lo cual puede traer como consecuencia la caída de servicios de tecnologías de la información y pérdida de comunicación en los equipos que conforman la infraestructura tecnológica.
Estrategia	1. Contar con switches de respaldo que como mínimo sean de capa 3 de modelo OSI, almacenados en un ambiente separado al centro de datos 2. Realizar copias de respaldo periódicas de la configuración de los equipos de comunicaciones 3. Contar con acuerdos de niveles de servicio (SLA) con los proveedores para que en caso sea necesario, puedan sustituir de manera inmediata los equipos de comunicaciones del Centro de Datos
Servicios TI	Red de Datos (Equipos de comunicaciones)

1. PLAN DE ACCIÓN – Red de Datos (Equipos de comunicaciones)

Componentes:
Switches Core, switches de distribución
Enlace de datos con proveedor de hosting

Etapas:

a) Antes de la Contingencia

Ejecutante	Actividad
Técnico en Redes y Comunicaciones	1. Realizar copias de respaldo mensuales de la configuración de los equipos de comunicación
Técnico en Redes y Comunicaciones	2. Mantener actualizado el diagrama de conexiones físicas y las ubicaciones de los equipos
Técnico en Redes y Comunicaciones	3. Mantener un switch administrable de contingencia, que mínimo sea de capa 3 del modelo OSI
Responsable de ETI	4. Revisar el cumplimiento de las copias de respaldo y de la operatividad del equipo de contingencia

b) Durante la Contingencia

Ejecutante	Actividad
Técnico en Redes y Comunicaciones	1. Revisar la operatividad del Switch Core y equipos de comunicación del Centro de Datos. En caso de estar inoperativos realizar el punto 2, caso contrario ir al punto 3
Técnico en Redes y Comunicaciones	2. Realizar las configuraciones de red en el Switch capa 3 de contingencia
Técnico en Redes y Comunicaciones	3. Reemplazar equipo dañado y probar conectividad con los servidores

c) Después de la Contingencia

Ejecutante	Actividad
Técnico en Redes y Comunicaciones	1. Gestionar con el proveedor de soporte la reparación o reemplazo del equipo averiado
Técnico en Redes y Comunicaciones	2. Configurar el hardware nuevo o reparado
Responsable de ETI	3. Verificar el cumplimiento del procedimiento de recuperación y conectividad con los servidores

ANEXO 02

Formato para la evaluación de conocimiento del Plan de Contingencia

Pregunta	Respuesta	Puntaje
Nombre	Nombre de la persona que toma el test	N/A
Cargo	Cargo de la persona que toma el test	N/A
Rol en el plan de contingencia informático	Depende de la persona	10
Describa sus responsabilidades de acuerdo al rol	Depende de la persona	30
Indique cuales son los escenarios que deben cumplirse para invocar la activación de este plan		30
Indique usted que persona o rol aprueba el inicio del plan de continuidad informático		10
Si durante la contingencia, hay la necesidad de comunicarse con la prensa, usted como miembro del equipo de continuidad de TI está en facultad de hacer de vocero (S/N)	No	10
Si durante la contingencia, personal de la DRELM que no forma parte del equipo de contingencia informática, se comunica con usted para solicitarle información del problema, usted como miembro del equipo de contingencia informática esta en facultad de darle toda la información que tiene a mano sobre el problema (S/N)	No. Se debe esperar a reunir al equipo que forma parte de la contingencia informática para tener coherencia con lo que se va a comunicar	10
	TOTAL	100

ANEXO 03

Formato de control y certificaciones de las pruebas

Prueba N°	
Escenario de prueba	
Área responsable	

INFORMACIÓN DEL PROCESO

Metodología				
Alcance				
Condiciones de ejecución	Equipo		Aplicación / sistema	
	Ubicación		Fecha de backup	

RESULTADO DE LA PRUEBA

Resultado	Satisfactorio		
	Satisfactorio con Observaciones	con	
	Deficiente		
Observaciones			
Cambios o Actualizaciones			

Participante	Cargo	Firma