PLAN DE CONTINUIDAD OPERATIVA DEL INSTITUTO TECNOLÓGICO DE LA PRODUCCIÓN
ITP Red CITE

2023

Firma Digital

Firmado digitalmente por EGUSQUIZA ROMERO Mariela Soledad FAU 20131369477 soft
Motivo: Doy V° B°
Fecha: 22.09.2023 14:05:26 -05:00

Firma Digital

Firmado digitalmente por GARCIA RAMOS Santiago Alonso FAU 20131369477 soft
Motivo: Doy V° B°
Fecha: 22.09.2023 09:31:30 -05:00

Firma Digital

Firmado digitalmente por CRUCES GUERREROS Rosse Mary FAU 20131369477 soft
Motivo: Doy V° B°
Fecha: 22.09.2023 09:44:37 -05:00

Firma Digital

Firmado digitalmente por RODRIGUEZ NIQUE Beatriz Marlene FAU 20131369477 hard
Motivo: Doy V° B°
Fecha: 22.09.2023 10:09:42 -05:00

Firma Digital

Firmado digitalmente por ESQUIAGOLA ARANDA John Edward FAU 20131369477 hard
Motivo: Doy V° B°
Fecha: 22.09.2023 10:28:11 -05:00

Firma Digital

Firmado digitalmente por YARANGA DE LA CRUZ Marcos Roberto FAU 20131369477 soft
Motivo: Doy V° B°
Fecha: 22.09.2023 11:11:37 -05:00

Firma Digital

Firmado digitalmente por GALLARDO CAMACHO Lenin Horacio FAU 20131369477 soft
Motivo: Doy V° B°
Fecha: 22.09.2023 13:03:51 -05:00

CONTROL DE REVISIONES

Versión	Fecha	Descripción del cambio
1	09/2023	Añadido de secciones: Identificación de recursos, procedimiento de convocatoria del personal involucrado en la ejecución de las actividades críticas, directorio del Grupo de Comando y cronograma de implementación de la gestión de la continuidad operativa.

CONTENIDO

RELACIÓN DE TABLAS

ACRÓNIMOS

- **CENEPRED** Centro Nacional de Estimación, Prevención y Reducción del riesgo de desastres.
- **CITE** Centro de Innovación Productiva y Transferencia Tecnológica
- **CITES** Centros de Innovación Productiva y Transferencia Tecnológica
- **CO** Continuidad Operativa
- **COES** Centro de Operaciones de Emergencia Sectorial
- **COES PRODUCE** Centro de Operaciones de Emergencia del Sector Producción
- **COEN** Centro de Operaciones de Emergencia Nacional
- **DE** Dirección Ejecutiva
- **DEDFO** Dirección de Estrategia, Desarrollo y Fortalecimiento de los Centros de Innovación Productiva y Transferencia Tecnológica
- **DSE** Dirección de Seguimiento y Evaluación
- **DIDITT** Dirección de Investigación, Desarrollo, Innovación y Transferencia Tecnológica
- **DO** Dirección de Operaciones
- **GRD** Gestión del Riesgo de Desastres
- **GCGCOOP** Grupo de Comando para la Gestión de la Continuidad Operativa
- **GCCOOP-ITP Red CITE** Grupo Comando para la Continuidad Operativa del Instituto Tecnológico de la Producción.
- **GTGRD** Grupo de Trabajo de la Gestión del Riesgo de Desastres
- **GTGRD-ITP Red CITE** Grupo de Trabajo de la Gestión del Riesgo de Desastres del Instituto Tecnológico de la Producción
- **iOS** iPhone Operating System – Sistema operativo del iPhone
- **ITP** Instituto Tecnológico de la Producción
- **ITP Red CITE** Instituto Tecnológico de la Producción y la Red de Centros de Innovación Productiva y Transferencia Tecnológica
- **Mypes** Mediana y pequeña empresa
- **OA** Oficina de Administración
- **OAJ** Oficina de Asesoría Jurídica
- **OCI** Órgano de Control Institucional
- **OGRRHH** Oficina de Gestión de Recursos Humanos
- **OPPM** Oficina de Planeamiento, Presupuesto y Modernización
- **OSDN** Oficina Nacional de Seguridad y Defensa Nacional
- **OTI** Oficina de Tecnologías de la Información
- **PCOOP** Plan de Continuidad Operativa
- **PRODUCE** Ministerio de la Producción
- **ROF** Reglamento de Organización y Funciones
- **SINAGERD** Sistema Nacional de Gestión del Riesgo de Desastres
- **SG** Secretaría General
- **SGD** Sistema de Gestión Documental
- **VHF** Very High Frequency – Muy alta frecuencia
- **UFACGD** Unidad Funcional de Gestión Documental y Atención al Ciudadano
- **UFCII** Unidad Funcional de Comunicaciones e Imagen Institucional
- **UUOO** Unidades Orgánicas
- **UFII** Unidad Funcional de Integridad Institucional
- **UT** Unidad Técnica
- **UTS** Unidades Técnicas

I. INFORMACIÓN GENERAL

1.1. Presentación

La Oficina de Gestión de Recursos Humanos del Instituto Tecnológico de la Producción (ITP Red CITE, en adelante), como unidad orgánica responsable de la Gestión de Continuidad Operativa[1], elabora el presente documento a fin de fortalecer la capacidad de respuesta ante la ocurrencia de eventos de gran magnitud que puedan interrumpir la operatividad de los servicios que brinda la Entidad.
Es así que, se elabora el Plan de Continuidad Operativa del Instituto Tecnológico de la Producción-ITP Red CITE en cumplimiento de la Resolución Ministerial N° 320-2021-PCM, que aprueba los "Lineamientos para la gestión de la Continuidad Opertaiva y la formulación de los Planes de Contiuidad Operativa de las Entidades Públicas de los tres niveles de gobierno", siendo una guía para elaborar este documento que servirá para afrontar los eventos que pongan en riesgo la continuidad de las operaciones de la Entidad.

En el marco de los mencionados lineamientos, se han identificado actividades críticas y de apoyo que se deberán priorizar ante la ocurrencia de un evento de gran magnitud que posiblemente interrumpa la operatividad de los servicios que brinda el ITP Red CITE. Teniendo en cuenta este posible escenario, el Plan de Continuidad Operativa se ha elaborado con información actualizada de la Sede Central y los CITE y el personal mínimo esencial para el desarrollo de actividades presenciales en las instalaciones antes mencionadas.

Asimismo, el presente plan contempla las acciones del ITP Red CITE en caso de presentarse eventos de gran magnitud que aseguren la continuidad de las actividades y operaciones en el marco de su competencia, impulsando la innovación tecnológica, el fomento de la investigación aplicada, la especialización, la transferencia tecnológica y la difusión de conocimientos tecnológicos en cada cadena productiva logrando la mejora de la productividad de la Mipymes.

Finalmente, se requiere de un alto grado de compromiso de la Alta Dirección, Directores, Jefes y todos los servidores de la entidad, para asumir responsabilidades en los roles que se asignarán con el fin de realizar actividades y/u operaciones críticas o de apoyo.

1.2. Alcance

El Plan de Continuidad Operativa del Instituto Tecnológico de la Producción-ITP Red CITE es de aplicación y cumplimiento obligatorio de todos los órganos que componen la estructura orgánica de la Entidad.

1.3. Definiciones

- **Actividades Críticas:** Están constituidas por las actividades que la Entidad ha identificado como indispensables y que no pueden dejar de realizarse, conforme a sus competencias señaladas en las normas vigentes sobre la materia.

[1] Resolución Ejecutiva N° 028-2022-ITP/DE

- **Gestión de la Continuidad Operativa del Estado:** Proceso continuo que forma parte de las operaciones habituales de la Entidad Pública con el objetivo de que siga cumpliendo con su misión, mediante la implementación de mecanismos adecuados, con el fin de continuar brindando servicios necesarios a la población, ante la ocurrencia de un desastre o evento que produzca una interrupción prolongada de sus operaciones.

- **Unidad Orgánica a cargo de la Gestión de la Continuidad Operativa:** Designada por el titular de la Entidad. Responsable de articular y coordinar la Gestión de la Continuidad Operativa en la Entidad, y de prestar el soporte y apoyo para asegurar la participación de todo el personal en la continuidad operativa.

- **Grupo Comando:** Es el conjunto de profesionales que se encarga de la elaboración del Plan de Continuidad Operativa de la Entidad y de la toma de decisiones respecto a la implementación de dicho plan.

- **Plan de Continuidad Operativa:** Instrumento a través del cual se implementa la continuidad operativa, tiene como objetivo garantizar que la Entidad ejecute las actividades críticas identificadas previamente. Contiene la identificación de riesgos y recursos, acciones para la continuidad operativa y el cronograma de ejercicios.

- **Plan de recuperación de los servicios informáticos:** Plan que forma parte del Plan de Continuidad Operativa, el cual busca, inicialmente, restaurar los servicios de tecnología de información necesarios para ejecutar las actividades críticas identificadas permitiendo una posterior recuperación de las condiciones previas a su ocurrencia. Para su desarrollo toma en cuenta la Norma Técnica Peruana NTP ISO/IEC 20071:2014.

- **Sede Alterna de la Entidad Pública:** Espacio físico o infraestructura segura y accesible, determinada con anterioridad y de disponibilidad inmediata, que permite la ejecución de los servicios o actividades críticas señaladas en el Plan de continuidad Operativa de la Entidad. Para ello, cuenta con el equipamiento necesario y servicios básicos indispensables, que opera con autonomía energética y de conectividad.

  La sede alterna se ocupa cuando la sede principal de la entidad ha colapsado o su condición de operatividad ha sido afectada y pone en riesgo la seguridad del personal, pudiéndose establecer sedes alternas compartidas, que albergan a dos o más Entidades Públicas.

II. BASE LEGAL

- Ley N° 29664, que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD) y sus modificatorias.
- Decreto Supremo N° 048-2011-PCM, que aprueba el reglamento de la Ley N° 29664 y sus modificatorias.
- Decreto Supremo N° 005-2016-PRODUCE, que aprueba el Reglamento de Organización y Funciones del Instituto Tecnológico de la Producción.

- Decreto Supremo N° 038-2021-PCM, que aprueba la Política Nacional de Gestión del Riesgo de Desastres al 2050.
- Decreto Supremo N° 115-2022-PCM, que aprueba el Plan Nacional de Gestión del Riesgo de Desastres-PLANAGERD 2022-2030.
- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana NTP ISO/IEC 27001:2014, Tecnologías de la información Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2° Edición.
- Resolución Ministerial N° 320-2021-PCM que aprueba los Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Públicas de los tres niveles de gobierno.
- Resolución Ejecutiva N° 028-2022-ITP/DE, que designa a la Oficina de Gestión de Recursos Humanos como Unidad Orgánica responsable de la Gestión de Continuidad Operativa.
- Resolución Ejecutiva N° 186-2022-ITP/DE, que aprueba la conformación del grupo Comando para la Gestión de la Continuidad Operativa del Instituto Tecnológico de la Producción.

III. OBJETIVOS

3.1. Objetivo General

Fortalecer la capacidad de respuesta del Instituto Tecnológico de la Producción-ITP Red CITE, ante la ocurrencia de un evento inesperado o desastre de gran magnitud que produzca inestabilidad en las operaciones de la Sede Central y la Red CITE.

3.2. Objetivos Específicos

- Asegurar la continuidad operativa de las actividades críticas identificadas en la Entidad, ante la ocurrencia de un desastre de gran magnitud o un evento que interrumpa su normal funcionamiento.
- Establecer los requerimientos y necesidades para la recuperación de la Entidad.
- Atenuar el impacto negativo que pudiera producir un fenómeno de gran magnitud sobre la imagen de la Entidad.

IV. ESTADO SITUACIONAL DEL INSTITUTO TECNOLÓGICO DE LA PRODUCCIÓN-ITP RED CITE

El Instituto Tecnológico de la Producción-ITP Red CITE, es un Organismo Técnico especializado adscrito al Ministerio de la Producción, con personería jurídica de derecho público interno, con autonomía administrativa, económica y técnica en el ejercicio de sus atribuciones, de acuerdo a los lineamientos técnicos del sector producción. Constituye un pliego presupuestal.

EL ITP Red CITE tiene competencia en materia de investigación, desarrollo, innovación, adaptación, transformación y trasferencia tecnológica, con el propósito de lograr el óptimo aprovechamiento de los recursos para contribuir al incremento de la competitividad del sector producción. Asimismo, promueve el aprovechamiento sostenible de recursos hidrobiológicos.

Cabe indicar que, tiene a su cargo la coordinación, orientación, concertación y calificación de los Centros de Innovación Productiva y Transferencia Tecnológica-CITE, en el marco del Decreto Legislativo N° 1228, Decreto Legislativo de Centros de Innovación Productiva y Transferencia Tecnológica-CITE, y su Reglamento.

4.1. Ubicación de la Entidad

a. Instituto Tecnológico de la Producción-Sede Central
Dirección: Av. República de Panamá N° 3418, Urb. Limatambo, San Isidro, Lima
Teléfono: (01) 6802150

Unidades de Organización:
- Consejo Directivo
- Dirección Ejecutiva
- Secretaría General
- Órgano de Control Institucional
- Dirección de Estrategia, desarrollo y fortalecimiento de los Centros de Innovación Productiva y Transferencia Tecnológica
- Dirección de Seguimiento y Evaluación
- Dirección de Operaciones
- Oficina de Asesoría Jurídica
- Oficina de Administración
- Oficina de Planeamiento, Presupuesto y Modernización
- Unidad Funcional de Imagen Institucional

b. Instituto Tecnológico de la Producción-Sede Callao
Dirección: Carretera a Ventanilla Km. 5.2, Prov. Constitucional del Callao, Callao
Teléfono: (01) 6802150

Unidades de Organización:
- Dirección de Investigación, Desarrollo, Innovación y Transferencia Tecnológica
- Dirección de Operaciones
- Oficina de Administración
- Oficina de Tecnologías de la Información
- Oficina de Gestión de Recursos Humanos
- Unidad Funcional de Atención al Ciudadano y Gestión Documentaria
- Unidad Funcional de Integridad Institucional

4.2. Ubicación de la Red CITE

Tabla N° 1. Ubicación de las sedes de la Red CITE.

N°	SEDE	DIRECCIÓN (Región, provincia y distrito)
1	CITE Acuícola pesquero Ahuashiyacu	Carretera a Bello Horizonte Km. 2.3 (interior de la Estación Pesquera Ahuashiyacu), La Banda de Shilcayo – Tarapoto – San Martín
2	CITEagroindustrial Chavimochic	Campamento San José – Km. 513, Panamericana Norte, Virú – La Libertad
3	CITEagroindustrial Huallaga	Carretera Tingo María-Aucayacu Km. 26, Localidad de Santa Lucia, Pueblo Nuevo, Leoncio Prado-Huánuco
4	CITEagroindustrial Ica	Panamericana Sur Km. 293.3, Salas Guadalupe – Ica
5	CITEagroindustrial Majes	Urb. Ciudad Majes, Módulo B, Sector 1, Mz. A-3, Lt.1, El Pedregal, Majes, Caylloma-Arequipa

N°	SEDE	DIRECCIÓN (Región, provincia y distrito)
6	CITEagroindustrial Moquegua	Carretera Costanera Sur Km. 7.6, Pampa de Palo – CETICO – Moquegua, Ilo – Moquegua
7	CITEagroindustrial Oxapampa	Av. Las Galaxias, Calle Francisco Cuñivo y Calle Venus S/N, Villa Rica, Oxapampa-Pasco (costado del Centro Interpretativo del Café, Villa Rica)
8	CITEagroindustrial VRAEM	Jr. Joaquín Dipas Huamán Mz. R Lote 14. Urb. Valle Dorado, Pichari – La Convención – Cusco
9	CITE ccal Arequipa	Parque Industrial Rio Seco, Mz. F, Lt. 3, Distrito de Cerro Colorado, Arequipa
10	CITE ccal Lima	Caquetá 1300, Rímac – Lima
11	CITE ccal Trujillo	N2 Lote 1 Barrio 5°, Centro Poblado Alto Trujillo – El Porvenir – Trujillo – La Libertad
12	CITEforestal Maynas	Carretera Iquitos Nauta Km. 3.9 – Distrito de San Juan Bautista
13	CITEforestal Pucallpa	Calle Flora y Fauna N° 199, Km. 4.2 – Pucallpa – Ucayali
14	CITE madera Lima	Jr. Solidaridad cuadra 3.Parcela II, Mz. F, Lt.11-A, Parque Industrial – Villa El Salvador
15	CITE pesquero Callao	Carretera a Ventanilla KM. 5.2, Ventanilla-Callao
16	CITE pesquero Ilo	Carretera Costanera Sur Km. 3.5 – Unidad Zonal Ilo, Puerto de Ilo – Moquegua
17	CITE pesquero Piura	Calle Fortunato Chirichigno A-2, Oficinas 305 y 306, Urbanización San Eduardo – Piura. Cámara de Comercio y Producción de Piura, tercer piso
18	CITE pesquero amazónico Pucallpa	Av. Túpac Amaru Km 5.800, Callería – Coronel Portillo – Ucayali
19	CITE productivo Madre de Dios	Carretera Puerto Maldonado-Cusco Km. 16.5, Tambopata-Tambopata-Madre de Dios
20	CITE productivo Maynas	Carretera Iquitos-Nauta km 2.5, San Juan Bautista – Maynas – Loreto
21	CITEtextil camélidos Arequipa	Calle 3 Mz. I', Lote 4, Primera Etapa, Parque Industrial Río Seco, Cerro Colorado, Arequipa
22	CITEtextil camélidos Cusco	Av. Las Américas J1, Urb. Parque Industrial, Distrito de Wanchaq, Cusco
23	CITEtextil Camélidos Puno	Jr. Libertad N° 230, Cercado de Puno
24	Unidad Técnica Agroindustrial Ambo	Jr. General Prado N° 1097 – 2do piso, Huánuco
25	Unidad Técnica Agroindustrial Huaura	28 de Julio N°1669, Santa María – Huaura – Lima

Fuente: Grupo de Comando para la Gestión de la Continuidad Operativa.

En la figura N° 1, se presenta el Organigrama del Instituto Tecnológico de la Producción-ITP Red CITE, según lo indicado en el Reglamento de Organización y Funciones de la Entidad.

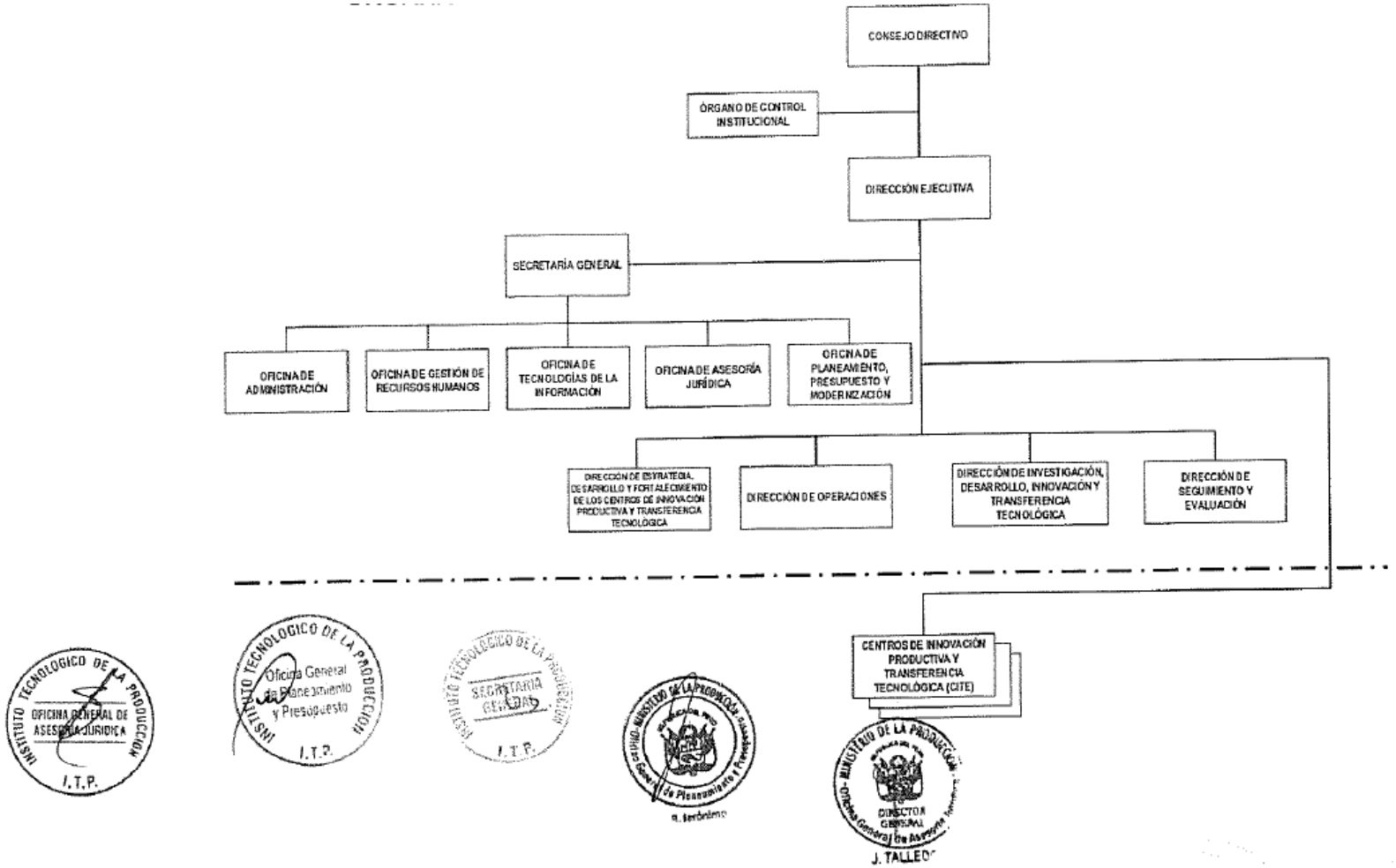


Figura N° 1. Organigrama del Instituto Tecnológico de la Producción-ITP Red CITE
Fuente: Grupo de Comando para la Gestión de la Continuidad Operativa.

V. IDENTIFICACIÓN DE RIESGOS

5.1. Matriz de riesgos

Para la identificación de riesgos, se elaboraron *"Lineamientos para identificación de peligros y riesgos"*, según lo señalado en el Anexo 2, de la Resolución Ministerial N° 320-2021-PCM, que aprueba los Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los planes de Continuidad Operativa de la Entidades Públicas de los tres niveles de gobierno.

Es así que, para el ITP en Sede Central y Red CITE, se identificaron los peligros de origen natural (sismos, tsunamis, inundaciones, movimientos en masa, entre otros) o inducidos por la acción humana (incendios, atentados terroristas, entre otros), los cuales pueden ocasionar una interrupción prolongada en el funcionamiento de las actividades de la Entidad. A continuación, en la tabla N° 02 se detalla los peligros identificados:

Tabla N° 2. Peligros identificados ITP red CITE

PELIGROS DE ORIGEN NATURAL	SEDE CENTRAL/RED CITE																									
	AREQUIPA			CALLAO	CUSCO		HUÁNUCO		ICA	LA LIBERTAD		LIMA				IQUITOS		MADRE DE DIOS	MOQUEGUA		PASCO	PIURA	PUNO	SAN MARTIN	UCAYALI	
	CITEAGROINDUSTRIAL MAJES	CITECCAL AREQUIPA	CITETEXTIL CAMELIDOS AREQUIPA	CITEPESQUERO CALLAO	CITEAGROINDUSTRIAL VRAEM	CITETEXTIL CAMELIDOS CUSCO	CITEAGROINDUSTRIAL HUALLAGA	UNIDAD TÉCNICA AGROINDUSTRIAL AMBO	CITEAGROINDUSTRIAL ICA	CITEAGROINDUSTRIAL CHAVIMOCHIC	CITECCAL TRUJILLO	CITECCAL LIMA	CITEMADERA LIMA	UNIDAD TÉCNICA AGROINDUSTRIAL HUAURA	SEDE CENTRAL	CITEFORESTAL MAYNAS	CITEPRODUCTIVO MAYNAS	CITEPRODUCTIVO MADRE DE DIOS	CITEAGROINDUSTRIAL MOQUEGUA	CITEPESQUERO ILO	CITEAGROINDUSTRIAL OXAPAMPA	CITEPESQUERO PIURA	CITETEXTIL CAMELIDOS PUNO	CITEACUICOLA PESQUERO AHUASHIYACU	CITEFORESTAL PUCALLPA	CITEPESQUERO AMAZONICO PUCALLPA
Exceso de lluvias	X	X	X		X	X	X	X	X	X	X			X		X	X	X	X	X	X	X	X	X	X	X
Déficit de lluvias	X	X	X				X	X				X	X	X	X						X	X	X	X			
Heladas	X	X	X		X	X	X	X	X	X	X								X	X	X	X	X				
Friaje					X	X	X	X								X	X	X			X		X	X	X	X
Sismos	X	X	X	X	X	X			X			X	X	X	X				X	X		X		X			
Tsunami	X	X	X	X					X			X	X	X	X				X	X		X					
Explosión volcánica	X	X	X																X	X			X				
Fenómeno El Niño	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X		X	X		X	X	X	X	X	X
Fenómeno La Niña	X	X	X	X					X	X	X	X	X	X	X				X	X		X					
PELIGROS POR ACCIÓN HUMANA																										
Incendio	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Ataque informático	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Conmoción social	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Atentado terrorista	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Pandemia	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Fuente: Manual para la evaluación de riesgos originados por fenómenos naturales. Versión 02. CENEPRED.

Posteriormente, teniendo en cuenta la vulnerabilidad de la Entidad (Sede Central y Red CITE), enfocada en la estructura que podría colapsar ante la ocurrencia de los peligros identificados, así como las afectaciones al personal y sus recursos; se evaluó cualitativamente tomando en cuenta los niveles *bajo, medio, alto y muy alto.*

Para determinar el nivel de riesgo, se consideró la matriz siguiente:

Tabla N° 3. Matriz de riesgo.

MATRIZ DE RIESGO				
Peligro Muy Alto	Riesgo Alto	Riesgo Alto	Riesgo Muy Alto	Riesgo Muy Alto
Peligro Alto	Riesgo Medio	Riesgo Alto	Riesgo Alto	Riesgo Muy Alto
Peligro Medio	Riesgo Medio	Riesgo Medio	Riesgo Alto	Riesgo Alto
Peligro Bajo	Riesgo Bajo	Riesgo Medio	Riesgo Medio	Riesgo Alto
P / **V**	**Vulnerabilidad Baja**	**Vulnerabilidad Media**	**Vulnerabilidad Alta**	**Vulnerabilidad Muy Alta**

Fuente: RM N° 320-2021-PCM, Anexo 2.

El nivel de riesgo identificado para el ITP Red CITE se indica en las tablas N° 3 y 4, respectivamente:

Tabla N° 4. Nivel de riesgo ITP-Sede Central.

PELIGROS	NIVEL DE RIESGO Sede Central	
	SEDE SAN ISIDRO	SEDE CALLAO
Exceso de lluvias	NO APLICA	NO APLICA
Déficit de lluvias	NO APLICA	NO APLICA
Heladas	NO APLICA	NO APLICA
Friaje	NO APLICA	NO APLICA
Sismos	ALTO	MUY ALTO
Tsunami	MEDIO	MUY ALTO
Explosión volcánica	NO APLICA	NO APLICA
Fenómeno El Niño	NO APLICA	NO APLICA
Fenómeno La Niña	NO APLICA	NO APLICA
Incendio	ALTO	ALTO
Ataque informático	ALTO	ALTO
Conmoción social	BAJO	MEDIO
Atentado terrorista	BAJO	BAJO
Pandemia	BAJO	BAJO

Fuente: Elaboración propia

Tabla N° 5. Nivel de riesgo ITP Red CITE.

PELIGROS	NIVEL DE RIESGO red CITE																							
	CITE ACUICOLA PESQUERO AHUASHIYACU	CITE AGROINDUSTRIAL CHAVIMOCHIC	CITE AGROINDUSTRIAL HUALLAGA	CITE AGROINDUSTRIAL ICA	CITE AGROINDUSTRIAL MAJES	CITE AGROINDUSTRIAL MOQUEGUA	CITE AGROINDUSTRIAL OXAPAMPA	CITE AGROINDUSTRIAL VRAEM	CITECCAL AREQUIPA	CITECCAL LIMA	CITECCAL TRUJILLO	CITE FORESTAL MAYNAS	CITE FORESTAL PUCALLPA	CITE MADERA	CITE PESQUERO CALLAO	CITE PESQUERO ILO	CITE PESQUERO PIURA	CITE PESQUERO AMAZÓNICO PUCALLPA	CITE PRODUCTIVO MADRE DE DIOS	CITE PRODUCTIVO MAYNAS	CITETEXTIL CAMÉLIDOS AREQUIPA	CITETEXTIL CAMÉLIDOS CUSCO	CITETEXTIL CAMÉLIDOS PUNO	UNIDAD TÉCNICA AGROINDUSTRIAL AMBO	UNIDAD TÉCNICA AGROINDUSTRIAL HUAURA
Exceso de lluvias	ALTO	ALTO	MEDIO	BAJO	BAJO	MEDIO	ALTO	ALTO	MEDIO	NO APLICA	MUY ALTO	MEDIO	MEDIO	NO APLICA	NO APLICA	BAJO	MEDIO	ALTO	ALTO	MEDIO	MEDIO	ALTO	BAJO	ALTO	BAJO
Déficit de lluvias	BAJO	NO APLICA	ALTO	ALTO	BAJO	MEDIO	BAJO	BAJO	BAJO	NO APLICA	BAJO	NO APLICA	BAJO	NO APLICA	NO APLICA	BAJO	BAJO	NO APLICA	NO APLICA	NO APLICA	BAJO	NO APLICA	NO APLICA	ALTO	MEDIO
Heladas	NO APLICA	NO APLICA	BAJO	NO APLICA	BAJO	NO APLICA	NO APLICA	NO APLICA	BAJO	NO APLICA	NO APLICA	NO APLICA	NO APLICA	NO APLICA	NO APLICA	NO APLICA	NO APLICA	NO APLICA	NO APLICA	NO APLICA	BAJO	ALTO	MEDIO	BAJO	NO APLICA
Friaje	BAJO	NO APLICA	BAJO	NO APLICA	NO APLICA	NO APLICA	NO APLICA	BAJO	NO APLICA	NO APLICA	NO APLICA	BAJO	BAJO	NO APLICA	NO APLICA	NO APLICA	NO APLICA	BAJO	BAJO	BAJO	NO APLICA	ALTO	BAJO	BAJO	NO APLICA
Sismos	ALTO	ALTO	BAJO	MUY ALTO	ALTO	ALTO	ALTO	BAJO	ALTO	ALTO	ALTO	BAJO	BAJO	ALTO	MUY ALTO	MEDIO	ALTO	BAJO	BAJO	BAJO	ALTO	MEDIO	BAJO	BAJO	MUY ALTO
Tsunami	NO APLICA	NO APLICA	NO APLICA	NO APLICA	NO APLICA	ALTO	NO APLICA	NO APLICA	NO APLICA	BAJO	NO APLICA	NO APLICA	NO APLICA	BAJO	MUY ALTO	ALTO	NO APLICA	NO APLICA	NO APLICA	NO APLICA	NO APLICA	NO APLICA	NO APLICA	NO APLICA	BAJO
Explosión volcánica	NO APLICA	NO APLICA	NO APLICA	NO APLICA	ALTO	BAJO	NO APLICA	NO APLICA	ALTO	NO APLICA	NO APLICA	NO APLICA	NO APLICA	NO APLICA	NO APLICA	BAJO	NO APLICA	NO APLICA	NO APLICA	NO APLICA	ALTO	NO APLICA	NO APLICA	NO APLICA	NO APLICA
Fenómeno El Niño	NO APLICA	ALTO	MEDIO	BAJO	BAJO	BAJO	ALTO	NO APLICA	BAJO	BAJO	MUY ALTO	NO APLICA	NO APLICA	BAJO	BAJO	BAJO	ALTO	NO APLICA	NO APLICA	NO APLICA	BAJO	BAJO	BAJO	BAJO	BAJO
Fenómeno La Niña	NO APLICA	BAJO	NO APLICA	BAJO	BAJO	BAJO	NO APLICA	NO APLICA	BAJO	BAJO	MUY ALTO	NO APLICA	NO APLICA	BAJO	BAJO	BAJO	ALTO	NO APLICA	NO APLICA	NO APLICA	BAJO	NO APLICA	NO APLICA	NO APLICA	BAJO
Incendio	ALTO	MEDIO	MEDIO	ALTO	ALTO	MUY ALTO	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO	MUY ALTO	ALTO	ALTO	MEDIO	MEDIO	ALTO	BAJO	ALTO	MEDIO	BAJO	MEDIO	MEDIO
Ataque informático	BAJO	BAJO	BAJO	BAJO	BAJO	MEDIO	BAJO	BAJO	BAJO	BAJO	BAJO	BAJO	BAJO	BAJO	BAJO	BAJO	BAJO	BAJO	BAJO	BAJO	BAJO	BAJO	BAJO	BAJO	BAJO
Conmoción social	MEDIO	BAJO	BAJO	ALTO	MEDIO	BAJO	BAJO	MEDIO	MEDIO	MEDIO	ALTO	MEDIO	BAJO	MEDIO	MEDIO	MEDIO	MEDIO	BAJO	MEDIO	MEDIO	MEDIO	MEDIO	BAJO	BAJO	MEDIO
Atentado terrorista	NO APLICA	NO APLICA	BAJO	BAJO	BAJO	BAJO	BAJO	BAJO	BAJO	BAJO	BAJO	NO APLICA	NO APLICA	BAJO	BAJO	NO APLICA	BAJO	NO APLICA	NO APLICA	NO APLICA	BAJO	BAJO	NO APLICA	BAJO	BAJO
Pandemia	BAJO	ALTO	MEDIO	ALTO	MEDIO	ALTO	ALTO	ALTO	MEDIO	BAJO	BAJO	MEDIO	BAJO	BAJO	BAJO	ALTO	MEDIO	ALTO	ALTO	MEDIO	MEDIO	MEDIO	BAJO	MEDIO	MEDIO

Fuente: Elaboración propia

5.2. Determinación del Nivel de Impacto

El ITP Red CITE, respecto a su infraestructura, personal y recursos se podría encontrar vulnerable ante la ocurrencia de los eventos indicados en la identificación de riesgos, provocando la interrupción parcial o total de los servicios que brinda la Entidad.

