Tribunal Constitucional

PLAN DE CONTINUIDAD OPERATIVA

2024-2025

INDICE

DIRECCIÓN GENERAL DE ADMINISTRACIÓN V°B°

1. Información general

El Tribunal Constitucional es el órgano supremo de interpretación y control de la constitucionalidad. Es autónomo e independiente y se encuentra sometido sólo a la Constitución y a su Ley Orgánica, Ley 28301. Tiene como finalidad defender el principio de supremacía constitucional, cuidando que las leyes, los órganos del Estado y los particulares, no vulneren lo dispuesto en la Carta Magna. Es su misión "garantizar la supremacía constitucional y protección de los derechos fundamentales de las personas de manera oportuna y transparente."

La Sede Central del Tribunal Constitucional está ubicada Jr. Ancash 390 Cercado de Lima Perú en la histórica Casa de Pilatos. El Tribunal Constitucional.

El Tribunal Constitucional en el área de Lima Metropolitana y el Callao Constitucional cuenta con tres locales:

- Local 01: Jr. Ancash 390 Cercado de Lima, donde funciona la Oficina de Tramite Documentario y Archivo, la Oficina de Control Institucional, Despachos de los Magistrados y Sala de Audiencias.

- Local 02: Av. Arequipa 2720 San Isidro Lima donde funciona la Dirección General de Administración, Oficina de Servicios Generales, Oficina de Logística, Oficina de Contabilidad y Tesorería, Oficina de Tecnologías de la Información, Oficina de Gestión y Desarrollo Humano, Oficina de Planeamiento y Desarrollo, Oficina de Presupuesto, Oficina de Asesoría Jurídica, Gabinete de Asesores Jurisdiccionales, Oficina de Imagen Institucional, las oficinas administrativas del Centro de Estudios Constitucionales y la Alta Dirección.

- Local 03: Los Cedros 209 San Isidro Lima donde funciona principalmente la Biblioteca del Centro de Estudios Constitucionales, así como salas de lectura y aulas.

Asimismo, en el departamento de Arequipa cuenta con un local:

- Local 04: Calle Misti 102 Yanahuara Arequipa, en el que funcionan la oficina de atención al ciudadano, el Centro de Estudios Constitucionales y algunos ambientes para audiencias y reuniones del Pleno.

Las funciones asignadas al Tribunal Constitucional se enmarcan en la Ley 28301, Ley Orgánica del Tribunal Constitucional y su Reglamento Normativo aprobado con Resolución Administrativa 095-2004-P-TC.

En cuanto a su estructura organizacional, el Tribunal Constitucional está constituido de la siguiente manera:

ÓRGANOS DE ALTA DIRECCIÓN
- Pleno del Tribunal Constitucional
- Presidencia
- Secretaría General

ÓRGANO DE CONTROL INSTITUCIONAL
- Oficina de Control Institucional

ÓRGANO DE DEFENSA JURÍDICA
- Procuraduría Pública

ÓRGANOS DE ASESORAMIENTO
- Oficina de Planeamiento y Desarrollo

DIRECCIÓN GENERAL DE ADMINISTRACIÓN V°B°

- Oficina de Asesoría Jurídica
- Oficina de Presupuesto

ÓRGANOS DE APOYO

- Dirección General de Administración
- Oficina de Gestión y Desarrollo Humano
- Oficina de Contabilidad y Tesorería
- Oficina de Logística
- Oficina de Servicios Generales
- Oficina de Tecnologías de la Información
- Oficina de Imagen Institucional
- Oficina de Trámite Documentario y Archivo

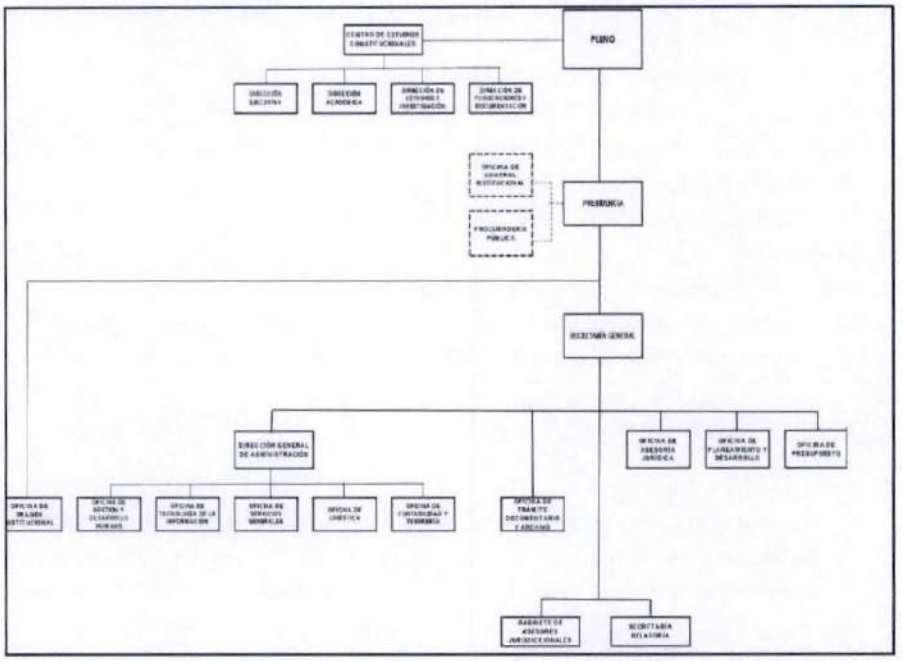
ÓRGANOS DE LÍNEA

- Gabinete de Asesores Jurisdiccionales
- Secretaría Relatoría

ÓRGANO ACADÉMICO Y DE INVESTIGACIÓN

- Centro de Estudios Constitucionales

Imagen 1: Organigrama del Tribunal Constitucional



De acuerdo a lo señalado Resolución Ministerial 320-2021-PCM, la gestión de la continuidad operativa del estado es el 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, pueda continuar brindando servicios necesarios a la población, ante la ocurrencia de un desastre o evento que produzca una interrupción prolongada de sus operaciones.

En ese sentido, el Plan de Continuidad Operativa del Tribunal Constitucional tiene como finalidad, garantizar que la entidad ejecute las actividades críticas del Tribunal Constitucional identificadas previamente, ante situaciones de desastres naturales o fenómenos inducidos o provocados que interrumpan las labores cotidianas. En consecuencia, este plan permitirá mediante un enfoque integral identificar posibles riesgos, así como sus consecuencias a fin de lograr estrategias de mitigación para la continuidad operativa del Tribunal Constitucional.

DIRECCIÓN GENERAL DE ADMINISTRACIÓN V°B°

Este plan es elaborado en el marco de la gestión de la continuidad operativa del Estado, tomando como referencia la Resolución Ministerial 320-2021-PCM la cual establece los procedimientos para la implementación de 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, con el fin de continuar funcionando ante un desastre o cualquier evento que interrumpa prolongadamente sus operaciones.

El desarrollo e implementación de la continuidad operativa requiere de un alto grado de compromiso institucional, voluntad de la alta dirección y responsabilidad de cada miembro del Tribunal Constitucional.

Asimismo, es necesario indicar que la ocurrencia de alguna de las amenazas consideradas en el presente Plan no tendrá un efecto directo en la población, debido a que las funciones podrán ser ejercidas de manera virtual mediante se ejecute las actividades críticas.

2. Base Legal

- Ley 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
- Decreto Supremo 048-2011-PCM que aprueba el Reglamento de la Ley 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGER), aprobado por el Decreto Supremo 048-2011-PCM.
- Resolución Ministerial 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".
- Ley 28301, Ley Orgánica del Tribunal Constitucional.
- Resolución Administrativa 095-2004-P/TC, que aprueba el Reglamento Normativo del Tribunal Constitucional y sus modificatorias.
- Resolución Administrativa 084-2023-P/TC, que aprueba el Reglamento de Organización y Funciones del Tribunal Constitucional y sus modificatorias.

3. Objetivos

3.1. Objetivo General

Asegurar la continuidad operativa del Tribunal Constitucional, ante la ocurrencia de un desastre natural o cualquier evento que interrumpa o produzca limitaciones e inestabilidad a su funcionamiento a través de la ejecución de las actividades criticas identificadas.

3.2. Objetivos Específicos

a. Identificar las actividades críticas que requieran ser ejecutadas de manera ininterrumpida.
b. Determinar los recursos humanos, materiales, equipos e infraestructura, así como los aplicativos informáticos necesarios para ejecutar las funciones críticas.

4. Identificación de riesgos y recursos

4.1. Matriz de riesgos

La matriz de riesgo que se presenta a continuación identifica los peligros y su nivel de impacto en las actividades críticas identificadas para el Tribunal Constitucional.Asimismo, se debe precisar que estas actividades identificadas tienen como escenario la sede de Lima Centro y la sede de San Isidro, como sede alterna.

4.2. Descripción de peligros identificados

- Sismo de gran magnitud: Los sismos son movimientos bruscos de la tierra originados por la liberación de energía acumulada durante un largo tiempo. Habitualmente estos movimientos son lentos e imperceptibles, pero en algunos el desplazamiento libera una gran cantidad de energía, cuando una de las placas se mueve bruscamente contra la otra, rompiéndola y originando el terremoto. El Perú se encuentra en el llamado Cinturón de Fuego del Pacífico, que concentra 90% de la actividad sísmica del planeta, por lo que la peligrosidad sísmica es "Alta".

  En lo que respecta a la ciudad de Lima, es la zona del país donde se ha acumulado la mayor cantidad de energía sísmica; de acuerdo con el Instituto Geofísico del Perú, se pronostica un movimiento telúrico de magnitud 8.8 Mw por el silencio sísmico desde el terremoto de 1746, cuando cerca del 10% de la población perdió la vida. Un terremoto de esta magnitud dejaría inmersa en un caos a Lima y Callao.

  Un evento de este tipo generará problemas en los servicios esenciales de suministro de energía, agua y saneamiento, además de los problemas de accesibilidad por las vías terrestres, asimismo se comprometería la estabilidad de las estructuras de los locales del Tribunal Constitucional, lo que significará complejidad para la continuidad de la prestación de servicios que brinda la entidad.

- Incendio: La ocurrencia de un incendio puede afectar las estructuras de las sedes y a los trabajadores por la exposición directa al fuego y calor, la inhalación, intoxicación y asfixia por humo o la muerte por aplastamiento o presión de las mismas personas atrapadas en los accesos y salidas de las edificaciones.

  Un incendio puede ocurrir tanto en el horario laboral o fuera de este debido al aumento de los espacios dedicados a oficinas, la instalación de equipos eléctricos, electrónicos, etc. Estar preparados para combatir un incendio, se vuelve un tema central; sobre todo con el objetivo de garantizar la seguridad de las personas y, en un segundo plano, resguardar la inversión en equipos, con el fin de reducir los tiempos requeridos para reiniciar las actividades.

- Ataque informático: También llamado ciberataque, es el intento de acceder a equipos informáticos o servidores mediante la introducción de virus o archivos malware, para alterar su funcionamiento, producir daños o sustraer información sensible. Ante este evento se puede paralizar parcial o totalmente el sistema por la pérdida o alteración de información institucional, poniendo en riesgo la seguridad y el desempeño de los ordenadores, lo que imposibilitaría la prestación de los servicios que brinda la entidad. El Tribunal Constitucional cuenta con diversos sistemas informáticos que dan soporte a las áreas jurisdiccionales y administrativas por lo que, ante un posible escenario de ataque informático, generaría impacto en la continuidad de las actividades.

4.3. Descripción de la infraestructura

- Local 01: Jr. Ancash 390 Cercado de Lima
  Sede central, local propio, con un área total de 5154.02 M2, área construida de 3372.15, cuenta con tres (3) niveles, con una antigüedad de la edificación mayor a 50 años. La edificación es de adobe, es considerada Patrimonio Cultural de la Nación.

- Local 02: Av. Arequipa 2720 San Isidro Lima
  Local propio con un área total de 18436.72 M2, área construida de 15583.53 y se ha afectado en uso al Banco de la Nación un área de terreno 172,81 m2 y un área construida de 943,86m2, cuenta con 12 niveles (8 pisos y sótanos), antigüedad entre 40 a 50 años. La edificación es de bloques de cemento.

- Local 03: Centro de Estudios Constitucionales (CEC) Los Cedros 209 San Isidro
  Local propio con un área total de 895.43 M2, área construida de 526.18 cuenta con 02 niveles, antigüedad mayor a 50 años. La edificación es de bloques de cemento.

- Local 04: Calle Misti 102 Yanahuara Arequipa
  Local propio con un área total de 1346.26 M2, área construida de 572.01 cuenta con 02 niveles, antigüedad mayor a 50 años.

4.4. Determinación del Riesgo

La evaluación de riesgos para el Tribunal Constitucional se basa en aquellos eventos que de ocurrir ocasionarían la interrupción de los servicios en forma total o parcial afectando la infraestructura, recursos y la vida humana sobre todo a las principales actividades que soportan el cumplimiento de los objetivos estratégicos institucionales de la institución, cuyos locales se encuentran dentro del ámbito de Lima Metropolitana.

Cuadro 01: Determinación del nivel de riesgo del TC

Peligros	Sede Central	Sede San Isidro	CEC
Sismo de gran magnitud y Tsunami en Lima y Callao	Muy alto	Alto	Alto
Incendio	Muy alto	Alto	Muy Alto
Ataque informático	Medio	Alto	Bajo

4.5. Determinación del Nivel de Impacto

Se estima el impacto que causaría la interrupción prolongada de las actividades críticas que soportan el cumplimiento de la misión del Tribunal Constitucional, estableciendo el período máximo tolerable de interrupción. En este sentido, se ha establecido un tiempo máximo de interrupción de acuerdo al tipo de riesgo.

Cuadro 02: Determinación del nivel de impacto

Riesgos	Periodo tolerable máximo de interrupción
Riesgo muy alto	10 días
Riesgo alto	4 días
Riesgo medio	12 horas

En el siguiente cuadro se observa la estimación del nivel de impacto que afectaría a la institución por sede relacionando el peligro con variables de operatividad determinados para el presente plan:

DIRECCIÓN GENERAL DE ADMINISTRACIÓN V°B°

Cuadro 03: Determinación del nivel de impacto por peligro por sede

N.°	SEDE	DIRECCIÓN	PELIGRO IDENTIFICADO	VARIABLE OPERATIVA
1	Local 01: Sede Central	Jr. Ancash 390 Cercado de Lima	Sismo de gran magnitud	Muy alto
			Incendio	Muy alto
			Ataque informático	Medio
2	Local 02: Sede San Isidro	Av. Arequipa 2720 San Isidro	Sismo de gran magnitud	Medio
			Incendio	Medio
			Ataque informático	Alto
3	Local 03: Centro de Estudios Constitucionales (CEC)	Ca. Los Cedros 209 San Isidro	Sismo de gran magnitud	Muy alto
			Incendio	Alto
			Ataque informático	Medio

4.6. Identificación de recursos

A continuación, se detallan los recursos con que cuenta el Tribunal Constitucional en sus sedes de Lima Metropolitana.