Para determinar la vulnerabilidad de la Entidad, se ha considerado los impactos que ocasionarían algún evento determinado asignando los siguientes coeficientes:

Tabla N° 6. Niveles de impacto.

Coeficiente de impactos	
Muy Alto	5
Alto	4
Medio	3
Bajo	2
Muy Bajo	1

Fuente: RM N° 320-2021-PCM, Anexo 2.

A continuación, en los cuadros siguientes se detalla el análisis de vulnerabilidad considerado para Sede Central y Red CITE, respectivamente:

a. Sede Central

Tabla N° 7. Análisis de vulnerabilidad en Sede Central.

Impactos	Sismo de gran magnitud	Tsunami	Incendio	Conmoción social	Ataque informático	Pandemia	Atentado terrorista
Colapso total o parcial de la infraestructura	5	4	4	2	3	1	3
Corte de suministro de energía eléctrica	5	4	3	3	2	1	2
Colapso de suministro de agua	4	5	4	2	2	1	2
Estabilidad de servicios informáticos	5	5	4	3	5	2	3
Operatividad de equipos y mobiliario	3	3	3	4	3	1	2
Disponibilidad documentaria	3	3	3	2	3	2	3
Disponibilidad de personal	3	3	3	4	2	4	3
Disponibilidad de recursos financieros	2	2	2	2	2	2	2

Fuente: Grupo de Comando para la Gestión de la Continuidad Operativa

b. Red CITE

Tabla N° 8. Análisis de vulnerabilidad en Red CITE.

Impactos	Sismo de gran magnitud	Exceso de lluvias (inundación)	Déficit de lluvias (sequía)	Heladas	Friaje	Fenómeno del Niño/Niña	Explosión volcánica	Incendio	Conmoción social	Ataque informático	Pandemia	Atentado terrorista
Colapso total o parcial de la infraestructura	4	3	1	1	1	3	4	3	2	1	1	3
Corte de suministro de energía eléctrica	4	3	3	2	2	3	4	3	3	1	1	2
Colapso de suministro de agua	4	5	2	3	3	5	3	4	2	1	1	2
Estabilidad de servicios informáticos	5	4	2	3	2	4	4	4	3	5	2	3
Operatividad de equipos y mobiliario	3	4	4	4	4	3	3	3	4	3	1	2
Disponibilidad documentaria	3	4	4	4	3	4	3	3	3	2	3	3
Disponibilidad de personal	3	4	4	4	4	3	3	3	3	2	4	2
Disponibilidad de recursos financieros	2	2	2	2	2	2	2	2	2	2	2	2

Fuente: Fuente: Grupo de Comando para la Gestión de la Continuidad Operativa.

De las tablas realizadas, se observa que el impacto más severo en Sede Central como en la Red CITE lo ocasionaría un sismo de gran magnitud, ocasionando la interrupción de los servicios que brinda el ITP Red CITE.

5.3. Identificación de Recursos

Para la identificación de los recursos disponibles que aportan al manejo de la emergencias o desastres y ejecutar la continuidad operativa, se ha contado con los datos brindados desde la oficina de administración, la dirección de operaciones, los diferentes CITES y UTS del ITP Red CITE.

Conociendo los peligros y niveles de impacto que ocasionaría algún evento disruptivo es necesario mencionar que el uso de los recursos debe relacionarse al tipo de evento y sus efectos colaterales.

Tabla N° 9. Identificación de tipos de Recursos en el ITP Red CITE.

RECURSOS DISPONIBLES		SEDES ITP LIMA CALLAO	CITES Y UTS	TOTAL
Recursos humanos	Personal permanente	222	366	588
	Personal temporal	137	255	392
	Brigadistas	26	174	200
Recursos Materiales	Alarma contra incendios	0	14	14
	Avisador sonoro	0	1	1
	Botiquín	1	56	57
	Camillas	0	5	5
	Casco de seguridad	0	4	4
	Celulares	14	0	14
	Chalecos	0	4	4
	Computadoras	786	1225	2011
	Collarín	0	1	1
	Detectores de humo	0	177	177
	Equipo de radio móvil	5	0	5
	Extintores	54	374	428
	Gabinete contra incendio	0	5	5
	Guantes esterilizados	0	1	1
	Grupo Electrógeno	0	4	4
	Impresoras y scanner	126	184	310
	Laptops	83	222	305
	Lavaojos de emergencia	0	1	1
	Linterna	0	1	1
	Luces de emergencia	0	208	208
	Manguera contra incendio	0	2	2
	Negatoscopio	2	0	2
	Otoscopio	2	0	2
	Pantoscopio	1	0	1
	Señalética	0	199	199
	Silla de ruedas	0	1	1
	Tensiómetro	3	1	4
	Termómetro digital	0	1	1
	Vehículos	13	49	62

Fuente: Grupo de Comando para la Gestión de la Continuidad Operativa.

VI. ACCIONES PARA LA CONTINUIDAD OPERATIVA

6.1. Determinación de actividades críticas

Para determinar las actividades críticas en el ITP Red CITE, se elaboró el Lineamiento *"Identificación de actividades críticas"*, según lo indicado Resolución Ministerial N° 320-2021-PCM, que aprueba los Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los planes de Continuidad Operativa de la Entidades Públicas de los tres niveles de gobierno.

6.1.1. Actividades Críticas ante emergencias y/o desastres

Según los lineamientos de la Gestión de Continuidad Operativa, esta consiste en determinar las actividades que no pueden interrumpirse, en tanto ello afectaría seriamente el cumplimiento de la misión de la Entidad, incluye la identificación de los servicios y proveedores internos y externos críticos indispensables para su ejecución.

Es así que, se identificaron las siguientes actividades críticas tanto en la Sede Central como la red CITE:

a. Sede Central

Las actividades críticas identificados según los órganos con los que cuenta el ITP Red CITE, en su Sede Central, se indica a continuación:

Tabla N° 10. Actividades críticas Sede Central-ITP Red CITE.

N°	ÓRGANO	OFICINA/DIRECCIÓN	ACTIVIDAD CRÍTICA
1	Alta Dirección	Dirección Ejecutiva (DE)	Supervisar las acciones de los diferentes órganos del ITP Red CITE, de acuerdo al cumplimiento de metas establecidas.
2			Coordinar con los órganos del ITP Red CITE las acciones a realizar en caso de eventos y/o emergencias de gran magnitud
3		Secretaría General (SG)	Dirigir y supervisar las acciones administrativas del ITP Red CITE.
4			Seguimiento de las acciones a realizar en caso de eventos y/o emergencias de gran magnitud
5	Unidades Funcionales	SG-Unidad Funcional de Comunicaciones e Imagen Institucional (UFCII)	Elaborar piezas gráficas y/o comunicaciones para publicar en los canales del ITP Red CITE
6		SG-Unidad Funcional de Integridad Institucional (UFII)	Gestionar la información sobre el evento de gran magnitud y/o emergencia para la toma de decisiones
7		SG-Unidad Funcional de Atención al Ciudadano y Gestión Documental (UFACGD)	Atender a los usuarios en mesa de partes de ITP Red CITE en caso de eventos y/o emergencias de gran magnitud
8			Custodiar el acervo documentario del ITP Red CITE
9	Control Institucional	Órgano de Control Institucional (OCI)	Ejecutar los servicios de control en el ITP red CITE sujeto a la normativa vigente establecida por la Contraloría General de la República.
10	Asesoramiento	Oficina de Asesoría Jurídica (OAJ)	Asesorar en normativa vigente, documentos y otros asuntos internos del ITP red CITE
11			Emitir opinión legal sobre proyectos de dispositivos legales expedidos por Alta Dirección
12		Oficina de Planeamiento, Presupuesto y Modernización (OPPM)	Evaluar requerimientos y elaborar propuestas de transferencias de partidas, transferencias financieras y otras modificaciones presupuestarias
13			Aprobar la asignación presupuestal multianual

14			Seguimiento de la ejecución presupuestal
15			Evaluar y establecer presupuesto para rehabilitación en caso de eventos y/o emergencias de gran magnitud
16	**Apoyo**	**Oficina de Administración (OA)**	Emitir órdenes de servicios en el marco de la normativa vigente
17			Realizar pago a proveedores y terceros
18			Contratación de bienes y servicios para el ITP red CITE en caso de eventos y/o emergencias de gran magnitud
19			Abastecer al ITP red CITE de servicios básicos
20			Efectuar el control patrimonial y custodia de activos del ITP red CITE
21		**Oficina de Gestión de Recursos Humanos (OGRRHH)**	Elaborar las planillas de pagos de los servidores y practicantes del ITP red CITE
22			Diseñar y administrar los perfiles de puestos del ITP red CITE
23			Supervisar los procesos de selección de personal
24			Seguimiento del registro de personal activo y cesante
25			Seguimiento médico y de bienestar de los servidores y practicantes del ITP red CITE
26		**OGRHH-Secretaría Técnica**	Gestionar los Procedimientos Administrativos Disciplinarios (PAD), notificar documentos que cuenten con plazo
27		**Oficina de Tecnologías de la Información (OTI)**	Administrar los recursos informáticos del ITP red CITE
28			Asegurar el funcionamiento de los recursos informáticos en caso de eventos y/o emergencias de gran magnitud
29			Proveer soporte técnico a las áreas usuarias
30	**Línea**	**Dirección de Operaciones (DO)**	Implementar la mejora de la infraestructura física, tecnológica y servicios tecnológicos delo CITE
31			Dirigir el funcionamiento del registro de los CITE
32			Supervisar y realizar el seguimiento de la ejecución de proyectos de inversión pública
33			Promover suscripción de convenios con entidades públicas o privadas para contribuir a la implementación y operación de los CITE
34		**Dirección de Estrategia, Desarrollo, Innovación y Fortalecimiento de los Centros de Innovación Productiva y Transferencia Tecnológica (DEDFO)**	Elaborar estudios de demanda relacionados con la implementación de los Centros de Innovación Productiva y Transferencia Tecnológica (CITE).
35			Identificar necesidades y requerimientos de servicios y de información en el ámbito de influencia de los CITE
36			Elaborar expedientes técnicos de proyecto de inversión pública de los CITE
37			Proponer la ubicación de los CITE y sus unidades técnicas (UT)
38			Proponer la creación de Unidades Técnicas (UT) de CITE
39		**Dirección de Investigación, Desarrollo, Innovación y Transferencia Tecnológica (DIDITT)**	Brindar servicios de investigación, desarrollo, innovación, adaptación, transformación y transferencia tecnológica al sector producción
40		**Dirección de Seguimiento y Evaluación (DSE)**	Realizar la evaluación periódica de los CITE
41			Gestionar la información estadística mediante reportes estadísticos de las actividades realizadas por los CITE
42			Evaluar la evolución y los resultados de los convenios de desempeño

Fuente: Grupo de Comando para la Gestión de la Continuidad Operativa

b. Red CITE

Las actividades críticas identificados en la red CITE se indica a continuación:

Tabla N° 11. Actividades críticas Sede Central-ITP Red CITE.

N°	ÓRGANO	CITE/UT	ACTIVIDADES CRÍTICAS
1	Desconcentrados	CITE Acuícola pesquero Ahuashiyacu	Proceso productivo en acciones I+D+i: Laboratorios de I+D+i peces amazónicos
2			Proceso productivo en acciones I+D+i: Laboratorio de producción de alimento vivo
3			Proceso productivo en acciones I+D+i: Laboratorios de I+D+i Tilapia
4			Proceso de análisis: Laboratorio de investigación y análisis
5			Procesamiento primario de recursos hidrobiológicos-Planta de Procesamiento Primario
6		CITEagroindustrial Chavimochic	Servicios de asistencia técnica en Implementación de sistemas de gestión en empresas de la región y a nivel nacional
7			Servicios de capacitación en gestión de la cadena agroindustrial
8			Servicios de laboratorio microbiológico y fisicoquímico
9			Servicios de estudio de estabilidad de alimentos
10			Elaboración de normas técnicas
11			Servicio de Diseño, Desarrollo y/o mejora de productos (bienes y servicios)
12			Servicio de capacitación en producción en la cadena agroindustrial
13			Participación y formulación de proyectos de investigación aplicada
14			Servicios de competencias laborales
15			Formulación de proyectos
16			Imagen y diseño grafico
17			Capacitaciones
18			Trámites administrativos
19			Servicio de Diseño, Desarrollo y/o mejora de productos (bienes y servicios)
20		CITEagroindustrial Huallaga	Área de Mantenimiento
21			Laboratorio de Microbiología
22			Laboratorio de Físico-Química
23			Oficina Administrativa-Oficina de Especialistas
24			Planta Piloto derivados de cacao
25			Planta Piloto de frutas
26			Planta Piloto de Café
27		Unidad Técnica Agroindustrial Ambo	Asistencia Técnica
28			Laboratorio
29			Diseño y desarrollo de nuevos productos-transferencia tecnológica
30			Proyectos
31			Capacitación
32			Articulación
33		CITEagroindustrial Ica	Atención de unidades productivas
34			Gestión Operativa
35			Gestión administrativa
36			Gestión del CITE
37		Unidad Técnica Agroindustrial Huaura	Atención de proceso productivo para la UP en el sector agroindustrial
38			Atención y orientación al usuario
39			Asistencia y asesoramiento técnicos
40		CITEagroindustrial Majes	Capacitaciones
41			Desarrollo de actividades administrativas

42		**CITEagroindustrial Moquegua**	Atención al cliente para recepción de solicitudes de servicios y recepción de documentos del ITP
43			Atención de servicios de asistencia técnica, capacitación, soporte productivo
44			Elaboración de requerimientos y seguimientos de pago de proveedores
45		**CITEagroindustrial Oxapampa**	Atención al cliente para recepción de solicitudes de servicios, y recepción de documentos del ITP
46			Atención de servicios de asistencia técnica, capacitación y formulación de proyectos en modalidad virtual
47			Elaboración de requerimientos y seguimientos de pago de proveedores
48		**CITEagroindustrial VRAEM**	Soporte productivo
49			Ensayo de laboratorio
50		**CITE Ccal Arequipa**	Sismos: Durante el sismo las personas deben mantenerse ubicados en las zonas de seguridad del área de trabajo, las cuales deben estar señalizadas.
51			Explosión volcánica: Difundir las rutas de evacuación más apropiada y menos expuesta a los efectos de la erupción.
52			Incendio: Contar con todos los medios de extinción operativos y vigentes.
53		**CITE Ccal Lima**	Área Administrativa: Evaluar de daños en las instalaciones del CITE Ccal y reportar al ITP. Elaborar el Plan de trabajo del CITE Ccal en el contexto de emergencia
54			Área Administrativa: Actividades de gestión presupuestal, de acuerdo al resultado de la evaluación del CITE Ccal. Coordinar las actividades de limpieza y mantenimiento del CITE Ccal con el personal de mantenimiento
55			Área Administrativa: Actividades de trámite documentario asociadas a la respuesta a la emergencia. (Presencial o virtual)
56			Área Administrativa: Coordinar con el Director las actividades de seguridad salud en el trabajo y participar en la elaboración del Plan de trabajo del CITE Ccal en el contexto de emergencia.
57			Área Administrativa: Evaluar el funcionamiento de los equipos informáticos y ponerlos en funcionamiento (internet, computadoras, etc.).
58			Área Administrativa: Actividades de comunicación al personal. Actualización de redes sociales del CITE Ccal en el contexto de emergencia.
59			Área Administrativa: Mantener informado a los clientes sobre los servicios que se brindan en el contexto de emergencia
60			Unidades Operativas: Evaluar la condición de operación de la Unidad de ID y determinar la posibilidad de brindar servicios dentro del contexto de emergencia. Definir fecha de operaciones
61			Unidades Operativas: Evaluar la condición de operación del área de CCL y determinar la posibilidad de brindar servicios dentro del contexto de emergencia. Definir fecha de operaciones
62			Unidades Operativas: Evaluar la condición de operación del área de AT y determinar la posibilidad de brindar servicios dentro del contexto de emergencia. Realizar un sondeo de impacto en las empresas. Estimar daños en el sector. Definir fecha de operaciones.
63			Unidades Operativas: Evaluar la condición de operación de la Unidad de Laboratorio y determinar la posibilidad de brindar servicios dentro del contexto de emergencia. Definir fecha de operaciones
64			Unidades Operativas: Evaluar la condición de operación del área de capacitación y determinar la posibilidad de brindar servicios dentro del contexto de emergencia. Definir fecha de operaciones
65		**CITE Ccal Trujillo**	Limpieza y mantenimiento del CITE
66			Actividades administrativas
67			Actividad de soporte técnico

68			Verificar el adecuado funcionamiento de equipos de las plantas piloto
69			Área de Diseño
70		**CITEforestal Maynas**	Área Administrativa: Revisión de correos electrónicos institucionales. Ingresar al SGD
71			Área de Capacitación: Gestión documentaria y desarrollo de cursos virtuales y presenciales
72			Área de Asistencia Técnica: Atención a las empresas del sector forestal para el desarrollo de asistencia técnica o asesorías técnicas
73			Área de Dirección: Gestión Documentaria
74			Área de Transferencia Tecnológica: Gestión documentaria de todos los servicios de soporte productivo
75		**CITE forestal Pucallpa**	Desarrollo de registros, facturas, reportes por medio de los sistemas de gestión implementado por el ITP, e internos
76			Operación de las plantas piloto
77		**CITE madera**	Área Administrativa
78			Soporte Productivo
79			Servicios de Asistencia Técnica
80			Capacitación
81		**CITE pesquero Callao**	Provisión de energía eléctrica y agua potable
82			Manipuleo
83			Producción de pastas y preformados
84			Producción de Conservas
85			Aseguramiento de la calidad
86		**CITE pesquero Ilo**	Dirección del CITE pesquero Ilo
87			Administración
88			Área Técnica
89		**CITE pesquero Piura**	Verificar el estado de la infraestructura de las oficinas, equipos de cómputo y mobiliario
90			Limpieza y desinfección de las oficinas y mobiliario
91			Verificar el estado de la infraestructura dela almacén y equipos de laboratorio
92			Limpieza y desinfección del almacén y de los equipos
93		**CITE pesquero amazónico Pucallpa**	Gestión Operativa del CITE
94			Emisión y/o recepción de documentación
95			Atención de servicios solicitados
96			Reporte de servicios atendidos
97			Contratación de servicios para el mantenimiento de equipos
98			Contratación de servicios de terceros
99			Compra de bienes y/o suministros
100			Soporte Informático
101			Generación de contenidos comunicacional
102			Transporte Institucional
103		**CITE productivo Maynas**	Atención y envío de información que solicite el ITP, trabajo articulado con instituciones y autoridades locales
104			Atención y envío de cartas, oficios, memorandos, contratos locadores, pagos de proveedores de bienes y servicios, entre otros
105			Traslados del personal del CITE de acuerdo a las necesidades
106			Brindar atención a las unidades productivas agroindustriales y pesqueras de la región Loreto
107		**CITE productivo Madre de Dios**	Actividades laborales de forma remota
108			Asistencia técnica a usuarios vía remota
109			Capacitaciones a usuarios vía remota
110			Actividades administrativas
111			Adquisición de bienes y servicios
112		**CITEtextil camélidos Arequipa**	Realizar servicios de capacitación de manera virtual o utilizando las instalaciones de otras entidades
113			Asistencia técnica
114			Promoción de I+D+i

115			Articulación
116			Información tecnológica especializada.
117			Realizar servicios de soporte productivo siempre y cuando la infraestructura y/o equipamiento tecnológico lo permita
118		**CITEtextil camélidos Cusco**	Arranque, operación y/o parada de la planta de teñido, acabados, PTARND
119			Difusión de información y supervisión de los medios de comunicación (redes sociales)
120			Acciones Administrativas
121		**CITEtextil camélidos Puno**	Capacitación en clasificación de fibra de alpaca, lavado de fibra de alpaca y prendas y accesorios textiles
122			Cursos de capacitación a medida o Asistencia Técnica programados por el mismo cliente.
123			Coordinación, Seguimiento y reporte de informes de servicios ejecutados y acciones de articulación con entidades de apoyo.

Fuente: Grupo de Comando para la Gestión de la Continuidad Operativa.

6.2. Aseguramiento del Acervo Documentario

La Unidad Funcional de Atención al Ciudadano y Gestión Documental (UFACGD), deberá contar con el acervo documentario digitalizado, asegurando su valor legal y conservación adecuada en caso de suscitarse un evento y/o emergencia de gran magnitud.

En el anexo N° 6, se adjunta el Procedimiento de aseguramiento del acervo documentario.

6.3. Aseguramiento de la Base de Datos

La Oficina de Tecnologías de la Información (OTI), deberá de establecer las medidas necesarias para el funcionamiento de los servicios de tecnología de información necesarios que permitan una posterior recuperación en caso de ocurrir un evento y/o emergencia de gran magnitud, que permita la continuidad en la ejecución de las actividades identificadas como críticas.
En el anexo N° 7, se adjunta el Plan de Recuperación de los servicios informáticos; asimismo en el anexo N° 8, el Informe de Implementación de Mejoras de los Servicios Informáticos.

6.4. Roles y responsabilidades para el desarrollo de las actividades críticas

a. Actividades de Apoyo ante desastres y/o emergencias

Ante la ocurrencia de eventos de gran magnitud se han considerado como actividades de apoyo, aquellos procesos que se relacionados con brindar soporte y facilidades de operación de las actividades críticas identificadas, para lo cual se considera a las siguientes oficinas para ejecutar los procesos mínimos requeridos de la Entidad:

Tabla N° 12.Oficinas de Apoyo.

Oficinas	Áreas	Funciones
Unidad Orgánica para la gestión de la Continuidad Operativa	OGRRHH (encargado)	Asegurar la implementación de la Continuidad Operativa
OA	Servicios Generales	Asegurar la disponibilidad de recursos físicos para la ejecución de actividades críticas y de apoyo
	Abastecimiento	
	Contabilidad	
	Tesorería	

	Transporte	
OPPM	Aprobar requerimientos presupuestales	Asegurar la disponibilidad de presupuesto para la ejecución de actividades críticas y de apoyo
	Proponer y gestionar las modificaciones presupuestarias	
OTI	Soporte Técnico	Asegurar la disponibilidad de los medios informáticos para el soporte en la ejecución de las actividades críticas y de apoyo
	Gestionar la capacidad de procesamiento de redes y seguridad informática	
OGRRHH	Administración de personal	Asegurar la disponibilidad de recursos humanos para la ejecución de las actividades críticas y de apoyo
	Bienestar Social	
	Seguridad y Salud en el Trabajo	

Fuente: Grupo de Comando para la Gestión de la Continuidad Operativa.

Asimismo, en caso de la ocurrencia de un desastre y/o emergencia de gran magnitud en alguna de las regiones donde se ubica la red CITE, se deberá coordinar con las oficinas de apoyo de la Sede Central señaladas en la tabla N° 9, a fin de continuar con el funcionamiento mínimo para el apoyo a las empresas y sectores productivos:

Tabla N° 13. Órganos desconcentrados-Red CITE.

	Funciones
Red CITE	Brindar asistencia técnica y capacitación en relación a procesos, productos y servicios que se podrían ejecutar posterior al evento de gran magnitud.
	Asesorar iniciativas de cooperación empresarial y de interrelación con otros agentes estratégicos que puedan generar mayor productividad durante la emergencia.
	Brindar los servicios de forma accesible a los empresarios, según la cadena productiva mientras dure la emergencia.

Fuente: Grupo de Comando para la Gestión de la Continuidad Operativa.

6.5. Requerimientos

6.5.1. Requerimiento de Personal

a. Sede Central

El personal determinado para el desarrollo de las actividades críticas, considerando un escenario de continuidad operativa lo conforman **85 trabajadores** de las cuales **30 corresponden a la modalidad presencial** y **55 a modalidad remota**. A continuación, se detalla la distribución en la tabla siguiente:

Tabla N° 14. Distribución de personal-Sede Central.

DIRECCIÓN/OFICINA	**MODALIDAD**	
	PRESENCIAL(Sede Alterna)	**REMOTO**
DE	1	1
SG	1	1
SG – UFII	1	1
SG – UFCII	1	2
SG - UFACGD	1	2
DEDFO	2	3
DIDITT	2	4
DSE	2	3
DO	2	8
OA	12	9

OAJ	1	2
OCI	1	1
OTI	3	4
OGRRHH	4	3
OPPM	1	6
TOTAL	**30**	**55**

Fuente: Data personal de OGRRHH (CAS, 728, Practicantes). Junio 2023. Elaboración propia

También se considera el personal que, sin intervenir de forma directa en la ejecución de las actividades relacionadas a continuidad operativa, se considera a quienes toman decisiones estratégicas o como apoyo en caso de interrupción de labores, a este grupo se le ha considerado para labores remotas en caso de activarse el Plan de Continuidad Operativa. El número es de **13 personas.**

Tabla N° 15. Personal Clave-Sede Central.

PERSONAL CLAVE	**MODALIDAD**	
	PRESENCIAL (Sede Alterna)	**REMOTO**
GRUPO COMANDO		7
GRUPO DE TRABAJO DE GESTIÓN DE RIESGO DE DESASTRES		2
OGRRHH (SST, Bienestar Social)	4	
TOTAL	**4**	**9**

Fuente: OGRRHH. Elaboración propia

El total de personal a considerar en caso de continuidad operativa es de **98 personas.**

b. Red CITE

Tabla N° 16. Distribución de personal - Red CITE.

CITE	**RECURSO HUMANO REQUERIDO**
CITE ACUICOLA PESQUERO - AHUASHIYACU	9
CITEAGROINDUSTRIAL - CHAVIMOCHIC	11
CITEAGROINDUSTRIAL - HUALLAGA	9
UNIDAD TÉCNICA AGROINDUSTRIAL AMBO	6
CITEAGROINDUSTRIAL - ICA	10
UNIDAD TÉCNICA AGROINDUSTRIAL HUAURA	9
CITEAGROINDUSTRIAL - MAJES	5
CITEAGROINDUSTRIAL - MOQUEGUA	7
CITEAGROINDUSTRIAL - OXAPAMPA	7
CITEAGROINDUSTRIAL - VRAEM	4
CITECCAL - AREQUIPA	7
CITECCAL - LIMA	12
CITECCAL - TRUJILLO	8
CITEFORESTAL - PUCALLPA	4
CITEFORESTAL MAYNAS	7
CITEMADERA - LIMA	15
CITEPESQUERO - CALLAO	15
CITEPESQUERO - ILO	7
CITEPESQUERO - PIURA	6
CITEPESQUERO AMAZÓNICO - PUCALLPA	9
CITEPRODUCTIVO - MADRE DE DIOS	5
CITEPRODUCTIVO - MAYNAS	5

CITEPESQUERO - PIURA	6
CITEPESQUERO AMAZÓNICO - PUCALLPA	9
CITEPRODUCTIVO - MADRE DE DIOS	5
CITEPRODUCTIVO - MAYNAS	5
CITETEXTILCAMELIDOS - AREQUIPA	8
CITETEXTILCAMELIDOS - CUSCO	4
CITETEXTILCAMELIDOS - PUNO	7

Fuente: Red CITE. Elaboración propia.

c. Personal Clave y de apoyo ante desastre y/o emergencia

Para la Continuidad Operativa se deberá de disponer de personal clave que será convocado para realizar las actividades críticas en el caso de que la infraestructura haya resultado afectada restringiendo su acceso, habilitando los sistemas de información para la continuidad del servicio.

El personal que será convocado se señala en las tablas siguientes:

Tabla N° 17. Personal clave titulares y suplentes del GCGCOOP.

UNIDADES DE ORGANIZACIÓN	PERSONAL CLAVE	
	Titular	**Suplente**
DE	Director/a Ejecutivo/a	Secretario/a General
SG	Secretario/a General	Asesor/a
DO	Director/a	Personal alterno designado
OGRRHH	Jefe/a	Personal alterno designado

Fuente: OGRRHH. Elaboración propia.

Tabla N° 18. Personal de Apoyo-Titulares y Suplentes.

UNIDADES DE ORGANIZACIÓN	PERSONAL CLAVE	
	Titular	**Suplente**
OPPM	Jefe/a	Personal alterno designado
	Especialista	Personal apoyo designado
OA	Jefe/a	Personal alterno designado
	Coordinador de Abastecimiento	Personal alterno designado
	Encargado de Servicios Generales	Personal apoyo designado
	Analista de compras	Personal apoyo designado
	Especialista de Ejecución Contractual	Personal apoyo designado
	Coordinador de Tesorería	Personal alterno designado
	Especialista	Personal apoyo designado
	Coordinador de Contabilidad	Personal alterno designado
	Especialista	Personal apoyo designado
OGRRHH	Especialista SSOMA	Personal apoyo designado
	Especialista de Bienestar Social	Personal apoyo designado
	Médico Ocupacional	Personal apoyo designado
	Especialista de Compensaciones	Personal apoyo designado
OTI	Jefe/a	Personal alterno designado
	Especialista Soporte Técnico	Personal apoyo designado
	Especialista en Redes	Personal apoyo designado
	Analista en Asistencia Técnica	Personal apoyo designado
UFACGD	Coordinadora/a	Personal alterno designado
	Analista	Personal apoyo designado

Fuente: OGRRHH. Elaboración propia.