4.6.1. Determinación de los recursos humanos

Unidades orgánicas	DL 728 CAP	DL 1057 CAS	Practicantes
Pleno del Tribunal Constitucional	7		
Secretaría General	27	7	13
Oficina de Trámite Documentario y Archivo	6	7	
Oficina de Control Institucional		3	
Oficina de Procuraduría Pública	1		
Oficina de Planeamiento y Desarrollo	3		
Oficina de Asesoría Jurídica	1		1
Oficina de Presupuesto	3		
Dirección General de Administración	4		
Oficina de Gestión y Desarrollo Humano	9	8	2
Oficina de Contabilidad y Tesorería	5		
Oficina de Logística	5	4	
Oficina de Servicios Generales	15	4	
Oficina de Tecnologías de la Información	3	3	2
Gabinete de Asesores Jurisdiccionales	35	6	8
Secretaría Relatoría	18	11	1
Centro de Estudios Constitucionales	8	6	5
Oficina de Imagen Institucional	6	4	

En Anexo 6 se detalla la distribución del personal por sede del Tribunal Constitucional.

4.6.2. Determinación de los recursos informáticos e información crítica.

Se cuenta con los siguientes equipos relevantes para la continuidad operativa, los que están distribuidos en entre las sedes institucionales.

a. Equipos informáticos

Ítem	Equipos	Cantidad
1	Equipos de computo	141
2	Computadoras portátiles	48
3	UPS	8
4	Impresoras	134
5	Proyectores	9
6	Televisores	35
7	Discos duros	23
8	Switch de red	64
9	Videograbadora	1
10	Capturador de imágenes (escáner)	63

b. Aplicaciones e Información almacenada

La información producida por la entidad se encuentra almacenada en los servidores de la entidad. A continuación, se detallan los programas necesarios para el funcionamiento habitual del Tribunal Constitucional

Item	Programas/Aplicaciones	Tipo
1	Sistema integrado de Gestión de Expedientes (SIGE)	Institucional
2	Sistema de Gestión Documental (SGD)	Institucional
3	Sistema de Planillas (SISPER)	Institucional
4	Sistema para el Control de los libros de la Biblioteca del CEC (KOHA)	Institucional
5	Sistema mediante el cual los justiciables pueden ingresar escritos a los expedientes (Ventanilla Jurisdiccional)	Institucional
6	Jurisprudencia Sistematizada	Institucional
7	Ventanilla Administrativa	Institucional
8	Página Web Institucional	Institucional
9	Sistema Integrado de Gestión Administrativa (SIGA)	Gubernamental
10	Sistema Integrado de Administración Financiera	Gubernamental
11	Sistema Integrado de Administrativo y Jurisdiccional	Gubernamental
12	Office	Comercial
13	Acceso a Internet y Seguridad perimetral de red	Comercial
14	Alojamiento en la nube	Comercial

4.6.3. Determinación de los recursos físicos críticos

A continuación, se detalla equipamiento (mobiliario) que se encuentra en las sedes del Tribunal Constitucional, en Lima Metropolitana. Asimismo, en el Anexo 5, se detalla el listado total de bienes que se encuentra por sede.

Ítem	Equipos	Cantidad
1	Archivador de madera/melamina/metal	35
2	Armario de madera/ melamina	175
3	Carro de metal transportador plegable con plataforma de metal	8
4	Carpeta de metal unipersonal	120
5	Credenza de madera / melamina	11
6	Escritorio de madera / melamina	183

DIRECCIÓN GENERAL DE ADMINISTRACIÓN V°B°

7	Estante archivador de madera melamina/metal	81
8	Módulo de madera/melamina /metal	167
9	Silla fija de madera/metal	366
10	Silla giratoria de metal	392
11	Sillón giratorio de metal	91

5. Acciones para la Continuidad Operativa

5.1. Determinación de las Actividades Críticas

Se han identificado cuatro actividades críticas por el Tribunal Constitucional ligadas a los productos que desarrolla la Institución. A continuación se detalla las unidades orgánicas que van a participar por cada actividad.

Actividades críticas	Áreas que las desarrollan
Atención al usuario (ingreso de expedientes y otros documentos), ya sea de manera presencial o virtual	Oficina de Trámite Documentario y Archivos (OTDA)
Recepción, registro, digitalización, archivo y distribución de expedientes digitalizados a las distintas comisiones ordinarias.	Oficina de Trámite Documentario y Archivos (OTDA)
Elaboración de proyectos de ponencia	Gabinete de Asesores
Programación y realización de vistas de causa y audiencias	Secretaria de Relatoría
Revisión de proyectos y distribución de los mismos a despachos de magistrados, para su aprobación y firma	Secretaria de Relatoría
Firma de resoluciones	Pleno
Publicación de Resoluciones	Secretaria de Relatoría
Devolución y archivo de cuadernillos.	Oficina de Trámite Documentario y Archivos (OTDA)

5.2. Aseguramiento del acervo documentario

Tomando en cuenta que una de las actividades críticas del Tribunal Constitucional es la gestión de la documentación recibida a través de la mesa de partes a cargo de la Oficina de Trámite Documentario y Archivo (OTDA), se deben establecer procedimientos con la finalidad de organizar, almacenar y controlar el contenido físico y digital del archivo documentario.

La unidad orgánica responsable del acervo documentario de actividades jurisdiccionales del Tribunal Constitucional es la OTDA; en cuanto a la documentación administrativa, cada oficina es responsable del manejo, custodia y almacenamiento.

En este sentido, para el aseguramiento del acervo documentario se deberá realizar las siguientes actividades:

- La OTDA, como archivo central del Tribunal Constitucional debe elaborar un plan de trabajo para el empaquetamiento, codificación y digitalización en medios magnéticos de los expedientes, sentencias, etc.
- Se debe coordinar con la Oficina de Tecnologías de la Información (OTI) mantener un dispositivo de almacenamiento en la "nube" a modo de back up de los medios magnéticos.

DIRECCIÓN GENERAL DE ADMINISTRACIÓN V°B°

- Las unidades orgánicas administrativas tienen la responsabilidad de digitalizar la documentación generada, manteniendo copias de seguridad través del sistema de gestión documentario (SGD).

5.3. Aseguramiento de la base de datos mediante la ejecución del Plan de recuperación de los servidores informáticos

Para el desarrollo y ejecución de las funciones críticas identificadas es necesario que la Oficina de Tecnologías de la Información cuente con mecanismos que inhiban posibles ciberataques, así como mantener activa y actualizada la base de datos del Tribunal Constitucional.

Al respecto, el Tribunal Constitucional cuenta con un FIREWALL y un Web Aplicación Firewall (WAF) cuyo objetivo es proteger de múltiples ataques al servidor de aplicaciones web en el backend, siendo la principal función del WAF garantizar la seguridad del servidor web mediante el análisis de paquetes de petición HTTP / HTTPS y modelos de tráfico.

En este sentido, la Oficina de Tecnologías de la Información se basará en la Norma Técnica Peruana NTP-ISO/IEC 27001-2014: Tecnología de la información técnicas de seguridad, sistemas de gestión de seguridad de la información, para la ejecución de su Plan de recuperación de los servicios informáticos, adjunto en el Anexo 1.

5.4. Roles y Responsables para el desarrollo de las actividades criticas

De conformidad con lo establecido en la Resolución Ministerial 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", para la gestión de la continuidad operativa se encuentran involucrados las siguientes instancias:

- Unidad a cargo de la gestión de la continuidad operativa

  La Dirección General de Administración es la encargada de implementar en la entidad el proceso de la gestión de la continuidad, tiene entre sus funciones;
  - Remitir el Plan de Continuidad al Titular de la entidad para su aprobación.
  - Mantener actualizada la documentación de las actividades desarrolladas como para de la continuidad operativa
  - Difundir el Plan de Continuidad Operativa en la entidad
  - Coordinar y ejecutar las simulaciones para el funcionamiento del Plan de Continuidad Operativa.

- Grupo de comando para la Continuidad Operativa (GCCO)
  Es el conjunto de profesionales que se encarga de la elaboración del Plan de Continuidad Operativa de la entidad el cual ha sido designado mediante Resolución Administrativa 054 -2024P/TC, constando de los siguientes miembros:

Integrantes Del Grupo De Comando	Órgano / Unidad Orgánica
Un (01) representante de las unidades orgánicas que apoyan directamente el desarrollo de las actividades identificadas como críticas.	Oficina de Planeamiento y Desarrollo.
Un (01) representante de la unidad orgánica de tecnologías de la información y comunicaciones	Oficina de Tecnologías de la Información.
Un (01) representante de la unidad orgánica de	Oficina de Tecnologías de

tecnología de la información y comunicaciones.	la Información.
Un (01) representante de la unidad orgánica a cargo de la Gestión de la Continuidad Operativa.	Dirección General de Administración.
Un (01) representante de la unidad orgánica de Servicios Generales.	Oficina de Servicios Generales.
Un (01) representante de la unidad orgánica de Servicios Generales.	Oficina de Servicios Generales.
Un (01) representante de la unidad orgánica de Servicios Generales.	Oficina de Servicios Generales.
Un (01) representante de la unidad orgánica de recursos humanos.	Oficina de Gestión y Desarrollo Humano.
Un (01) representante de la unidad orgánica cuya actividad ha sido identificada como crítica.	Oficina de Trámite Documentario y Archivo.
Un (01) representante de la unidad orgánica cuya actividad ha sido identificada como crítica.	Oficina de Trámite Documentario y Archivo.

- Representante de la unidad orgánica a cargo de la Gestión de la Continuidad Operativa
  - Gestionar la difusión del Plan de Continuidad Operativa y su publicación en la sede digital de la entidad.
  - Mantener actualizada la documentación de las actividades desarrolladas como para de la continuidad operativa.
  - Difundir el Plan de Continuidad Operativa en la entidad.
  - Coordinar y ejecutar las simulaciones para el funcionamiento del Plan de Continuidad Operativa.

- Representantes de la unidad orgánica de servicios generales:
  - Consolidar la información de daños ocasionados por el evento crítico para ser transmitida.
  - Advertir los riesgos que afecten la continuidad en la prestación del servicio critico dentro de sus funciones.
  - Disponer con el apoyo de la Oficina de Servicios Generales cuente con lineamientos de seguridad en las zonas afectadas.
  - Coordinar el traslado de los recursos esenciales para la continuidad operativa.
  - Gestionar, trasladar y verificar que se brinde la seguridad a las operaciones de continuidad en la sede alterna.

- Representante de la unidad orgánica de gestión de recursos humanos:
  - Coordinar con la jefatura de gestión de recursos humanos mantener actualizada el listado de personal del Tribunal Constitucional.
  - Coordinar con la asistenta social los servicios sociales.
  - Evaluar y gestionar la cantidad de personal necesario para la ejecución del Plan de Continuidad Operativa conforme a sus competencias.
  - Gestionar los recursos humanos del Tribunal Constitucional.

- Representante de la unidad orgánica de tecnología de la información y comunicaciones:
  - Identificar la infraestructura tecnológica necesaria para continuar con las actividades criticas contando con la disponibilidad de información y aplicativos informáticos.
  - Ejecutar el plan de recuperación de servicios informáticos.
  - Apoyar las necesidades de soporte técnico de los usuarios.

- Representante de la unidad orgánica de identificada como crítica:

DIRECCIÓN GENERAL DE ADMINISTRACIÓN V°B°

- Identificar la cantidad de personal necesario para la ejecución de las actividades críticas.
- Asegurar el equipo y material necesario para apoyar la ejecución de las actividades críticas.

- Representante de la unidad orgánica que apoyan directamente el desarrollo de las actividades identificadas como críticas:
  - Evaluar y gestionar la cantidad de personal necesario para el apoyo a la ejecución de las actividades críticas de su competencia.
  - Asegurar el equipo y material necesario para apoyar la ejecución de las actividades críticas.

5.5. Requerimientos

La Dirección General de Administración, a través de las oficinas de gestión y desarrollo humano, servicios generales, oficina de logística y la de tecnologías de la información, son los encargados de centralizar y abastecer los requerimientos de personal, informáticos, bienes y equipos necesarios para la continuidad operativa ante la ocurrencia de eventos que interrumpan el normal funcionamiento de las actividades críticas de la institución.

Para el análisis se evaluará a las actividades críticas a desarrollarse en la sede central y los requerimientos mínimos necesarios para la continuidad operativa.

5.5.1. Requerimientos de Personal

Actividades críticas	Requerimiento de personal
Atención al usuario	2
Recepción, registro, digitalización, archivo y distribución de expedientes digitalizados a las distintas comisiones ordinarias.	6
Elaboración de proyectos de ponencia	30
Programación y realización de vistas de causa y audiencias	15
Revisión de proyectos y distribución de los mismos a despachos de magistrados, para su aprobación y firma	15
Firma de resoluciones	35
Publicación de Resoluciones	15
Devolución y archivo de cuadernillos	3
Total	121

5.5.2. Requerimientos de Material y Equipo

Actividades críticas	Equipamiento y materiales			
	Radio	Escritorio	Silla	Celular
Atención al usuario	1	2	2	1

DIRECCIÓN GENERAL DE ADMINISTRACIÓN V°B°

Recepción, registro, digitalización, archivo y distribución de expedientes digitalizados a las distintas comisiones ordinarias.		6	6	2
Elaboración de proyectos de ponencia	1	30	30	3
Programación y realización de vistas de causa y audiencias	1	7	7	2
Revisión de proyectos y distribución de los mismos a despachos de magistrados, para su aprobación y firma	0	7	7	1
Firma de resoluciones	2	14	14	3
Publicación de Resoluciones	0	1	1	1
Devolución y archivo de cuadernillos	1	3	3	1
Total	6	70	70	14

Para el desarrollo de las actividades críticas se necesitan los siguientes recursos mínimos:

Tipo de recurso	Descripción
Recursos físicos críticos	Buscar en la sede alterna un depósito para los recursos informáticos
Recursos logísticos	Escritorios, estantes, mesas, sillas, luces de emergencia, linternas de mano, útiles de escritoriobásicos
	Materiales de limpieza y desinfección

5.5.3. Requerimiento de Recursos Informáticos

Actividades críticas	Recursos informáticos		
	Computadora	Impresora multifuncional	Escáner
Atención al usuario	2	0	1
Recepción, registro, digitalización, archivo y distribución de expedientes digitalizados a las distintas comisiones ordinarias.	6	3	4
Elaboración de proyectos de ponencia	30	1	1
Programación y realización de vistas de causa y audiencias	7	2	1
Revisión de proyectos y distribución de los mismos a despachos de magistrados, para su aprobación y firma	7	1	1
Firma de resoluciones	35	1	1
Publicación de Resoluciones	1	0	1

DIRECCIÓN GENERAL DE ADMINISTRACIÓN V°B°

Devolución y archivo de cuadernillos	3	3	0
Total	91	10	10

5.5.4. Requerimiento Presupuestal

La Oficina de Presupuesto trabaja con la Alta Dirección para realizar las modificaciones presupuestarias necesarias para atender la gestión del riesgo de desastres de acuerdo a lo establecido en el Plan de Continuidad Operativa. Asimismo, se solicitará incluir la gestión de continuidad operativa dentro del proceso de planificación y disponer un presupuesto para estas actividades.