6.5.2. Requerimiento de Recursos Informáticos

Es necesario asegurar la disponibilidad de los equipos, sistemas y aplicaciones informáticas, ya sea para realizar trabajo remoto o para los servicios que se ejecutarán en la Sede Alterna de la Entidad. Los equipos informáticos mínimo necesarios para el personal clave y de apoyo para la Continuidad Operativa, se detalla en las tablas a continuación:

a. Sede Central

Tabla N° 19. Recursos Informáticos-Sede Central.

DIRECCIÓN/OFICINA	RESPONSABLE	CANTIDAD	RECURSOS INFORMÁTICOS	
			HARDWARE	SOFTWARE
DE	Director/a Ejecutivo/a Asesor/a	2	Laptop	Office, SGD, Programas para reuniones virtuales (Teams, Zoom), Correo electrónico
SG	Secretario/a General Asesor/a	2	Laptop	Office, SGD, Programas para reuniones virtuales (Teams, Zoom), Correo electrónico
SG – UFII	Coordinador/a Especialista	2	Laptop	Office, SGD, Programas para reuniones virtuales (Teams, Zoom), Correo electrónico
SG – UFCII	Coordinador/a Especialistas (2)	3	Laptop	Office, SGD, Programas de diseño de contenido, acceso a redes sociales, Programas para reuniones virtuales (Teams, Zoom), Correo electrónico
SG - UFACGD	Coordinador/a Profesional (1) Asistente (1)	3	Laptop	Office, SGD, Programas para reuniones virtuales (Teams, Zoom), Correo electrónico
DEDFO	Director/a Asistente (1) Especialistas (3)	5	Laptop	Office, SGD, Programas para reuniones virtuales (Teams, Zoom), Correo electrónico
DIDITT	Director/a Asistente (1) Especialistas (4)	6	Laptop	Office, SGD, Programas para reuniones virtuales (Teams, Zoom), Correo electrónico
DSE	Director/a Asistente (1) Especialistas (3)	5	Laptop	Office, SGD, Programas para reuniones virtuales (Teams, Zoom), Correo electrónico
DO	Director/a Asistente (1) Especialistas (4) Coordinadores (2) Analistas (2)	10	Laptop	Office, SGD, Programas para reuniones virtuales (Teams, Zoom), Correo electrónico, Programas de diseño (Arc GIS, AutoCAD)
OA	Jefe/a Asistente (1) Abastecimiento (8) Contabilidad (3) Tesorería (3)	16	Laptop	Office, SGD, Programas para reuniones virtuales (Teams, Zoom), Correo electrónico, SIGA, SIAF
OAJ	Jefe/a Especialistas (2)	3	Laptop	Office, SGD, Programas para reuniones virtuales (Teams, Zoom), Correo electrónico

OCI	Jefe/a Asistente (1)	2	Laptop	Office, SGD, Programas para reuniones virtuales (Teams, Zoom), Correo electrónico
OTI	Jefe/a Especialista (2) Analista (3) Técnico (1)	7	Laptop	Office, SGD, Programas para reuniones virtuales (Teams, Zoom), Correo electrónico, software de base de datos, programación
OGRRHH	Jefe/a Especialistas (2) Gestor (1) Analista (1) Médico Ocupacional (2)	7	Laptop	Office, SGD, Programas para reuniones virtuales (Teams, Zoom), Correo electrónico
OPPM	Jefe/a Especialistas (3) Coordinadores (3)	7	Laptop	Office, SGD, Programas para reuniones virtuales (Teams, Zoom), Correo electrónico, SIGA, SIAF

Fuente: OGRRHH. Elaboración propia

b. Red CITE

Tabla N° 20. Recursos Informáticos-red CITE.

CITE	RESPONSABLE	CANTIDAD	RECURSOS INFORMÁTICOS	
			HARDWARE	SOFTWARE
CITE ACUICOLA PESQUERO - AHUASHIYACU	Técnico (1) Especialista (1)	2	Laptop	Office, SGD, Correo electrónico
CITEAGROINDUSTRIAL - CHAVIMOCHIC	Coordinador (3) Especialista (1)	4	Computadora de escritorio/laptop/proyector	Office, SGD, Correo electrónico
CITEAGROINDUSTRIAL - HUALLAGA	Especialista (2) Analista (1)	3	Monitores, CPU, impresoras, UPS	Office, SGD, Correo electrónico
UNIDAD TÉCNICA AGROINDUSTRIAL AMBO	Coordinador (1) Especialista (3) Analista (1) Asistente (1)	6	Laptop/proyector/USB	Office, Google Chrome
CITEAGROINDUSTRIAL - ICA	Director Especialista (6)	7	Laptop/cables de red	Office, SGD, SIGA, SSIPRO, Programas para reuniones virtuales (Teams, Zoom, Meet), Antivirus, Correo electrónico
UNIDAD TÉCNICA AGROINDUSTRIAL HUAURA	Especialista (1) Profesional (1) Responsable de área (1)	3	Laptop/Celular	Office, SGD, Programas para reuniones virtuales (Teams, Zoom), Correo electrónico
CITEAGROINDUSTRIAL - MAJES	Director (1) Especialistas (3) Asistente (1)	5	Laptop/Computadoras de escritorio	Office, SGD, SSIPRO, SIGA, E-STATAL, Programas para reuniones virtuales (Teams, Zoom), Correo electrónico
CITEAGROINDUSTRIAL - MOQUEGUA	Asistente (1) Especialista (1)	2	Laptop/Computadora de escritorio/Celular	Office, SGD, SIGA, Programas para reuniones virtuales (Teams, Zoom), Correo electrónico
CITEAGROINDUSTRIAL - OXAPAMPA	Especialista (3) Asistente (2)	5	Laptop/Celular	Office, SGD, SSIPRO, SIGA, Programas para reuniones virtuales (Teams, Zoom), Correo electrónico

CITEAGROINDUSTRIAL - VRAEM	Especialista (1)	1	Laptop	Office, SGD, Google, SSIPRO, E-STATAL
CITECCAL - AREQUIPA	Director Brigadistas (3) Supervisor (1)	5	Laptops/Computadoras de escritorio/Impresoras	Office, SGD, Conexión a internet
CITECCAL - LIMA	Director/a Coordinador (1) Asistente (1) Analistas (6)	9	Computadora de escritorio	Office, SGD, Conexión a internet
CITECCAL - TRUJILLO	Especialista (1) Analista (1) Auxiliar (1) Asistente (4) Técnico (1)	8	Computadora de escritorio/ laptop/impresora/cables de red	Office, SGD, firma ONPE, correo electrónico, SIGA MEF, software de diseño
CITEFORESTAL - PUCALLPA	Especialista (1) Asistente (1)	2	Computadora de escritorio/disco duro	Office, SGD, correo electrónico, software de gestión-instalador, software para servidor local, software de gestión de almacén
CITEFORESTAL MAYNAS	Director Asistente (2) Analista (3) Especialista (1)	7	Laptop/Celular	Office, SGD, Programas para reuniones virtuales (Zoom, Classroom), Correo electrónico, SSIPRO, whatsapp
CITEMADERA - LIMA	Especialista (1) Coordinador (1) Capacitador (1)	3	Computadoras/Teléfonos/ Radios	Office, SGD, Programas para reuniones virtuales (Zoom, Meet), Correo electrónico
CITEPESQUERO - CALLAO	Especialista (3) Técnico (2)	5	Laptops	Ofimática básica
CITEPESQUERO - ILO	Especialista (2) Asistente (1)	3	Laptop/Celular	Office, SGD, Correo electrónico, firma digital
CITEPESQUERO - PIURA	Director Coordinador (1)	2	Laptop/Computadoras de escritorio	Office, SGD, Correo electrónico
CITEPESQUERO AMAZÓNICO - PUCALLPA	Director/a Asistente (1) Especialistas (2) Coordinador (1) Comunicador (1)	6	Laptop/ Impresora	Office, correo electrónico firma ONPE, SGD, redes sociales
CITEPRODUCTIVO - MADRE DE DIOS	Director/a Especialista (3 Asistente (1)	5	Laptop/Celular/Computadora de escritorio	Office, SGD, Programas para reuniones virtuales (Zoom, Teams), servidor del CITE
CITEPRODUCTIVO - MAYNAS	Director/a Asistente (1) Especialista (2)	4	Laptop/Celular/Computadora de escritorio/impresora	Office, SGD, Programas para reuniones virtuales (Zoom, Teams)
CITETEXTILCAMELIDOS - AREQUIPA	Especialista (3) Asistente (1)	4	Laptop/Celular/Computadora de escritorio/mouse	Office, SGD, SSIPRO, STATAL, softwares especializados Shima Seiki-SDS ONE APEX, Illustrator Programas para reuniones virtuales (Zoom, Teams)
CITETEXTILCAMELIDOS - CUSCO	Asistentes (3)	3	Computadoras de escritorio	Office, SGD, SIGA, SIAF, Google Chrome
CITETEXTILCAMELIDOS - PUNO	Especialista (1) Analista (2)	3	Laptop/Celular/Computadora de escritorio/impresora	Office, SGD, Programas para reuniones virtuales (Zoom, Teams)

Fuente: Red CITE.

6.5.3. Requerimiento de Recursos Físicos Críticos

La disponibilidad para de mobiliario para ejecutar las labores en la Sede Alterna de la Entidad, se detalla en las tablas a continuación:

a. Sede Central

Tabla N° 21. Recursos Físicos-Sede Central.

DIRECCIÓN/OFICINA	RESPONSABLE	RECURSOS FÍSICOS	
		SILLA	ESTACIÓN DE TRABAJO
DE	Director/a Ejecutivo/a	1	1
	Asesor/a	1	1
SG	Secretario/a General	1	1
	Asesor/a	1	1
SG – UFII	Coordinador/a	1	1
	Especialista	1	1
SG – UFCII	Coordinador/a	1	1
	Especialistas	2	2
SG - UFACGD	Coordinador/a	1	1
	Profesional	1	1
	Asistente	1	1
DEDFO	Director/a	1	1
	Asistente	1	1
	Especialistas	3	3
DIDITT	Director/a	1	1
	Asistente	1	1
	Especialistas	4	4
DSE	Director/a	1	1
	Asistente	1	1
	Especialistas	3	3
DO	Director/a	1	1
	Asistente	1	1
	Especialistas	4	4
	Coordinadores	2	2
	Analistas	2	2
OA	Jefe/a	1	1
	Asistente	1	1
	Abastecimiento	8	8
	Contabilidad	3	3
	Tesorería	3	3
OAJ	Jefe/a	1	1
	Especialistas	2	2
OCI	Jefe/a	1	1
	Asistente	1	1
OTI	Jefe/a	1	1
	Especialista	2	2
	Analista	3	3
	Técnico	1	1
OGRRHH	Jefe/a	1	1
	Especialistas	2	2
	Gestor	1	1
	Analista	1	1
	Médico Ocupacional	2	2
OPPM	Jefe/a	1	1
	Especialistas	3	3
	Coordinadores	3	3

Fuente: GCGCOOP.

b. Red CITE

Tabla N° 22. Recursos Físicos-Red CITE.

CITE	RECURSOS FÍSICOS		
	OFICINA	**LABORATORIO**	**PLANTA PILOTO**
CITE ACUICOLA PESQUERO - AHUASHIYACU	Escritorios, armarios, sillas	**Laboratorios de I+D+i, Peces amazónicos:** Multiparámetro, kit de calidad de agua, hidrolavadora, balde, recogedor, escobas, bombas de agua, alimento balanceado, bicarbonato de sodio o sesquicarbonato, blowers, filtro de arena, tanques de fibra de vidrio, filtro UV. **Laboratorio de Producción de alimento vivo**: luminarias, matraces, tubos, aire acondicionado, microalgas y levadura, pipeteaor automático, pipetas, phmetro, equipo multiparámetro, tanques de fibra de vidrio, blowers, luminarias, materiales de limpieza. **Laboratorios de I+D+i Tilapia:** Blowers, bombas de agua, tanques de fibra de vidrio, tanques de geomembrana, filtros de arena, filtro UV. **Laboratorio de investigación y análisis:** Ultracongeladora, tanques de CO2, cabina de flujo laminar, microscopios, esteroscopios, refrigeradoras, autoclaves, incubadoras, estufas, balanzas, congeladoras, baño maría, mufla, campana de extracción, determinador de grasa, proteína y fibra, fotómetro, centrifugas, procesador de tejido, micrótomo.	**Planta de procesamiento primario:** Hidrolavadora, mangueras, escobas, escobillas, recogedores, canastillas, cajas plásticas, contenedores isotérmicos, parihuelas, mesas de acero inoxidable, máquina de hielo, secador de aire frío, selladora al vacío, cortadora de carne y hueso, mezcladora de carne, selladora continua.
CITEAGROINDUSTRIAL - CHAVIMOCHIC	Escritorios, sillas, material didáctico (servicios del CITE)	**Laboratorio Microbiológico y fisicoquímico:** Equipos de laboratorio (según análisis), material de vidrio, medios de cultivo y reactivos.	**Servicios de estudio de estabilidad de alimentos:** incubadoras. **Servicios de diseño, desarrollo y/o mejora de productos (bienes y servicios):** Maquinaria de planta

CITEAGROINDUSTRIAL - HUALLAGA	**Oficinas administrativas/especialistas:** Puertas, ventanas y mamparas de vidrio laminado, equipos de ventilación y tomacorrientes, extintor (PQS-CO2) **Área de Mantenimiento**: Grupo electrógeno, cuartos de electrobombas presurizadas, equipo de presión contra incendio, PETAR, cabes eléctricos subterráneos, luminarias, puertas, ventanas y mamparas de vidrio laminado.	Puertas, ventanas y mamparas de vidrio laminado. Muflas, cromatógrafo, contador de coloninas, espectofotómetro, generadores de hidrógeno, bombas de vacío, equipo de tratamiento de agua, colorímetros, centrífugas de vacío, incubadoras, refrigeradoras, estufas, balanzas. Reactivos. Extintores (CO2-PQS)	**Derivados de Cacao:** Planta Molino de discos de dos etapas, contadora de nylon, molino pulverizador, prensa hidráulica de manteca de cacao, grajeadora, mezcladoras, molino refinadoras de villas, cámaras de frío, selladoras continuas, atemperador vertical aire acondicionado, triturador de tortas filtros de manteca. **Frutas:** Etiquetadora semiautomática, dosificador de líquidos semiautomática, cerradoras de latas, autoclaves, lavadoras sumergibles, concentrador de vacío, escaldadora, pulpeadora de frutas, rodajadora, exhauster, dosificar en polvo, marmita, licuadora industrial, deshidratador de frutas, molino de polvo. **Café:** Balanzas, molino de discos, selladora continua.
UNIDAD TÉCNICA AGROINDUSTRIAL AMBO	**Asistencia Técnica:** kit de herramientas	Potenciómetro, estufa, mufla, balanza (analítica, precisión, humedad), conductimetro	Cocina, utensilios, jarras medidoras
CITEAGROINDUSTRIAL - ICA	Camioneta institucional, grupo electrógeno	-	-
UNIDAD TÉCNICA AGROINDUSTRIAL HUAURA	**Atención y orientación al usuario:** Escritorios, sillas, block de notas, formularios y registros impresos	**Asistencia y asesoramiento técnicos:** Indumentaria institucional, block de notas, instrumentos de laboratorio, material bibliográfico.	**Proceso productivo:** tanques alimentarios, mesas de acero inoxidable para proceso alimentario, bandejas de plástico para botellas de producto terminado, indumentaria institucional, block de notas.
CITEAGROINDUSTRIAL - MAJES	Escritorios, sillas	-	-
CITEAGROINDUSTRIAL - MOQUEGUA	Escritorios, sillas	-	-
CITEAGROINDUSTRIAL - OXAPAMPA	Escritorios, sillas	-	-
CITEAGROINDUSTRIAL - VRAEM	Escritorios, sillas	Zaranda, tostador de laboratorio, descascarillador de laboratorio, triturador, refinador de laboratorio	Seleccionador de granos, tostador de granos, descascarillador, molino, balanza, refinadores, conchadores, micrómetro, cámara de frío, homogenizador
CITECCAL - AREQUIPA	Grupo electrógeno, camioneta	-	Máquina del taller de aparado, maquinaria de planta de curtiembre, equipos de la PTAR
CITECCAL - LIMA	Bienes de oficina, implementos de limpieza	Bienes de oficina	Bienes de oficina

CITECCAL - TRUJILLO	**Actividades Administrativas:** Escritorios, sillas, papelería. **Limpieza y mantenimiento del CITE:** escobas, trapos, desinfectante, lejía, baldes, mangueras, recogedores, proveedor de cisterna de agua, bolsas de basura	-	**Área de diseño:** Cuchillas, chavetas, planchas de cartón piedra, mantas de cuero, punzones y cabezal de reemplazo para pantógrafo. **Planta piloto:** Aditivos, pegamento, insumos para la fabricación de calzado **Soporte técnico:** desarmadores, alicates, guantes aislantes, multímetro digital, fusibles, llaves térmicas, switch, repetidores
CITEFORESTAL - PUCALLPA	Archivadores, estabilizador de corriente, grupo electrógeno de 5 KV.	-	Red de tuberías contra incendios (tubos, mangueras, válvulas, entre otros)
CITEFORESTAL MAYNAS	Escritorios, sillas, grupo electrógeno	-	-
CITEMADERA - LIMA	Herramientas, señalizaciones, luces de emergencia, bienes de oficina **Capacitación:** transporte, economato	-	**Soporte productivo:** Energía eléctrica, aceite, fajas, aditivos, herramientas, señalizaciones, luces de emergencia, gas licuado de petróleo **Servicios de asistencia técnica:** transporte, equipos de seguridad (EPP), megáfono
CITEPESQUERO - CALLAO	**Provisión de energía eléctrica y agua potable:** Subestación eléctrica compuesta por: (1) Transformador de potencia BBICT 640 KVA TENSIÓN 10/0.46, (2) Transformador de potencia OSAKA 300 KVA Tensión 10/0.23, (3) Transformador de potencia ELECTROVARA 400 KVA Tensión 10/0.11, (4) Transformador de potencia S/M 50 KVA Tensión 10/0.11, (5) Transformador de potencia S/M 50 KVA Tensión 10/0.11. Bomba sumergible de alta potencia (10 hp profundidad: 35 m.) Tanques de ablandamiento de agua por resina (2 Tanques de 40 pies cúbicos) 30 m3/regeneración (3 sacos de sal 50 kilos cada saco) 30-70 m3 por día de producción. Tanque Cloro (68 kg) Cloro gaseoso (0.8 -	**Aseguramiento de la calidad:** Termómetro, balanza de humedad, pH-metro, Kit de Cloro / Dureza, Tiras de pH, Balanza 10 Kg, Cocina freidora, Horno microondas, Insumos químicos para limpieza (Lejía, jabón, detergente, quita sarro)	**Manipuleo:** Mesas de Acero Inoxidable 314 (3m*1m.), balanza de Plataforma (1000 Ton capacidad), Productor de hielo en cubos - 700 Kg/día, Cámaras de refrigeración Refrigerante Amoniaco, Carretillas hidráulicas (x2), Contenedores isotérmicos ("DYNO") x 5 unidades. **Producción de pastas y preformados:** Sierra cinta, Balanza Producto Terminado (60 kg), Trituradora (250 kg/hora), Mezcladora (250 kg/batch) Balanza Materia Prima (500 kg), 100 Cajas de plástico duro alimentario, Balanza (5 kg), 2 unidades - Balanza de control de peso (5 kg), 2 unidades - Selladora Continua, Equipo de inspección por Rayos X, Congelado continuo en IQF o túnel de congelación, 2

	producción. Tanque Cloro (68 kg) Cloro gaseoso (0.8 - 1 ppm) dosificador de cloro. 2 tanques de almacenamiento (tanque dura 100 m3 -> ablandamiento -> 70 m3). 1 motobomba (7 hp)-jardines y alimentar agua blanda. 1 motobomba (10 hp)-jardines y alimentar agua blanda. 1 motobomba (5 hp), agua ablandada para planta.		Congelado continuo en IQF o túnel de congelación, 2 Traspaletas (1500 kg y 2000 kg) **Producción de conservas:** 02 Autoclaves, 06 cerradoras de latas, cocinador continuo y estático, Línea de Codificado, Línea de Procesamiento de Conservas de Anchoveta, HERMASA, Línea de Procesamiento de Conservas Tradicionales, 06 cerradoras, 01 cocinador continuo, 02 cocinadores estáticos, 01 exhaustor, 01 línea de codificado, 02 marmitas, 02 licuadoras 04 balanzas, 01 licuadora, 04 balanzas
CITEPESQUERO - ILO	Unidad vehicular	-	-
CITEPESQUERO - PIURA	Equipamiento, escritorios, sillas, mesón de reuniones, archivadores	Selladora al vacío, selladora de pedal, autoclave, multiparametro, microscopio, contador de partículas, luxómetro, anemómetro, colorimetro	-
CITEPESQUERO AMAZÓNICO - PUCALLPA	Escritorios, sillas, grupo electrógeno, camioneta	-	Equipos de planta (diversos por servicios)
CITEPRODUCTIVO - MADRE DE DIOS	Camioneta, motocicleta, bicicleta	-	-
CITEPRODUCTIVO - MAYNAS	Energía eléctrica, combustible, camioneta, escritorios, sillas, hojas bond, lapiceros, engrapador, sobres, ente otros	-	Equipos para plantas de procesos agroindustriales y pesqueros
CITETEXTILCAMELIDOS - AREQUIPA	Escritorios, sillas, movilidad	-	-
CITETEXTILCAMELIDOS - CUSCO	Escritorios, sillas, grupo electrógeno	-	**Teñido, Acabados, PTARND**: Grupo electrógeno, caldero, bombas de agua, ablandador de gua, tanque de condensado, vaporizadora, lavadora, secadora, máquina de teñido, embobinadora, tanque de dosificación, tanque de regulación de pH, bombas peristálticas, bomba de aire, tanque de tratamiento químico
CITETEXTILCAMELIDOS - PUNO	Escritorios, sillas, grupo electrógeno, útiles de oficina, banners institucionales, agua	**Capacitación a medida o asistencia técnica programados por el mismo cliente:** balanzas, materiales (ollas, cocinas, insumos, jarras, termómetro digital, phmetro, cucharas de laboratorio, equipo analizador de fibras.	**Clasificación de fibra de alpaca, lavado de fibra de alpaca, prendas y accesorios textiles:** termómetro digital, phmetro digital.

Fuente: Red CITE - GCGCOOP.

6.5.4. Requerimiento Presupuestal

A fin de dar cumplimiento a lo detallado en las actividades críticas, así como los recursos de personal, informáticos y físicos, se deberá gestionar y coordinar una partida presupuestal tanto para la Sede Central como la red CITE con la Oficina de Planeamiento, Presupuesto y Modernización (OPPM), para la disponibilidad en la ejecución de lo señalado en el presente Plan y la implementación de la Sede Alterna en el marco de la Gestión de la Continuidad Operativa.

6.6. Determinación de la Sede Alterna de Trabajo

a. Sede Central

La Sede Alterna es el espacio físico o infraestructura segura y accesible, determinada con anterioridad y de disponibilidad inmediata, que permite la ejecución de los servicios o actividades críticas señaladas en el Plan de Continuidad Operativa de la Entidad. Para ello, cuenta con el equipamiento necesario y servicios básicos indispensables, que opera con autonomía energética y de conectividad.

En caso de que no fuese posible continuar la ejecución de los servicios de la Entidad en las instalaciones principales mencionadas en el numeral 4.1, para el desarrollo de las actividades críticas señaladas en el presente Plan, con el fin de que se garantice el cumplimiento de la misión de la Entidad, se considerará como Sede Alterna para la Sede Central del ITP red CITE al CITE Ccal Lima ubicado en Av. Caquetá 1300, Rímac.

Para determinar como Sede Alterna al CITE Ccal Lima, se consideró la evaluación de nivel de riesgos en las infraestructuras del sector Producción ubicadas en Lima Metropolitana y Callao, realizado por la Oficina de Seguridad y Defensa Nacional del Ministerio de la Producción (OSDN-PRODUCE), en el cual se determinó el nivel de peligro por sismos, así como el nivel de vulnerabilidad teniendo como resultado para el CITE en mención nivel de peligro y de vulnerabilidad bajo, lo cual representa un riesgo bajo, que no presenta un peligro significativo para la priorización de actividades, acciones, proyectos de inversión vinculados a la prevención y/o reducción del riesgo de desastres.

La Sede Alterna en mención deberá acondicionarse para que las oficinas de la Sede Central puedan ubicarse de forma que continúen con los principales servicios. Asimismo, la Sede Alterna deberá implementarse con módulos de trabajo de uso compartido, equipados con laptops, impresoras multifuncionales, teléfonos IP y analógico, mini central telefónica y red con conectividad independiente.

b. Red CITE

En el caso de ocurrir una afectación de gran envergadura en la red CITE, estas deberán articular con otras Instituciones ubicadas en la región donde ocurra el evento, a fin de colaborar interinstitucionalmente compartiendo un espacio físico para que pueda funcionar como Sede Alterna hasta la recuperación y/o reconstrucción de los espacios propios de los CITE que podrían verse afectados.

6.7. Activación del Plan de Continuidad Operativa

Para la activación del presente Plan se deberá considerar lo siguiente:

Tabla N° 23. Activación Plan de Continuidad Operativa.

FASES	MOMENTOS
Previa	Gestionar la disposición de recursos económicos a fin de implementar lo señalado en el Plan de Continuidad Operativa.
	Asegurar la disposición y/o adquisición de los requerimientos indicados para la gestión de la continuidad operativa.
Activación	Evaluación inicial y reporte de afectaciones en el lugar donde ha ocurrido la emergencia.
	Activación del PCO determinada por el Titular de la Entidad y/o a propuesta del Grupo Comando.
	Comunicación de la activación del PCO a cargo de la Unidad Orgánica responsable de la Gestión de la Continuidad Operativa: OGRRHH.
	Asegurar la disponibilidad de recursos para la óptima ejecución de actividades críticas.
	Convocatoria del personal involucrado en la ejecución de actividades críticas.
	Traslado de personal a la Sede Alterna y/o trabajo remoto de personal designado.
	Coordinación con proveedores externos para las condiciones de seguridad de personal e instalaciones.
	Coordinación con entidades de saneamiento y servicios básicos a fin de asegurar la operatividad de las actividades críticas.
	Coordinación con el Ministerio de la Producción para toma de decisiones.
Desactivación	Evaluación y reporte de las acciones de rehabilitación y/o reconstrucción de la infraestructura afectada de la Entidad.
	Desactivación del Plan de Continuidad Operativa.

Fuente: OGRRHH. Elaboración propia

a. Comunicación interna y externa

La Unidad Orgánica a cargo de la Continuidad Operativa (OGRRHH), coordinará con la Unidad Funcional de Comunicaciones e Imagen Institucional (UFCII), la emisión de una comunicación pública en la cual se indique la continuidad en la atención de los servicios.

Internamente, la OGRRHH, comunicará a los servidores del ITP red CITE de forma permanente la situación de las operaciones en la Entidad.

b. Punto de reunión del personal de apoyo ante desastres y/o emergencias

La Unidad Orgánica a cargo de la Continuidad Operativa (OGRRHH), convoca al personal de apoyo ante desastres y/o emergencias de las Direcciones y Oficinas que requieren ser trasladados a la Sede Alterna.

El punto de reunión para el traslado a la Sede Alterna (CITE Ccal Lima) sería la Sede San Isidro (Edificio Barlovento).

En la red CITE, el/la Director/a deberá informar a la Unidad Orgánica de la Continuidad Operativa (OGRRHH) el personal de apoyo y emergencia designado que asistirá al CITE y/o a la Sede Alterna definida.

c. Traslado del personal de apoyo ante desastres y/o emergencias

Para el traslado del personal de apoyo ante desastres y/o emergencias a la Sede Alterna la Oficina de Administración (OA), a través del área de Transporte trasladará al personal en mención desde el punto indicado en el literal anterior hasta la Sede Alterna indicada, en coordinación con la Unidad Orgánica de la Continuidad Operativa (OGRRHH).

En la red CITE, el/la Director/a deberá coordinar con la Oficina de Administración (OA), el traslado del personal de apoyo y emergencia designado que asistirá al CITE y/o a la Sede Alterna definida, en coordinación con la Unidad Orgánica de la Continuidad Operativa (OGRRHH).

d. Trabajo remoto

El personal designado por su Jefe y/o Director para desarrollar sus actividades críticas de forma remota, en caso de activación del Plan de Continuidad Operativa, deberá solicitar los equipos informáticos en coordinación con la Oficina de Tecnologías de la Información (OTI).

e. Evaluación y reporte de afectaciones

Para realizar la evaluación correspondiente a las afectaciones en la Entidad ante un evento de gran magnitud, se solicitará la designación de personal especialista a la Dirección de Operaciones (DO), a fin de señalar las medidas de rehabilitación y/o reconstrucción, el tiempo de ejecución y presupuesto requerido.

La DO deberá remitir el informe a la Unidad Orgánica de la Continuidad Operativa (OGRRHH), a fin de elevarlo al Grupo Comando y al Titular de la Entidad.

6.8. Activación y desactivación de la Sede Alterna

Para la activación y desactivación de la Sede Alterna se deberá considerar lo siguiente:

Tabla N° 24. Activación/desactivación Sede Alterna.

FASES	MOMENTOS
Previa	Gestionar la disposición de recursos económicos a fin de implementar la Sede Alterna.
	Asegurar la disposición y/o adquisición de bienes/servicios para el funcionamiento de la Sede Alterna.
Activación	Evaluación inicial de afectaciones.
	Reporte de afectaciones.
	Activación de la Sede Alterna.
	Actividades de rehabilitación y/o reconstrucción.
Desactivación	Evaluación y reporte de las acciones de rehabilitación y/o reconstrucción de la infraestructura afectada.
	Desactivación de la Sede Alterna.

Fuente: OGRRHH. Elaboración propia

6.9. Desarrollo de las actividades críticas

El capítulo seis del presente muestra las actividades críticas que deben ser desarrolladas luego de que el personal clave es convocado y comunicado por parte del GCGCOOP, mediante los procedimientos estipulados en anexos.

Con la finalidad de realizar el aseguramiento de a continuidad operativa de servicios y bienes del ITP se deben desarrollar labores que permitan el cumplimiento de las actividades críticas identificadas en los diversos procesos considerados como indispensables.

Para tal fin se ha estipulado el requerimiento e personal oficial y alterno, recursos informáticos, físicos y presupuestales para la organización para el desarrollo de las actividades críticas, en base a lo mencionado se realizan las especificaciones en el anexo número 4 del presente documento: Organización para el desarrollo de actividades críticas.

6.10. Cadena de Mando

Para la gestión de la Continuidad Operativa en la Entidad, se conformó el Grupo Comando, el cual está integrado por los siguientes miembros:

Tabla N° 25. Integrantes del GCGCOOP.

DIRECCIÓN/OFICINAS	INTEGRANTE
OGRRHH	Jefe/a o su representante
DO	Director/a o su representante
OA	Jefe/a o su representante
OTI	Jefe/a o su representante
OPPM	Jefe/a o su representante
OA	Jefe/a o su representante
UFACGD	Coordinador/a o su representante

Fuente: OGRRHH. Elaboración propia

El Grupo Comando deberá considerar el grado de afectación de la Entidad ante la ocurrencia de un evento de gran magnitud a fin de ejecutar las acciones pertinentes para la continuidad operativa:

Tabla N° 26. Acciones ante eventos de magnitud.

EVALUACIÓN DE DAÑOS A LA INFRAESTRUCTURA	HABITABILIDAD	DISPONIBILIDAD	ACCIONES A EJECUTAR
Sin afectaciones	Sin daños estructurales	Personal y recursos disponibles	Revisión de posibles riesgos secundarios. Continuidad de los servicios en la Sede Institucional.
Leve	Daños mínimos no estructurales	Persona y recursos sin daño, pero con afectación emocional	Evaluación de las condiciones de riesgo.

Moderado	Daños de fisuras u grietas en la estructura	Mínimo porcentaje de daño y afectación de personal e infraestructura	Evacuación de personal. Valoración de evacuación de equipos de la Institución. Activación de Sede Alterna temporal.
Grave	Daño estructural en más dl 50% de la infraestructura	En hora laborable: afectación del personal y recursos	Coordinación para rescate. Atención de víctimas. Activación de Sede Alterna temporal.
Muy grave	Sede institucional colapsada o inminente colapso	En hora laborable: heridos, fallecidos, desaparecidos, recursos destruidos	Perímetro de seguridad de infraestructura colapsada. Identificación de personal afectado. Activación de Sede Alterna temporal.

Fuente: Oficina de Seguridad y Defensa Nacional-OSDN-PRODUCE

VII. CRONOGRAMA DE EJERCICIOS DEL PLAN DE CONTINUIDAD OPERATIVA

A fin de cumplir con los ejercicios de activación del Plan de Continuidad Operativa, se deberá integrar la Gestión de Continuidad Operativa a la cultura organizacional de la Entidad fortaleciendo el conocimiento de los servidores mediante capacitaciones sobre la implementación del Plan de Continuidad Operativa, así como los requerimientos necesarios para ello.

Es así que, se define el siguiente cronograma de ejercicios posterior a la aprobación mediante Resolución Ejecutiva del Plan de Continuidad Operativa del ITP red CITE:

Tabla N° 27. Cronograma de ejercicios.

FECHA	TIPO DE EVENTO Y/O EMERGENCIA	RESPONSABLES
Seis (06) meses	Sismo de gran magnitud	Grupo Comando ITP red CITE OGRRHH
Doce (12) meses	Incendio	
Dieciocho (18) meses	Ataque informático	

Fuente: Oficina de Seguridad y Defensa Nacional-OSDN-PRODUCE

Cabe mencionar que, lo detallado en el Plan se considerará en las simulaciones y simulacros programados según normativa vigente.

7.1. Actualización del Plan de Continuidad Operativa

El Grupo Comando del ITP red CITE en coordinación con la OGRRHH, en calidad de Unidad Orgánica a cargo de la Gestión de la Continuidad Operativa, se encargará de la actualización del presente Plan, considerando los motivos siguientes:

Tabla N° 28. Motivos de actualización del PCO.

N°	Motivo
1	A solicitud del Titular de la Entidad
2	A solicitud del Grupo Comando
3	Modificación de la normativa vigente

4	Modificación del Reglamento de Organización y Funciones
5	Modificación en la ubicación de la Sede Central, Sede Alterna y/o CITE
6	Creación de nuevo CITE público y/o Unidad Técnica
7	En caso de presentarse algún incidente posterior a los ejercicios de activación del Plan

Fuente: OGRRHH. Elaboración propia.

Asimismo, el Grupo Comando del ITP red CITE, realizará la revisión del presente Plan a los tres (03) meses posteriores a la aprobación del mismo mediante Resolución Ejecutiva, a fin de considerar los avances en su implementación y mejoras pertinentes.

VIII. INTEGRACIÓN DE LA GESTIÓN DE LA CONTINUIDAD OPERATIVA A LA CULTURA ORGANIZACIONAL

Para la integración de la Gestión de la Continuidad Operativa a la cultura organizacional, el ITP red CITE, a través de la OGRRHH, en calidad de Unidad Orgánica responsable de la continuidad operativa, deberá realizar las acciones siguientes[2]:

- Evaluar el grado de conocimiento del personal de la entidad sobre la gestión de continuidad operativa, en relación a los procedimientos implementados, las tareas específicas señaladas en el plan de continuidad, entre otros aspectos que se estimen convenientes.
- Diseñar e implementar planes de capacitación y entrenamiento respectivo, a fin de fortalecer las capacidades del personal de la entidad.
- Monitorear permanentemente el nivel de entendimiento de la gestión de continuidad operativa mediante acciones inopinadas al personal, a fin de identificar requerimientos adicionales de fortalecimiento de capacidades.
- Supervisar la implementación de la Gestión de la Continuidad Operativa e informar a la Alta Dirección.

IX. ANEXOS

1. Plan de Contingencia y recuperación de servicios de tecnologías de la información del Centro de Datos
2. Procedimiento para la convocatoria del personal involucrado en la ejecución de las actividades.
3. Directorio del Grupo de Comando
4. Organización para el desarrollo de las actividades criticas
5. Protocolo de Comunicación interna ante eventos de gran magnitud
6. Cronograma de implementación de la Gestión de la continuidad operativa
7. Lineamientos para la identificación de peligros y riesgos
8. Lineamientos para la definición de actividades críticas
9. Números de emergencia a nivel nacional
10. Plano de ubicación de Sede Alterna
11. Procedimiento de aseguramiento del acervo documentario
12. Informe de Implementación de Mejoras de los servicios informáticos

[2] Numeral 5.2.4, Resolución Ministerial N° 320-2021-PCM. “Lineamientos para la gestión de la continuidad operativa y formulación de planes de continuidad Operativa de las Entidades Públicas de los tres niveles de gobierno”

ANEXO N° 1: PLAN DE CONTINGENCIA Y RECUPERACIÓN DE SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN DEL CENTRO DE DATOS

PLAN DE CONTINGENCIA Y RECUPERACIÓN DE SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN DEL CENTRO DE DATOS

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

2021

CONTENIDO

PLAN DE CONTINGENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN DEL INSTITUTO TECNOLÓGICO DE LA PRODUCCION (ITP)

1. INTRODUCCIÓN

La administración de continuidad de los servicios de TI se encarga de prevenir y proteger a la institución de los efectos que pudiera tener una interrupción de los servicios de TI ocasionados por una falla técnica, por causas naturales como terremotos, incendios, pandemias entre otros o por alguna persona de manera voluntaria o involuntaria.

La administración de la continuidad de los servicios de TI debe combinar equilibradamente procedimientos y pautas como son:

- **Preventivos,** medidas y procedimientos que buscan eliminar o mitigar los riesgos de la interrupción y sus posibles efectos.

- **Reactivos,** procedimientos cuyos propósitos es reanudar el servicio tan pronto como sea posible después de cualquier interrupción.

Estos procedimientos y pautas deben ser enmarcados en un Plan de Contingencia que la Institución debe de elaborar para ser ejecutadas en cada uno de los eventos que alteren el normal funcionamiento de los servicios críticos. Además, debe detallar los alcances conceptuales que permitirán a la persona que accede a este documento reforzar y ampliar sus capacidades para que pueda familiarizarse con el plan de contingencia para ampliar sus habilidades de reacción ante las situaciones inesperados que pueda ocasionar la paralización de las actividades en el ámbito de las TIC.

El Plan de Contingencia también puede considerarse como marco de referencia, para la elaboración de las políticas, normas y procedimientos de contingencias.

El estado peruano a través de la Resolución Ministerial N° 028-2015-PCM, aprueba los Lineamientos para la Gestión de la Continuidad Operativa de entidades públicas en los tres niveles de gobierno, se señala que el Plan de Continuidad Operativa comprende, entre otros planes específicos, el Plan de Contingencia y el Plan Recuperación de Servicios de Tecnología de la Información. En ese sentido, el Instituto Tecnológico de la Producción – ITP a través de su Oficina de Tecnologías de la Información (OTI) presenta el Plan de Contingencias que permitirán mantener la continuidad de sus sistemas de información frente a eventos críticos para minimizar el impacto negativo sobre la misma y sus colaboradores.

2. OBJETIVOS

2.1. Objetivo General

- Establecer los principios básicos y el marco necesario para garantizar la continuidad operativa de los servicios críticos de Tecnologías de Información que brinda el ITP ante eventos que puedan alterar su normal funcionamiento parcial o totalmente, restableciéndolo en el menor tiempo posible, a través de la puesta en marcha del plan que contempla los procedimientos, actividades y elementos requeridos para afrontar la contingencia.

2.2. Objetivos específicos

- Asegurar la pronta recuperación de los servicios críticos de TI después de cualquier evento o desastre que afecte la Continuidad de los Servicios de TI.

- Establecer políticas, tomar medidas y desarrollar procedimientos para evitar, dentro de lo posible, las consecuencias de cualquier desastre natural o eventos accidentales o voluntarios realizado por las personas.

- Proteger los activos informáticos del ITP.

- Identificar y analizar los riesgos posibles que pueden afectar las operaciones, procesos y servicios de tecnologías de la información y comunicaciones de la Entidad.

- Organizar y disponer al personal técnico debidamente capacitado para afrontar adecuadamente las contingencias que puedan presentarse.

3. ALCANCE

El Plan de Contingencia Informático y Recuperación de Servicios de Tecnología de la Información y Comunicaciones, incluye los elementos del Centro de Datos referidos a los sistemas de información, aplicativos informáticos, bases de datos, equipos, personal, servicios y otros administrados por la Oficina de Tecnologías de la Información (OTI), direccionado a minimizar eventuales riesgos ante situaciones adversas que atentan contra el normal funcionamiento de los servicios informáticos de la entidad.

4. BASE LEGAL

- Ley Nª 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
- Decreto Supremo N° 034-2014-PCM, Decreto Supremo que aprueba el Plan Nacional de Gestión del Riesgos de Desastres - PLANAGERD 2014-2021.

- Decreto Supremo Nº 048-2011-PCM, Decreto Supremo que aprueba el Reglamento de la Ley Nº 29664, que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
- Resolución Ministerial N° 004-2016-PCM - Aprueban 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.
- Resolución Ministerial N° 028-2015-PCM, que aprueban los lineamientos para la gestión de la Continuidad Operativa de entidades públicas en los tres niveles de gobierno.
- Decreto Supremo N° 111-2012-PCM, que incorpora la Política Nacional de Gestión de Riesgos de Desastres de cumplimiento obligatorio para las entidades del Gobierno Nacional.
- "Guía práctica para el desarrollo de Planes de Contingencia de Sistemas de Información" – Elaborado por INEI el 2001.

5. DEFINICIONES

a) Activo de información:
Comprende a cada elemento que soporta la información, es decir que la contiene, la procesa y la transporta.

b) Amenaza:
Es una situación o acontecimiento que pueda causar daño a los bienes informáticos; puede ser una persona, un programa malicioso o un suceso natural de otra índole y representan los posibles atacantes o factores que inciden negativamente sobre las debilidades del sistema.

c) Incidente:
incidente es cualquier interrupción de servicios de Tecnología de la Información que afecta desde un solo usuario hasta la Institución.

d) Vulnerabilidad:
Debilidad de un activo o control que puede ser explotada por una o más amenazas

e) Impacto:
Es el daño producido por la materialización de una amenaza.

f) Contingencia:
Se define como contingencia a la alteración en la continuidad del negocio, que impacta en forma relevante el normal desarrollo de un servicio

considerado crítico, teniendo su origen en la falla de uno o varios componentes o la interrupción de una
tarea, sin estar necesariamente prevista.

g) Punto de Recuperación Objetivo (RPO):

El objetivo del punto de recuperación (RPO) se utiliza como métrica para la recuperación de los datos. También se mide en términos de tiempo, pero hace referencia a la edad o a la frescura de los datos requeridos para restaurar la operación que sigue a un acontecimiento adverso. Los datos, en este contexto, pueden también incluir la información con respecto a las transacciones no registradas o no capturadas. Como el RTO, cuanto más pequeño es el RPO, más alto
son los costos de la recuperación prevista de los datos.

h) Plan de contingencia:

Es el proceso para desarrollar, comunicar y mantener documentados y aprobadas las acciones que permitan restituir rápidamente los servicios tecnológicos de la organización ante una eventualidad que pueda paralizar, ya sea de forma parcial o total de la Institución.

i) Probabilidad:

Posibilidad de que algún evento de contingencia se materialice.

j) Riesgo:

Incertidumbre que podría desencadenar una interrupción indeterminada en los
servicios de TI.

k) Riesgo Operativo:

Riesgo vinculado a la administración y supervisión del personal.

l) Riesgo Técnico:

Riesgo vinculado a fallas en los suministros de energía y servicios complementarios.

m) Riesgo Tecnológico:

Riesgo vinculado a los servicios de tecnologías de la información.

n) Servicio crítico:

Servicio de gran valor para el cumplimiento de los objetivos del ITP.

o) Tiempo de inactividad o downtime:

El término tiempo de inactividad (downtime) es usado para definir cuándo el sistema no está disponible. Los casos de dowtime pueden ser Planeado o No planeados.

p) El Tiempo de Recuperación Objetivo (RTO):
Es el tiempo que un proceso permanecerá detenido antes de que su funcionamiento sea restaurado. Debe medirse desde el momento en que ocurre la interrupción hasta que se reanude la operación.

q) MTD:
Se define como el Tiempo de inactividad máximo tolerable que define la cantidad total de tiempo que un proceso de negocio puede interrumpirse sin causar consecuencias inaceptables.

r) Tiempo de recuperación de la red:
Es el tiempo para restaurar la comunicación de datos y voz después de un evento adverso. Esta posiblemente tendrá impacto sobre otras actividades.

6. METODOLOGÍA DE DESARROLLO DEL PLAN DE CONTINUIDAD TECNOLÓGICA

La metodología de referencia utilizada es la BCM (Business Continuity Management), la cual nos permite definir y establecer el Plan de Contingencia para reducir el impacto provocado por una paralización total o parcial de la operación de la Institución y garantizar así, la recuperación ágil y progresiva de los servicios tecnológicos y procesos críticos afectados.

La continuidad operativa del ITP dependerá del evento y/o desastre sucedido y ante ello se debe asegurar los procesos y servicios tecnológicos críticos, según la estrategia
desarrollada.

Para la elaboración del plan de contingencia tecnológico se han establecido las siguientes
fases:

- **Fase 1: Planificación:**
  Se define y prepara los esfuerzos de planificación de las actividades en cada etapa de contingencia (Prevención, Ejecución y Recuperación).

- **Fase 2: Determinación de vulnerabilidades y escenarios de contingencia:**
  Se busca minimizar las fallas generadas por los eventos en contra del normal desempeño de los sistemas de información a partir del análisis de la criticidad de los eventos identificados.

- **Fase 3: Identificador de soluciones:**
  Para reducir los costos se han establecido soluciones en la medida de lo posible, a tiempo de documentar los riesgos de fallas e interrupciones identificadas.

- **Fase 4: Estrategias:**
  Se identifican las prioridades y se determina en forma razonable las actividades hacer implementadas en cada etapa desarrollada (Prevención, Ejecución y Recuperación).

- **Fase 5: Documentación del proceso:**
  Desarrollo de procedimientos y/o actividades en las etapas de prevención, ejecución y recuperación desarrolladas en cada evento.

- **Fase 6: Realización de pruebas:**
  Se identifica los escenarios/eventos con probabilidad de recuperación aceptable por la Institución a través de actividades en cada etapa de recuperación.

- **Fase 7: Monitoreo:**
  Se establecen las actividades preventivas y mantenimiento que permita reaccionar en el tiempo preciso y se tomen las acciones correctas.

La materialización de los riesgos contrae consecuencias para la Institución, para ello es necesario identificar, determinar y evaluar los niveles de impacto que puedan afectar la continuidad operativa del Centro de Datos del ITP.

El Plan de Contingencia determina los posibles riesgos e impactos en la Institución considerando las áreas de impacto: operacional, lega e imagen, tal como se muestra en el siguiente cuadro:

Cuadro N°01. Tabla de impactos

Impacto	Áreas de impacto		
	Operacional	Legal	Imagen
Leve	Paralización o trastornos en las actividades. El daño se revierte inmediatamente después de lo ocurrido.	-	Percepción negativa de la imagen institucional por un número reducido de usuarios finales.
Moderado	Paralización o trastornos en las actividades. El daño se revierte en un tiempo menor o igual al RTO.	Amonestación administrativa	Percepción negativa de la imagen institucional por parte de las organizaciones políticas.
Alto			Percepción negativa de la imagen institucional por

	Paralización o trastornos en las actividades. El daño se revierte en un tiempo mayor al RTO.	Acciones judiciales, contenciosas, civiles.	parte de las organizaciones políticas y las entidades públicas.
Severo	Paralización o trastornos en las actividades. El daño se revierte en un tiempo mayor al MTD.	Denuncias penales contra funcionarios del ITP.	Pérdida de la confianza y la credibilidad de la institución por parte de la ciudadanía en general.

6.1. Descripción de los Eventos de Contingencia

Cuadro N°02. Descripción de Eventos

TIPO		EVENTO	DESCRIPCIÓN
Externo	Tecnológico	Caída o interrupción de energía eléctrica (E1)	Corresponde al corte del servicio de energía en la Sede Callao del ITP ubicado en el Km 5.2 Carretera Ventanilla, corte eléctrico que genera interrupción del funcionamiento de los servidores donde se alojan los sistemas de información y/oaplicaciones del ITP. Esta situación impacta en la disponibilidad de los servicios de TI.
		Infección masiva por software malicioso (E3)	Es el riesgo de infección de los equipos de cómputo que puede presentarse en la entidad por mala configuración del sistema antivirus o por ausencia de política de seguridad lo que genera la suspensión total o parcial del funcionamiento o de la prestación de las unidades de trabajo.
		Ataque informático (E11)	Consiste en aprovechar alguna debilidad o falla en el software o hardware, para obtenerun beneficio, por lo general de condición económica, causando un efecto negativo enla seguridad del sistema, que luego pasa directamente en los activos de la organización.
	Operativo	Suspensión de las actividades por sismo, inundación o incendio (E4)	Hace referencia al riesgo que corre la entidad para que se presente un evento de sismo o incendio que afecte la infraestructura tecnológica del Centro de Datos del ITP generando suspensión total o parcial de su funcionamiento o prestación de servicios de TI

	Técnico	Caída de internet (E2)	Consiste en las fallas técnicas por parte del proveedor del servicio de internet en el Centro de Datos del ITP, lo que ocasionaríasuspensión de los servicios de TI incluyendocorreo, red, sistemas y aplicativos de información del ITP.
Interno	Tecnológico	Falla técnica en equipos servidores (E6)	Corresponde al daño físico o lógico de un equipo servidor, que afecta el funcionamiento de un sistema de información crítico por falta de mantenimiento preventivo a los equipos o por mal uso de los equipos por parte de los responsables que hace que el servicio de TI quede inoperante o Inestable.
		Falla técnica en equipos de comunicación (E10)	Corresponde al daño físico o lógico de un equipo de comunicación, que afecta el funcionamiento de los servicios de información crítico por falta de mantenimiento preventivo a los equipos o por mal uso de los equipos por parte de los responsables que hace que el servicio de TI quede inoperante o Inestable.
		Falla técnica en Sistemas de Información critico (E7)	Representa una falla técnica en alguna funcionalidad de los sistemas de información y aplicativos críticos del ITP que se vea afectada la integridad de la información en el continuo uso de estos.
	Operativo	Accesos no autorizados al Centro de Datos del ITP – (E5)	Consiste en el acceso al Centro de Datos de personal no autorizadas que pueden ocasionar sabotaje, robo, alteración o extracción de información que es considerada confidencial o clasificada, así como también el daño a los componentes informáticos. El impacto es negativo ya que puede ocasionar demandas y sanciones a la entidad, mala imagen institucional.
		Ausencia de personal de la Oficina de Tecnologías de la Información que brindan soporte y mantenimiento a los sistemas de información, servidores y redes – (E8)	Corresponde a la falta o inasistencia en un momento dado, de un trabajador crítico de la OTI que realiza actividades de soporte a usuarios sobre un sistema de información crítico del ITP por enfermedad, epidemia muerte o incapacidad, lo que genera inoperancia o inestabilidad de los sistemas de información, servidores y redes
	Técnico	Calentamiento del centro de datos – (E9)	Consiste en el aumento de temperatura dentro del centro de datos y falta de ventilación, por deficiencia del sistema de ventilación o ausencia de un sistema de ventilación de precisión acorde a las necesidades de la entidad lo que puede generar recalentamiento de los equipos servidores, dejándolos inoperantes junto con los servicios que se encuentran alojados en ellos.

6.2. Valoración de los Eventos de Contingencia

Para la valoración de los eventos identificados, se utiliza la matriz del cuadro N° 1, donde se categorizan los niveles de probabilidad y niveles de impacto (consecuencias). La descripción de cada categoría se muestra a continuación:

Niveles de probabilidad

- Casi Seguro: probabilidad muy alta.
- Muy probable: probabilidad alta.
- Posible: probabilidad media.
- Poco probable: probabilidad baja.
- Raro: sería especialmente que ocurriera raramente.

Niveles de impacto (consecuencias)

- Catastrófico: pérdida de negocio o posibilidad de pérdida de vidas o lesiones graves.
- Mayor: afección grave al negocio, posibilidad de lesiones moderadas.
- Moderado: causarán problemas no significativos en el negocio, posibilidad de lesiones leves.
- Menor: muy poca influencia sobre el negocio, impacto leve.
- Despreciable: prácticamente ninguna influencia negativa sobre el negocio, pueden dejarse sin mediar.

		PROBABILIDAD				
		Raro	Poco probable	Posible	Muy probable	Casi seguro
CONSECUENCIAS	Despreciable	Bajo	Bajo	Bajo	Medio	Medio
	Menores	Bajo	Bajo	Medio	Medio	Medio
	Moderadas	Medio	Medio	Medio	Alto	Alto
	Mayores	Medio	Medio	Alto	Alto	Muy alto
	Catastróficas	Medio	Alto	Alto	Muy alto	Muy alto

Figura N° 1: Mapa de Calor de Riesgos (Fuente: Gestión de riesgos ISO 31000)

La valoración de los riesgos tiene 4 posibles resultados: bajo, medio, alto y muy alto. Para efectos de la formulación del presente plan de contingencia, se tomarán en cuenta los riesgos valorados como alto y muy alto. Los

riesgos con valoración bajo y medio se deben mantener en lista de observación a fin de que de manera periódica se pueda evaluar si en el tiempo va cambiando dicha valoración.

En función a ello, los eventos de contingencia descritos en el numeral 6.1 precedente, tienen la siguiente valoración:

Cuadro N° 03: Valorización de riesgos

N°	EVENTO	PROBABILIDAD	IMPACTO	VALORACIÓN
E1	Caída o interrupciónde energía eléctrica.	Poco probable	Catastrófico	ALTO
E2	Caída de internet.	Poco probable	Mayor	ALTO
E3	Infección masiva porsoftware malicioso.	Muy probable	Mayor	ALTO
E4	Suspensión de las actividades por sismo,inundación o incendio.	Poco probable	Catastrófico	ALTO
E5	Accesos no autorizados al Centro de Datos del ITP.	Poco probable	Mayor	MEDIO
E6	Falla técnica en equipos servidores,de escritorio o de Comunicaciones.	Posible	Mayor	ALTO
E7	Falla técnica en los Sistemas de Información critico.	Muy probable	Mayor	ALTO
E8	Ausencia de personalde la Oficina de Tecnologías de la Información que brindan soporte y mantenimiento a los alos sistemas de información y comunicaciones.	Muy probable	Moderado	ALTO
E9	Calentamiento delcentro de datos.	Posible	Mayor	ALTO
E10	Falla técnica en los equipos de comunicación.	Posible	Mayor	ALTO
E11	Ataque informático	Muy probable	Mayor	ALTO

7. RESULTADOS ESPERADOS

El presente Plan de Contingencia de TI buscar restablecer los servicios de TI en un margen aceptable a cada tipo de servicio que pueden ir desde 50% hasta 100% dependiendo del tipo de servicio impactado.

8. ESTRATEGIAS

8.1. Desarrollo de la estrategia para los Planes de Contingencia

Desarrollaremos las estrategias relacionadas con cada evento o incidente que provoque alto impacto en la continuidad de los servicios de TI de la OTI. Para lo cual se está dividiendo en 3 partes:

a. **Prevención:** Mecanismos para prevenir dichos eventos antes de que sucedan; ayudan a reducir el impacto y estar siempre preparados ante eventualidades de desastres.

b. **Ejecución:** Después de iniciado el evento y ayuda a la recuperación de las funciones críticas, se considera los tiempos de continuidad.

c. **Recuperación:** Procedimientos para retomar las actividades ya recuperadas en su lugar de origen.

8.2. Estrategia del Plan de Contingencia para cada evento

8.2.1. Evento N°01: Caída o interrupción de energía eléctrica - (E1)

ITP	Evento: Caída o interrupción de energía eléctrica - (E1)	OTI
1. PLAN DE PREVENCIÓN		
1.1. Descripción del evento		
Falla general del suministro de energía eléctrica por parte del proveedorde servicios y fallo y/o no disponibilidad del grupo electrógeno. Este evento incluye los siguientes elementos mínimos identificados por el ITP, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia: • Servicios Públicos • Suministro de Energía Eléctrica • Hardware • Servidores • Estaciones de Trabajo • Equipos Diversos • UPS **1.2. Objetivo** Restablecer energía eléctrica en el Centro de Datos del ITP ante un evento de contingencia para asegurar la continuidad operativa de los sistemas críticos de TI.		

1.3. Valoración

Este evento es considerado alto.

1.4. Entorno

Se delimita al Centro de Datos ubicado de la sede Central del ITP.

1.5. Personal encargado

- Oficial de seguridad de la información.
- Especialista en administración de Data Center o quien haga sus veces.

1.6. Condiciones de Prevención de Riesgo

- Verificar que durante las operaciones diarias de servicio u operaciones del ITP se contará con los UPS necesarios para asegurar el suministro eléctrico en el Centro de Datos del ITP.
- Asegurar que los equipos UPS cuenten con el mantenimiento debido y con suficiente energía para soportar una operación continua de 45 minutos como mínimo.
- Realizar pruebas periódicas de los equipos UPS para asegurar su correcto funcionamiento.

2. PLAN DE EJECUCIÓN

2.1. Eventos que activan la Contingencia

Corte de suministro de energía en EL Centro de Datos por un tiempo mayor a 30 minutos.

2.2 Procesos relacionados antes del evento

Cualquier actividad de servicio dentro de las instalaciones de la sede principal del ITP.

2.3. Personal que autoriza la Contingencia

- Jefe de la Oficina de Tecnologías de la Información.

2.4. Personal encargado

- Especialista en administración de Data Center.

2.5. Descripción de los procedimientos después de activar la contingencia:

- Informar a la Jefatura de la Oficina de Tecnologías de la Informaciónsobre el evento presentado.
- Verificar la activación automática de los UPS.
- Comunicar a todas las Unidades Orgánicas del ITP del evento y coordinar las acciones necesarias.
- En caso la interrupción de energía sea mayor a 30 minutos se deberá apagar los servidores (Virtuales y físicos) que alojen los sistemas, aplicaciones, servicios de TI y demás servidores en siguiente orden:
    - Servidores de aplicación, Base de datos, servicios TI, otros, servicio de Directorio Activo y finalmente los servidores físicos(Hypervisores)
    - Apagar los servicios los equipos de seguridad perimetral y comunicaciones.
- Monitorear el uso de equipos UPS para el restablecimiento de energía en los servidores de soporte a los sistemas críticos.

Coordinar con las Unidades Orgánicas afectadas de tomar las medidas necesarias ante la activación del Plan de Contingencia de TI.

3. PLAN DE RECUPERACIÓN

3.1. Personal operativo encargado

- Especialista de administración de Data Center o quien haga susveces
- Especialista en redes y comunicaciones.
- Administrador de Base de Datos o quien haga sus veces.
- Personal de desarrollo de sistemas o quien haga sus veces.

3.2. Descripción de actividades

- Verificar el estado de la infraestructura tecnológica impactada por elevento.
- Verifica el restablecimiento de la energía eléctrica y el funcionamientodel Centro de Datos.
- En caso de que se cuente con energía eléctrica, se procederá a la activación de los servicios en la siguiente secuencia:
  - Encendido de los equipos de seguridad perimetral y comunicaciones.
  - Encendido de los servidores físicos (Hypervisores).
  - Encender servidores de Directorio Activo, Base de datos,Aplicaciones, otros.
- Analizar la necesidad de usar las copias de respaldo y backups.
- Verificar el restablecimiento de los sistemas críticos de información.
- Comunicar a las Unidades Orgánicas afectadas el restablecimientode los sistemas de información críticos.
- Registrar aquellas actividades que sirva para actualizar el Plan deContingencia de TI en caso vuelva a presentarse dicha eventualidad.
- Registrar el evento en el Formato Registro de Contingencias

3.3. Mecanismo de comprobación

- Verificar a través del software de Monitoreo que todos los servicios estén activos.
- Comunicar a todas las Unidades Orgánicas del ITP a fin de constatar el correcto funcionamiento de los sistemas de información críticos en cada Oficina de trabajo.
- Garantizar la funcionalidad de las instalaciones eléctricas en la SedeCentral del ITP.

3.4. Desactivación del Plan de Contingencia de TI

El Jefe de la Oficina de Tecnologías de la Información desactivaráel Plan de Contingencia una vez se haya restablecido la energía eléctricaal Centro de Datos y los servicios de TI.

3.5. Informe de resultados

Elaborar un informe a la Jefatura de la Oficina de Tecnologías de la Información sobre el problema presentado y el procedimiento usado para atender el evento.

3.6. Proceso de actualización del Plan

Se tomarán las recomendaciones formuladas en los informes presentados a la Jefatura de la Oficina de Tecnologías de la Informaciónpara la presente contingencia.

3.7. Tiempo de Recuperación

El tiempo máximo de duración de la contingencia dependerá del proveedor externo de energía eléctrica.

8.2.2. Evento N°02: Caída de Internet - (E2)

ITP	Evento: Caída de Internet – (E2)	OTI
1. PLAN DE PREVENCIÓN		

1.1. Descripción del evento

Perdida de servicio de Internet a la conexión de la red externa del servicio principal de ITP.

1.2. Objetivo

Restaurar los servicios críticos de comunicaciones a la red externa que soportan los servidores del Centro de Datos a través del Servicio de Internet de Contingencia.

1.3. Valoración

Este evento es considerado alto.

1.4. Entorno

Se puede producir durante el servicio, o en horario no laborable en el Centrode Datos del ITP.

1.5. Personal encargado

- Oficial de seguridad de la información.
- Especialista en Redes y Comunicaciones o quien haga sus veces.

1.6. Condiciones de Prevención de Riesgo

- Contar con equipos de comunicación y respaldo ante posibles fallas delrouter principal, a través del contrato con el proveedor del servicio de Internet se contempla el reemplazo del router en caso falle.
- Contar con mantenimiento preventivo para los equipos de comunicaciones dos veces al año. (Equipo alquilado) y otro mantenimiento programado por el proveedor en su nodo de comunicaciones.
- Libreta de números de contacto del proveedor al alcance.

2. PLAN DE EJECUCIÓN

2.1. Eventos que activan la Contingencia.

- Falla del sistema de router principal para el servicio de Internet
- Falla de los circuitos digitales de comunicación de red externa. (Ej.Rotura de enlace de fibra u otros medios)
- Falla del nodo de comunicación del proveedor de internet del ITP.

2.2. Procesos relacionados antes del evento.

Cualquier actividad de servicio dentro de las instalaciones del ITP.

2.3. Personal que autoriza la Contingencia.

- Jefe de la Oficina de Tecnologías de la Información del ITP.

3. PLAN DE RECUPERACIÓN

3.1. Personal encargado

- Oficial de seguridad de la información.
- Especialista en Redes y Comunicaciones o quien haga sus veces

3.2. Descripción de actividades

- Validar que los servicios y circuitos estén conforme por las áreas usuarias.
- El proveedor del servicio de Internet una vez reparado el fallo emitirá un informe a la Jefatura de Tecnologías de la Información, detallando la causa origen del evento y las acciones realizadas.
- El evento será evaluado y registrado de ser necesario en el formato de ocurrencias de eventos.
- Se informará a la Jefatura de la Oficina de Tecnologías de la Información sobre el evento de contingencia presentado y el procedimiento usado.