5.6. Determinación de la Sede Alterna de Trabajo

Con la finalidad de garantizar la ejecución del presente plan con el menor tiempo de interrupción de las operaciones que brinda la entidad, es necesario identificar con anticipación por lo menos una eventual sede donde se desplazarían las áreas que actualmente funcionan en la Sede Central en Cercado de Lima para seguir con sus procesos críticos. Al respecto, se ha considerado como sede alterna, la sede San Isidro sito Av. Arequipa 2720 San Isidro.

Esto implica realizar las coordinaciones necesarias para que la sede alterna cuente con los recursos necesarios para la continuidad operativa como áreas para el desarrollo de actividades críticas, acceso a la información contenida en las bases de datos, así como medicamentos y equipos de protección personal.

Activación del Plan de Continuidad Operativa.

La activación del Plan de Continuidad Operativa inicia una vez ocurrido el evento desencadenante.

El presidente del GCCO y el Titular de la entidad o su alterno, en su ausencia, determina la activación del plan de continuidad operativa.

El presidente del GCCO evaluará la magnitud del evento y la situación de operatividad de la sede central (Av. Ancash 390) y decidirá, con la información disponible, si se requiere el traslado a la sede alterna. El desplazamiento será identificando las unidades orgánicas que deberán ser trasladadas, con el personal priorizado y el equipamiento mínimo identificado.

Se activa el procedimiento para la comunicación y convocatoria de personal señalado en el Anexo 2.

5.7. Activación y desactivación de la sede alterna

Las acciones a seguir serán determinadas por la naturaleza del impacto de cada amenaza (sismo, incendio, ataque informático). Sin embargo, las acciones que se deben gestionar se dividen en cuatro (4) fases:

5.7.1. Primera Fase: Fase Inicial

Esta fase inicia con el acopio y reporte de la información inicial de los daños ocasionados por la amenaza. Para tal fin, el GCCO recaba información y reporta el impacto del daño generado, así como la situación operativa de la Sede Central, para lo cual coordinará con el proveedor del servicio de seguridad que opera en dicha sede, a fin de que reporte a la brevedad, lo pertinente.

El tiempo máximo de duración de esta fase no debe superar las cinco (5) horas, tomando en

consideración que esta fase es la que brindará los insumos para la decisión de activación del Plan de Continuidad Operativa (fase de ejecución).

5.7.2. Segunda Fase: Fase de ejecución

Esta fase se inicia con la activación del Plan de Continuidad Operativa propiamente dicha, y su principal función es la gestión de la crisis. Cuenta con cuatro momentos:

- Primer Momento: Activación de Plan de Continuidad Operativa:
  El presidente del GCCO del Tribunal Constitucional o su alterno en su ausencia, determina la activación del Plan de Continuidad Operativa, tomando como referencia el reporte obtenido en la fase de alerta y determinará con la información disponible la necesidad de traslado a la sede alterna.

  El presidente del GCCO-TC dispone el inicio del traslado considerando el equipamiento mínimo identificado y personal priorizado. Asimismo, cada órgano y unidades orgánicas consideradas en el presente plan deben activar los procedimientos de convocatoria de su personal.

- Segundo Momento: Acondicionamiento y puesta en operaciones de la sede alterna
  Tomada la decisión, se debe realizar las coordinaciones y acciones con la sede alterna, para que de inmediato se entreguen los ambientes y equipamiento necesario para la continuidad operativa del Tribunal Constitucional. Cabe señalar que los ambientes y equipos deben haber sido identificados con anterioridad, en previsión de la probabilidad de que ocurra el evento.

  La Oficina de Servicios Generales es la responsable de conducir el proceso para el traslado a la sede alterna elegida, bajo la supervisión de la Dirección General de Administración; asimismo se verificará la conectividad y sistemas de comunicación con el apoyo de la Oficina de Tecnologías de la Información.

  La Oficina de Gestión y Desarrollo Humano se encargará de realizar el censo de personal institucional, y de ser necesario realizará el acompañamiento emocional a los trabajadores que por el impacto de la amenaza tenga deudos.

- Tercer momento: Inicio de operaciones en la sede alterna
  Obtenida la confirmación de que la sede alterna se encuentra en condiciones de iniciar operaciones, acondicionada con el equipamiento y servicios mínimos indispensables que aseguren las comunicaciones y las operaciones, así como la seguridad y salud del personal, el personal priorizado y designado se desplazará a dicha instalación lo antes posible.

  Las operaciones se deben dar inicio en el menor tiempo posible, no excediendo las cuarenta y ocho (48) horas de producido el evento.

- Cuarto momento: indicaciones para el personal que no se desplaza a la sede alterna.

  En cuanto al personal que no fue designado como prioritario para el desplazamiento a la sede alterna, es necesario contar con información actualizada de su ubicación, asistencia y permanencia, ya que podría ser llamado a integrar los equipos de trabajo, ante cualquier eventualidad. La Oficina de Gestión y Desarrollo Humano es la encargada de avisar de la convocatoria.

  La Dirección General de Administración y la Oficina de Imagen Institucional, previa

DIRECCIÓN GENERAL DE ADMINISTRACIÓN V°B°

autorización de la Alta Dirección, es la encargada de establecer las comunicaciones con otros organismos que conduzcan operaciones de gestión de riesgos de desastres como son el Ministerio de Defensa, InstitutoNacional de Defensa Civil, CENEPRED y Centro de Operaciones de Emergencia Nacional (COEN).

5.7.3. Tercera fase: Desactivación

El Presidente del GCCO del TC decidirá la culminación de la ejecución del Plan de Continuidad Operativa y, por ende, el retorno a la ejecución de sus actividades previas a la ocurrencia del evento que activó el Plan de continuidad operativa; optimizando los procesos estratégicos, misionales y de apoyo.

6. Desarrollo de las actividades criticas

Con el fin de asegurar el desarrollo de las actividades críticas, el Grupo de Comando debe realizar el seguimiento y monitoreo correspondiente, para tal efecto deberá utilizar la matriz de Seguimiento y Monitoreo de la ejecución de las Actividades Críticas del Plan de Continuidad Operativa establecida en el Anexo 4 de la R.M. 320-2021-PCM del 30.12.2021, según detalle:

Actividad crítica	Responsables	Actividades desarrolladas	Personal asignado	Material asignado	Equipo Asignado	Presupuesto asignado	Fecha de actualización	Observaciones
N°1 Atención al usuario	OTDA/OSG	a)...						
		b)...						
		c)...						
N°2 Recepción, registro, digitalización, archivo y distribución de expedientes digitalizados a las distintas comisiones ordinarias.		a)...						
		b)...						
		c)...						
N°8 Devolución y archivo de cuadernillos		a)...						
		b)...						
		c)...						
N° 3 Elaboración de proyectos de ponencia	Gabinete de Asesores Jurisdiccionales	a)...						
		b)...						
		c)...						
N° 4 Programación y realización de vistas de causa y audiencias	Secretaría Relatoría	a)...						
		b)...						
		c)...						
N° 5 Revisión de proyectos y distribución de los mismos a despachos de magistrados, para su aprobación y firma.		a)...						
		b)...						
		c)...						
N° 7 Publicación de Resoluciones		a)...						
		b)...						
		c)...						
N° 6 Firma de resoluciones	Secretaria Relatoría y Pleno	a)...						
		b)...						
		c)...						

7. Cronograma de Ejercicios del Plan de Continuidad Operativa

Para que el personal institucional de los órganos y unidades orgánicas de la institución tengan conocimiento de la operatividad del plan de continuidad operativa, la Dirección General de Administración ha previsto desarrollar simulacros o ensayos ante situación de desastre natural o cualquier evento que interrumpa nuestras operaciones, las cuales son programadas de acuerdo al cronograma siguiente:

DIRECCIÓN GENERAL DE ADMINISTRACIÓN V°B°

N.°	FECHA	SUPUESTO	RESPONSABLE
1	4ta semana de mayo 2024	Sismo de gran magnitud afectó a la sede central.	GCCO
2	1era semana de agosto 2024	Ataque informático.	GCCO
3	2da semana de noviembre 2024	Incendio afecto a la sede central	GCCO
4	4ta semana de mayo2025	Sismo de gran magnitud afectó totalmente a la sede central.	GCCO
5	1era semana de agosto 2025	Ataque informático.	GCCO
6	2da semana de noviembre 2025	Incendio afecto a la sede central	GCCO

8. Anexos

Anexo 1: Plan de recuperación de los servicios informáticos

Anexo 2: Procedimiento para la comunicación y convocatoria del personal involucrado en la ejecución de las actividades críticas.

Anexo 3: Sistema de comunicaciones de emergencia

Anexo 4: Cronograma de la Gestión de la Continuidad Operativa

Anexo 5: Caso especial ante una epidemia -pandemia

Anexo 6: Listado de recursos por sede

Anexo 7: Listado de personal

Anexo 1: PLAN DE RECUPERACIÓN DE LOS SERVICIOS INFORMÁTICOS

2024

Índice

1. OBJETIVOS

1.1 Objetivo general

Contar con un Plan de recuperación organizado, viable y ágil que permita reestablecer los Servicios Informáticos ofrecidos por la Oficina de Tecnologías de la Información los alojados localmente, así como aquellos que se encuentran en la nube, ante un evento crítico que cause la indisponibilidad por tiempo prolongado de dichos servicios.

1.2 Objetivos específicos

- Identificar la estructura organizacional necesaria para restaurar las operaciones en el Tribunal Constitucional.
- Definir acciones y procedimientos necesarios para recuperar las operaciones y los servicios de TI en los plazos definidos.
- Familiarizar al equipo de recuperación con pruebas periódicas y en escenarios cercanos a la realidad.

2. ALCANCE

La implementación del Plan de Recuperación de los Servicios Informáticos del Tribunal Constitucional (en adelante, TC) abarca todos los sistemas de información que alojan los servidores, las instalaciones tecnológicas, equipos, personal y servicios ofrecidos por terceros, los mismos que son gestionados por la Oficina de Tecnologías de la Información (en adelante OTI), ubicado em la Av. Arequipa N° 2720 San Isidro - Lima - Lima – Sede Central, y su vigencia está sujeta a los cambios tecnológicos, de equipamiento y de los sistemas de información relacionados al TC, según informe la OTI.

Si bien el concepto de Servicios informáticos, también conocidos como servicios de tecnología de la información (TI), abarca una amplia gama de actividades y recursos que se utilizan para gestionar, mantener y optimizar sistemas y tecnologías de información en una organización. En el contexto de este Plan, este concepto se referirá a la "*Determinación de los recursos informáticos e información crítica*"[1] que permitirán restaurar los Servicios Ofrecidos por la Oficina de TI, que permitan la continuidad operativa del Tribunal Constitucional.

Los Servicios informáticos que ofrece la OTI pueden clasificarse en dos grupos:

a) Servicios ofrecidos y administrados por la OTI

Entre estos podemos encontrar

- Soporte técnico: Asistencia técnica para usuarios finales y empleados de una organización en relación con problemas de hardware, software, redes y otros aspectos de TI.
- Mantenimiento de sistemas: Actualizaciones, parches y mantenimiento preventivo de sistemas informáticos para garantizar su funcionamiento eficiente y seguro.

[1] Literal b.2 del numeral del Numeral 5.2.1 Identificación de Riesgos y Recursos de la R.M. 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",

- Gestión de redes: Configuración, monitoreo y administración de redes informáticas para garantizar la conectividad, seguridad y rendimiento óptimo.
- Seguridad informática interna: Implementación y gestión de medidas de seguridad para proteger los sistemas, datos y redes de una organización contra amenazas cibernéticas como virus, malware, piratería informática y accesos no autorizados.
- Administración de bases de datos: Gestión de bases de datos, incluyendo diseño, implementación, mantenimiento y optimización de bases de datos para garantizar la integridad, disponibilidad y seguridad de la información almacenada.
- Desarrollo y mantenimiento de software: Creación, personalización, actualización y mantenimiento de aplicaciones informáticas y sistemas de software para satisfacer las necesidades específicas de una organización.
- Virtualización: Implementación y gestión de tecnologías de virtualización para optimizar el uso de recursos informáticos, reducir costos y mejorar la flexibilidad y escalabilidad de la infraestructura de TI.

b) Servicios ofrecidos por terceros y administrados por la OTI
- Computación en la nube: Provisionamiento, administración y optimización de recursos de computación en la nube, incluyendo almacenamiento, procesamiento y aplicaciones alojadas en la nube. Este servicio también incluye servicios de seguridad del ambiente en dicho espacio
- Provisión del Acceso a Internet: Aprovisionamiento del servicio de acceso a Internet, incluyendo la seguridad perimetral (Firewall) para todos los equipos que se conecten mediante el acceso provisto por el proveedor.
- Herramientas colaborativas en la nube: Servicio, también, en la nube que provee un conjunto de herramientas para el trabajo diario, como el correo electrónico, espacio de almacenamiento (Drive), chat en línea, reuniones virtuales, hoja de cálculo, presentador gráfico, diseñador de formularios etc,

3. BASE LEGAL

La normatividad legal que sustenta el presente plan es la siguiente:

- Ley N° 28716, Ley de Control Interno de las Entidades del Estado.
- Ley N° 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres - SINAGERD.
- Decreto Supremo N° 038-2021-PCM, que aprueba la Política Nacional de Gestión del Riesgo de Desastres al 2050.
- Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital.
- Decreto Supremo N° 034-2014-PCM que aprueba el Plan Nacional de Gestión del Riesgo de Desastres – PLANAGERD 2014-2021.
- Decreto Supremo N° 118-2018-PCM, que declara de interés nacional el desarrollo del Gobierno Digital, la innovación y la economía digital con enfoque territorial.
- 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 Ministerial N° 004-2016-PCM, modificada por Resolución Ministerial 166-2017-PCM, que aprueba 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. 2da Edición", en todas las entidades integrantes del Sistema nacional de Informática.