3.3. Mecanismos de comprobación

La OTI deberá asegurarse que las pruebas y revisiones periódicas al sistema de

comunicaciones y circuiros de la red externa (Internet), los cuales se lleven a cabo semestralmente.

3.4. Desactivación del Plan de Contingencia

La Jefatura de la Oficina de Tecnologías de la Información desactivará el Plan de Contingencia una vez que se recupere la funcionalidad de trabajo con los sistemas.

3.5. Proceso de actualización

En base al informe presentado por el proveedor del sistema de comunicaciones y circuitos de red externa (Internet), se tomarán las acciones correctivas para la actualización del Plan de Contingencia.

3.6. Tiempo de Recuperación

- Falla del Router: El reemplazo por el proveedor no debe exceder a 1 hora.
- Falla de Circuito digital: El tiempo del SLA establecido con el proveedor es 4 horas.

8.2.3. Evento N°03: Infección masiva por software malicioso - (E3)

ITP	Evento: Infección masiva por software malicioso – (E3)	OTI

1. PLAN DE PREVENCIÓN

1.1. Descripción del evento

Los softwares maliciosos son programas informáticos que se propagan deun equipo a otro y que interfieren en su correcto funcionamiento. Además, pueden dañar o eliminar los datos de un equipo. Este evento incluye los siguientes elementos mínimos identificados, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación:

- Servidores
- Estaciones de trabajo (PC y Laptops)
- Software base datos.
- Aplicativos y sistemas de información del ITP.

1.2. Objetivo

Restaurar la operatividad de los activos informáticos después de eliminar el software malicioso que causa la contingencia.

1.3. Valoración

Este evento es considerado alto.

1.4. Entorno

Los activos informáticos (PC, Laptops, servidores y sistemas de información) de la Sede Central y Callao del ITP.

1.5. Personal encargado

- Oficial de seguridad de la información.
- Especialista en administración de Data Center o quien haga sus veces.
- Soporte Técnico o quien haga sus veces.

1.6. Condiciones de prevención de riesgos

- Establecer políticas y normativas de seguridad que regulen el uso adecuado de los activos de información.
- Utilizar mecanismos de seguridad que restrinja el acceso a páginas de internet de contenido malicioso.
- Restringir el acceso a las grabadoras de CD y USB en las estaciones detrabajo que no lo requieran.
- Aplicar filtros para restricción de correo entrante y así prevenir la infección de los terminales de trabajo por virus.

- Verificar que el antivirus instalado en cada estación de trabajo deba estar actualizado permanentemente.
- Verificar que los sistemas operativos cuenten con los parches de actualización constantemente, a través de la herramienta WSUS la cualdebe estar operativa.
- Escanear la red constantemente a fin de identificar instalaciones de agentes maliciosos.
- Contar con un mínimo de tres equipos de respaldo ante posibles fallas de las estaciones, para su reemplazo provisional hasta la operatividad del equipo cliente afectado.
- Capacitar y concientizar al personal del ITP sobre temas de seguridad de la información.
- Contar con Backups y copias de respaldo de la información
- Encriptación de los datos críticos
- Segmentar la red para asilar los casos de activos infectados por Malware o software malicioso.
- Controlar el nivel de obsolescencia tecnológica aceptable a nivel Hardware y Software.

2. PLAN DE EJECUCIÓN

2.1. Eventos que activan la Contingencia

- Mensajes de error o mensajes de alerta durante la ejecución de lossistemas de información y aplicaciones.
- Lentitud o paralización de los sistemas de información y aplicaciones.
- Falla general en los activos de informáticos (PC, Laptops, servidores ysistemas de información).
- Reporte de usuarios.

2.2. Procesos relacionados antes del evento

Cualquier proceso relacionado con el uso de sistemas y aplicaciones enlas. estaciones de trabajo y servidores

2.3. Personal que autoriza la Contingencia

- Jefe de la Oficina de Tecnologías de la Información.

2.4 Personal encargado

- Especialista en administración de Data Center o quien haga sus veces.
- Soporte técnico o quien haga sus veces.

2.5. Descripción de actividades

- Comunicar o escalar aL Jefe de OTI para activar al equipo derespuesta de incidentes.
- Desconectar preventivamente los equipos infectados de la red delITP.
- Comunicar a los usuarios de los servicios de los equipos impactados.
- Verificar el estado actualizado de las firmas del software antivirus, IPS,Antimalware
- Verificar la infección de los equipos afectado y el alcance de este.
- Rastrear de ser necesario el origen de la infección (archivo infectado, correo electrónico, etc.) para su remisión y revisión por el fabricante de la solución antivirus y antimalware.
- Eliminar el agente viral causante de la infección.
- Escanear la red del ITP en virtud de eliminar posibles agentes virales informáticos.
- En caso no solucionarse el problema:
  - Formatear el equipo
  - Personalizar la estación para el usuario.
- Conectar las estaciones o equipo servidor a la red del ITP.
- Efectuar las pruebas necesarias con el usuario.
- Solicitar conformidad del servicio.

3. PLAN DE RECUPERACIÓN

3.1. Personal encargado

- Oficial de seguridad de la información.
- Especialista en la administración de Data Center o quien haga susveces
- Especialista en redes y comunicaciones o quien haga sus veces.
- Soporte técnico o quien haga sus veces.

3.2. Descripción de actividades

- Registrar la conformidad del usuario una vez se haya eliminado la amenaza de virus en su estación de trabajo.
- Realizar pruebas de funcionamiento en las estaciones de trabajo (Sistemas de información, servicios tecnológicos y aplicaciones del ITP).
- Coordinar con el usuario responsable el procedimiento para reanudar laslabores normales en el ambiente de trabajo original.
- Dar indicaciones de seguridad y prevención a los usuarios.
- Recomendar capacitación a la OTI de ser necesario.
- Realizar informe de las acciones tomadas durante el evento.

Se informará a la Jefatura de la Oficina de Tecnología de la Información eltipo de software malicioso encontrado y el procedimiento usado pararemoverlo. En función a esto, se tomarán las medidas preventivas del caso.El evento será evaluado y registrado en el formato de registro de contingencia.

3.3. Mecanismo de comprobación

- Asegurar que el antivirus funcione correctamente y se encuentre enconstante actualización.
- Verificar que el Sistema Operativo se encuentre con las actualizacionesy parches.

3.4. Desactivación del plan de continuidad

El Jefe de la Oficina de Tecnologías de la Información desactivará elpresente Plan una vez se haya eliminado la amenaza.

3.5. Proceso de actualización

En base al informe presentado que identifica las causas de la infección de virus informático, se determinará las acciones preventivas necesarias que deberán incluirse en el presente Plan.

3.6. Tiempo de Recuperación

La duración del evento dependerá de la eficacia en detección de infección masiva, por efecto de actualización de firmas no mayor a 24 horas, así como también el tiempo de respuesta de los fabricantes en caso infeccionesde día Cero.

Los usuarios deberán esperar las indicaciones del personal de soporte parareanudar el trabajo.

8.2.4. Evento N°04: Suspensión de actividades por sismo, inundación o incendio – (E4)

ITP	Evento: Suspensión de las actividades por sismo, inundación o incendio – (E4)	OTI
1. PLAN DE PREVENCIÓN		

1.1. Descripción del evento

Constituye la situación en la que el Centro de Datos del ITP se encuentra declarada inhabitable, producto de un desastre de mayores magnitudes, pudiendo provocar derrumbe de la infraestructura, perdida demateriales, recursos informáticos y humanos.
Las causas que pueden provocar este evento encontramos las siguientes:

Incendio: Es un proceso de combustión caracterizado por la emisión de calor acompañado de humo, llamas o ambas que se propaga de manera incontrolable en el tiempo y en el espacio. Se producen en materiales sólidos, líquidos combustibles inflamables, equipos e instalaciones bajo carga eléctrica entre otros.

Sismo de gran intensidad en Lima: Los sismos son movimientos en el interior de la tierra y que generan una liberación repentina de energía que se propaga en forma de ondas provocando el movimiento errático del terreno.

Inundación: Flujo descontrolado de agua producto de lluvias torrenciales ofugas y/o daños en el sistema hidráulico.

1.2. Objetivo

Establecer las acciones que se tomarán ante un incendio, inundación o sismo de grandes magnitudes a fin de minimizar el tiempo de interrupción de los servicios críticos de TI, establecidos en el numeral 6.3 cuadro de valoración de Alto y Muy Alto

1.3. Valoración

Este evento es considerado como alto.

1.4. Entorno

Este evento se localiza en las instalaciones del Centro de Datos de la sede Callao del ITP.

1.5. Personal encargado

- Oficial de seguridad de la información.
- Especialista en administración de Data Center o quien haga sus veces.
- Especialista en redes y comunicaciones.
- Especialista de Base de Datos
- Especialistas de Desarrollo

1.6. Condiciones de prevención de riesgos

Incendio de grandes magnitudes en uno o más ambientes:

- Realizar inspecciones de seguridad periódicamente.
- Mantener las conexiones eléctricas seguras en el rango de su vida útil.
- Asistir a charlas sobre el uso y manejo de extintores de cada uno de lostipos.

Acatar las indicaciones de Defensa Civil, en torno al evento.

- Contar con una relación de teléfonos de emergencia que incluya a los bomberos, ambulancias, y personal responsable de las acciones de prevención y ejecución de la contingencia.
- Verificar el funcionamiento de los detectores de humo en el Centro de Datos del ITP.
- Contar con una lista de contactos de las personas responsables yproveedores de servicios de contingencia.
- Conocer el grupo de brigadistas asignados por el ITP.
- Identificar la ubicación de las estaciones manuales de alarma contraincendio.

Sismo de gran intensidad en Lima

- Solicitar el plan de evacuación de las instalaciones del ITP, elmismo que debe ser de conocimiento de todo el personal que labora.
- Participar en los simulacros de evacuación con la participación de todoel personal del ITP.

- Mantener las salidas libres de obstáculos en Centro de Datos
- Señalizar todas las salidas del Centro de Datos
- Señalizar las zonas seguras del Centro de Datos
- Contar con una lista de contactos de las personas responsables yproveedores de servicios de contingencia.
- Conocer el grupo de brigadistas asignados por el ITP.

Inundaciones de grandes magnitudes

- Solicitar a Servicios Generales la coordinación del mantenimiento y/oestado de las instalaciones hidráulicas del ITP.
- Posicionar los activos estratégicos del Centro de Datos en plataformaselevadas.
- Contar con una lista de contactos de las personas responsables yproveedores de servicios de contingencia.
- Conocer el grupo de brigadistas asignados por el ITP.

2. PLAN DE EJECUCIÓN

2.1. Eventos que activan la Contingencia

El proceso de contingencia se activará inmediatamente después de ocurrido los eventos descritos en el numeral 1.1.

2.2. Personal que autoriza la Contingencia

La Jefatura de la Oficina de Tecnologías de la Información con laautorización de la Dirección ejecutiva del ITP.

2.3. Personal encargado Operativo

- Especialista en administración de Data Center o quien haga sus veces.
- Especialista en redes y comunicaciones.
- Administrador de base de datos o quien haga sus veces.
- Personal de desarrollo de sistemas o quien haga sus veces.
- Web Master o quien haga sus veces.

2.4. Descripción de actividades para la restauración del Centro de Datos

- Evaluar los daños ocasionados en el Centro de Datos del ITP.
- Verificar la disponibilidad del espacio físico que hará las veces de Centrode Datos alterno provisional del ITP, en caso de inoperancia del Centro de Datos Principal.
- Trasladar el equipamiento que se encuentre en buenas condiciones del Centro de Datos, asegurando que las características ambientales sean las mínimas necesarias para su implementación.
- Asegurar las condiciones eléctricas y de refrigeración mínimas para el funcionamiento del Centro de Datos alterno provisional.
- Considerar la adquisición de equipamiento tecnológico que asegure la disponibilidad del Centro de Datos provisional.
- Configurar la infraestructura tecnológica que soporte el levantamiento delos sistemas de información críticos del ITP.
- Coordinar el traslado seguro de las copias de seguridad en custodia porel proveedor al nuevo ambiente de físico del Centro de Datos provisional.
- Restaurar las copias de seguridad de los sistemas de información del ITP.
- Ejecutar las pruebas necesarias para asegurar la disponibilidad de losservicios críticos de TI.
- Informar a la Jefatura de la Oficina de Tecnologías de la Información el restablecimiento del Centro de Datos alterno provisional del ITP.
- Instalación de los servicios Internet y enlace de datos.

3. PLAN DE RECUPERACIÓN

3.1. Personal encargado

- Oficial de seguridad de la información.
- Especialista en administración de Data Center o quien haga sus veces.
- Especialista en redes y comunicaciones.
- Personal de desarrollo de sistemas o quien haga sus veces.
- Administrador de base de datos o quien haga sus veces.
- Web Master o quien haga sus veces.

3.2. Descripción de actividades

- Verificar los daños a los componentes informáticos del Centro de Datosprincipal.

Realizar el inventario general de la documentación, personal, equipos,etc. y/o recursos afectados, indicando el estado de estos.

- Trasladar hacia el Centro de Datos alterno provisional los componentesinformáticos en buen estado.
- Habilitar los muebles y logística necesaria para su operatividad.
- Garantizar la habilitación del servicio de fluido eléctrico.
- Reinstalación del personal critico de TI.
- Monitorear constantemente la funcionalidad de los servicios críticos deTI.

3.3. Mecanismo de comprobación

Elaborar un informe a la Jefatura de Tecnologías de la Información detallando los daños afectados a los activos de Información críticos del ITP y las acciones tomadas.
Se llenará el formato de ocurrencia de eventos para este fin.

3.4. Desactivación del Plan de Recuperación

Se desactivará una vez se tome por superado el desastre y se retome las actividades de origen.

3.5. Proceso de actualización

El proceso de actualización será en base al informe presentado a laDirección Ejecutiva a efectos que determine las acciones a tomar.

3.6. Tiempo de Recuperación

El proceso de implementar un Centro de Datos provisional (de ser necesario) tomara un tiempo no mayor a 5 días.

La duración total del evento dependerá del grado del sismo, la probabilidadde réplicas y los daños a la infraestructura.

8.2.5. Evento N°06: Falla técnica en servidores – (E6)

ITP	Evento: Falla técnica en servidores – (E6)	OTI

1. PLAN DE PREVENCIÓN

1.1. Descripción del evento

Falla técnica de los servidores asociados a los servicios críticos de TI, sistemas de información y aplicaciones del ITP.

1.2. Objetivo

Asegurar la continuidad y operatividad de los servidores asociados a los servicios críticos de TI, sistemas de información y aplicaciones del ITP.

1.3. Valoración

Este evento es considerado alto.

1.4. Entorno

Servidores de soporte para los servicios críticos de TI, sistemas deinformación y aplicaciones localizados en el Centro de Datos del ITP.

1.5. Personal encargado

- Oficial de seguridad de la información.
- Especialista en administración de Data Center o quien haga sus veces.
- Administrador de base de datos o quien haga sus veces.
- Personal de desarrollo de sistemas o quien haga sus veces.

1.6. Condiciones de Prevención de Riesgo

- Revisión periódica técnica de los servidores del Centro de Datos.
- Mantener actualizada la garantía de equipos y servidores vigentes.
- Copias de seguridad de los sistemas de información y aplicaciones del ITP.
- Monitoreo periódico de red del ITP.
- Seguridad periférica.
- Protección física adecuada al Centro de Datos.
- Mecanismos de seguridad y controles de acceso.
- Adecuada ventilación y refrigeración en el Centro de Datos.
- Procedimientos para el uso correctos de los activos de información.

1.7. Copias de respaldo o Backup y custodia en una locación externa.

- Tener las copias de respaldo de información disponibles para su aplicación en los servidores de contingencia del ITP.
- Traslado de las copias de seguridad en poder del proveedor de custodia a la Sede Central del ITP.

2. PLAN DE EJECUCIÓN

2.1. Eventos que activan la Contingencia

- Fallas en la conexión, servidores no responden.
- Indisponibilidad de uso de los sistemas y aplicativos del ITP.

2.2. Personal encargado

- Especialista en administración de Data Center o quien haga sus veces.
- Especialista en redes y comunicaciones.
- Administrador de Base de Datos o quien haga sus veces.
- Personal de desarrollo de sistemas o quien haga sus veces.

2.3. Descripción de los procedimientos después de activar la contingencia:

- Analizar la causa resultante o disparador del evento.
- Realizar un diagnóstico rápido de los sistemas críticos afectados o involucrados en la ejecución. Para este caso se debe revisar el inventario de los sistemas o aplicaciones críticas del ITP.
- Contactar a las partes interesadas que sean afectadas por laindisponibilidad de los servicios de TI.
- Comunicar a los proveedores del equipo servidor e informar la incidenciacomo parte del soporte y garantía.
- Desconectar de la red el servidor afectado.
- Activar y configurar el equipo necesario de contingencia para el levantamiento de los servicios de TI en los servidores alternos decontingencia.
- Ejecutar las restauraciones de los backups de los sistemas yaplicaciones críticos en los servidores alternos de contingencia en caso se requiera.

- Realizar las pruebas de funcionamiento.
- Comunicar a los usuarios el restablecimiento de los servicios de TI.

3. PLAN DE RECUPERACIÓN

3.1. Personal encargado

- Oficial de seguridad de la información.
- Especialista en administración de Centro de Datos.
- Especialista en redes y comunicaciones.
- Administrador de Base de Datos o quien haga sus veces.
- Personal de desarrollo de sistemas o quien haga sus veces.

3.2. Descripción de actividades

- Conectar a la red el equipo inicial reparado.
- El Especialista en Administración de Centro de Datos verifica el correctodesempeño de los servidores reparados y de los sistemas de informacióncríticos que soportan.
- Se informará a la Jefatura de Oficina de Tecnologías de la Información la causa del problema presentado y el procedimiento usado para atenderel problema. En función a esto, se tomarán las medidas preventivas del caso.
- El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

3.3. Mecanismos de Comprobación

- Una vez identificada el origen de la falla de los servidores que ocasionóel evento, se deberá realizar un informe técnico detallado y consolidandolas acciones tomadas.
- Revisar las configuraciones y programar con el proveedor de los equipos,revisiones periódicas a fin de reducir la amenaza que vuelva a suceder.

3.4. Desactivación del Plan de Contingencia

El Jefe de la Oficina de Tecnologías de la Información desactivará el Plan de Contingencia una vez que el especialista en administración de DataCenter informe la operatividad de los servidores.

3.5. Proceso de actualización

El proceso de actualización será en base al informe presentado a la Dirección Ejecutiva quien determinará las acciones a tomar.

3.6 Tiempo de RecuperaciónDuración de 4-8 horas.

8.2.6. Evento N°07: Falla técnica en Sistemas de Información Critico – (E7)

ITP	Evento: Falla en Sistemas de Información Críticos – (E7)	OTI

1. PLAN DE PREVENCIÓN

1.1. Descripción del evento

Es el uso defectuoso de los sistemas de información críticos del ITP,haciendo que el uso de estos corresponda a un elevado riesgo en la integridad de la información que se procese o simplemente este último dejede funcionar.

1.2. Objetivo

Restaurar el funcionamiento de los sistemas de información y aplicacionescríticos del ITP de acuerdo con el numeral 6.3 cuadro de valoración de Alto y Muy Alto.

1.3. Valoración

Este evento es considerado alto.

1.4. Entorno

Sistemas de información y aplicativos críticos del ITP.

1.5. Personal encargado

- Oficial de seguridad de la información
- Personal de desarrollo de sistemas o quien haga sus veces.
- Administrador de base de datos o quien haga sus veces.

1.6. Condiciones de Prevención de Riesgo

- Copia de seguridad de la información críticos para asegurar la integridadde la información. También se obtienen copias de seguridad de la base de datos relacionadas.
- Mantener actualizado el software de gestión de BD, con todos losparches del producto según el fabricante y licencias vigentes.
- Evitar el uso de software no licenciado que pueda estar corrupto
- Revisión preventiva de los sistemas y mantenimiento general de las bases de datos.
- Directivas o procedimiento de desarrollo seguro.
- Implementar y mantener un repositorio de código fuente institucional.

2. PLAN DE EJECUCIÓN

2.1. Eventos que activan la Contingencia

Fallas en el uso de los sistemas de información que generen suinoperatividad. Información procesada no cuenta con integridad y fiabilidad.

2.2. Procesos relacionados antes del evento

Respaldo disponible de los sistemas de información críticos.

2.3. Personal que autoriza la Contingencia

- Jefe de la Oficina de Tecnologías de la Información del ITP.

2.4. Personal encargado

- Personal de desarrollo de sistemas o quien haga sus veces.
- Administrador de base de datos o quien haga sus veces.

2.5. Descripción de las actividades después de activar la contingencia:

- Desconectar de la red el equipo afectado.
- Configurar equipo de respaldo para el sistema de información oaplicación crítica afectada.
- Restaurar la copia de seguridad más reciente del aplicativo críticocorrespondiente.
- Crear los permisos a cada carpeta compartida.
- Verificar la existencia del servidor nuevo en el dominio y colocarlo enproducción.
- Informar a los usuarios la nueva ruta del servidor del aplicativo

3. PLAN DE RECUPERACIÓN

3.1. Personal encargado

- Oficial de seguridad de la información.
- Especialista en administración de Centro de Datos.
- Administrador de Base de Datos o quien haga sus veces.
- Personal de desarrollo de sistemas o quien haga sus veces.

3.2. Descripción de actividades

- Revisar el sistema de Información o aplicativo dañado para determinarla falla o error lógico presentado.

- Hacer pruebas al sistema de Información o aplicativo una vez entregadala solución por el proveedor, en ambiente de pruebas.
- Realizar copia de la base de datos del sistema de Información oaplicativo que está en funcionamiento como contingencia.
- Restaurar la copia de seguridad más reciente del aplicativo afectado enel servidor inicial.
- Verificar los permisos sobre el sistema de información o aplicativo.
- Informar a los usuarios la ruta del servidor del sistema de información oaplicativo.
- Conectar a la red el equipo inicial reparado.

3.3. Mecanismos de comprobación
El Especialista en administración de Centro de Datos presentara un informea la Jefatura de la Oficina de Tecnologías de la Información explicando queservicio ha sido afectado y cual son las acciones tomadas.

3.4. Desactivación del Plan de Contingencia
La Jefatura de la Oficina de Tecnologías de la Información desactivará el Plan de Contingencia una vez que se resuelva la ausencia del personal crítico.

3.5. Proceso de actualización
En base al informe presentado a la Jefatura de Oficina de Tecnologías de la información y las causas identificadas en el Servicio informático se determinará las acciones a tomar.

3.6. Tiempo de Recuperación
El tiempo máximo de duración de la contingencia será máximo en 24 horasdependiendo de la causa que originó la contingencia.

8.2.7. Evento N°08: Ausencia de personal de la Oficina de Tecnologías de la Información que brindan soporte y mantenimiento a los sistemas de información, servidores y redes– (E8)

ITP	Evento: Ausencia de personal de la Oficina de Tecnologías de la Información que brindan soporte y mantenimiento a los sistemas de información, servidores y redes– (E8)	OTI

1. PLAN DE PREVENCIÓN

1.1. Descripción del evento
Ausencias del personal (enfermedad, epidemias, renuncias masivas, ceses), critico que brinda soporte y mantenimiento a los sistemas de información, servidores y redes que mediante su ausencia pueda originar paralización en las operaciones del ITP.

1.2. Objetivo
Reemplazar al personal crítico ausente con elementos capacitados que puedan cubrir sus funciones hasta la inserción o reemplazo del ausente.

1.3. Valoración
Este evento es considerado Alto.

1.4. Entorno
Oficina de Tecnologías de la Información.

1.5. Personal encargado
- efe de la Oficina de Tecnologías de la Información.

- Oficial de seguridad de la información.

1.6. Condiciones de Prevención de Riesgo

- Asegurar la capacitación adecuada de los equipos técnicos en su especialidad, Analistas de sistemas, redes, infraestructura y Seguridad Informática y Administración de BD con el fin de que cumplan con el perfil, conocimiento y capacidad de reemplazar la ausencia de los especialistas en caso de ausencia.
- Incluir como parte de las funciones del personal, comunicar anticipadamente la inasistencia a su centro de labor.
- Elaborar diccionarios de datos y/o manuales o procedimientos operativosde uso para facilitar las actividades del reemplazante.
- Programar chequeos preventivos médicos al personal crítico en periodossemestrales o anuales.
- Mantener operativas las herramientas de trabajo remoto.

2. PLAN DE EJECUCIÓN

2.1. Eventos que activan la Contingencia

Inasistencia no premeditada del personal crítico (administrador de sistemasy redes).

2.2. Procesos relacionados antes del evento

La Jefatura de la Oficina de Tecnologías de la Información tieneconocimiento de inasistencia del personal crítico.

2.3. Personal que autoriza la Contingencia

- Jefe de la Oficina de Tecnologías de la Información del ITP.

2.4. Personal encargado

- Jefe de la Oficina de Tecnologías de la Información.
- Oficial de seguridad de la información.

2.5. Descripción de las actividades después de activar la contingencia:

- Confirmada la inasistencia del personal, la Jefatura de la Oficina de Tecnologías de la Información asignara al reemplazo provisional del personal ausente.
- Poner a disposición los recursos necesarios para que el personal suplente lleve a cabo sus actividades efectivamente.

3. PLAN DE RECUPERACIÓN

3.1. Personal encargado

Jefe de la Oficina de Tecnologías de la Información

3.2. Descripción de actividades

- Facilitar la reinserción del personal ausente
- Regularización en los servicios pendiente durante la ausencia.
- Revisión de los servicios atendidos si fuera el caso.
- Definir los ajustes para asegurar rápida y mejora en la acción yprevención del presente evento.

3.3. Mecanismos de comprobación

Informes de desempeño laboral cuando sea requerido por la Jefatura de laOficina de Tecnologías de la Información

3.4. Desactivación del Plan de Contingencia

La Jefatura de la Oficina de Tecnologías de la Información desactivará el Plan de Contingencia una vez que se resuelva la ausencia del personal crítico.

3.5. Proceso de actualización

En base al informe presentado a la Jefatura de Oficina de Tecnologías de la información y

las causas identificadas en el Servicio informático se determinará las acciones a tomar.

3.6. Tiempo de Recuperación
El tiempo máximo de duración de la contingencia dependerá de la causaque originó la ausencia temporal, sin embargo se dispondrá de un reemplazo temporal en un plazo máximo de 24 horas.

8.2.8. Evento N°09: Calentamiento del Centro de Datos – (E9)

ITP	Evento: Calentamiento del Centro de Datos – (E9)	OTI

1. PLAN DE PREVENCIÓN

1.1. Descripción del evento
Aumento de temperatura dentro del Centro de Datos y falta de sistema de aire acondicionado, en el centro de datos de ITP o ausencia de un sistema de ventilación acorde a las necesidades del ITP.

1.2. Objetivo
Restaurar los servicios críticos de TI que soportan los servidores del Centrode Datos.

1.3. Valoración
Este evento es considerado alto.

1.4. Entorno
Se puede producir durante el servicio, o en horario no laborable en el Centrode Datos del ITP.

1.5. Personal encargado
- Oficial de seguridad de la información.
- Especialista en administración de Data Center o quien haga sus veces.

1.6. Condiciones de Prevención de Riesgo
- Contar con equipos de respaldo ante posibles fallas de los servidores.
- Contar con un sistema de aire acondicionado adecuado en el Centro deDatos.
- Contar con mantenimiento preventivo para los equipos de aireacondicionado.
- Libreta de números de contacto del proveedor al alcance.

2. PLAN DE EJECUCIÓN

2.1. Eventos que activan la Contingencia
- Falla del sistema de aire acondicionado del Centro de Datos
- Falla de los servicios críticos del ITP

2.2. Procesos relacionados antes del evento
Cualquier actividad de servicio dentro de las instalaciones del ITP.

2.3. Personal que autoriza la Contingencia
- Jefe de la Oficina de Tecnologías de la Información del ITP.

2.4. Personal encargado
- Especialista en administración de Data Center o quien haga sus veces.

2.5 Descripción de los procedimientos después de activar la contingencia:
- Verificar la magnitud del fallo o avería al sistema de ventilación delCentro de Datos.
- Notificar al proveedor de aire acondicionado sobre la magnitud de fallos

o avería.

- Encender el aire acondicionado de contingencia.
- Instalar equipos de ventilación provisionales.
- Apagar los equipos electrónicos no críticos.
- Restablecer el sistema de aire acondicionado del Centro de Datos.

3. PLAN DE RECUPERACIÓN

3.1. Personal encargado

- Especialista en administración de Data Center o quien haga sus veces.

3.2. Descripción de actividades

- El especialista de administración de Data Center revisara que el sistema de Aire Acondicionado haya sido reparado y funcione con normalidad.
- Encender equipos no críticos
- El proveedor del sistema de aire acondicionado una vez reparado el falloemitirá un informe a la Jefatura de Tecnologías de la Información,detallando la causa origen del evento y las acciones realizadas.
- El evento será evaluado y registrado de ser necesario en el formato de ocurrencias de eventos.
- Se informará a la Jefatura de la Oficina de Tecnologías de la Informaciónsobre el evento de contingencia presentado y el procedimiento usado.

3.3. Mecanismos de comprobación

La OTI deberá asegurarse que las pruebas y revisiones periódicas al sistema de ventilación del Centro de Datos se lleven a cabo semestralmente.

3.4. Desactivación del Plan de Contingencia

La Jefatura de la Oficina de Tecnologías de la Información desactivará el Plan de Contingencia una vez que se recupere la funcionalidad de trabajo con los sistemas.

3.5. Proceso de actualización

En base al informe presentado por el proveedor del sistema de ventilaciónde Centro de Datos se tomarán las acciones correctivas para la actualización del Plan de Contingencia.

3.6. Tiempo de Recuperación

El tiempo máximo de duración de la contingencia dependerá del proveedordel sistema del aire acondicionado, se estima un tiempo máximo de 2 horas.

8.2.9. Evento N°10: Falla técnica de equipos de Comunicación – (E10)

ITP	Evento: Falla técnica de equipos de Comunicación – (E10)	OTI
1. PLAN DE PREVENCIÓN		

1.1. Descripción del evento

Caída de los equipos de comunicación (Switches) o fallas en los enlaces defibra en la sede Callao . (Principal o redundante)

1.2. Objetivo

Restaurar los servicios críticos de comunicaciones de la red interna quesoportan los Sistemas de ITP.

1.3. Valoración

Este evento es considerado alto.

1.4. Entorno

Se puede producir durante el servicio, o en horario no laborable en el Centrode Datos del ITP.

1.5. Personal encargado

- Oficial de seguridad de la información.
- Especialista en redes y comunicaciones o quien haga sus veces

1.6. Condiciones de Prevención de Riesgo

- Contar con equipo en configuración redundante y alta disponibilidad.
- Contar con equipos de Switches de respaldo ante posibles fallas de losequipos de comunicación.
- Enlaces redundantes entre equipos de comunicación a nivel de SwitchCore
- Los Switches de distribución también estarían en configuraciónredundante.
- Los Switches de acceso que conecta a las PCs, se cuenta con equiposde respaldo.
- Contar con mantenimiento preventivo para los equipos de comunicación(Switch Core y Distribución).
- Libreta de números de contacto del proveedor al alcance.

2. PLAN DE EJECUCIÓN

2.1. Eventos que activan la Contingencia

- Falla del Switchs Core, Distribución y acceso a las PCs
- Falla de los enlaces de cobre o fibra en la red interna.