- Resolución de Contraloría N° 320-2006-CG, que aprueba las Normas de Control Interno.
- Resolución de Contraloría N° 146-2019-CG, que aprueba la Directiva N° 006-2019-CG-INTEG "Implementación del Sistema de Control Interno en las Entidades del Estado".

4. RESPONSABILIDADES

La OTI tiene entre sus funciones "*Elaborar, ejecutar y evaluar el plan estratégico informático, el plan de seguridad informática y* ***el plan de contingencia tecnológica,*** *de acuerdo a los lineamientos y normas establecidos por su ente rector, elevándolos para su aprobación*".[2]

En razón a ello es responsabilidad de la OTI las actividades la elaboración de planea para afrontar situaciones que pongan en riesgo la continuidad operativa institucional. En dicho contexto, la OTI entiende que se debe formar un Equipo de Recuperación el cual debe estar integrado, principalmente, por especialistas, analistas y técnicos de TI de la Institución, que se encarguen de ejecutar actividades, de manera preventiva y correctiva del esquema y estrategia de recuperación. Los miembros que conformen el Equipo de Recuperación deberán toman acciones y decisiones dependiendo de la situación que se suscite; dichas acciones están direccionadas a recuperar y restablecer las operaciones de los servicios brindados por la OTI.

Asimismo, se encargarán de llevar a cabo actividades permanentes con la finalidad de asegurar y cumplir con los tiempos de recuperación de los servicios de TI que la institución requiere ante un incidente severo.

El jefe de la Oficina de Tecnologías de la Información (OTI) del Tribunal Constitucional será responsable de liderar el equipo de recuperación de los Sistemas Informáticos para la continuidad operativa; no obstante, debe organizar los distintos equipos para que trabajen de manera articulada con el objetivo de minimizar el impacto de los daños ante una situación indeseada y lograr mantener la continuidad operativa.

5. DEFINICIONES

- **Amenaza (ISO/IEC 27000 – 2014)**

  Causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización

- **Plan de recuperación de desastre de TIC (ISO/IEC 27031 – 2015)**

  Un plan claramente definido y documentado que recupera las capacidades de TIC cuando ocurre una interrupción

- **Recuperación de desastre de TIC (ISO/IEC 27031 – 2015)**

  La capacidad de los elementos de TIC de una organización para apoyar a sus funciones críticas de negocio a un nivel aceptable dentro de un periodo predeterminado de tiempo después de una interrupción

- **Adecuación de TIC para la continuidad del negocio (ISO/IEC 27031 – 2015)**

[2] Literal c del Artículo 38 del Reglamento de Organización y Funciones del TC aprobado mediante R.A. 083-2023-TC/P

La capacidad de una organización para apoyar a sus operaciones de negocio mediante la prevención, detección y la respuesta a una interrupción y la recuperación de los servicios de TIC

- **Continuidad de negocio (ISO/IEC 22300 – 2018)**

  Capacidad de una organización para continuar la entrega de productos o servicios a un nivel aceptable.

  niveles predefinidos después de una interrupción

- **Plan de continuidad de negocio (ISO/IEC 22300 – 2018)**

  Los procedimientos documentados que guían a las organizaciones a responder, recuperar, reanudar, restaurar hasta un nivel predefinido de operación luego de la interrupción

  NOTA Típicamente esto cubre a los recursos, los servicios y las actividades requeridas para asegurar la continuidad de funciones críticas del negocio.

- **Gestión de continuidad del negocio (ISO/IEC 22300 – 2018)**

  Proceso holístico de gestión que identifica amenazas potenciales para una organización y los impactos que dichas amenazas podrían causar en las operaciones del negocio, si estas se produjesen, lo que proporciona un marco de referencia para construir una resistencia organizacional con la capacidad de una respuesta eficaz que salvaguarda los intereses de sus partes relacionadas claves, la reputación, la marca y actividades de creación de valor

- **Riesgo (ISO/IEC 27000 – 2014)**
  Efecto de la incertidumbre sobre la consecución de los objetivos.
  NOTA 1: Un efecto es una desviación, positiva y/o negativa, respecto a lo previsto.
  NOTA 2: Los objetivos pueden tener diferentes aspectos (tales como financieros, de salud y seguridad, o ambientales) y se pueden aplicar a diferentes niveles (tales como, nivel estratégico, nivel de un proyecto, de un producto, de un proceso o de una organización completa).
  NOTA 3: Con frecuencia, el riesgo se caracteriza por referencia a sucesos potenciales y a sus consecuencias, o a una combinación de ambos.
  NOTA 4: Con frecuencia, el riesgo se expresa en términos de combinación de las consecuencias de un suceso (incluyendo los cambios en las circunstancias) y de su probabilidad.
  NOTA 5: La incertidumbre es el estado, incluso parcial, de deficiencia en la información relativa a la comprensión o al conocimiento de un suceso, de sus consecuencias o de su probabilidad.
- **Control (ISO/IEC 27000 – 2014)**
  Medida que modifica un riesgo.
  Nota 1: Los controles incluyen cualquier proceso, a política, dispositivo, práctica, u otras opciones que modifiquen un riesgo.
  Nota 2: Los controles no siempre puede) proporcionar el efecto de modificación previsto o asumido.
- **Objetivo de Control (ISO/IEC 27000 – 2014)**
  Declaración que describen lo que se quiere lograr como resultado de la implementación de los controles.
- **Consecuencia (ISO/IEC 27000 – 2014)**
  Resultado de un evento que afecta a los objetivos.
  Nota 1: Un evento puede conducir a una serie de consecuencias.

Nota 2: Una consecuencia puede ser cierta o incierta, y puede tener efectos positivos o negativos sobre la consecución de los objetivos.
Nota 3: Las consecuencias pueden ser expresadas cualitativa o cuantitativamente.
Nota 4: Las consecuencias inicio les pueden convertirse en reacciones en cadena.

- **Desastre (ISO/IEC 22300 – 2018)**

  Situación en la que se han producido pérdidas humanas, materiales, económicas o ambientales generalizadas que superó la capacidad de la organización afectada, comunidad o sociedad para responder y recuperar con recursos propios.

- **Evento/ Suceso (ISO/IEC 27000 – 2014)**
  Ocurrencia o cambio de un conjunto particular de circunstancias.
  Nota 1: Un evento puede ser una o más ocurrencias, y puede tener varias causas.
  Note 2: Un evento puede consistir en algo que no sucede.
  Nota 3: Un evento a veces puede ser referido como un "incidente " o "accidente".
- **Aceptación de riesgos (ISO/IEC 27000 – 2014)**
  Decisión informada para tomar un riesgo en particular.
  Nota 1: la aceptación del riesgo puede ocurrir sin el tratamiento del riesgo (2,79) o durante el proceso de tratamiento de riesgos.
  Nota 2: riesgos aceptados están sujetos a supervisión y revisión.
- **Nivel de riesgo (ISO/IEC 27000 – 2014)**

  Magnitud de un riesgo, expresados en términos de la combinación de las consecuencias y de su probabilidad.

- **Probabilidad (ISO/IEC 27000 – 2014)**

  Posibilidad de que algún hecho se produzca

- **Análisis de riesgo (ISO/IEC 27000 – 2014)**
  Proceso de comprender la naturaleza del riesgo y determinar el nivel de riesgo.
  Nota 1: El análisis de riesgos proporciona las bases para la evaluación del riesgo y pare tomar las decisiones sabre el tratamiento del riesgo.
  Nota 2: El análisis de riesgo incluye la estimación del riesgo.
- **Interrupción (ISO/IEC 27031 – 2015)**
  Incidente, ya sea anticipado o no, que causa una desviación negativa no planificada de la entrega esperada de productos y servicios de acuerdo con los objetivos de una organización
- **Evaluación del riesgo (ISO/IEC 27000 – 2014)**

  Proceso general de la identificación del riesgo, el análisis de riesgo y la evaluación del riesgo.

- **Vulnerabilidad (ISO/IEC 27000 – 2014)**

  Debilidad de un activo o de control que puede ser explotado par una o más amenazas

- **RPO: Recovery Point Objective (ISO/IEC 27031 – 2015)**

  Un punto en el tiempo hasta el cual todos los datos tienen que ser recuperados después de que haya ocurrido una interrupción

- **RTO: Recovery Time Objective (ISO/IEC 27031 – 2015)**

  Periodo de tiempo dentro del cual los niveles mínimos de servicios o productos y los sistemas, las aplicaciones, o funciones de apoyo se tienen que recuperar después de que haya ocurrido una interrupción.

- **Registro vital (ISO/IEC 27031 – 2015)**

Un registro electrónico o en papel que es esencial para preservar, continuar o reconstruir las operaciones de una organización y para proteger los derechos de una organización, sus empleados, sus clientes y sus partes relacionadas

6. ESTRUCTURA ORGANIZACIONAL DEL EQUIPO

6.1 Organización de la Oficina de Tecnologías de la Información

El Tribunal Constitucional considera dentro su Cuadro para Asignación de Personal Provisional (CAP-P)[3] tres personas para su Oficina de Tecnologías de la Información:

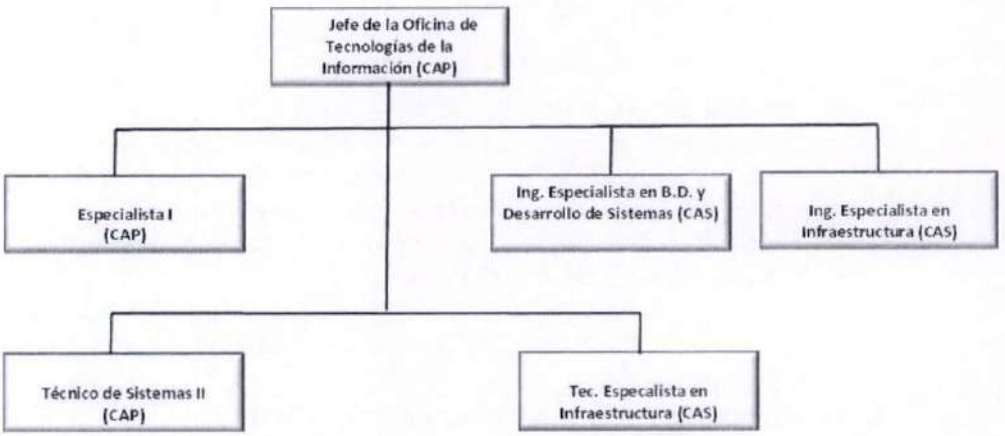
- Un Jefe de la Oficina de Tecnologías de la Información
- Un Especialista I
- Un Técnico de Sistemas II

En adición a ello, se cuenta con tres profesionales contratados bajo el régimen del D.L. 1057 también denominado Contrato Administrativo de Servicios

- Un Ingeniero especialista en B.D. y desarrollo de sistemas
- Un Ingeniero Especialista en Infraestructura Tecnológica
- Un Técnico Especialista en Infraestructura Tecnológica

Este será el personal técnico que conformará el equipo de recuperación

Organización de la Oficina de TI del Tribunal Constitucional



6.2 Equipo de Recuperación

Como se mencionó, el Equipo de Recuperación está conformado por personal de la OTI del Tribunal Constitucional, y tiene por finalidad participar en el Plan de recuperación de los servicios Informático y ejecutar los procedimientos establecidos en éste.

Las actividades de este Equipo, no se limitan al momento de la ocurrencia de un desastre, sino que su labor debe desarrollarse antes, durante y después de un incidente o situación adversa que ponga en riesgo la información o servicios de información del del Tribunal Constitucional.

Las principales actividades del Equipo de Recuperación son:

- Coordinar las acciones a ejecutar con todas las instancias correspondientes ante una situación de contingencia.

[3] Aprobado mediante R.A. 109-2023-P/TC

- Conseguir los recursos necesarios para reiniciar los sistemas y las comunicaciones críticas.
- Coordinar los traslados de equipos y recursos necesarios para la operación en contingencia.
- Notificar a proveedores e instituciones el esquema de atención a brindar mientras dure la contingencia.
- Coordinar y restablecer los sistemas y las telecomunicaciones.
- Mantener actualizado el Plan de recuperación de los servicios Informáticos.
- Realizar las pruebas de recuperación de los sistemas (plataformas tecnológicas, aplicaciones) y las comunicaciones de acuerdo al programa de pruebas anual establecido.

6.3 Organización

En razón a lo anterior, es recomendable que se organice un equipo de Recuperación de los Servicios Informáticos, liderados por el Jefe de la Oficina de Tecnologías de la Información que junto a tres grupos de trabaje se responsabilice de superar una situación que atente contra la continuidad operativa

Equipo de Recuperación de los Servicios Informáticos

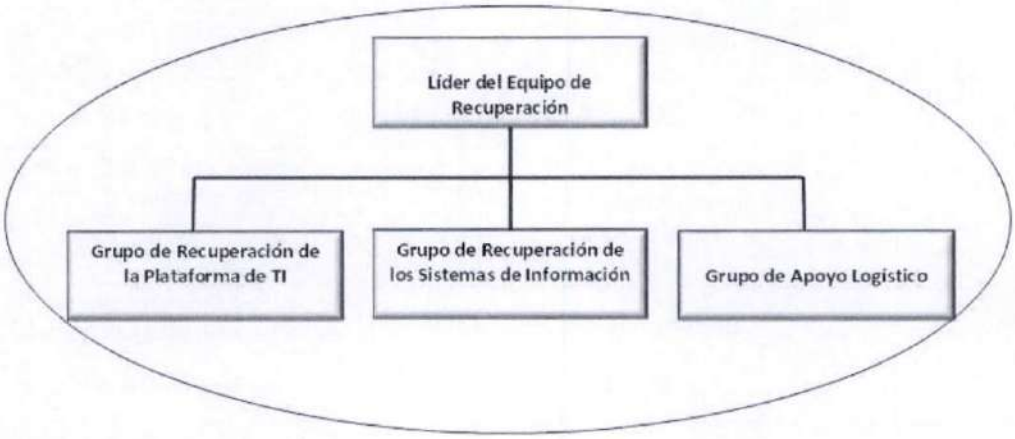


Diagrama 1. Organización del Equipo de Recuperación del TC Elaborado por: OTI

Líder del Equipo de Recuperación: Personificado en el Jefe de la Oficina de TI, es el responsable último que la continuidad operativa institucional se mantenga ante una situación de desastre. Es quien debe liderar y articular el funcionamiento y operatividad del resto de equipos a su cargo.