2.2. Procesos relacionados antes del evento

Cualquier actividad de servicio dentro de las instalaciones del ITP.

2.3. Personal que autoriza la Contingencia

- Jefe de la Oficina de Tecnologías de la Información del ITP.

2.4. Personal encargado

- Especialista en Redes y Comunicaciones o quien haga sus veces

2.5. Descripción de los procedimientos después de activar la contingencia:

- Validación física de la caída de red y dimensionar el alcance del impacto(Usuarios y pisos afectados)
- Si se trata un Switchs de acceso se reemplaza en caso este en garantía,caso contrario se envía a reparación el equipo de comunicación que presenta fallas.
- Se valida el estado de los servicios por usuarios y pisos afectado.
- Si trata de fallas en los enlaces, se verifica con la herramienta demonitoreo los estados y alertas reportadas.
- Se realiza una validación física de las conexiones de fibra (Cuarto de comunicaciones), si implica algún cambio se notifica al proveedor.
- El proveedor realiza un diagnóstico para detectar falla y proceder con sureparación.

- Se valida que los servicios en la herramienta de monitoreo estén activospara los usuarios y pisos afectados.

3. PLAN DE RECUPERACIÓN

3.1. Personal encargado

- Oficial de seguridad de la información.
- Especialista en Redes y Comunicaciones o quien haga sus veces

3.2. Descripción de actividades

- Validar que los equipos de comunicación y enlace de la red interna esténactivos para las áreas usuarias.
- El proveedor de los equipos de comunicaciones una vez reparado el falloemitirá un informe a la Jefatura de Tecnologías de la Información,detallando la causa origen del evento y las acciones realizadas.
- El evento será evaluado y registrado de ser necesario en el formato de ocurrencias de eventos.
- Se informará a la Jefatura de la Oficina de Tecnologías de la Informaciónsobre el evento de contingencia presentado y el procedimiento usado.

3.3. Mecanismos de comprobación

La OTI deberá asegurarse que las pruebas y revisiones periódicas al sistema de comunicaciones de la red interna se lleven a cabosemestralmente (Equipos en garantía).

3.4. Desactivación del Plan de Contingencia

La Jefatura de la Oficina de Tecnologías de la Información desactivará el Plan de Contingencia una vez que se recupere la funcionalidad de trabajo con los sistemas.

3.5. Proceso de actualización

En base al informe presentado por el proveedor del sistema de comunicaciones y circuitos de red interna se tomarán las acciones correctivas para la actualización del Plan de Contingencia.

3.6. Tiempo de recuperación

- Falla de switches Core y Distribución, el tiempo máximo de reemplazopor el proveedor será de 1 hora.
- Switchs de accesos PCs máx. 1 hora.
- En caso falla de enlace digital dependerá de los SLAs del proveedor,se estima máximos 24 horas.

8.2.10. Evento N°11: Falla técnica de equipos de Comunicación – (E11)

ITP	Evento: Ataque Informático – (E11)	OTI

1. PLAN DE PREVENCIÓN

1.1. Descripción del evento

Afectación por parte de algún sistema informático de un tipo específico de programa malintencionado que restringe el acceso mediante cifrado o determinadas partes o archivos del sistema infectado y pide un rescate(Generalmente en moneda virtual) a cambio de eliminar dicha restricción.

1.2. Objetivo

Restaurar los servicios críticos de TI que soportan las estaciones detrabajo y

servidores del Centro de Datos.

1.3. Valoración

Este evento es considerado alto.

1.4. Entorno

Se puede producir durante el servicio, o en horario no laborable en elCentro de Datos del ITP.

1.5. Personal encargado

- Oficial de seguridad de la información.
- Especialista en administración de Data Center o quien haga sus veces.
- Especialistas de Desarrollo y Aplicaciones
- Especialista de Base de Datos
- Especialista de redes y comunicaciones o quien haga sus veces
- Especialista de Soporte Técnico de OTI o quien haga sus veces.

1.6. Condiciones de Prevención de Riesgo

- Contar con equipos de respuesta ante incidentes de seguridad anteposibles ataques informáticos en estaciones de trabajo y servidores.
- Contar con las copias de respaldo y cintas de backup probadas yactualizadas.
- Contar con antivirus actualizado en las estaciones de trabajo yservidores.

Libreta de números de contacto del proveedor al alcance.

2. PLAN DE EJECUCIÓN

2.1. Eventos que activan la Contingencia

- Infección de virus informáticos en las estaciones de trabajo o servidoresdel centro de datos.

2.2. Procesos relacionados antes del evento

Cualquier actividad de servicio dentro de las instalaciones del ITP.

2.3. Personal que autoriza la Contingencia

- Jefe de la Oficina de Tecnologías de la Información del ITP.

2.4. Personal encargado

- Oficial de seguridad de la información.
- Especialista en administración de Data Center o quien haga sus veces.
- Especialistas de Desarrollo y Aplicaciones
- Especialista de Base de Datos

Especialista de redes y comunicaciones o quien haga sus veces

- Especialista de Soporte Técnico de OTI o quien haga sus veces.

2.5. Descripción de los procedimientos después de activar la contingencia:

- Detección del evento de infección de virus informático.
- Validar si trata de un ataque tipo RANSOMWARE
- Notificar al Jefe de OTI y equipo de respuesta de Incidentes deSeguridad.
- Establecer las medidas de contención para evitar su propagación a niveltoda la red.
- Validar si se puede apagar el equipo informático afectado, si es posiblese procede a desconectar de la red al equipo informático.
- Si no es posible apagarlo, se verifica que no allá más equipos afectados.
- Se realiza un análisis inmediato considerando los siguientes criterios:
    - Riesgos e impactos en toda la red.
    - Clonación de discos

- Deshabilitar servicios o sistemas
- Ajustar reglas del Firewall y equipos de seguridad perimetral
- Actualización de Antivirus.

- Proceder con las acciones de mitigación, considerando si equipoafectado está cifrado y posible su recuperación (Descifrable)
- Si no es posible proceder con la restauración de la copia de seguridaddisponible.
- Si no es posible la restauración, se procede a formatear el equipoinformático afectado.

Restablecer las estaciones de trabo o servidores recuperados.

3. PLAN DE RECUPERACIÓN

3.1. Personal encargado

- Oficial de seguridad de la información.
- Especialista en administración de Data Center o quien haga sus veces.
- Especialistas de Desarrollo y Aplicaciones
- Especialista de Base de Datos
- Especialista de redes y comunicaciones o quien haga sus veces
- Especialista de Soporte Técnico de OTI o quien haga sus veces.

3.2. Descripción de actividades

- El especialista de administración de Data Center revisara que losservidores afectados se han restaurado y funcione con normalidad.
- El especialista de Soporte Técnico de OTI revisara que las estacionesde trabajo afectadas se han restaurado y funcione con normalidad
- El proveedor del Software Antivirus una vez solucionado el incidenteemitirá un informe a la Jefatura de Tecnologías de la Información,

detallando la causa origen del evento y las acciones realizadas.

- El evento será evaluado y registrado de ser necesario en el formato deocurrencias de eventos.
- Se informará a la Jefatura de la Oficina de Tecnologías de la Información sobre el evento de contingencia presentado y el procedimiento usado.

3.3. Mecanismos de comprobación

La OTI deberá asegurarse que las pruebas y revisiones periódicas a los servidores del Centro de Datos y estaciones de trabajo se lleven a cabo semestralmente.

3.4. Desactivación del Plan de Contingencia

La Jefatura de la Oficina de Tecnologías de la Información desactivará el Plan de Contingencia una vez que se recupere la funcionalidad de trabajo con los sistemas.

3.5. Proceso de actualización

En base al informe presentado por el proveedor del sistema seguridad antivirus se tomarán las acciones correctivas y lecciones aprendidas para la actualización del Plan de Contingencia.

3.6. Tiempo de recuperación

El tiempo máximo de duración de la contingencia dependerá de la cantidad de equipos afectados, sin embargo, a nivel de tiempo por equipo informáticose estima un máximo de 24 horas.

9. CRONOGRAMA DEL PLAN DE PRUEBAS

9.1. Plan de Pruebas:

El Plan de Contingencias de TI comprende, el desarrollo de un plan de pruebas en el cual se incluye diferentes escenarios (Priorizados según plan) para comprobar que el plan diseñado es eficaz o, en caso contrario, se le debe efectuar ajustes correspondientes.

Los siguientes son los objetivos de control de las pruebas del plan:

- Validar la habilidad de los responsables y la consistencia de los procedimientos en eventos de recuperación de siniestros.
- Probar la factibilidad y compatibilidad de las instalaciones de respaldo y de los procedimientos relacionados
- Identificar y corregir falla en el Plan de Contingencias de TI
- Facilitar la divulgación y el entrenamiento en los procedimientos de recuperación.
- Fomentar el respeto por el plan y la seguridad en su efectiva aplicación en caso de presentarse emergencias.
- Motivar a los encargados involucrados en el diseño y desarrollo del Plan a mantener actualizados los procedimientos inherentes.

9.2. Cronograma del plan de pruebas

N°	EVENTO	2021					2022					
		May	Jun	Sep	Oct	Dic	Mar	May	Jun	Sep	Oct	Dic
E1	Caída o interrupción de energía eléctrica	X										
E2	Caída de internet										X	
E3	Infección masiva por software malicioso					X						
E4	Suspensión de las actividadespor sismo o incendio											X
E6	Falla técnica en servidores		X									
E7	Falla en Sistemas de Información críticos								X			
E8	Ausencia de personal de la Oficina de Tecnologías de la Información que brindan soporte y mantenimiento a los a los sistemas de información, servidores y redes							X				
E9	Calentamiento del Centro deDatos						X					
E10	Falla técnica en equipos de comunicación				X							
E12	Ataque informático									X		

El escenario 5 (E5) no se ha considerado porque solo se van a tratar los eventos de riesgos Muy Altas y Alta para el presente Plan de Contingencia de Tecnología de Información del ITP.

10. PRESUPUESTO PARA LA EJECUCIÓN DEL PLAN DE CONTINGENCIA DE TI

El Plan de Contingencia de Tecnologías de la Información, contiene actividades que serán desarrolladas por el personal de la Oficina de Tecnologías de la Información de acuerdo con sus competencias; dichas actividades planificadas están contempladas en el presupuesto asignado a la OTI en el presente año y en los subsiguientes años fiscales.

11. SEGUIMIENTO Y MEJORA CONTINUA

El responsable del mantenimiento y mejora continua del plan es el Oficial de Seguridad de la Información. El plan debe ser revisado, probado y actualizado en su documentación y su alcance, esto quiere decir que el plan debe mejorado permanentemente a través de revisiones de acuerdo con los siguientes parámetros:

- Implementación de nuevos servicios críticos de TI: En caso se realicen nuevos Sistemas o servicios que soporten procesos críticos de la Institución se deberá realizar un mantenimiento de Plan de Contingencia.
- Resultados de una nueva evaluación de riesgos: Si dentro de la evaluación de riegos se identificación nuevos escenarios de criticidad Muy Alta o alta se deberán desarrollo o actualizar los procedimientos de recuperación.
- Requisitos legales o contractuales: Ante nuevas regulaciones establecidos por la administración pública a través de los TUPAs o normativas específicas.

ANEXO N° 2: PROCEDIMIENTO PARA LA CONVOCATORIA DEL PERSONAL INVOLUCRADO EN LA EJECUCIÓN DE LAS ACTIVIDADES

En el marco del desarrollo del procedimiento para convocar al personal a cargo de las actividades críticas se presentan los componentes que permiten contactar con los involucrados:

- Comunicaciones
- Flujo de comunicación para la Continuidad Operativa
- Procedimiento de convocatoria
- Ejecución del procedimiento

Comunicaciones

El manejo de las comunicaciones es un elemento fundamental sobre el que descansa el Plan de Continuidad Operativa, más aún en caso de una emergencias o desastre, el personal debe ser capaz de comunicarse, por medios comúnmente utilizados o medios alternos, entre sí, con las Mypes y socios estratégicos.

Para realizar las comunicaciones se crea el sistema que garantiza la interacción remota para responder a la activación del Plan de Continuidad Operativa, en ese sentido, las comunicaciones se ejecutarán mediante radio VHF, telefonía móvil, mensajería instantánea, mensajería por correo electrónico, mensajería de voz y datos:

1. Radio VHF: Canal fundamental utilizado por caracterizarse en posibilitar la trasmisión de señales a través de la modulación de ondas electromagnéticas que se propagan a través de aire como el espacio y no requiere de un medio físico de transporte.
2. Telefonía móvil: La alta dirección del ITP, directivos y coordinadores de áreas técnicas cuentan con equipos móviles (sistemas son Android e iOS) integran el directorio almacenado en sus teléfonos, a utilizarse para ejercer la comunicación mediante llamada, mensajería instantánea, mensajería de voz y de datos.
3. Correo electrónico: La alta dirección del ITP, directivos y coordinadores de áreas técnicas integran servicios de correo electrónico en PC y móviles en sus teléfonos celulares.

De esta manera, se tomaría concomimiento de forma oportuna de los peligros y emergencias, del alcance de daño, características e implicancias, promoviendo las disposiciones para su atención inmediata a través de las coordinaciones pertinentes para la movilización del recurso humano, la logística permitiendo dar continuidad a las operaciones de la institución.

Flujo de comunicación para la Continuidad Operativa

Para la conducción de la continuidad de funciones es fundamental gestionar la información de manera correcta ejerciendo una comunicación asertiva para la toma de decisiones. Se obtendrán mensajes por parte de la Oficina de Seguridad y Defensa Nacional del Ministerio de la Producción - OSDN quienes también reportan al Centro de Operaciones de Emergencia Sectorial del PRODUCE - COES PRODUCE.

La comunicación se ejecuta mediante mensajes claros, sencillos y cortos, considerando la activación del Plan de Continuidad Operativa del ITP. De esta manera se inicia con los siguientes procedimientos específicos:

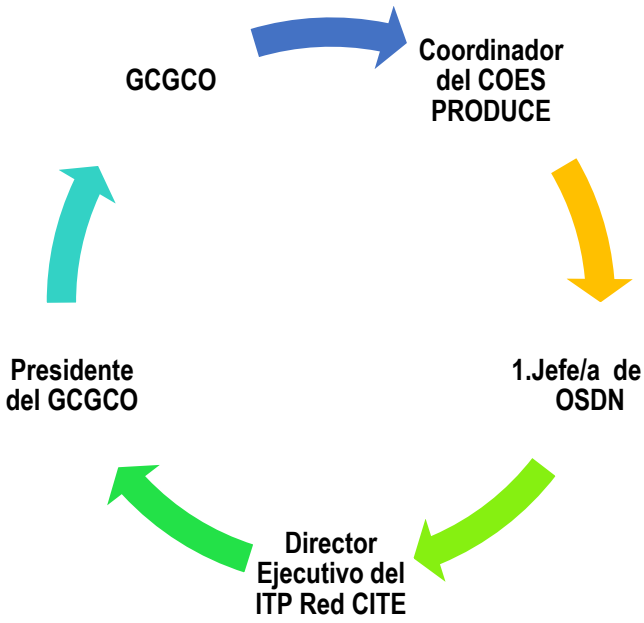
- Procedimiento de reporte inicial: Acciones realizadas en áreas afectadas del ITP como primer reporte.

- Procedimiento de convocatoria: Acciones realizadas con la finalidad de comunicar al personal clave la activación del Plan de Continuidad Operativa del ITP

En ese sentido, el Grupo de Comando para la Gestión de la Continuidad Operativa del ITP activa el Plan de Continuidad Operativa y sus procedimientos para realizar los reportes correspondientes sobre decisiones a la OSDN.

En el flujo de comunicación para la Continuidad Operativa del ITP intervienen los siguientes actores:

1. Coordinador del Centro de Operaciones de Emergencia Sectorial del PRODUCE: Recibe mensajes desde el COEN, y comunica a la OSDN
2. Jefe de la Oficina de Seguridad y Defensa Nacional, comunica a la DE del ITP Red CITE
3. Director Ejecutivo del ITP Red CITE, coordina con el funcionario responsable de la Gestión de la Continuidad Operativa.
4. Presidente del Grupo de Comando para la Gestión de la Continuidad Operativa, toma la decisión de activar el plan de Continuidad Operativa y realiza los procedimientos estipulados.
5. Grupo de Comando para la Gestión de la Continuidad Operativa, reenvía información actualizada hacia el COES PRODUCE.



Procedimiento de Convocatoria

El procedimiento de convocatoria permite que el proceso de comunicación de la activación del plan de continuidad se realice de manera rápida, por que comprende el rombo de la movilización

o comunicación, el cual consta de la delegación de funciones por parte de la Unidad Orgánica a cargo de la Continuidad Operativa, para constatar que el personal clave tenga conocimiento de la activación del plan.

Una vez activado el Plan de Continuidad Operativa, se procede a realizar la convocatoria del personal clave en la ejecución de las actividades críticas confirmando su presencia y conciencia para mantenerse enfocado en el desarrollo de las actividades encomendadas, se comunica la activación del Plan de Continuidad Operativa.

Para convocar a los responsables, se aplica el Rombo de Movilización de Emergencias que se materializa en cadenas de llamadas mediante radio o mensaje de texto o cualquier otro medio que permita su comunicación. El procedimiento de convocatoria constituye cadenas de activación en los diferentes niveles de la organización.

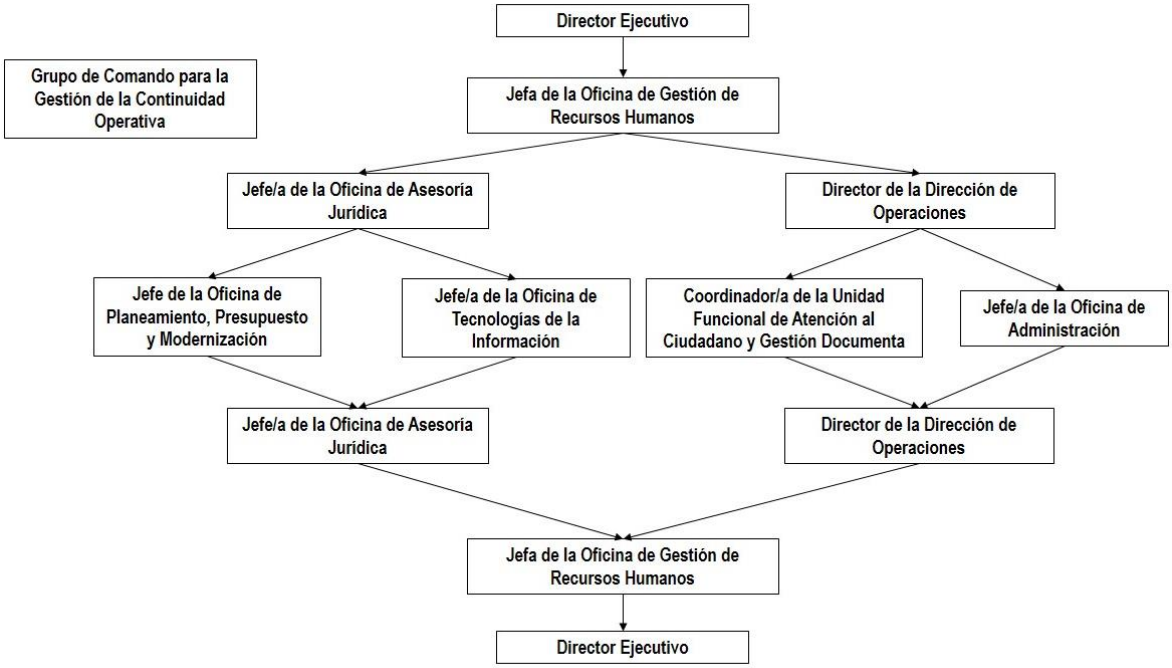
Ejecución del procedimiento

El Rombo de movilización para convocar al personal involucrado en la ejecución de las actividades críticas.

1. El titular de la institución toma la decisión de convocar al personal empleando el Rombo de Movilización o comunicación de Emergencias y, en concordancia con la condición del funcionamiento de la entidad, se comunica con la presidencia del Grupo de Comando para la Gestión de la Continuidad Operativa - GCGCOOP.
2. Asimismo, la presidencia del GCGCOOP convoca a los integrantes del grupo a través del Rombo de Movilización o Comunicación de Emergencias de manera inmediata. Los integrantes del GCGCOOP que prosiguen en el orden de comunicaciones es el jefe/a de la Oficina de Asesoría Jurídica para coordinaciones de actividades referidas a la sede principal del ITP y el director de Operaciones para las convocatorias a encargados de los CITES y UT.
3. El jefe/a de la Oficina de Asesoría Jurídica convoca al jefe/a de la Oficina de Planeamiento, Presupuesto y Modernización y al jefe/a de la Oficina de Tecnologías de la Información que verificaran la asistencia de las personas encargadas de las actividades críticas de la Sede Central y regresan la comunicación confirmando o comunicando inconvenientes al jefe/a de la Oficina de Asesoría Jurídica
4. El director de Operaciones convoca a la Coordinadora de la Unidad Funcional de Atención al Ciudadano y Gestión Documental y al jefe/a de la Oficina de Administración, ambos realizan la convocatoria de las personas encargadas de las actividades críticas en los CITES y UT. Regresa la comunicación confirmando la asistencia o comunicando inconvenientes al director de Operaciones.
5. El jefe/a de la Oficina de Asesoría Jurídica y el director de Operaciones confirman las convocatorias y asistencias de las personas encargadas de las actividades en la sede central y CITES, respectivamente, a la presidencia del GCGCOOP, el jefe/a de la Oficina de Gestión de Recursos Humanos.
6. Finalmente, el jefe/a de la Oficina de Gestión de Recursos Humanos comunica al titular de la institución que las convocatorias han sido efectivas o inconvenientes presentados.

Adicionalmente a las convocatorias generales, cada Unidad Orgánica establece su respectivo rombo. Los jefes de cada UUOO comunican a dos personas predefinidas la condición de funcionamiento de la entidad a fin de tomar acción para dar continuidad de las operaciones y la comunicación con el personal clave.

Rombo de comunicación y coordinación:



ANEXO N° 3: DIRECTORIO DEL GRUPO DE COMANDO PARA LA GESTIÓN DE LA CONTINUIDAD OPERATIVA

JEFE O DIRECTOR O DE UNIDAD ORGÁNICA	CARGO	CONTACTO TELEFÓNICO	DIRECCIÓN ELECTRÓNICA
Rosse Mary Cruces Guerreros Jefa de la Oficina de Gestión de Recursos Humanos	Presidente	968 419 845 01 680 2150	rcruces@itp.gob.pe
Ronal Américo Barrio De Mendoza Vílchez Director de la Dirección de Operaciones	Miembro	991 102 798 01 680 2150	rbarrio@itp.gob.pe
Beatriz Marlene Rodríguez Ñique Jefe/a de la Oficina de Administración	Miembro	953 520 627	brodriguez@itp.gob.pe
John Edward Esquiagola Aranda Jefe/a de la Oficina de Tecnologías de la Información	Miembro	991 932 870	jesquiagola@itp.gob.pe
Lenin Horacio Gallardo Camacho Jefe/a de la Oficina de Planeamiento, Presupuesto y Modernización	Miembro	949 917 284 01 680 2150 / Anexo 1501	lgallardo@itp.gob.pe
Santiago Alonso García Ramos Jefe/a de la Oficina de Asesoría Jurídica	Miembro	998 044 780 01 680 2150 / Anexo 1600	sgarcia@itp.gob.pe
Soledad Carol Arteaga Paniagua Coordinador/a de la Unidad Funcional de Atención al Ciudadano y Gestión Documental	Miembro	991 406 308	sarteaga@itp.gob.pe

ANEXO N° 4: ORGANIZACIÓN PARA EL DESARROLLO DE LAS ACTIVIDADES CRÍTICAS

La organización se encuentra fundamentada en el conocimiento de las actividades críticas correspondientes a cada Oficina Dirección, por parte de todos los funcionarios, con la finalidad de evitar la duplicidad de funciones y esfuerzos.

El cumplimiento de la organización para el desarrollo de las actividades críticas requiere de la interiorización de los siguientes componentes:

- Conocimiento del Plan de Continuidad Operativa
- Entendimiento de la correspondencia de actividades criticas
- Comunicación entre el Grupo de comando para la Gestión de Continuidad Operativa
- Atención a la convocatoria del personal clave
- Ejecución de cronograma de implementación del Plan de Continuidad Operativa

Luego de ejecutar la fase previa del Plan de Continuidad Operativa, es decir el momento en que se gestiona la disposición de recursos y la adquisición de los requerimientos indicados para la Gestión de la Continuidad Operativa, la Dirección Ejecutiva y el Grupo de Comando coordinan permanentemente para realizar la activación, comunicación y convocatoria que permita llevar a cabo las actividades críticas.

ÓRGANO	OFICINA/DIRECCIÓN	ACTIVIDAD CRÍTICA
Alta Dirección	**Dirección Ejecutiva (DE)**	Supervisar las acciones de los diferentes órganos del ITP red CITE, de acuerdo al cumplimiento de metas establecidas.
		Coordinar con los órganos del ITP red CITE las acciones a realizar en caso de eventos y/o emergencias de gran magnitud
	Secretaría General (SG)	Dirigir y supervisar las acciones administrativas del ITP red CITE.
		Seguimiento de las acciones a realizar en caso de eventos y/o emergencias de gran magnitud
Unidades Funcionales	**SG-Unidad Funcional de Comunicaciones e Imagen Institucional (UFCII)**	Elaborar piezas gráficas y/o comunicaciones para publicar en los canales del ITP red CITE
	SG-Unidad Funcional de Integridad Institucional (UFII)	Gestionar la información sobre el evento de gran magnitud y/o emergencia para la toma de decisiones

	SG-Unidad Funcional de Atención al Ciudadano y Gestión Documental (UFACGD)	Atender a los usuarios en mesa de partes de ITP red CITE en caso de eventos y/o emergencias de gran magnitud
		Custodiar el acervo documentario del ITP red CITE
Control Institucional	**Órgano de Control Institucional (OCI)**	Ejecutar los servicios de control en el ITP red CITE sujeto a la normativa vigente establecida por la Contraloría General de la República.
Asesoramiento	**Oficina de Asesoría Jurídica (OAJ)**	Asesorar en normativa vigente, documentos y otros asuntos internos del ITP red CITE
	Oficina de Planeamiento, Presupuesto y Modernización (OPPM)	Evaluar requerimientos y elaborar propuestas de transferencias de partidas, transferencias financieras y otras modificaciones presupuestarias
		Aprobar la asignación presupuestal multianual
		Seguimiento de la ejecución presupuestal
		Evaluar y establecer presupuesto para rehabilitación en caso de eventos y/o emergencias de gran magnitud
Apoyo	**Oficina de Administración (OA)**	Emitir órdenes de servicios en el marco de la normativa vigente
		Realizar pago a proveedores y terceros
		Contratación de bienes y servicios para el ITP red CITE en caso de eventos y/o emergencias de gran magnitud
		Abastecer al ITP red CITE de servicios básicos
		Efectuar el control patrimonial y custodia de activos del ITP red CITE
	OGRHH-Secretaría Técnica	Gestionar los procedimientos de Continuidad Operativa, coordinación con la alta dirección y delegación de funciones al GCGCO.
		Seguimiento médico y de bienestar de los servidores y practicantes del ITP red CITE
		Seguimiento del registro de personal activo y cesante

	Oficina de Tecnologías de la Información (OTI)	Asegurar el funcionamiento de los recursos informáticos en caso de eventos y/o emergencias de gran magnitud
		Proveer soporte técnico a las áreas usuarias
Línea	**Dirección de Operaciones (DO)**	Implementar la mejora de la infraestructura física, tecnológica y servicios tecnológicos de los CITE
	Dirección de Estrategia, Desarrollo, Innovación y Fortalecimiento de los Centros de Innovación Productiva y Transferencia Tecnológica (DEDFO)	Identificar necesidades y requerimientos de servicios y de información en el ámbito de influencia de los CITE
	Dirección de Seguimiento y Evaluación (DSE)	Realizar la evaluación periódica de los CITE

ANEXO N° 5: PROCEDIMIENTO DE COMUNICACIÓN INTERNA ANTE EMERGENCIAS O EVENTOS DE GRAN MAGNITUD (SISTEMA DE COMUNICACIONES)

1. Objetivo

Mantener la comunicación entre el Grupo Comando y personal clave y de apoyo a fin de determinar el nivel de afectación en el ITP red CITE a fin de activar el Plan de Continuidad Operativa.

2. Escenario de activación

Ocurrencia de eventos de gran magnitud: sismos, incendios, inundaciones, ataques informáticos, entre otros que ponen en riesgo la integridad de los servidores, así como la infraestructura del ITP Red CITE.

3. Participantes

- Titular de la Entidad
- Grupo Comando
- Personal clave y de apoyo ante emergencias
- Grupo de Trabajo de Gestión de riesgos de desastres
- Servidores ITP Red CITE

4. Canales de comunicación

- Radios Tetra
- Telefonía celular (mensajes de texto)
- Correos electrónicos
- Aplicativos de mensajería instantánea
- Medios de comunicación social (radio, redes sociales, televisión)

5. Procedimiento de comunicación

Emisor	Destinatario	Instrucción	Medios	Acciones	Tiempo
OGRRHH (Unidad Orgánica de Gestión de Continuidad Operativa)	Grupo Comando	Notifica la situación en la Sede donde ocurre la emergencia	• Telefonía celular (mensaje de texto) • Correo electrónico	Nivel de afectación	Inmediato
Grupo Comando	Titular de la Entidad	Propone la activación del Plan de Continuidad Operativa	• Telefonía celular (mensaje de texto) • Correo electrónico	Activación del Plan de Continuidad Operativa	Inmediato
Grupo Comando	Personal clave y de apoyo ante emergencias	Informa sobre la situación y las acciones iniciales que se realizan	• Telefonía celular (mensaje de texto) • Correo electrónico	Coordinaciones para ejecución de actividades en Sede Alterna	Inmediato
Grupo Comando	Grupo de Trabajo GRD	Articulación para ejecución de plan de contingencia de la Sede	• Telefonía celular (mensaje de texto) • Correo electrónico	Coordinaciones para apoyo en ejecución del plan de contingencia	Inmediato

Emisor	Destinatario	Instrucción	Medios	Acciones	Tiempo
Grupo de Trabajo GRD	COES PRODUCE	Notifica acciones realizadas donde ocurre la emergencia	• Radios Tetra • Telefonía celular (mensaje de texto) • Correo electrónico	• Acciones ejecutadas y nivel de afectación • Solicitud de apoyo en gestión de riesgo de desastres	Inmediato
OGRRHH (Unidad Orgánica de Gestión de Continuidad Operativa)	Servidores	Notifica decisiones tomadas	• Telefonía celular (mensaje de texto) • Correo electrónico	Personal designado para trabajo presencial en Sede Alterna y/o teletrabajo	Hasta 1 hora (el tiempo dependerá de la magnitud del evento)

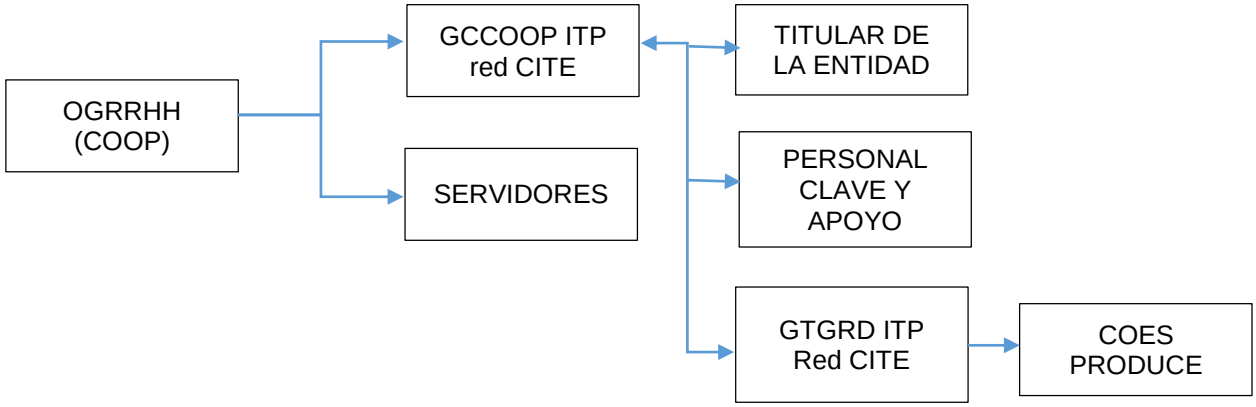
En caso de la Red CITE se realizará de la siguiente forma:

Emisor	Destinatario	Instrucción	Medios	Acciones	Tiempo
Director/a CITE	OGRRHH (Unidad Orgánica de Gestión de Continuidad Operativa)	Notifica la magnitud del evento en el CITE	• Telefonía celular (mensaje de texto) • Correo electrónico	Nivel de afectación	Inmediato
OGRRHH (Unidad Orgánica de Gestión de Continuidad Operativa)	Grupo Comando	Notifica la situación en el CITE donde ocurre la emergencia	• Telefonía celular (mensaje de texto) • Correo electrónico	Nivel de afectación	Inmediato
Grupo Comando	Titular de la Entidad	Propone la activación del Plan de Continuidad Operativa	• Telefonía celular (mensaje de texto) • Correo electrónico	Activación del Plan de Continuidad Operativa	Inmediato
Grupo Comando	Personal clave y de apoyo ante emergencias Director/a CITE	Informa sobre la situación y las acciones iniciales que se realizan	• Telefonía celular (mensaje de texto) • Correo electrónico	• Coordinación para la gestión de Sede Alterna mediante sinergia con otras Instituciones • Coordinaciones para ejecución de actividades en Sede Alterna	Inmediato
Grupo Comando	Grupo de Trabajo GRD	Articulación para ejecución de plan de contingencia del CITE	• Telefonía celular (mensaje de texto) • Correo electrónico	Coordinaciones para apoyo en ejecución del plan de contingencia del CITE	Inmediato
Grupo de Trabajo GRD	COES PRODUCE	Notifica acciones realizadas donde ocurre la emergencia	• Radios Tetra • Telefonía celular (mensaje de texto) • Correo electrónico	• Acciones ejecutadas y nivel de afectación • Solicitud de apoyo en gestión de	Inmediato

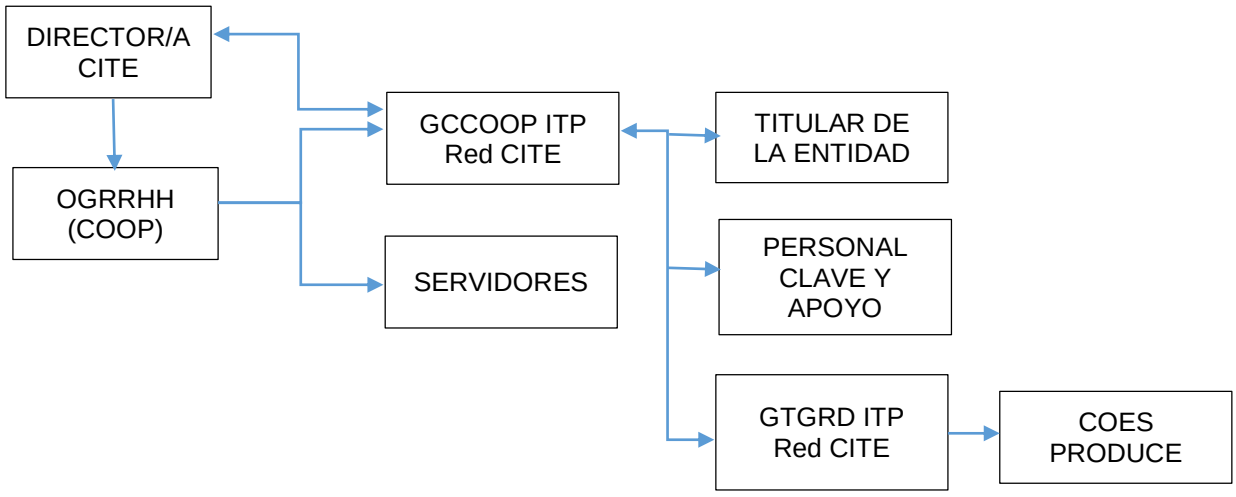
Emisor	Destinatario	Instrucción	Medios	Acciones	Tiempo
				riesgo de desastres	
OGRRHH (Unidad Orgánica de Gestión de Continuidad Operativa)	Servidores del CITE	Notifica decisiones tomadas	• Telefonía celular (mensaje de texto) • Correo electrónico	Personal designado para trabajo presencial en Sede Alterna y/o teletrabajo	Hasta 1 hora (el tiempo dependerá de la magnitud del evento)

6. Flujo de comunicación

SEDE CENTRAL



RED CITE



ANEXO N° 6: CRONOGRAMA DE IMPLEMENTACIÓN DE LA GESTIÓN DE LA CONTINUIDAD OPERATIVA

ETAPA	ACTIVIDAD	RESPONSABLE	2022	2023				2024				2025			
			4 T	1 T	2 T	3 T	4 T	1 T	2 T	3 T	4 T	1 T	2 T	3 T	4 T
ANÁLISIS DE RIESGO, PROCESOS Y RECURSOS	1.1 Designar al grupo de comando para la gestión de la continuidad operativa de la entidad.	Dirección Ejecutiva	X												
	1.2 Identificar los procesos y actividades críticas del ITP Red CITE.	Dirección Ejecutiva/ Unidades Orgánicas		X											
	1.3 Identificar y evaluar los riesgos que pueden causar interrupción de las actividades de la entidad.	Dirección Ejecutiva/ Unidades Orgánicas		X											
	1.4 Determinar el impacto de la interrupción de las actividades del ITP.	Dirección Ejecutiva/ Unidades Orgánicas		X											
	1.5 Realizar el diagnóstico del estado y riesgo de los recursos humanos necesarios para la ejecución de actividades críticas identificadas.	Oficina de Recursos Humanos		X											
	1.7 Realizar el diagnóstico del estado y riesgo de la infraestructura y recursos físicos para la ejecución de las actividades críticas identificadas.	Oficina de Administración		X											
	1.9 Realizar el diagnóstico del estado y riesgo de la infraestructura de tecnologías de la información para la ejecución de las actividades críticas identificadas.	Oficina de Tecnologías de la Información		X											
DESARROLLO DEL PLAN DE CONTINUIDAD OPERATIVA	2.1 Elaborar el proyecto de plan de continuidad operativa del ITP Red CITE.	Grupo de Comando			X										
	2.2 Revisar y aprobar el plan de continuidad operativa del ITP Red CITE.	Dirección Ejecutiva			X										
INTEGRACIÓN DE LA CO A LA CULTURA ORGANIZACIONAL	3.1 Programar charlas de difusión orientadas al desarrollo de la cultura de continuidad operativa	Oficina de Recursos Humanos				X				X				X	
	3.2 Evaluar e informar al GCGCOOP sobre la evolución de la Continuidad Operativa del ITP Red CITE.	Grupo de Comando					X				X				X

ETAPA	ACTIVIDAD	RESPONSABLE	2022	2023				2024				2025			
			4 T	1 T	2 T	3 T	4 T	1 T	2 T	3 T	4 T	1 T	2 T	3 T	4 T
ACTUALIZACIÓN DEL PLAN DE CONTINUIDAD OPERATIVA	4.1 Programar ensayos y pruebas de acuerdo al Plan de Continuidad Operativa del ITP Red CITE.	Grupo de Comando					X				X				X
	4.2 Elaborar el reporte de los resultados y recomendaciones para la mejora de la Gestión de la Continuidad Operativa	Grupo de Comando					X				X				X
	4.3 Elaborar la propuesta de actualización del plan de continuidad operativa del ITP	Grupo de Comando					X				X				X
	4.4 Revisar y aprobar el plan de continuidad operativa del ITP actualizado	Dirección Ejecutiva					X				X				X
	4.5 Realizar el seguimiento de la implementación de la Continuidad Operativa	Grupo de Comando						X		X		X		X	

*Trimestre

ANEXO N° 7: LINEAMIENTOS PARA LA IDENTIFICACIÓN DE PELIGROS Y RIESGOS

1. DEFINICIONES[3]

- **Peligro:** Probabilidad de que un fenómeno, potencialmente dañino, de origen natural o inducido por la acción humana, se presente en un lugar específico, con una cierta intensidad y en un período de tiempo y frecuencia definidos.
- **Riesgo:** Es la probabilidad de que la población y sus medios de vida sufran daños y pérdidas a consecuencia de su condición de vulnerabilidad y el impacto de un peligro.
- **Vulnerabilidad:** Es la susceptibilidad de la población, la estructura física o las actividades socioeconómicas, de sufrir daños por acción de un peligro.
- **Fenómeno de origen natural:** Es toda manifestación de la naturaleza que puede ser percibido por los sentidos o por instrumentos científicos de detección. Se refiere a cualquier evento natural como resultado de su funcionamiento interno.
- **Fenómenos inducidos por la acción humana:** Es toda manifestación que se origina en el desarrollo cotidiano de las actividades, tareas productivas (pesquería, minería, agricultura, ganadería, etc.) o industriales (comerciales y/o de fabricación industrial, etc.) realizadas por el ser humano, en la que se encuentran presentes sustancias y/o residuos (biológicos, físicos y químicos) que al ser liberados pueden ser percibidos por los sentidos o por instrumentos científicos de detección.

2. IDENTIFICACIÓN DE PELIGROS Y RIESGOS[4]

$$R_{ie} \mid_t = f(P_i, V_e) \mid_t$$

Dónde:

R= Riesgo.
f= En función
$\mathbf{P_i}$ =Peligro con la intensidad mayor o igual a i durante un período de exposición t
$\mathbf{V_e}$ = Vulnerabilidad de un elemento expuesto $_e$

El Riesgo (R) es una función del Peligro (P) y la Vulnerabilidad (V) que se expresa como la probabilidad de que ocurra una pérdida en un elemento “e”, como resultado de la ocurrencia de un fenómeno con una intensidad mayor o igual a “i”, en un determinado tiempo “t”.

La identificación de los peligros de origen natural (sismos, tsunamis, inundaciones, movimientos en masa, etc.) o inducidos por la acción humana (incendios, atentado terrorista, etc.) y la determinación de los riesgos que forman parte del Plan de Continuidad Operativa, se realiza teniendo en cuenta los siguientes pasos:

[3] Anexo N° 2. Terminología Básica. “Manual para la evaluación de riesgos originados por fenómenos naturales”.
[4] Resolución Ministerial N° 320-2021-PCM. “Lineamientos para la gestión de la continuidad operativa y formulación de planes de continuidad Operativa de las Entidades Públicas de los tres niveles de gobierno”

a. Identificar los peligros que pueden ocasionar una interrupción prolongada en el funcionamiento de la Oficina, Dirección y/o CITE y evaluarlo cualitativamente tomando en cuenta los niveles Bajo, Medio, Alto y Muy Alto.
b. Identificar las vulnerabilidades de la Oficina, Dirección y/o CITE, enfocada en la estructura que podría colapsar ante la ocurrencia de los peligros identificados, así como la afectación al personal de la entidad y evaluarlo cualitativamente tomando en cuenta los niveles de Bajo, Medio, Alto y Muy Alto.
c. Realizar la intersección de ambos (peligro y vulnerabilidad) y determinar el nivel de riesgo, tomando en cuenta la matriz siguiente:

MATRIZ DE RIESGO				
Peligro Muy Alto	Riesgo Alto	Riesgo Alto	Riesgo Muy Alto	Riesgo Muy Alto
Peligro Alto	Riesgo Medio	Riesgo Alto	Riesgo Alto	Riesgo Muy Alto
Peligro Medio	Riesgo Medio	Riesgo Medio	Riesgo Alto	Riesgo Alto
Peligro Bajo	Riesgo Bajo	Riesgo Medio	Riesgo Medio	Riesgo Alto
P / **V**	**Vulnerabilidad Baja**	**Vulnerabilidad Media**	**Vulnerabilidad Alta**	**Vulnerabilidad Muy Alta**

d. Posterior al análisis de cada peligro identificado y haber determinado el nivel de riesgo por cada uno de ellos elaborar la tabla resumen siguiente:

PELIGROS	**NIVEL DE RIESGO**			
	BAJO	**MEDIO**	**ALTO**	**MUY ALTO**
Exceso de lluvias				
Déficit de lluvias				
Heladas				
Friaje				
Sismos				
Tsunami				
Explosión volcánica				
Fenómeno El Niño				
Fenómeno La Niña				
Incendio				
Ataque informático				
Conmoción social				
Atentado terrorista				
Pandemia				

(*) Inundaciones, deslizamientos, huaycos

(**) Sequía

e. La tabla resumen servirá para elaborar el Plan de Continuidad Operativa.

ANEXO N° 8: LINEAMIENTOS PARA LA IDENTIFICACIÓN DE ACTIVIDADES CRÍTICAS[5]

1. DEFINICIÓN

- **Actividades críticas:** Están constituidas por las actividades que la entidad ha identificado como indispensables y que no pueden dejar de realizarse, conforme a sus competencias señaladas en las normas vigentes sobre la materia.

2. DETERMINACIÓN DE ACTIVIDADES CRÍTICAS

Consiste en determinar las actividades que no pueden interrumpirse, en tanto ello afectaría seriamente el cumplimiento de la misión de la entidad, incluye la identificación de los servicios y proveedores internos y externos críticos indispensables para su ejecución.

Asimismo, es necesario identificar los recursos necesarios para continuar con el cumplimiento de las actividades críticas; para ello se considera lo siguiente:

b. *Determinación de los recursos humanos:* Consiste en determinar el personal necesario para la ejecución de las actividades críticas identificadas, que incluya titulares y alternos.
c. *Determinación de los recursos informáticos e información crítica:* Consiste en determinar los aplicativos informáticos necesarios para la ejecución de las actividades críticas, así como la información que se requiere, sea en físico o digital según sea el caso, respetando los principios de seguridad de la información.
d. *Determinación de los recursos físicos críticos:* Consiste en determinar los bienes y equipos indispensables para asegurar la ejecución de las actividades críticas de la Entidad.

El Ministerio de la Producción, mediante el Centro de Operaciones de Emergencia Sectorial (COES-PRODUCE) recomienda la ejecución de un 10% de las actividades de la Entidad en caso de emergencias de gran magnitud.

3. MATRIZ PARA DETERMINACIÓN DE ACTIVIDADES CRÍTICAS

Para determinar las actividades críticas se deberá usar la siguiente matriz:

[5] Resolución Ministerial N° 320-2021-PCM. “Lineamientos para la gestión de la continuidad operativa y formulación de planes de continuidad Operativa de las Entidades Públicas de los tres niveles de gobierno”

MATRIZ DE DETERMINACIÓN DE ACTIVIDADES CRÍTICAS

DIRECCIÓN/OFICINA/CITE:

ACTIVIDAD CRÍTICA	RESPONSABLE/S	ACTIVIDADES A DESARROLLAR	RECURSO HUMANO (Indicar titulares y alternos)	RECURSOS INFORMÁTICOS	BIENES Y EQUIPOS
ACTIVIDAD CRÍTICA 1:		a.			
		b.			
		c.			
		d.			
		e.			
ACTIVIDAD CRÍTICA 2:		a.			
		b.			
		c.			
		d.			
		e.			
ACTIVIDAD CRÍTICA 3:		a.			
		b.			
		c.			
		d.			
		e.			

ANEXO N° 9: NÚMEROS DE EMERGENCIA A NIVEL NACIONAL

DEPENDENCIA	NÚMERO
Central Policial	105
EsSalud para información sobre Coronavirus (COVID-19)	107
Policía de carreteras	110
Infosalud	113
Defensa Civil	115
Bomberos	116
Cruz Roja	(01) 2660481

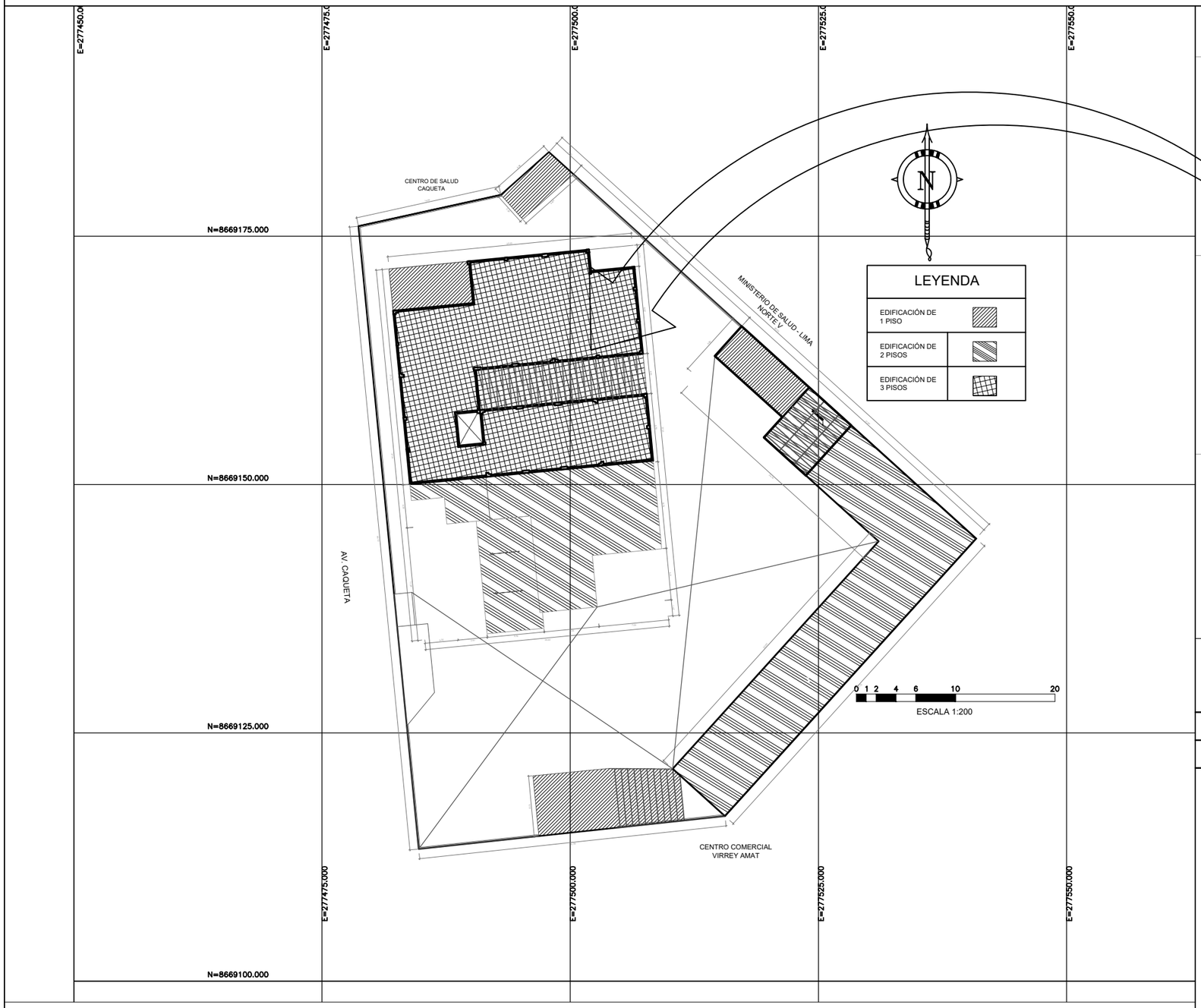
SISTEMA DE ATENCIÓN MÉDICA MÓVIL DE URGENCIA (SAMU)	NÚMERO
Para atención en las regiones: Amazonas, Ancash, Ayacucho, Huancavelica, Huánuco, Junín, La Libertad, Madre de Dios, Piura, Lima Región, Tacna, Tumbes, Ucayali, Lambayeque y Pasco	106

AMBULANCIAS EN LIMA	NÚMERO
Alerta Médica	(01) 4166777
Clave Médica	(01) 2658783
Sistema de Atención Médica Móvil de Urgencia (SAMU)	106
Ambulancias de EsSalud en Lima	117

SERVICIO DE MENSAJERÍA GRATUITA PARA EMERGENCIAS-DESASTRES NATURALES (MTC)	NÚMERO
Línea de Emergencia en caso de desastres naturales Para grabar un mensaje: 119+1 (y se graba el mensaje después del tono) Para escuchar el mensaje: 119+2+el número de la persona de la cual queremos tener información Desde teléfono fijo: 119+2+ el teléfono fijo incluyendo el código de área.	119

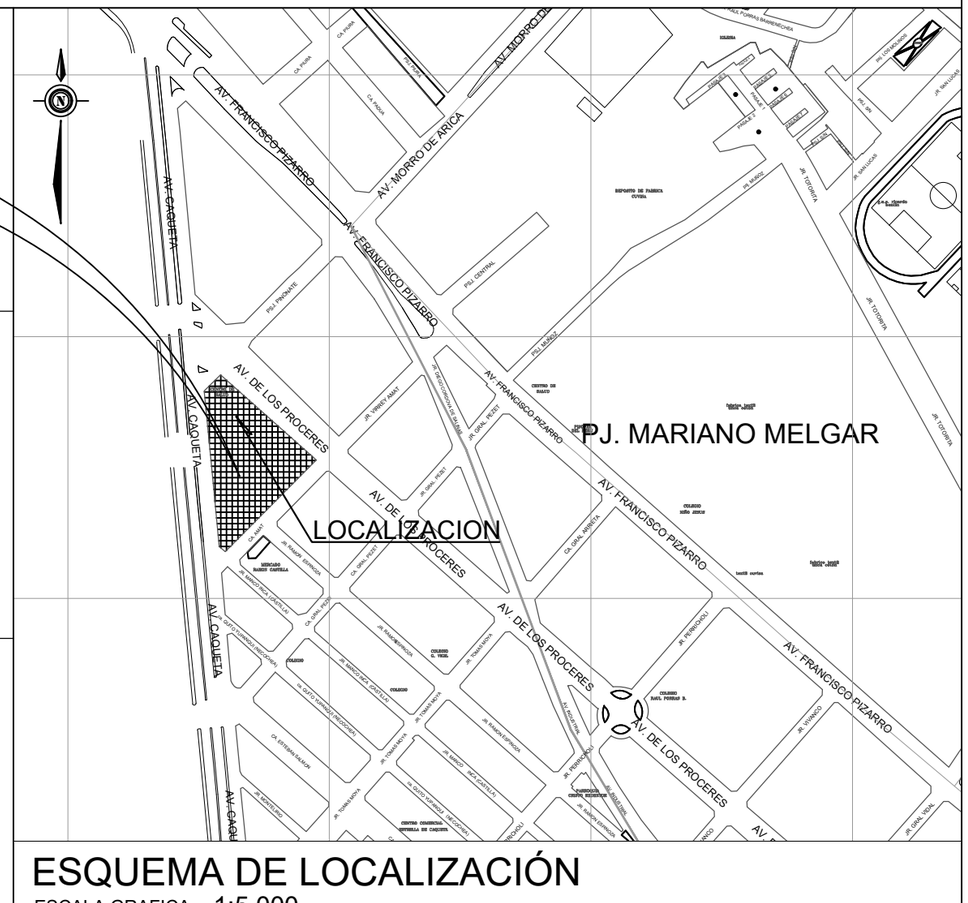
Fuente: PCM (https://www.gob.pe/547-telefonos-de-emergencia).
MTC (https://www.gob.pe/institucion/mtc/noticias/727420-mtc-linea-de-emergencia-119-se-encuentra-activa-a-nivel-nacional)

ANEXO N° 10: PLANO DE UBICACIÓN DE SEDE ALTERNA



PLANO DE UBICACION

Esc. 1:5,000



ESQUEMA DE LOCALIZACIÓN

ESCALA GRAFICA 1:5,000

ZONIFICACION : CZ

AREA ESTRUCTURACION URBANA : I

DEPARTAMENTO : LIMA
DISTRITO : RIMAC
URBANIZACION : ---
NOMBRE DE LA VIA : AV. CAQUETA
N° DEL INMUEBLE : 1300
LOTE : ---

PROVINCIA : LIMA
MANZANA : ---
SUBLOTE : ---

CUADRO NORMATIVO

PARAMETROS		NORMATIVO	PROYECTO
USOS		COMERCIO ZONAL (CZ), OU	OU
DENSIDAD NETA		----	----
COEFICIENTE EDIFICACION		----	----
% AREA LIBRE		NO EXIGIBLE	55.19%
ALTURA MAXIMA		5 PISOS	3 PISOS
RETIRO MINIMO	Frontal	----	2.65
	Lateral	----	----
	Posterior	----	----
ALINEAMIENTO DE FACHADA		----	----
LOTE MINIMO NORMATIVO		----	----
FRENTE MINIMO DE LOTE		----	----
ESTACIONAMIENTO		1/60M2	8 AUTOS

CUADRO DE AREAS (m2)

PISOS	Existente	Ampliación	Area a regularizar	Area a Remodelar		Area a ampliar	Area sol y sombra nueva	TOTAL
				Techada	Sin techar			
1ER PISO	634.01	–	–	1233.71	–	599.70	37.58	1233.71
2DO PISO	269.44	–	–	1125.07	–	855.63	39.24	1125.07
3ER PISO	269.44	–	–	493.70	–	194.26	66.46	493.70
								2852.48
AREA CONSTRUIDA TOTAL								2852.48
AREA LIBRE								1521.72
AREA DEL TERRENO								2755.48

PERÚ Ministerio de la Producción — Instituto Tecnológico de la Producción ITP

PROYECTO:
"MEJORAMIENTO DE LOS SERVICIOS TECNOLÓGICOS DEL CENTRO DE INNOVACION TECNOLÓGICA DEL CUERO , CALZADO E INDUSTRIAS CONEXAS (CITECCAL), EN EL DISTRITO DE RIMAC, PROVINCIAY DEPARTAMENTO DE LIMA"

LÁMINA: U-1

PLANO: UBICACION - LOCALIZACION

FECHA: JULIO - 2015

RESPONSABLE: INSTITUTO TECNOLOGICO DE LA PRODUCCION

PROYECTISTA: CARMEN VIOLETA QUISPE ANAYA — ARQUITECTA — 10571 CAP

DISTRITO: RIMAC
PROVINCIA: LIMA
REGION: LIMA

DIBUJO: A.J.S.S.

ESCALA: INDICADA

ANEXO N° 11: PROCEDIMIENTO DE ASEGURAMIENTO DEL ACERVO DOCUMENTARIO

PROCEDIMIENTO DEL ASEGURAMIENTO DEL ACERVO DOCUMENTARIO

UNIDAD FUNCIONAL DE ATENCIÓN AL CIUDADANO Y GESTIÓN DOCUMENTAL

2023

Procedimiento de aseguramiento del acervo documentario

OBJETIVOS

- Contar con procedimientos que aseguren la preservación y conservación requeridos para garantizar la integridad del acervo documental físico y electrónico, para el resguardo de la evidencia de los proceso y funciones de las unidades de organización y descentralizadas del ITP.
- Establecer acciones de prevención de emergencias y atención de desastres la administración adecuada de los riesgos y/o factores de deterioro biológico, químicos o físicos, que potencialmente puedan causar algún tipo de deterioro en el acervo documental físico y electrónico.

MEDIDAS PREVENTIVAS

- Una vez identificados y valorados los riesgos que pueden poner en peligro la integridad del acervo documental
- Realizar verificación del cableado eléctrico, los sistemas de agua y desagüe que estén cera de los repositorios de los Archivos de Gestión, Archivo Central y realizar coordinaciones con OTI de verificación de los repositorios digitales.
- Realizar coordinaciones con Servicios Generales de mantenimiento a las instalaciones, instalaciones eléctricas, de agua y desagüe.
- Asegurar el funcionamiento de las salidas de emergencia, que sean de fácil acceso y debidamente marcadas.
- Contar con extintores y números de emergencias: AGN, bomberos y policía.
- Creación de backup de los repositorios de los Archivos de Gestión Digital del ITP y la Red CITE.

ACCIONES DE EMERGENCIA

• Planos de los repositorios, que muestren: los extinguidores y materiales para intervención, y los puntos donde la electricidad y el agua pueden suspenderse entre otros, así como el Planos de evacuación.

• Contar con una lista de los documentos a salvar con prioridad de conservación permanente y vigente.

• Contar con una lista de Restauradores, empresas especializadas en el tratamiento, de transporte, y para el almacenamiento eventual.

ACCIONES DE RESCATE

INUNDACIONES

- En todas las situaciones de emergencia hay que controlar el pánico.
- Asegurar en primera instancia la seguridad de las personas y alertar a los servicios de intervención de las emergencias.
- Instale deshumidificadores, pero asegúrese de contar con un mecanismo que evacue el agua que recolecte.
- Colocar ventiladores en diferentes puntos del espacio para hacer circular el aire, abrir las ventanas.

- Hacer controles de la humedad relativa y la temperatura, para mantenerlo dentro de los rangos recomendados.
- De ser necesarios solicitar que se realicen exámenes de microbiología para verificar el nivel de carga microbiana e identifique en el ambiente.
- Brindarle al personal que va a ingresar al espacio y/o va a tener contacto con la documentación elementos de seguridad (guantes, guardapolvos o mandiles anti fluidos, mascarilla KN95).
- Los documentos deben ser envueltos en papel alcalino, movilízalos en cajas.
- Traslade la documentación ambiente que se encuentren en bunas condiciones, y coordinar con el con el Archivo General de la Nación, pertinente para su recuperación.
- Determinar la magnitud de los daños ocasionados por el siniestro tanto de las personas como los repositorios del acervo documental, para determinar qué acciones y recursos se requieren.

INDENCIO

- De ser necesario sin tomar riesgos adicionales hacer el uso de extintores si el incendio es pequeño, suspender las redes de agua, de electricidad y de gases entre otros.
- Verificar que el fuego no impida la salida de las personas y la evacuación de los documentos, que en principio deben rescatarse los de valor permanente y si se pudiera rescatar otros documentos sean los que estén vigente.
- Alertar de llamar a la compañía de bomberos y dar la alerta del siniestro.
- La prioridad debe siempre será salvar vidas, motivar a guardar la calma, seguir las indicaciones para realizar la evacuación del área de ser necesario, utilizando las rutas de emergencia.
- Realizar un inventario de los documentos siniestrados y el estado en que se encuentran para realizar las coordinaciones con el Archivo General de la Nación, pertinente para su recuperación.
- Asimismo, evitar mover los documentos, ya que son afectados por el fuego y los materiales que se usaron para extinguir, estos deben levantarse con papeles alcalinos para que se movilicen áreas que se encuentren en buen estado para proceder a su tratamiento.

SISMOS

- Realizar la verificación de los lugares por donde transitar no haya vidrios rotos o cables eléctricos, así como tocar objetos metálicos que estén en contacto con cualquier fuente de energía.
- Dar aviso de los derrumbes o riesgos de colapso en el mobiliario, a la autoridad correspondiente y esperar las indicaciones para su remoción.
- Verificar el funcionamiento de los sistemas eléctricos y de ventilación (aire acondicionado), en caso de que no se hayan dañado durante el siniestro.
- Examinar el estado de la estantería, y muebles de los repositorios.