Grupo de Recuperación de la Plataforma de TI: Es el equipo de personas que se responsabilizará que la plataforma tecnológica, en cuanto a equipos se refiere, se encuentre lista para operar.

Grupo de Recuperación de los Sistemas de Información: Este grupo será el encargado de restaurarlos sistemas y programas, su actividad debe darse una vez que el Equipo de Recuperación de la Plataforma de TI, tenga todos los equipos listos para la restauración de los sistemas.

Grupo de Apoyo Logístico: Este grupo si bien no es un equipo altamente técnico; no obstante, su presencia servirá para articular cualquier necesidad de naturaleza logística que fuera menester para que la restauración de los servicios regrese, en la medida de los posible a los causes normales.

La conformación de profesionales de este Equipo de Recuperación, se especifica en el cuadro siguiente:

Cuadro de Roles en cada uno de los equipos de Recuperación del personal de la OTI

Equipos	Rol		Cargo
Supervisión	Líder de Equipos	Titular	Jefe de la Oficina de Tecnologías de Información
		Suplente	Especialista I
Recuperación de la Plataforma de TI	Responsable de Equipo		Especialista I
	Administrador de Servidores	Titular	Ing. Especialista en Infraestructura Tecnológica (CAS)
		Suplente	Técnico de Infraestructura Tecnológica (CAS)
	Especialista de Redes y Comunicaciones	Titular	Ing. Especialista en Infraestructura Tecnológica (CAS)
		Suplente	Técnico de Infraestructura Tecnológica (CAS)
Recuperación de Sistemas de Información	Responsable de Equipo		Especialista I
	Administrador de Base de Datos	Titular	Ing. Especialista en B.D. y desarrollo de sistemas (CAS)
		Suplente	Técnico de Sistemas II
	Especialista en Sistemas de Información	Titular	Ing. Junior Especialista de Desarrollo de software (Locador)
		Suplente	Técnico de Sistemas II
Apoyo Logístico en TI	Apoyo Logístico	Titular	Jefe de la Oficina de Tecnologías de Información
	Apoyo Logístico	Suplente	Técnico de Infraestructura Tecnológica (CAS)

Cuadro 1. Distribución del personal de la OTI en los distintos Equipo de Recuperación

6.4 Roles y Actividades

En el Anexo I se muestran los Roles y Actividades de cada uno de los integrantes de los distintos Grupos que conforman el equipo de Recuperación de los Servicios Informáticos.

7. POLÍTICA DE CONTINGENCIA

Las Políticas que rigen el presente documento, así como el marco en el que se desarrolla y ejecuta el Plan de recuperación Informático son las siguientes:

- El Plan de recuperación de los servicios Informáticos se ejecuta únicamente cuando una indisponibilidad severa y por tiempo prolongado afecte negativamente los Servicios Informáticos del Tribunal Constitucional. Sin embargo, puede servir como referente ante contingencias parciales.
- La ejecución del Plan de recuperación de los servicios Informáticos es realizada íntegramente por los especialistas de la OTI, junto con los proveedores de los distintos servicios previamente identificados en el literal del numeral 2 del presente documento.
- El Plan de recuperación de los servicios Informáticos, debe contar con un sólido procedimiento de respaldo y recuperación de información que garantice la confidencialidad, integridad y disponibilidad de la información.

La estrategia de recuperación de los servicios informáticos del Tribunal Constitucional debe permitir recobrar los servicios de TI críticos del Tribunal Constitucional, dentro de un tiempo de recuperación definido, minimizando el impacto del evento

8. REGISTROS Y SERVICIOS CRÍTICOS

8.1 Registros Vitales

Para afrontar una situación de contingencia, existen tres aspectos básicos que bajo ninguna circunstancia pueden ser soslayados: La estructura organizacional (Personas), Planes y procedimientos documentados y los Registros Vitales.

Los Registros Vitales constituyen la información y data crítica y sensible que la Institución necesita generar, resguardar y recuperar en caso ocurra un incidente crítico que afecte la disponibilidad de los servicios.

Los Registros Vitales se pueden encontrar en formato electrónico, impreso o escrito, esta clasificación permitirá asignar los controles de seguridad necesarios para su respaldo, custodia y recuperación en una situación de indisponibilidad de los servicios.

Los registros vitales (información/datos) por buenas prácticas son respaldados regularmente en medios externos (cintas, discos externos, solución en la nube).

Los registros vitales para el caso del Tribunal Constitucional, serán los siguientes:

Ítem	Registros Vitales	Detalle del contenido de los Registros Vitales
1	Bases de Datos	Esquemas, tablas e información almacenada en la Base de Datos.
2	Servidor de Archivos	Información de los aplicativos que se almacena en archivos. Copias de respaldo de la Base de Datos
3	Archivos de Configuración	Los archivos necesitan en el servidor de aplicaciones para que el sistema funcione adecuadamente.

4	Fuentes	Código fuente, librerías, manuales, documentación, etc. Recursos necesario para el mantenimiento de aplicativos.

Elaborado: OTI

Con el objetivo de mantener permanentemente actualizados y a buen recaudo los Registros Vitales se debe tener en cuenta:

- La frecuencia de respaldo de los Registros Vitales del Tribunal Constitucional debe obedecer a los requerimientos y necesidades de la Institución, requisitos de seguridad de la información y la criticidad de la información para la continuidad de los servicios que ofrece la institución.
- Los respaldos de los Registros Vitales deben estar ubicados y almacenados en un local remoto y a distancia suficiente para evitar los daños colaterales ante la eventualidad de un incidente, este local debe cumplir los requisitos mínimos indispensables de confidencialidad, seguridad física y medio ambiente.
- Los Registros Vitales deben probarse regularmente para asegurar su integridad y fiabilidad en caso de contingencia.

8.2 Servicios Críticos y Variables de Recuperación

La OTI brinda una diversidad de servicios de TI, los cuales son gestionados, algunos, desde el Centro de Datos del Tribunal Constitucional y otros desde un servicio de alojamiento en la nube. De todos los servicios que se ofrecen, se han identificado aquellos que no pueden estar inoperativos por largos periodos de tiempo dado que afectan significativamente al normal funcionamiento de los procesos del Tribunal Constitucional, a ellos se les ha denominado Servicios Críticos de TI.

Para cada Servicio Crítico de TI se tiene que determinar los siguientes valores, definidos previamente en el apartado 5 del presente documento.

- Tiempo Objetivo de Recuperación (RTO)
- Punto Objetivo de Recuperación (RPO)

En el anexo A, se muestran los servicios considerados críticos para el TC

9. ANÁLISIS DE RIESGOS

Con el objetivo de identificar los riesgos que pueden evitar o retrasar la continuidad operativa del Tribunal Constitucional se realizaron las siguientes actividades:

- Identificación de activos de información, relacionados con los servicios identificados como críticos para la continuidad operativa del Tribunal Constitucional (Ver Anexo II).
- Identificación de las amenazas a los que pudieran estar expuestos estos activos críticos (Ver Anexo III).
- Identificación de las vulnerabilidades de los activos críticos y que pudieran ser explotadas por las amenazas (Ver Anexo III).
- Identificación de los riesgos a los que estarían expuestos los activos críticos al ser explotadas las vulnerabilidades por parte de las amenazas (Ver Anexo III).
- Asignación de valores (probabilidades de ocurrencia e impactos) para cada uno de los riesgos identificados (Ver Anexo IV).

- Aplicación de los controles de la "NTP-ISO/IEC 27001:2014" a los riesgos que están sometidos los activos de Información relacionados con los servicios Críticos del Tribunal Constitucional, que afectaría la continuidad operativa institucional, (Ver Anexo V).

Para la determinación de la Probabilidad de ocurrencia, la naturaleza del impacto y la valoración del nivel de riesgos se usarán las siguientes tablas:

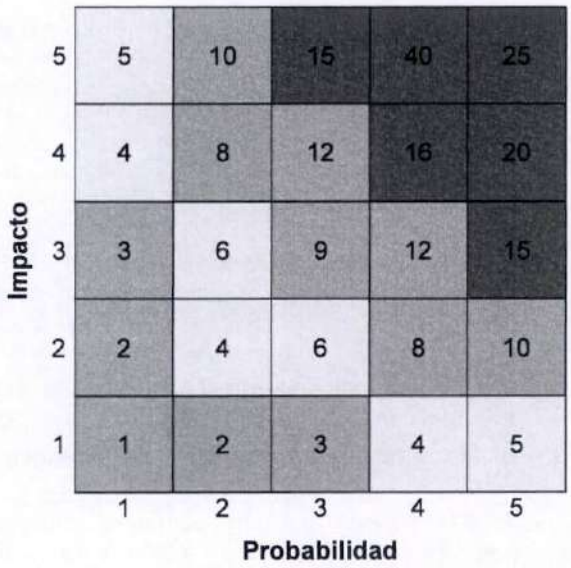
Tabla de Probabilidad de ocurrencia de un Riesgo

Valor	Calificación	Definición
1	**Muy Baja**	El evento no ha ocurrido o ha ocurrido al menos 1 vez al año.
2	**Baja**	Si bien el evento puede ocurrir, el periodo entre uno y otro puede ser muy grande. Al menos 2 veces al año.
3	**Moderada**	Es posible que ocurra el evento con una frecuencia baja. 3 o 4 veces al año.
4	**Alta**	Existen antecedentes de que el evento ocurrirá, dentro de un plazo de tiempo que implique una acción para enfrentarlo, pero la frecuencia no es alta. 1 vez al mes.
5	**Muy Alta**	El evento se sabe que ocurre con cierto grado de certeza y que la frecuencia es alta. 1 vez a la semana o más.

Tabla del impacto que provoca la materialización de un Riesgo

Nivel	Calificación	Descripción del Impacto
5	**Extremo**	Impacta en forma severa en la operatividad del TC al punto de comprometer la confidencialidad o integridad de información crítica y/o la continuidad de las operaciones por paralización de los servicios fundamentales por encima de los tiempos tolerables por la institución. El impacto es a todo el Tribunal Constitucional y su efecto repercute en todo el personal involucrado.
4	**Significativo**	Impacta en forma grave a un área o servicio específico del Tribunal Constitucional, puede llegar a comprometer documentos internos importantes, paralizar o retrasar procesos claves por un tiempo considerable. Su efecto está limitado a un área o servicio específico del TC.
3	**Moderado**	El impacto sobre la confidencialidad, integridad y disponibilidad de la información es limitado en tiempo y alcance. Su efecto es para un proceso de soporte o actividad específica que puede subsanarse en corto plazo.
2	**Menor**	El impacto es leve y se puede prescindir del mismo en un tiempo limitado.
1	**No Significativo**	No representa un impacto importante para el Tribunal Constitucional

Mapa Térmico del Nivel de Riesgo
(Impacto x Probabilidad)



Nivel de Riesgo

Extremo
Alto
Moderado
Bajo

10. DESARROLLO

10.1 Escenario de Contingencia y/o Desastre

El Plan de recuperación de los servicios Informáticos se activa en escenarios de desastres catastróficos que imposibiliten la operación normal de entrega de servicios de TI, siendo indispensable para la continuidad operativa del Tribunal Constitucional.

No obstante, pueden presentarse otro tipo de escenarios cuyo impacto no es generalizado y sólo afecta a servicios puntuales que ofrece el TC, por lo que se podría tomar acciones y respuesta de contingencia precisas.

A continuación, se describen los posibles escenarios identificados en función a la mayor probabilidad de ocurrencia e impacto sobre los servicios informáticos del TC.

10.1.1. Destrucción e indisponibilidad del Centro de Datos

Producto de la revisión de las amenazas y el impacto a la Organización, se determina como el primer escenario la Destrucción / Indisponibilidad Total del Centro de Datos, debido a la criticidad e importancia de las plataformas tecnológicas y las aplicaciones que estas contienen, siendo consideradas las amenazas como incendio, terremoto devastador, atentado terrorista o ataque cibernético como las más probables de acontecer.

10.1.2. Falla de los Servidores y/o las unidades de Almacenamiento

Se ha determinado también la posibilidad de presentarse fallas de hardware en los servidores donde se alojan las aplicaciones y las Bases de Datos críticas y sensibles para el Tribunal Constitucional, entre las que podemos enumerar:

- Fallas por falta de mantenimiento preventivo.
- Falla de discos duros, fuentes o partes del servidor en general, por causas de deterioro o mala manipulación (golpes al trasladarlo) o trabajos dentro del Centro de Datos.
- Obsolescencia tecnológica.

10.1.3. Falla de las Comunicaciones

Los componentes de comunicaciones como routers, switches o cableado estructurado pueden presentar fallas debido a lo siguiente:

- Fallas por falta de mantenimiento preventivo.
- Fallas por deterioro o tiempo de uso del equipo.
- Obsolescencia tecnológica.
- Cableado con desfase tecnológico, sin certificación y baja performance.

Estas posibles causas pueden traer como consecuencia la desconexión de los equipos cortando la transferencia de los datos y por ende la indisponibilidad de los sistemas de la red LAN para los usuarios finales.

10.1.4. Falla de la Energía Eléctrica

Entre las fallas de la energía eléctrica que pueden afectar los equipos del Centro de Datos, se encuentran las siguientes:

- Falla del suministro de energía eléctrica (corriente externa).
- Mal suministro de energía (corriente inestable).
- Condiciones ambientales (exceso de humedad) en la sala de energía.
- Pozos a tierra inoperativos.
- Falla en los componentes del equipo de protección eléctrica (UPS).

10.1.5. Mal funcionamiento del aire Acondicionado

Los equipos de Aire Acondicionado (AA), utilizados en el Centro de Datos, pueden presentar fallas debido a lo siguiente:

- Falla de la Unidad Evaporadora.
- Deterioro de filtros y/o fajas
- Falla de la Unidad Condensadora.
- Falla en tuberías de gas refrigerante
- Obsolescencia tecnológica.