- Revisar el estado de las unidades de conservación y archivamiento, si se registra movimiento o caída, organizar equipos de trabajo para recogerlos y recolocarlos en su lugar, si la estantería está en condiciones, sino apilar máximo de 3 cajas.
- Remplazar las cajas que hayan sufrido daños, y ubicándolas en lugares seguros.
- Evitar mover cualquier documento que haya sido afectado por agua, fuego o sustancias químicas sin la ayuda de un soporte auxiliar rígido (un cartón o una hoja de polipropileno, entre otros).
- Revisar el funcionamiento de los equipos de cómputo y verificar si hubo pérdida de información en las bases de datos.
- Adaptar y acondicionar un sitio provisional para instalar la documentación que haya sido rescatada, así como organizar los documentos por grupo de origen para identificar faltantes.
- Identificar las unidades de conservación y archivamiento por la magnitud de los daños que estas hubieran sufrido.
- Evitar realizar reparaciones de urgencia.
- Limpiar la documentación dañada, haciendo uso del material protección personal y de conservación documentaL.
- Informar a la Unidad Funcional de Atención al Ciudadano y Gestión Documental, el estado de las personas, si el evento se dio en horas laborales, del acervo documental, de las instalaciones y muebles de los Archivos de Gestión y Central.

ANEXO N° 12: INFORME DE IMPLEMENTACIÓN DE MEJORAS DE LOS SERVICIOS INFORMÁTICOS

INFORME DE IMPLEMENTACIÓN DE MEJORAS DE LOS SERVICIOS INFORMÁTICOS

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

2023

1. ANTECEDENTES

El centro de datos situado en la sede de Callao representa la **plataforma o base tecnológica** que proporciona los servicios básicos computacionales necesarios para el soporte de los procesos administrativos destinados al logro de los objetivos estratégicos de la entidad en el corto plazo.

El centro de datos se encarga de ofrecer diversos servicios, recursos y sistemas informáticos a cerca de 1000 usuarios ubicados en Lima y Regiones, que constituyen el núcleo laboral del mismo **ITP** y la **Red CITE**, extendido por todo el territorio nacional.

El despliegue del centro de datos es una implementación basada en tecnología de ***infraestructura convergente (CI)*** que se puso en marcha en el año 2017 para reemplazar todo el equipamiento obsoleto y precario, que representaba un obstáculo frente a los nuevos requerimientos por servicios más robustos y resilientes.

En la sección **Anexo 1**, se adjunta la **orden de compra Nº 0000117** del año 2017, en la cual se detalla el equipamiento considerado para la instalación del centro de datos que estuvo a cargo de la empresa **TECNOLOGÍA & CREATIVIDAD S.A.C.**

El despliegue de dicha infraestructura se hizo con equipos y dispositivos modernos de la época consistentes en hardware y software de la marca americana **HPE**, que aún a la fecha sigue siendo líder en el rubro tecnológico a nivel global.

El centro de datos se diseñó desde la planificación para soportar toda la carga de transacciones operacionales y computacionales de los usuarios, para lo cual se dispuso la implementación de recursos informáticos con grandes capacidades de poder de cómputo, repositorios para el almacenamiento y medios de conectividad, para la transmisión de los datos.

La plataforma tecnológica del Callao se encuentra ubicada en un espacio controlado, según estándares técnicos de cumplimiento mundial, ya que se busca garantizar la integridad física de todo el equipamiento informático ante diversas acciones de robo o vandalismo.

2. CONTEXTO ACTUAL

Debido a la antigüedad de la actual infraestructura tecnológica, que ya cuenta con más de 6 años de operatividad ininterrumpida, se hace muy urgente la renovación de todo el parque informático instalado en centro de datos desde 2017.

La plataforma tecnológica se entregó incluyendo un período de soporte y garantía de 3 años efectivos, condiciones que vencieron a inicios de 2020, próximo a la alerta lanzada por motivo de la propagación del virus SARS-CoV-2.

Debido a la obsolescencia de la implementación tecnológica, varios de los componentes instalados están presentando fallos en su funcionamiento, que están poniendo en riesgo la operatividad y disponibilidad de las aplicaciones de red que dan soporte sistémico a la gestión administrativa de la entidad.

A continuación, se menciona en forma resumida los eventos acontecidos en todo este

período de 6 años de servicio ininterrumpido, cumplidos entre fines de febrero e inicios de marzo de 2023:

- Reemplazo por garantía de la **solución de respaldos en cinta**, que estuvo presentando fallas durante el proceso de las copias de información, a los pocos años de haber iniciado el sistema.
- Cambio por garantía de una de las dos controladoras que se encargan de gestionar la solución de almacenamiento centralizado **SAN (Storage Attached Network)**.
- Reemplazo por garantía de los dos dispositivos de contingencia energética **(UPS)**, que mantienen energizados el clúster de servidores y el almacenamiento **SAN**, ya que las baterías no respondían con los tiempos de tolerancia establecidos.
- Cancelación de la adquisición de uno de los cabezales de escritura (drive) del equipo de respaldos de la información, que luego de un largo proceso se indicó que requería como respaldo el **informe técnico de estandarización**.
- Caída de uno de los servidores blade del **clúster de contingencia**, luego de un mantenimiento programado del sistema eléctrico en planta externa, con lo que se perdió capacidad de cómputo (CPU) y almacenamiento en memoria (RAM).
- Cancelación del servicio de **mantenimiento general de sala de servidores y sistema de ventilación de precisión**, luego que el proveedor no atendiera el requerimiento.
- Cancelación del pedido de **soporte técnico y garantía extendida del equipamiento** de servidores y almacenamiento, debido a la falta del presupuesto requerido.
- Cancelación de la adquisición de la **solución de grupo electrógeno**, cuyo proceso de compra se truncó por no haberse respetado los plazos indicados enla normativa actual.
- Anulación de la buena pro otorgada por el nuevo equipamiento en enero deeste período 2023 debido, supuestamente, a irregularidades en la documentación presentada por el proveedor.

Si llegara a fallar por completo el compartimento del chasis, que soporta las fuentes de poder, los 8 nodos o servidores de producción, los 2 equipos de conectividad, entre otros, prácticamente el centro de datos dejaría de funcionar con lo que quedaría totalmente inhabilitado para proporcionar los servicios básicos de red.

La degradación física del hardware se acentúa luego de los 3 o 4 años de operatividad de los equipos, con lo que se pone en gran riesgo la disponibilidad y la integridad de los recursos informáticos desplegados en la red institucional.

Luego de vencidos el soporte y la garantía contractuales del equipamiento, el centro de datos no ha recibido ningún servicio de revisión, mantenimiento o actualización, debido en gran parte por los problemas mundiales ocasionados por la pandemia del COVID-19.

Todo el equipamiento instalado en el centro de datos ya alcanzó la vida útil de operación y vigencia tecnológica, por lo que los componentes o repuestos ya no se fabrican ni comercializan a nivel mundial, con lo que es casi imposible encontrarlos en el mercado, salvo que haya algún saldo disponible en los almacenes locales de los proveedores asociados a la marca.

A inicios del año 2022, para paliar en alguna medida la falta de apoyo por parte del fabricante del hardware y software, se continuó con el proceso de renovación del soporte y garantía del equipamiento de centro de datos, a través de la **solicitud de adquisición del servicio de mantenimiento preventivo y correctivo de la plataforma tecnológica**.

Debido a la impugnación de uno de los dos postores durante el proceso respectivo, que

apeló aduciendo que no se estaba cumpliendo con los requisitos de calificación de los especialistas, el **Tribunal de Contrataciones del Estado** dejó a criterio de ITP la absolución del caso, por lo que la entidad sentenció en favor de la anulación de oficio del mencionado pedido de servicio.

3. OBJETIVOS DEL PLAN DE CONTINGENCIA

Con la propuesta de implementación tecnológica del centro de datos, se busca cubrir los siguientes objetivos en el mediano plazo:

- Contribuir con el logro de los objetivos estratégicos institucionales establecidos en el **Plan Estratégico Institucional (PEI).**
- Garantizar la continuidad de las operaciones transaccionales de la entidad asegurando un mayor tiempo de operatividad de los sistemas.
- Asegurar la implementación futura de aplicaciones, servicios y sistemas con el despliegue de mayores recursos computacionales-
- Incrementar la seguridad de los datos frente a los ataques de malware provenientes de la internet.
- Asegurar la disponibilidad y la integridad de la información con el fortalecimiento de las políticas de seguridad basadas en la norma **ISO 27001**.
- Incrementar la velocidad en el acceso a la información reduciendo las altastasas de latencia durante la lectura y escritura de los archivos.
- Aumentar las capacidades de procesamiento (**CPU**), almacenamiento (**storage**) y conectividad (**networking**).
- Asegurar las bases de datos, aplicaciones web y repositorios de archivos enmedios más modernos.
- Garantizar oportunamente las copias o respaldos de la información en disco ocinta como medida de contingencia.
- Garantizar una **alta disponibilidad** (**HA**) y **tolerancia a fallos** (**FT**) para no interrumpir las operaciones.
- Proveer sistemas más robustos que cuenten con mayores niveles de resilienciaante desastres inoportunos.
- Asegurar rápidamente los niveles de **escalabilidad vertical** y **horizontal** paracumplir con las mayores exigencias de los clientes.
- Mejorar la velocidad de las aplicaciones, a través del uso de tecnología de contenedores **(*Docker* y *Kubernetes*).**
- Acelerar el restablecimiento de los servicios y aplicaciones vulnerados, en casode algún ataque cibernético.
- Contribuir con los planes de ***Continuidad de los Negocios*** y ***RecuperaciónAnte Desastres.***
- Renovar el soporte y la garantía del equipamiento tecnológico para asegurar unmayor desenvolvimiento de la plataforma de sistemas.

4. ACCIONES PERTINENTES

Debido al conocimiento del estado situacional, descrito en los apartados previos, los encargados de la **Oficina de Tecnologías de la Información (OTI)** están tomando diferentes medidas y acciones, tanto en el corto como mediano plazo, en colaboración con otras dependencias, para fortalecer los procedimientos contenidos en el **Plan de Contingencia y Recuperación de los Servicios Tecnológicos del Centro de Datos**, desarrollado en 2021, con la ejecución de las siguientes implementaciones:

4.1. Servicio de acceso a internet

En el **corto plazo** se quiere asegurar el **servicio de conectividad a la internet**con la contratación del servicio de conexión por el período de tres (03) años con alguna de las empresas del medio local para fortalecer las comunicaciones con los diferentes profesionales, tanto de las entidades públicas como privadas, a nivel nacional e internacional.

A ese respecto, se van a realizar las coordinaciones respectivas, de igual manera, para asegurar los servicios de **interconexión entre sedes (LAN2LAN)** y **telefonía IP (troncal SIP)** con la contratación de dichas prestaciones por un período similar de tiempo, con miras a la consolidación de los servicios básicos de conectividad a los servicios de red, que la entidad ha desplegado en la intranetinstitucional.

4.2. Mantenimiento preventivo y correctivo del centro de datos

Asimismo, en el mismo **corto plazo**, se está buscando la contratación del **servicio de mantenimiento preventivo y correctivo del equipamiento** alojado en centro de datos que permita prolongar y asegurar el correcto estado de funcionamientode la sala de procesamiento para garantizar un ambiente controlado con las mejores condiciones técnicas con el objetivo de proteger los dispositivos de la plataforma tecnológica de la entidad donde se alojan los diferentes servicios básicos de red.

También, con dicha contratación se va a proceder con la renovación de la garantía por fallas en el hardware y software del equipamiento tecnológico, así como con la recuperación del soporte técnico por parte del fabricante, con lo que se va a robustecer en dichos aspectos la integridad y disponibilidad de los recursos informáticos.

4.3. Implementación del nuevo centro de datos basado en tecnología hiperconvergente (HCI)

En el **mediano plazo** se ha bosquejado la opción consistente en hospedar el nuevo equipamiento del centro de datos, que se piensa desplegar con tecnología de **Infraestructura de Hiperconvergencia (HCI, Hyperconverged Infrastructure)**, en alguna de las dos sedes que se mantiene en Lima Metropolitana, ya sea en las instalaciones de **CITEmadera Lima** (ubicado en Parque Industrial, Villa El Salvador) o **CITEccal Lima** (ubicado en Caquetá, Rímac), a fin de reducir el impacto en las operaciones del centro de datos localizado cerca al mar de Ventanilla.

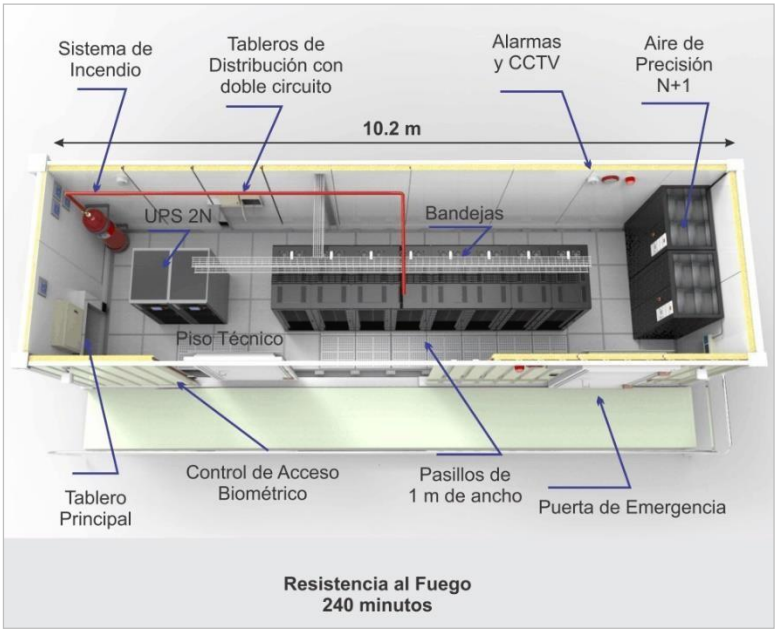
Esto último va a implicar realizar distintas coordinaciones de trabajo entre todoslos especialistas, administrativos, directores y proveedores de soluciones para generar un expediente técnico lo suficientemente robusto de la nueva **implementación informática** para que sea el sustento técnico del pedido de instalación y despliegue dela moderna plataforma virtual de servicios de red, como parte del aseguramiento de la información sensible manejada por los especialistas de la entidad.

Además, va a involucrar, indefectiblemente, la asignación de un espacio en alguno de los locales indicados para el funcionamiento del nuevo centro de operaciones, que va a requerir trabajos previos de **adecuamiento técnico** (**obra civil**, **red eléctrica**, **piso técnico**, **techo técnico**, **pozo a tierra**, **transformador de aislamiento**, **tablero principal**, **grupo electrógeno**, entre otros) para, en conjunto, proporcionar un adecuado nivel de seguridad a la nueva plataforma de recursos de la intranet empresarial.

Alternativamente, se cuenta con otra opción consistente en la implementación de la

infraestructura de cómputo en un **contenedor de material prefabricado**, que permite un nivel similar de seguridad física y eléctrica, ya que cuenta con mecanismos contra incendio, robo, vandalismo, saqueo; además de acceso biométrico, energía estabilizada, sensores de control, piso técnico, sistema de vigilancia, aires de precisión, sala de operaciones, tableros de energía, entre otros, como la de proporcionar la característica de transportabilidad, mediante la cual va a facilitar su traslado a cualquier lugar seguro en caso de riesgo inminente.

4.4. Arquitectura del contenedor de centro de datos



5. ALTERNATIVA TECNOLÓGICA

Ante lo expresado en los apartados previos, como **mejor opción**, se había presentado la alternativa de hospedar la actual plataforma de virtualización del ITP en alguna de las soluciones de nube ofrecidas por reconocidos proveedores internacionales, tales como **Amazon Web Services (AWS)**, **Microsoft Azure (MSA)** o**Google Cloud Platform (GCP)**, cuyas implementaciones cumplen con los requisitos tecnológicos requeridos para garantizar a los usuarios una alta disponibilidad de los servicios de red.

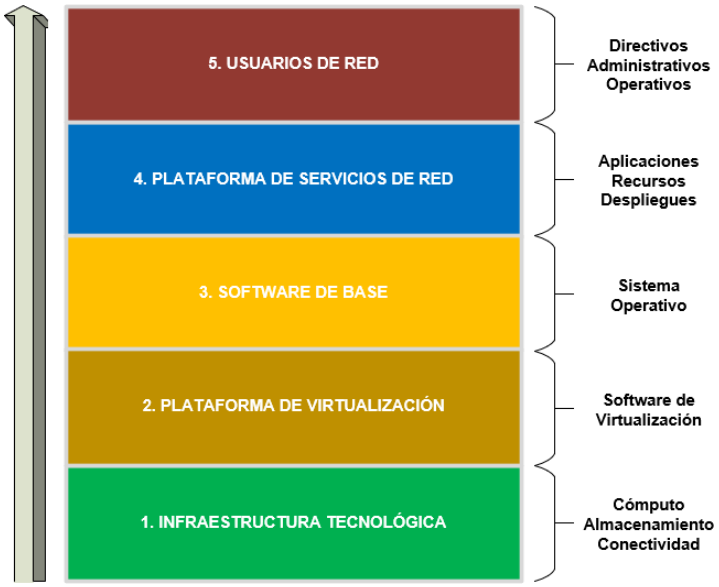
Dentro de esta opción en nube, también se estaba considerando incluir las alternativas ofrecidas por proveedores nacionales, tales como las desplegadas por las

empresas locales **Optical Technologies**, **Yachay**, **Movistar** y **Claro**, cuyas plataformas tecnológicas están desplegadas cumpliendo estándares mundiales de la industria para ofrecer las características técnicas que requiere el centro de datos de ITP, tales como:

- **Alta disponibilidad del servicio**
- **Sitio de replicación**
- **Crecimiento bajo demanda**
- **Respaldo energético**
- **Contingencia de la información**
- **Seguridad digital del perímetro**
- **Protección física**
- **Aprovisionamiento programado**
- **Sistemas de seguridad**
- **Consolas de gestión**

- **Tolerancia a fallos**
- **Balanceo de las cargas**
- **Rápida respuesta a caídas**
- **Acceso controlado**
- **Cumplimiento de la normatividad**
- **Alineación a estándares mundiales**
- **Aplicación de buenas prácticas**

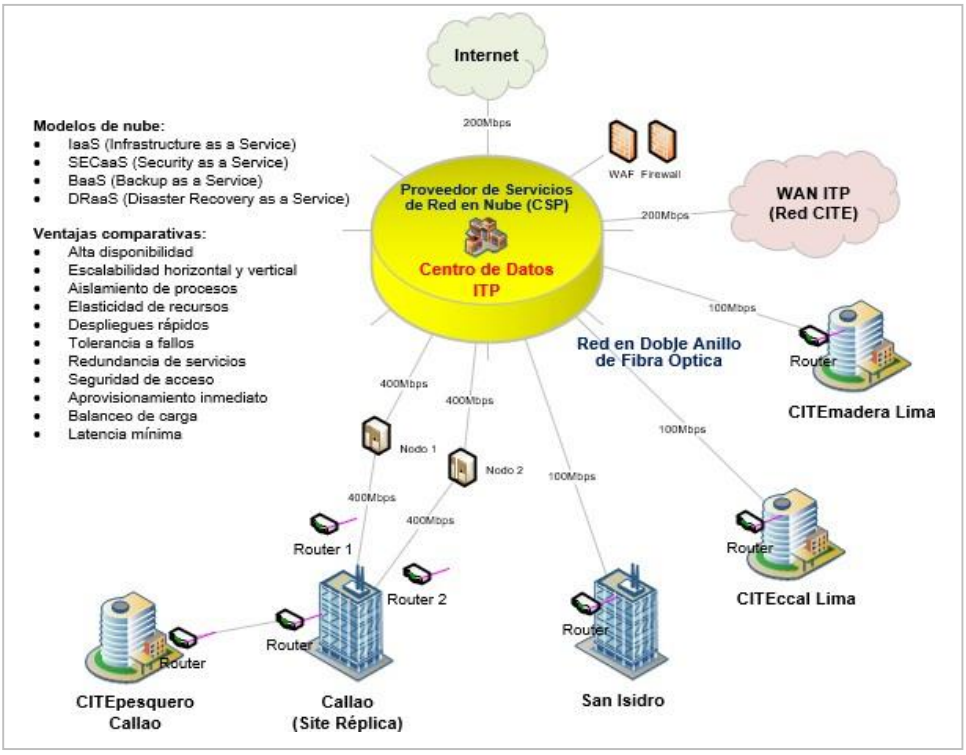
Dentro de la estructura de implementación sistémica, el despliegue de los servicios de red se ubica en la **Capa 4 (Plataforma de servicios de red)**, tal como se distingue en la siguiente imagen, que es el estrato que se requiere migrar a la infraestructura de nube para una mayor seguridad de la plataforma tecnológica que conforma el centro de datos.



5.1. Estructura de la intranet basada en capas

En adición a lo mencionado, como parte de las medidas de **mejoramiento y ampliación de la red de servicios**, también se están evaluando los requerimientos técnicos para la conectividad de la sede central y las diferentes instalaciones de la

Red CITE mediante la contratación del servicio de interconexión por fibra óptica ofrecido por la **Red Dorsal Nacional de Fibra Óptica (RDNFO)** cuya cobertura llega hasta las principales ciudades del país. Con lo indicado, se pretende conectar la infraestructura de la red institucional con toda la **Red CITE**, tal como se puede apreciaren la imagen siguiente:



5.2. Topología propuesta de la red de ITP

Sin embargo, luego de la reunión realizada el último 21 de marzo de los corrientes, entre el especialista de **OTI** y los miembros de la **Unidad Formuladora (OPPM)**, se determinó que la norma administrativa y jurídica actual del Estado no permitía la contratación del **servicio de plataforma de red virtual en la nube**, debido a que el pedido no calificaba dentro de los parámetros definidos en el **IOARR (Identificación de Inversiones de Optimización, de Ampliación Marginal, de Rehabilitación y de Reposición)** abierto, que había iniciado desde el período 2020,ya que este solo contempla bienes o activos tangibles.

Además, los especialistas de **Unidad Formuladora** enfatizaron que antes de cualquier otro pedido referente a la renovación, adecuación o actualización del parque informático de centro de datos, se debía concluir con el actual **IOARR** abierto que, justamente, se generó para contemplar dicho requerimiento de mejora de la infraestructura sistémica.

Asimismo, indicaron que el servicio de plataforma de red virtualizada en la nube**(IaaS, Infrastructure as a Service, Infraestructura como un Servicio)** iba a representar un gasto anual cuya cobertura no estaba asegurada presupuestalmente debido al alto monto calculado, es decir, que no había garantía sobre la previsión presupuestal para la continuidad del contrato durante los años que pudiera durar la prestación, con lo que se pondría en riesgo la vigencia de la plataforma virtual.

6. CONCLUSIONES

Como se ha podido demostrar durante la exposición de los argumentos técnicos, la necesidad por la renovación de la actual plataforma tecnológica de los sistemas y servicios de red es bastante apremiante ya que, debido a las amenazas indicadas, tanto materiales como humanas y naturales, existe una mayor probabilidad de falla en el equipamiento obsoleto de centro datos, donde se aloja la información que los distintos especialistas manejan para el cumplimiento de los objetivos estratégicos de la entidad.

El presente informe técnico se presenta como sustento documentario para poner en

conocimiento de las áreas involucradas la urgencia de los requerimientos por una moderna infraestructura computacional, que pueda constituirse como el soporte de la plataforma de servicios de red como medida básica para el aseguramiento de la información institucional.

ANEXO 1

Sistema Integrado de Gestión Administrativa
Módulo de Logística
Versión 21.01.01.U1

ORDEN DE COMPRA - GUíA DE INTERNAMIENTO Nº 0000117

Nº Exp. SIAF : 0000001611

Dia	Mes	Año
27	02	2017

UNIDAD EJECUTORA : 001 INSTITUTO TECNOLOGICO DE LA PRODUCCION - ITP
NRO. IDENTIFICACIÓN : 000194

1. DATOS DEL PROVEEDOR	2. CONDICIONES GENERALES
Señor(es) : TECNOLOGIA Y CREATIVIDAD S.A.C.	**Nº Cuadro Adquisic:** 000124
Dirección : AV. REPUBLICA DE PANAMA NRO. 3563 DPTO. 101 LIMA - LIMA - SAN ISID / / **CCI:** 00219300178188604616	**Tipo de Proceso :** LP - Nª 0002-2016-ITP
RUC : 20518446372 **Teléfono :** **Fax :**	**Nº Contrato :** 002-2017-ITP/SG/OA-A
	Moneda : S/ **T/C :**

Concepto : ADQUISICION DE EQUIPOS PARA EQUIPAMIENTO INTEGRAL DE SERVIDORES Y ALMACENAMIENTO EN RED PARA EL CENT

Código	Cant.	Unid. Med.	Descripción	Precio Unitario S/	Precio Total S/
740801620001	1.	UNIDAD	CHASIS PARA SERVIDORES TIPO HOJA/ULTRADELGADOS	164,366.000000	164,366.00
746444910099	2.	UNIDAD	GABINETE DE METAL 42 RU PARA EQUIPOS DE COMUNICACIONES	20,905.500000	41,811.00
740892000001	1.	UNIDAD	SERVIDOR	19,479.000000	19,479.00
740892000048	8.	UNIDAD	SERVIDOR BLADE	57,753.125000	462,025.00
740894810004	1.	UNIDAD	SOLUCION DE ALMACENAMIENTO EXTERNO SAN - STORAGE AREA NETWORK	477,000.000000	477,000.00
740899850001	1.	UNIDAD	UNIDAD PARA COPIA DE SEGURIDAD - TAPE BACKUP EXTERNO	135,309.000000	135,309.00
			LA CARACTERÍSTICAS DE LOS BIENES SERAN DE ACUERDO A LAS ESPECIFICACIONES TECNICAS DEL AREA USUARIA, BASES INTEGRADAS, PROPUESTA DEL PROVEEDOR Y CONTRATO N° 002-2017-ITP/SG-OA-ABAST.		
			PLAZO DE ENTREGA DE LOS BIENES:		
			20 DIAS CALENDARIOS DESDE SUSCRITO EL CONTRATO N° 002-2017-ITP/SG-OA-ABAST(21/02/2017).		
			PRUEBAS OPERATIVAS E IMPLEMENTACION DE LA SOLUCION SERÁ DE 03 DIAS CALENDARIOS DESDE FINALIZADA LA ETAPA DE ENTREGA.		
			LUGAR DE ENTREGA:		
			ALMACEN CENTRAL DEL ITP, SITUADO EN CARRETERA A VENTANILLA KM		

AFECTACION PRESUPUESTAL

Meta/ Mnemónico	Cadena Funcional	FF/Rb	Clasif. Gasto	Monto S/
0051	14.006.0008.9001.3999999.5000003	1 - 00	2.6. 3 2. 1 2	41,811.00
0051	14.006.0008.9001.3999999.5000003	1 - 00	2.6. 3 2. 3 1	1,093,813.00
0051	14.006.0008.9001.3999999.5000003	1 - 00	2.6. 3 2. 3 2	164,366.00

Van ... S/ **1,299,990.00**

Exonerado	:	1,299,990.00
V. Venta	:	0.00
I.G.V.	:	0.00
Total	:	1,299,990.00

Facturar a nombre de : INSTITUTO TECNOLOGICO DE LA PRODUCCION - ITP
Dirección : AV. REPUBLICA DE PANAMA N° 3418 SAN ISIDRO - LIMA 3418 / SAN ISIDRO - LIMA - LIMA
RUC : 20131369477
Agradecemos enviar los bienes a la siguiente dirección :
CARRETERA A VENTANILLA KM 5.2 / VENTANILLA - PROV. CALLAO - PROV.CONSTITUC.DEL

ELABORADO POR	ORDENACION DE LA COMPRA		CONFORMIDAD	
CACERES CAJAS, ROGER				CUENTAS X PAGAR S/ _____
	RESPONSABLE DE ADQUISICIONES	RESPONSABLE DE ABASTECIMIENTO Y SERV. AUXILIARES	RESPONSABLE DE ALMACEN	Fecha Dia Mes Año

NOTA IMPORTANTE :
- El Proveedor debe adjuntar a su Factura copia de la O/C atendida.
- Esta Orden es nula sin las firmas y sellos reglamentarios o autorizados.
- Nos reservamos el derecho de devolver la mercadería que no esté de acuerdo con las especificaciones técnicas.
- El Contratista (Proveedor) se obliga a cumplir las obligaciones que le corresponden, bajo sancion de quedar inhabilitado para contratar con el Estado en caso de incumplimiento

Sistema Integrado de Gestión Administrativa
Módulo de Logística
Versión 21.01.01.U1

ORDEN DE COMPRA - GUíA DE INTERNAMIENTO Nº 0000117

Nº Exp. SIAF : 0000001611

Dia	Mes	Año
27	02	2017

UNIDAD EJECUTORA : 001 INSTITUTO TECNOLOGICO DE LA PRODUCCION - ITP
NRO. IDENTIFICACIÓN : 000194

1. DATOS DEL PROVEEDOR	2. CONDICIONES GENERALES
Señor(es) : TECNOLOGIA Y CREATIVIDAD S.A.C.	**Nº Cuadro Adquisic:** 000124
Dirección : AV. REPUBLICA DE PANAMA NRO. 3563 DPTO. 101 LIMA - LIMA - SAN ISID	**Tipo de Proceso :** LP - Nº 0002-2016-ITP
/ / **CCI:** 00219300178188604616	**Nº Contrato :** 002-2017-ITP/SG/OA-A
RUC : 20518446372 **Teléfono :** **Fax :**	**Moneda :** S/ **T/C :**

Concepto : ADQUISICION DE EQUIPOS PARA EQUIPAMIENTO INTEGRAL DE SERVIDORES Y ALMACENAMIENTO EN RED PARA EL CENT

Vienen ... 1,299,990.00

Código	Cant.	Unid. Med.	Descripción	Precio Unitario S/	Precio Total S/
			5.2 KM CALLAO - CALLAO. FORMA DE PAGO: PAGO UNICO, LUEGO DE LA CONFORMIDAD DEL RESPONSABLE DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION. GARANTIA DE LOS BIENES: 03 AÑOS DE GARANTIA		
* * * * * * * * *			(UN MILLON DOSCIENTOS NOVENTA Y NUEVE MIL NOVECIENTOS NOVENTA Y 00/100 SOLES) * * * *	* * * * *	

AFECTACION PRESUPUESTAL

Meta/ Mnemónico	Cadena Funcional	FF/Rb	Clasif. Gasto	Monto	S/

TOTAL S/ 1,299,990.00

Exonerado	:	1,299,990.00
V. Venta	:	0.00
I.G.V.	:	0.00
Total	:	1,299,990.00

Facturar a nombre de : INSTITUTO TECNOLOGICO DE LA PRODUCCION - ITP
Dirección : AV. REPUBLICA DE PANAMA N° 3418 SAN ISIDRO - LIMA 3418 / SAN ISIDRO - LIMA - LIMA RUC : 20131369477
Agradecemos enviar los bienes a la siguiente dirección :
CARRETERA A VENTANILLA KM 5.2 / VENTANILLA - PROV. CALLAO - PROV.CONSTITUC.DEL

ELABORADO POR	ORDENACION DE LA COMPRA		CONFORMIDAD	
CACERES CAJAS, ROGER				CUENTAS X PAGAR S/ _____
	RESPONSABLE DE ADQUISICIONES	RESPONSABLE DE ABASTECIMIENTO Y SERV. AUXILIARES	RESPONSABLE DE ALMACEN	Fecha Dia Mes Año

NOTA IMPORTANTE :
- El Proveedor debe adjuntar a su Factura copia de la O/C atendida.
- Esta Orden es nula sin las firmas y sellos reglamentarios o autorizados.
- Nos reservamos el derecho de devolver la mercadería que no esté de acuerdo con las especificaciones técnicas.
- El Contratista (Proveedor) se obliga a cumplir las obligaciones que le corresponden, bajo sancion de quedar inhabilitado para contratar con el Estado en caso de incumplimiento