10.1.6. Ausencia del Personal de TI

Esto se puede producir por algún impedimento del personal de la OTI que no le permita acudir o ingresar al centro de labores, entre los motivos más comunes tenemos:

- Conmoción Civil.

- Pandemia.
- Accidentes.
- Culminación de contrato de servicios

10.2 Acciones Inmediatas ante accidentes

Luego de ocurrido el evento o incidente de alto riesgo o desastre, el primer paso es asegurar la integridad física de las personas, para ello se ejecutan los siguientes procedimientos.

10.2.1. Procedimiento de emergencia durante el incidente

Considerando que el objetivo principal, es salvaguardar la integridad física del personal que se encuentre en las instalaciones de la Institución; en caso de un evento severo o situación adversa que ponga en riesgo la vida del personal (Ejemplo: incendios, terremotos, atentados, etc.), antes de activar el proceso de recuperación de los sistemas y servicios informáticos se debe ejecutar el Procedimiento de Emergencia.
El responsable del equipo de TI o quien se encuentre encargado, debe de ejecutar las siguientes acciones:

- Notificar el evento, alertando al personal que se encuentra laborando en las oficinas.
- Dar aviso del siniestro a los bomberos, comisaría local, seguridad privada interna de la institución, personal médico, o quien corresponda. Para lo cual las Oficina de Gestión y Desarrollo Humano, Servicios Generales y Logística deben tener en cuenta la información que les permita una comunicación inmediata con dichos servicios
- Apoyar al personal a colocarse en zonas seguras y evacuar el edificio.
- Seguir siempre las indicaciones del Comité de Seguridad y salud en el Trabajo.
- No permitir que el personal retorne al lugar del siniestro, hasta que se evalúen los daños que ha sufrido el ambiente y éste sea seguro.

10.2.2. Determinación del tipo de Incidente

Debido a que un evento que atente contra la continuidad operativa institucional puede suceder en cualquier instante el Líder de Recuperación de los Servicios Informáticos debe determinar la naturaleza del evento y, dependiendo de ello, convocar al líder del grupo cuya participación será critica para conjurar el problema o en su defecto a los líderes de los distintos grupos de recuperación y en conjunto con ellos determinar la naturaleza del evento y quienes deben tener participación activa en superar el evento..
Luego de una evaluación inicial del espacio físico o virtual en donde se presentó el incidente, el Líder de Recuperación de los Servicios Informáticos deberá determinar cuál o cuáles de los siguientes escenarios es el que se está presentando:

- Destrucción o indisponibilidad del Centro de Datos
- Problemas de funcionamiento de los servidores

- Interrupción de las comunicaciones
- Falla de energía eléctrica
- Mal funcionamiento del Sistema de Aire Acondicionado

Una vez evaluado el escenario inicial, se procede con la notificación del mismo.

10.2.3. Notificación del Incidente

En caso de la ocurrencia de un Incidente, luego de ejecutar el procedimiento de emergencia y una vez identificado en qué escenario nos encontramos, se deben de realizar las siguientes acciones para la notificación del incidente.

- El Líder del Equipo de Recuperación debe de notificar al Secretario General y a la DIGA del Tribunal Constitucional.
- El Líder del Equipo de Recuperación debe de notificar a los Responsables de los Equipos la situación de contingencia e indicar las principales acciones a seguir. *Ver Diagrama de Comunicación*
- Los Responsables de cada Grupo de Recuperación se reunirán con los especialistas del grupo a fin de coordinar las primeras actividades a realizar.

10.3 Proceso de Contingencia ante accidentes

Es importante que, cuando se presente un evento o incidencia que amerite la activación del Plan de recuperación de los servicios Informáticos, se consideren determinadas las actividades que deben realizarse. Para ello, se ha definido el Proceso de Contingencia ante Incidentes.

Cuando se presenta una alerta por una Incidencia Crítica, es necesario analizar la incidencia, para determinar la mejor solución aplicable. Este proceso es ejecutado por el Equipo de Recuperación, contando siempre con la colaboración de los especialistas de la OTI en caso se requiera.

Las actividades a realizar son las siguientes:

Dentro de este proceso existen 3 actividades en las cuales es necesario definir qué las tareas que deben realizar, las cuales son:

Análisis Situacional

Cuando se presenta una alerta de Incidencia Crítica, es necesario realizar una evaluación rápida de la situación actual de los servicios de TI a fin de tener un mapa general del incidente y cuál es el impacto. Por ello los responsables de cada grupo de recuperación deben de elaborar un Informe Situacional para que el Líder del Equipo de Recuperación realice la evaluación respectiva.

Para poder elaborar el informe, las tareas a ejecutar son:

- El responsable de Equipos coordinará con su equipo la elaboración del informe.
- Los especialistas de cada equipo, de acuerdo a sus competencias, identifican los servicios de TI que se encuentran operativos e inoperativos.
- Los especialistas de cada equipo, de acuerdo a sus competencias, identificarán el estado de los equipos.

- El responsable y su Equipo, deben elaborar el Informe Situacional teniendo en cuenta la información levantada, y adicionando sus conclusiones y recomendaciones.
- El responsable de Grupo debe de remitir el Informe Situacional al Líder de Equipos.

Evaluación de Daños

Luego de tener una visión general del impacto causado por el Incidente, tomando como insumo el Informe Situacional, los integrantes de cada Equipo evaluarán a mayor detalle los daños sufridos, el tiempo estimado de recuperación y los recursos necesarios para que los servicios puedan ser recuperados.

El responsable de cada grupo consolida la información, notifica el resultado al Líder de Recuperación y coordina con el Apoyo Logístico la posibilidad de contar con los recursos necesarios, si fueran necesarios

Las tareas a ejecutar son:

- El responsable de Equipo distribuye las tareas en base a lo registrado en el Informe Situacional.
- El especialista del Equipo revisa detalladamente el estado de los equipos y/o servicios, teniendo como base el Informe Situacional.
- El Especialista del Equipo elabora una lista con los recursos necesarios para restaurar los servicios.
- El Especialista analiza los escenarios y estima el tiempo de recuperación de los servicios.
- El Responsable de Equipo consolida la información de los especialistas y elabora la Evaluación de Daños.
- El Responsable de Equipo entrega la Evaluación de Daños al Líder de Equipos para conocimiento, además, si es necesario, coordina con el Apoyo Logístico los recursos requeridos.

Recuperación de Servicios de TI

Activado el Plan de recuperación de los servicios Informáticos, conociendo la evaluación de los daños y contando con los recursos necesarios, se da inicio a la recuperación de los servicios.

Las tareas a ejecutar son:

- Cuando se cuente con la Evaluación de los Daños y con los recursos necesarios, el Líder del Equipo de Recuperación dará inicio a la Recuperación de los Servicios.
- Los responsables de cada Equipo identifican los procedimientos que se van a ejecutar.
- El Grupo de Recuperación de la Plataforma de TI cuenta con los siguientes procedimientos para la recuperación:
  - Procedimiento de apagado de los servidores.
  - Procedimiento de encendido de los servidores.
  - Procedimiento de apagado de los equipos de comunicación
  - Procedimiento de encendido de los equipos de comunicación

- El Grupo de Recuperación de Sistemas de Información cuenta con los siguientes procedimientos para la recuperación:
  - Procedimiento de apagado de bases de datos.
  - Procedimiento de encendido de bases de datos.
  - Procedimiento de apagado de los Sistemas de Información
  - Procedimiento de encendido de los Sistemas de Información.
- El Especialista de Equipo ejecuta los procedimientos necesarios para la restauración.
- El Especialista de Equipo realiza pruebas básicas de los servicios restaurados.
- Si las pruebas no son exitosas, se vuelven a ejecutar los procedimientos de restauración.
- Si las pruebas son exitosas, se coordina con los miembros del equipo de OTI para realizar pruebas de integración de los servicios restaurados.
- Si las pruebas no son exitosas, se vuelven a ejecutar los procedimientos de restauración.
- Si las pruebas son exitosas, se le notifica al Responsable del Equipo la recuperación de los servicios.
- El Responsable de Equipos notifica al Líder de Equipos los servicios recuperados.

11. PRUEBAS Y MANTENIMIENTO

En caso se presente algún evento crítico, una vez que el Equipo de Recuperación tenga toda la documentación requerida para poder realizar la recuperación de los servicios tecnológicos, deben realizar pruebas que permitan garantizar que estos procedimientos funcionan correctamente y a su vez permitan:

- Comprobar la eficacia de los procedimientos establecidos ante un incidente o desastre.
- Identificar actividades que se necesitan optimizar.
- Disponer del Plan de Recuperación de los Servicios Informáticos activo, actualizado, entendible y usable.
- Demostrar la destreza de los Equipos de Recuperación en la habilitación de los servicios.

Las pruebas deben ejecutarse durante un periodo de tiempo que no afecte la operatividad normal, o que el impacto sea mínimo. Estas pruebas deben ser realizadas bajo un escenario real y contener las siguientes tareas:

- Verificar la totalidad y precisión del Plan de recuperación de los servicios Informáticos.
- Evaluar el desempeño del personal involucrado.
- Evaluar la coordinación entre los miembros del equipo de contingencia, proveedores y otros.
- Identificar la capacidad de recuperar registros e información vital.
- Medir el desempeño de los sistemas operativos y computacionales.

11.1 Tipo de Pruebas

Durante esta etapa se debe establecer un programa de pruebas con escenarios simulados, considerando los requerimientos por prueba y una revisión detallada de los resultados obtenidos.

Se consideran tres tipos de pruebas:

- **Prueba de escritorio:** Los responsables de cada uno de los grupos de contingencia y recuperación, evalúan el Plan y la posibilidad de cumplir con las actividades asignadas dentro de los plazos establecidos. La evaluación es a partir de su experiencia, el conocimiento del tema y su capacidad para predecir escenarios supuestos de acuerdo a lo contemplado.
- **Prueba Parcial:** Es una revisión localizada y conlleva a la simulación de una ocurrencia parcial o aspectos parciales de la prueba total. De preferencia se deben considerar aquellos aspectos que han sido considerados débiles en las pruebas de escritorio y aquellos que son críticos.
- **Prueba Operativa Total:** Para llevar a cabo esta prueba, es necesario realizar una interrupción real de los servicios y se busca validar todos los procedimientos contemplados en el Plan de Recuperación de los Servicios Informáticos. Previo a su ejecución, es necesario haber realizado con éxito la prueba de escritorio y la prueba parcial. Deben ser realizadas en un periodo de tiempo que altere lo menos posible la operatividad de la institución (considerar fines de semana, feriados, etc.). Deben participar todos y cada uno de los miembros de los distintos grupos de Recuperación, de acuerdo a lo establecido en el Plan de recuperación de los servicios Informáticos.

Las pruebas de escritorio y las pruebas parciales, serán programadas en fechas específicas y deberán realizarse por lo menos una vez al año. Las pruebas totales se realizan posteriores a las parciales y son programadas por lo menos una vez cada dos años o cuando existieron cambios críticos en el Plan de recuperación de los servicios Informáticos.

11.2 Evaluación y Documentación de Pruebas

Durante toda la prueba, cada uno de los responsables debe registrar las dificultades encontradas, las observaciones, los logros obtenidos y comunicarlo al Líder del Equipo de Recuperación a través de un informe, considerando los objetivos y los aspectos que deben ser mejorados.

El Líder del Equipo de Recuperación analiza los resultados y adecua el Plan de recuperación de los servicios Informáticos, con los cambios necesarios, en un plazo no mayor a 30 días calendarios (contados a partir de la fecha de realización de las pruebas).

Para la validación de las pruebas, se deben considerar los siguientes indicadores:

- **Tiempo**, que demandó la ejecución de los procedimientos contemplados.
- **Eficiencia,** total de actividades y procedimientos que fueron realizados con éxito.
- **Operatividad,** recuperación total o parcial de los servicios.

11.3 Mantenimiento y Actualización del Plan

El Plan de recuperación de los servicios Informáticos, debe estar siempre actualizado de acuerdo a los cambios necesarios que mejoren su efectividad. Para ello debe ser revisado de manera periódica y programada.

Las revisiones periódicas coinciden con las pruebas programadas o cuando se presenten incidencias, concluidas éstas se realiza una revisión de la efectividad del Plan y si existiesen falencias, estas son consideradas con las modificaciones correspondientes.

La labor de mantenimiento, revisión y actualización del Plan Contingencia Informático está a cargo del Oficial de Seguridad y Confianza Digital, quien tiene a su cargo las siguientes responsabilidades:

- Desarrollar un cronograma de revisión y mantenimiento del Plan de recuperación de los servicios Informáticos comunicando a todos los involucrados, sus funciones y fechas límite para recibir observaciones y/o comentarios.
- Programar revisiones extraordinarias cuando existen cambios significativos.}
- Validar las pruebas y comentarios y actualizar el Plan de recuperación de los servicios Informáticos dentro de los 30 días calendarios, posteriores a la fecha de prueba.
- Coordinar y participar en las pruebas programadas.
- Establecer un cronograma de fortalecimiento de capacidades al personal de los Equipos de Recuperación, de acuerdo a la naturaleza de sus roles en el Plan de recuperación de los servicios Informáticos.
- Establecer una Bitácora de actividades de mantenimiento del Plan de recuperación de los servicios Informáticos (Pruebas, revisiones, capacitación, entre otros)

12. ANEXOS

Anexo I

1. Del Líder del Equipo de Recuperación de los Servicios Informáticos

ROL:	*Líder del Equipo de Recuperación*		
Titular:	Jefe de la Oficina de Tecnologías de Información	**Suplente:**	Especialista I
No	**Descripción de actividades**		
1	**Actividades de Prevención**		
1.1	Revisar periódicamente el funcionamiento de los Servicios de Informáticos para verificar el adecuado funcionamiento de: - Las medidas de seguridad de acceso tanto al Centro de Datos como a los servidores on cloud - Sistema de Aire Acondicionado, para el caso del CD (temperatura y humedad). - Sistema de alimentación ininterrumpida del CD - UPS. - Actualizar los procedimientos, si fuera necesario.		
1.2	Emitir un informe situacional a la DIGA acerca del funcionamiento de los Servicios Informáticos para validar el correcto funcionamiento en lo que se refiere a: - Funcionamiento de los servicios informáticos. - Principales incidentes reportados. - Actualización de procedimientos. - Respaldo de la Información.		
1.3	Validar el presente plan respecto al cumplimiento con el personal existente.		
1.4	Verificar y/o actualizar los datos del personal que faciliten la comunicación en caso de emergencia.		
1.5	Verificar y/o actualizar los datos de los proveedores de servicios que faciliten la comunicación en caso de emergencia.		
2	**Actividades de Respuesta**		
2.1	En caso de alerta de un incidente que podría activar el Plan de recuperación de los servicios Informáticos, realiza lo siguiente: - Coordina con el responsable de la Plataforma de TI y de Sistemas de Información on premise y on cloud, en la determinación de la naturaleza de la contingencia. - Iniciar el plan de restauración de sistemas en razón de la naturaleza de la contingencia presentada - Informar a la DIGA y al Secretario General sobre la ocurrencia y solicitar autorización para ejecutar el Plan de recuperación de los servicios Informáticos, informando los servicios afectados y el eventual tiempo de restauración. - Evaluar el estado situacional.		
2.2	Notificar a todo el Equipo de Recuperación cuando un incidente active el Plan de recuperación de los servicios Informáticos.		
2.3	Prepara el inventario de problemas iniciales y coordinar con los otros equipos de recuperación la posible solución.		
2.4	Informar al Secretario General la necesidad de la activación del Plan de recuperación de los servicios Informáticos.		
2.5	Monitorear la recuperación de los servicios afectados.		
2.6	Informar permanentemente la situación de los servicios a la DIGA y al Secretario General.		
3	**Actividades de Recuperación**		
3.1	Preparar junto a los responsables de cada equipo de recuperación, las actividades a realizar para restaurar los servicios y asignar responsabilidades.		
3.2	Informar a la DIGA y al Secretario General, la restauración de los principales servicios.		
3.3	Realizar sesiones de análisis de lecciones aprendidas para evaluar la ejecución del plan.		

TRIBUNAL CONSTITUCIONAL – Oficina de Tecnologías de la Información

DIRECCIÓN GENERAL DE ADMINISTRACIÓN – V°B°

2. **Del Líder del Grupo de Recuperación de la Plataforma de TI**

ROL:	*Líder del Grupo de Recuperación de la Plataforma de TI*		
Titular:	Ing. Especialista de Infraestructura Tecnológica (CAS)	**Suplente:**	Técnico Espec. en Infraestructura Tecnológica (CAS)

No	Descripción de actividades
1	**Actividades de Prevención**
1.1	Coordinar las pruebas del Plan de recuperación de los servicios Informáticos, en los aspectos referidos a la plataforma de TI.
	Verificar y mantener actualizados los procedimientos de encendido y apagado de los servidores.
1.3	Informar al Líder de Recuperación de los Servicios Informáticos los resultados obtenidos en las pruebas.
1.4	Actualizar el Plan de recuperación de los servicios Informáticos, en los aspectos referidos a la Plataforma de TI, cada vez que se requiera.
1.5	Mantener actualizadas las especificaciones de hardware, la configuración de los equipos y los procedimientos de recuperación.
1.6	Monitorear el comportamiento de los equipos conectados a la red.
1.7	Participar de la actualización del Plan de recuperación de los servicios Informáticos.
1.8	Resguardar los procedimientos de configuración de los S.O. de los servidores
1.9	Verificar y mantener actualizados los procedimientos de encendido y apagado de los equipos de comunicación.
1.1	Mantener actualizados los diagramas de Red, las especificaciones de hardware, la configuración de los equipos de comunicaciones y los procedimientos de recuperación.
1.11	Monitorear el comportamiento de la red.
1.12	Determinar medidas preventivas para minimizar el impacto en las fallas de comunicaciones.
1.13	Verificar y mantener actualizados los procedimientos de encendido y apagado de los equipos de comunicación.
1.14	Participar en las pruebas del Plan de recuperación de los servicios Informáticos.
2	**Actividades de Respuesta**
2.1	Hacer una evaluación rápida sobre la naturaleza del problema presentado.
2.2	Informar de la situación presentada al Líder de Equipo de Recuperación de los Servicios Informáticos, y analizar si el problema es de competencia de la plataforma TI o a nivel de los Sistemas de Información.
2.3	Realizar las coordinaciones para la puesta en servicio de los recursos que hubieran colapsado. En caso que solo se trate de un problema menor.
2.4	Coordinar con el Líder del Grupo de Apoyo Logístico y con el Líder del Equipo de Recuperación en caso se requiera la habilitación de algún ambiente especial y/o la compra de algunos materiales y/o equipos para la restauración de los servicios.
2.5	Revisión de los equipos de comunicación, si el problema se encontrara a ese nivel
2.6	Verificar las conexiones de Internet con el proveedor del servicio, revisando la conectividad con el resto de locales
2.7	Coordinar con el Líder del Equipo de Recuperación de Sistemas de Información los aspectos necesarios para iniciar la restauración de los equipos.

ROL:	*Líder del Grupo de Recuperación de la Plataforma de TI*		
Titular:	Ing. Especialista de Infraestructura Tecnológica (CAS)	**Suplente:**	Técnico Espec. en Infraestructura Tecnológica (CAS)

No	Descripción de actividades
3	**Actividades de Restauración**
3.1	Coordinar con el resto de personal el inicio de la restauración de los recursos que se hubieran visto afectados y se encuentren bajo su dominio
3.2	Informar permanentemente al Líder de Recuperación de los Servicios Informáticos el avance de su equipo en la restauración de los servicios.
3.3	De ser necesario, contactar con los proveedores de servicios que corresponda, para su apoyo en la restauración.
3.4	Notificar al Líder de Equipos cuando la restauración esté completada al 100%.
3.5	Realizar una evaluación del Plan de recuperación de los servicios Informáticos.
3.6	Documentar todos los inconvenientes encontrados en la restauración.

DIRECCIÓN GENERAL DE ADMINISTRACIÓN V°B°

TRIBUNAL CONSTITUCIONAL - Oficina de Tecnologías de la Información

3. Del Líder del Grupo de Recuperación de los Sistemas de Información

ROL:	*Líder del Grupo de Recuperación de los Sistemas de Información*		
Titular:	Ingeniero especialista en B.D. y desarrollo de sistemas (CAS)	Suplente:	Ing. Junior Especialista de Desarrollo de software (Locador)

No	Descripción de actividades
1	**Actividades de Prevención**
1.1	Verificar el cumplimiento de las actividades de prevención por parte de su equipo.
1.2	Coordinar las pruebas del Plan de recuperación de los servicios Informáticos.
1.3	Informar al Líder de Recuperación de S.I. sobre los resultados obtenidos en las pruebas.
1.4	Actualizar el Plan de recuperación de los servicios Informáticos, cada vez que se requiera.
1.5	Monitorear y administrar la seguridad de las Bases de Datos.
1.6	Mantener actualizado el diccionario de cada una de las tablas de la Base de Datos.
1.7	Participar de la actualización del Plan de recuperación de los servicios Informáticos.
1.8	Participar en las pruebas del Plan de recuperación de los servicios Informáticos.
1.9	Mantener Actualizado el procedimiento de encendido y apagado de bases de datos.
1.1	Identificar y verificar el procedimiento de respaldo y restauración de bases de datos.
1.11	Realizar pruebas de funcionamiento de los Backups: - Revisión periódica para detectar probables problemas de seguridad - Gestionar el creciente volumen de datos y diseñar los planes apropiados para administrarlos Hacer copias de seguridad periódicas de las bases de datos y mantenerlos a salvo de la destrucción accidental o intencional.
1.12	Mantener actualizado el inventario de los aplicativos informáticos.
1.13	Mantener Actualizado el procedimiento de alta y baja de sistemas de información.
1.14	Identificar y verificar el procedimiento de respaldo de sistemas de información.
2	**Actividades de Respuesta**
2.1	Apoyar en la evaluación preliminar de daños.
2.2	Identificar y notificar el estado situacional de los sistemas.
2.3	Verificar si es posible realizar la restauración de todos los sistemas de información.
2.4	Coordinar con el Ing. Especialista en Infraestructura el levantamiento de los sistemas.
2.5	Realizar las coordinaciones iniciales para realizar la restauración.
2.6	Coordinar con el Apoyo Logístico y con el Líder de Equipos en caso se requiera la habilitación de algún ambiente especial y/o la adquisición de algún material, software o servicio para los trabajos de restauración.
3	**Actividades de Restauración**
3.1	Realizar la restauración de los sistemas conforme se vayan levantando las bases de datos.
3.2	Informar al Líder del Equipo de Recuperación sobre el avance de la restauración de los sistemas.
3.3	Coordinar con el resto de integrantes de la OTI, las pruebas de los sistemas.
3.5	Notificar al Responsable del Equipo los sistemas que van quedando 100% operativos.
	Documentar todos los inconvenientes encontrados en la restauración.

ROL:	*Líder del Grupo de Recuperación de los Sistemas de Información*		
Titular:	Ingeniero especialista en B.D. y desarrollo de sistemas (CAS)	**Suplente:**	Ing. Junior Especialista de Desarrollo de software (Locador)

No	Descripción de actividades
	Identificar oportunidades de mejora al Plan de recuperación de los servicios Informáticos.
3.3	De ser necesario, contactar con los proveedores de servicios que corresponde, para su apoyo en la restauración.
3.4	Notificar al Líder del Equipo de Recuperación cuando la restauración esté completada al 100%.
3.5	Apoyar en la elaboración del Informe de Evaluación de Daños.
3.6	Realizar una evaluación del Plan de recuperación de los servicios Informáticos.

DIRECCIÓN GENERAL DE ADMINISTRACIÓN
V°B°

4. **Del Líder del Grupo de Apoyo Logístico**

ROL:	*APOYO LOGÍSTICO*		
Titular:	Jefe de la Oficina de Tecnologías de Información	**Suplente:**	Técnico de Sistemas II
No	**Descripción de actividades**		
1	**Actividades de Prevención**		
1.1	Coordinar con la DIGA, la Oficina de Presupuestos, la Oficina de Gestión y Desarrollo Humano y la Oficina de Logística los recursos necesarios para aplicar el Plan de recuperación de los servicios Informáticos.		
1.2	Mantener vigentes los contratos de bolsas de horas de soporte según crea conveniente el Líder del Equipo de Recuperación de la Plataforma de TI y el Líder de Recuperación de los Servicios Informáticos.		
1.3	Mantener actualizada la lista de proveedores de servicios necesarios para la recuperación, en coordinación con el Líder del Equipo de Recuperación de los Servicios Informáticos		
2	**Actividades de Respuesta**		
2.1	Coordinar con las jefaturas de las Oficinas de TI y Logística necesidad de reposición de equipos dañados y la posibilidad de adquirirlos en corto tiempo.		
2.2	Coordinar con los responsables de los equipos, la adquisición de equipos o materiales necesarios para la recuperación.		
2.3	Coordinar con los responsables de los equipos la necesidad de habilitar otros espacios físicos para la recuperación.		
3	**Actividades de Restauración**		
3.1	Identificar oportunidades de mejora al Plan de recuperación de los servicios Informáticos.		

Anexo II

Servicios críticos para la continuidad operativa del Tribunal Constitucional

Ítem	Nombre	Descripción	Categoría	Registros Críticos	Ubicación*
Servicios ofrecidos y administrados por la OTI					
1	**SIGE**	Sistema integrado de Gestión de Expedientes	Software con Mantenimiento Interno alojado localmente	Archivos de Configuración	
				Base de Datos	
				Servidor de Archivos	
2	**SGD**	Sistema de Gestión Documental	Software con Mantenimiento Interno alojado en la nube	Archivos de Configuración	
				Base de Datos	
				Servidor de Archivos	
3	**SIGA**	Sistema Integrado de Gestión Administrativa	Software con Mantenimiento Externo, alojado localmente	Archivos de Configuración	
				Base de Datos	
4	**SIAF**	Sistema Integrado de Administración Financiera	Software con Mantenimiento Externo, alojado localmente	Archivos de Configuración	
				Base de Datos	
				Servidor de Archivos	
5	**SIAJ**	Sistema Integrado de Administrativo y Jurisdiccional	Software con Mantenimiento Interno, alojado en la nube	Archivos de configuración	
6	**SISPER**	Sistema de Planillas	Software con Mantenimiento Externo, alojado localmente	Archivos de configuración	
7	**KOHA**	Sistema para el Control de los libros de la Biblioteca del CEC	Software con Mantenimiento Externo, alojado localmente	Archivos de configuración	
8	**Ventanilla Jurisdiccional**	Sistema mediante el cual los justiciables pueden ingresar escritos a los expedientes	Software con Mantenimiento Interno, alojado en la nube	Archivos de configuración Base de datos	

Item	Nombre	Descripción	Categoría	Registros Críticos	Ubicación*
9	**Jurisprudencia Sistematizada**	Sistema web para la búsqueda sistematizada de la jurisprudencia constitucional	Software con Mantenimiento Interno, alojado en la nube	Archivos de configuración Base de datos	
10	**Correo Electrónico**	Correo electrónico Institucional	Servicio Tercerizado como herramienta colaborativa		
11	**Drives**	Espacio de alojamiento de documentos digitalizados de distintas áreas	Servicio Tercerizado como herramienta colaborativa		
12	**Página Web Institucional**	Ambiente en la nube donde se aloja la página web	Software con Mantenimiento Interno, alojado en la nube	Archivos de Configuración	
				Base de Datos	
				Servidor de Archivos	
Servicios ofrecidos por terceros y administrados por la OTI					
13	**Acceso a Internet y Seguridad perimetral de red**	Servicio de acceso a Internet con Firewall en ISP	Servicio Tercerizado	Administrados por el proveedor	
14	**Herramientas colaborativas**	Servicio provisto por Google Inc.	Servicio Tercerizado	Administrados por el proveedor	
15	**Alojamiento en la nube**	Alojamiento en la nube	Servicio Tercerizado	Administrados por el proveedor	

Anexo III

Identificación de Activos de Información Asociados a los Servicios Críticos, las amenazas a las que están expuestos, vulnerabilidades que puedes ser aprovechadas por ellas y los riesgos potenciales

Ítem	Nombre	Activo de Información	Amenaza	Vulnerabilidad	Riesgo
Servicios ofrecidos y administrados por la OTI					
1	**SIGE**	Servidor	Fallo en el servidor que aloja la aplicación	Ausencia de Servicios de Mantenimiento y Garantía de los servidores locales	Servidor falle y deje de funcionar
		Base de datos	Fallo en la unidad de almacenamiento que aloja la Base de Datos	Ausencia de Servicios de Mantenimiento y Garantía de las Unidades de Almacenamiento	Unidad de almacenamiento falle, deje de funcionar y haya pérdida de información
		Código fuente del SIGE	Pérdida del Código fuente o código desactualizado	Indeterminación de la localización de los programas fuente, carencia de bitácora de modificaciones	Pérdida de los programas fuente del SIGE o contar con versiones desactualizadas de los mismos
		Copias de Respaldo de la Base de Datos	Fallo en la unidad de almacenamiento que aloja las copias de respaldo	Ausencia de Servicios de Mantenimiento y Garantía de las Unidades de Almacenamiento	Restricciones o imposibilidad de obtener las copias de respaldo para la restauración del sistema
		Analista responsable del SIGE	Ausencia del Analista responsable	Existencia de un único responsable de la administración del SIGE	Ante falla del sistema no hay quien pueda resolver los problemas
		Documentación del SIGE	Ausencia de manuales o manuales desactualizados	Ausencia de un repositorio que aloje los manuales actualizados	Pérdida de los manuales o no contar con ellos, cuando estos sean necesarios
		Sistema como aplicación	Malware que ataque la aplicación y los datos bajo su administración.	Ausencia de mecanismos de protección Antimalware en el servidor	Daño a los datos manejados por el sistema o robo de los mismos
		Acceso a Internet	Falta de conexión a Internet	Carencia de línea de contingencia por parte del proveedor o carencia de un proveedor alterno	Usuarios fuera de las instalaciones del TC no puedan acceder al SIGE
2	**STD**	Servidor	Pérdida de conexión con el Servidor en la nube	Servidor en la nube carece de mecanismos clusterización	El STD deje de funcionar

Item	Nombre	Activo de Información	Amenaza	Vulnerabilidad	Riesgo
		Base de datos	Fallo en la unidad de almacenamiento que aloja la Base de Datos	Unidad de almacenamiento en la nube carece de mecanismos clusterización	Unidad de almacenamiento falle, deje de funcionar y haya pérdida de información
		Código fuente del STD	Pérdida del Código fuente o código desactualizado	Indeterminación de la localización de los programas fuente, carencia de bitácora de modificaciones	Pérdida de los programas fuente del STD o contar con versiones desactualizadas de los mismos
		Analista responsable del STD	Ausencia del Analista responsable	Existencia de un único responsable de la administración del STD	Ante falla del sistema no hay quien pueda resolver los problemas
		Documentación del STD	Ausencia de manuales o manuales desactualizados	Ausencia de un repositorio que aloje los manuales actualizados	Pérdida de los manuales o no contar con ellos, cuando estos sean necesarios
		Sistema como aplicación	Malware que ataque la aplicación y los datos bajo su administración.	Ausencia de mecanismos de protección Antimalware en el servidor en la nube	Daño a los datos manejados por el sistema o robo de los mismos
		Acceso a Internet	Falta de conexión a Internet	Carencia de línea de contingencia por parte del proveedor o carencia de un proveedor alterno	Carecer de acceso al STD por parte de los equipos al interior del TC
3	SIGA	Servidor	Fallo en el servidor que aloja la aplicación	Ausencia de Servicios de Mantenimiento y Garantía de los servidores locales	Servidor falle y deje de funcionar
		Base de datos	Fallo en la unidad de almacenamiento que aloja la Base de Datos	Ausencia de Servicios de Mantenimiento y Garantía de las Unidades de Almacenamiento	Unidad de almacenamiento falle, deje de funcionar y haya pérdida de información
		Copias de Respaldo de la Base de Datos	Fallo en la unidad de almacenamiento que aloja las copias de respaldo	Ausencia de Servicios de Mantenimiento y Garantía de las Unidades de Almacenamiento	Restricciones o imposibilidad de obtener las copias de respaldo para la restauración del sistema
		Administrador de la Base de Datos	Ausencia del Analista responsable	Existencia de un único responsable de la administración de la B.D.	Ante falla del sistema no hay quien pueda resolver los problemas
		Sistema como aplicación	Malware que ataque la aplicación y los datos bajo su administración.	Ausencia de mecanismos de protección Antimalware en el servidor	Daño a los datos manejados por el sistema o robo de los mismos

Ítem	Nombre	Activo de Información	Amenaza	Vulnerabilidad	Riesgo
		Acceso a Internet	Falta de conexión a Internet	Carencia de línea de contingencia por parte del proveedor o carencia de un proveedor alterno	Usuarios no puedan enviar información al MEF
4	SIAF	Servidor	Fallo en el servidor que aloja la aplicación	Ausencia de Servicios de Mantenimiento y Garantía de los servidores locales	Servidor falle y deje de funcionar
		Base de datos	Fallo en la unidad de almacenamiento que aloja la Base de Datos	Ausencia de Servicios de Mantenimiento y Garantía de las Unidades de Almacenamiento	Unidad de almacenamiento falle, deje de funcionar y haya pérdida de información
		Copias de Respaldo de la Base de Datos	Fallo en la unidad de almacenamiento que aloja las copias de respaldo	Ausencia de Servicios de Mantenimiento y Garantía de las Unidades de Almacenamiento	Restricciones o imposibilidad de obtener las copias de respaldo para la restauración del sistema
		Administrador de la Base de Datos	Ausencia del Analista responsable	Existencia de un único responsable de la administración de la B.D.	Ante falla del sistema no hay quien pueda resolver los problemas
		Sistema como aplicación	Malware que ataque la aplicación y los datos bajo su administración.	Ausencia de mecanismos de protección Antimalware en el servidor	Daño a los datos manejados por el sistema o robo de los mismos
		Acceso a Internet	Falta de conexión a Internet	Carencia de línea de contingencia por parte del proveedor o carencia de un proveedor alterno	Usuarios no puedan enviar información al MEF
5	SIAJ	Servidor	Pérdida de conexión con el Servidor en la nube	Servidor en la nube carece de mecanismos clusterización	El SIAJ deje de funcionar
		Base de datos	Fallo en la unidad de almacenamiento que aloja la Base de Datos	Unidad de almacenamiento en la nube carece de mecanismos clusterización	Unidad de almacenamiento falle, deje de funcionar y haya pérdida de información
		Código fuente del SIAJ	Pérdida del Código fuente o código desactualizado	Indeterminación de la localización de los programas fuente, carencia de bitácora de modificaciones	Pérdida de los programas fuente del STD o contar con versiones desactualizadas de los mismos
		Analista responsable del SIAJ	Ausencia del Analista responsable	Existencia de un único responsable de la administración del SIAJ	Ante falla del sistema no hay quien pueda resolver los problemas

Ítem	Nombre	Activo de Información	Amenaza	Vulnerabilidad	Riesgo
		Documentación del SIAJ	Ausencia de manuales o manuales desactualizados	Ausencia de un repositorio que aloje los manuales actualizados	Pérdida de los manuales o no contar con ellos, cuando estos sean necesarios
		Sistema como aplicación	Malware que ataque la aplicación y los datos bajo su administración.	Ausencia de mecanismos de protección Antimalware en el servidor en la nube	Daño a los datos manejados por el sistema o robo de los mismos
		Acceso a Internet	Falta de conexión a Internet	Carencia de línea de contingencia por parte del proveedor o carencia de un proveedor alterno	Carecer de acceso al SIAJ por parte de los equipos al interior del TC
6	SISPER	Servidor	Fallo en el equipo que aloja la aplicación	Ausencia de Mantenimiento en el equipo que aloja la aplicación	Computadora falle y deje de funcionar
		Base de datos	Fallo en la Base de Datos o corrupción de la data	Ausencia de Mantenimiento en el equipo que aloja la aplicación	Unidad de almacenamiento en la nube falle, deje de funcionar y haya pérdida de información
		Administrador/operador del Sistema	Ausencia del operador del Sistema	Existencia de una sola de la OGDH encargada de operar el SISPER	Ante ausencia del operador no hay quien pueda ejecutar la planilla
		Sistema como aplicación	Malware que ataque la aplicación y los datos bajo su administración.	Ausencia de mecanismos de protección Antimalware en el equipo en que se ejecuta el SISPER	Daño a los datos manejados por el sistema o robo de los mismos
		Acceso a Internet	Falta de conexión a Internet	Carencia de línea de contingencia por parte del proveedor o carencia de un proveedor alterno	No se pueda acceder a la B.D.
7	KOHA	Servidor	Fallo en el equipo que aloja la aplicación	Ausencia de Mantenimiento en el equipo que aloja la aplicación	Computadora falle y deje de funcionar
		Base de datos	Fallo en la Base de Datos o corrupción de la data	Ausencia de Mantenimiento en el equipo que aloja la aplicación	Unidad de almacenamiento en la nube falle, deje de funcionar y haya pérdida de información
		Administrador del Sistema	Ausencia del especialista en la configuración de la aplicación	Existencia de una sola persona capacitada por la BNP en la configuración de la aplicación	Ante ausencia del operador no hay quien pueda ejecutar la planilla

Ítem	Nombre	Activo de Información	Amenaza	Vulnerabilidad	Riesgo
		Sistema como aplicación	Malware que ataque la aplicación y los datos bajo su administración.	Ausencia de mecanismos de protección Antimalware en el servidor que aloja el Koha	Daño a los datos manejados por el sistema o robo de los mismos
		Acceso a Internet	Falta de conexión a Internet	Carencia de línea de contingencia por parte del proveedor o carencia de un proveedor alterno	Ausencia del sistema por parte de los usuarios del Koha
8	**Ventanilla Jurisdiccional**	Servidor	Pérdida de conexión con el Servidor en la nube	Servidor en la nube carece de mecanismos clusterización	La Ventanilla Jurisdiccional deje de funcionar e impida el acceso a cualquier usuario
		Base de datos	Fallo en la unidad de almacenamiento que aloja la Base de Datos	Unidad de almacenamiento en la nube carece de mecanismos clusterización	Unidad de almacenamiento falle, deje de funcionar y haya pérdida de información
		Código fuente de la Ventanilla Jurisdiccional	Pérdida del Código fuente o código desactualizado	Indeterminación de la localización de los programas fuente, carencia de bitácora de modificaciones	Pérdida de los programas fuente de la Ventanilla Jurisdiccional o contar con versiones desactualizadas de los mismos
		Analista responsable del Desarrollo y Mantenimiento de la Ventanilla Jurisdiccional	Ausencia del Analista responsable	Existencia de un único responsable del Desarrollo y Mantenimiento de la Ventanilla Jurisdiccional	Ante falla del sistema no hay quien pueda resolver los problemas
		Documentación de la Ventanilla Jurisdiccional	Ausencia de manuales o manuales desactualizados	Ausencia de un repositorio que aloje los manuales actualizados	Pérdida de los manuales o no contar con ellos, cuando estos sean necesarios
		Sistema como aplicación	Malware que ataque la aplicación y los datos bajo su administración.	Ausencia de mecanismos de protección Antimalware en el servidor en la nube	Daño a los datos manejados por el sistema o robo de los mismos
		Acceso a Internet	Falta de conexión a Internet	Carencia de línea de contingencia por parte del proveedor o carencia de un proveedor alterno	Carecer de acceso al STD por parte de los equipos al interior del TC
9	**Jurisprudencia Sistematizada**	Servidor	Pérdida de conexión con el Servidor en la nube	Servidor en la nube carece de mecanismos clusterización	La Jurisprudencia Sistematizada deje de funcionar e impida el acceso a cualquier usuario

Ítem	Nombre	Activo de Información	Amenaza	Vulnerabilidad	Riesgo
		Base de datos	Fallo en la unidad de almacenamiento que aloja la Base de Datos	Unidad de almacenamiento en la nube carece de mecanismos clusterización	Unidad de almacenamiento falle, deje de funcionar y haya pérdida de información
		Código fuente de la Jurisprudencia Sistematizada	Pérdida del Código fuente o código desactualizado	Indeterminación de la localización de los programas fuente, carencia de bitácora de modificaciones	Pérdida de los programas fuente de la Ventanilla Jurisdiccional o contar con versiones desactualizadas de los mismos
		Analista responsable del Desarrollo y Mantenimiento de la Jurisprudencia Sistematizada	Ausencia del Analista responsable	Existencia de un único responsable del Desarrollo y Mantenimiento de la Jurisprudencia Sistematizada	Ante falla del sistema no hay quien pueda resolver los problemas
		Documentación de la Jurisprudencia Sistematizada	Ausencia de manuales o manuales desactualizados	Ausencia de un repositorio que aloje los manuales actualizados	Pérdida de los manuales o no contar con ellos, cuando estos sean necesarios
		Sistema como aplicación	Malware que ataque la aplicación y los datos bajo su administración.	Ausencia de mecanismos de protección Antimalware en el servidor en la nube	Daño a los datos manejados por el sistema o robo de los mismos
		Acceso a Internet	Falta de conexión a Internet	Carencia de línea de contingencia por parte del proveedor o carencia de un proveedor alterno	Carecer de acceso al STD por parte de los equipos al interior del TC
10	**Correo Electrónico**	Servidor de correo	Pérdida de conexión con el proveedor del Servicio	Pérdida de conexión con el servidor de correos	Los usuarios dejen de tener acceso a sus cuentas de correo electrónico
		Analista responsable de la Administración del conjunto de herramientas colaborativas	Ausencia del Analista responsable	Existencia de un único responsable de la Administración del contrato con el distribuidor autorizado	Ante falla del sistema no hay quien pueda resolver los problemas
		Acceso a Internet	Falta de conexión a Internet	Carencia de línea de contingencia por parte del proveedor o carencia de un proveedor alterno	Los usuarios que acceden desde el TC no pueden abrir sus respectivos corres electrónicos

Ítem	Nombre	Activo de Información	Amenaza	Vulnerabilidad	Riesgo
11	**Drives**	Servidor de alojamiento	Pérdida de conexión con el proveedor del Servicio	Pérdida de conexión con el servidor de almacenamiento de archivos	Los usuarios que acceden desde el TC no pueden abrir sus respectivos Drives
		Analista responsable de la Administración del conjunto de herramientas colaborativas	Ausencia del Analista responsable	Existencia de un único responsable de la Administración del contrato con el distribuidor autorizado	Ante falla del sistema no hay quien pueda resolver los problemas
		Acceso a Internet	Falta de conexión a Internet	Carencia de línea de contingencia por parte del proveedor o carencia de un proveedor alterno	Los usuarios que acceden desde el TC no pueden acceder a su información alojada en sus Drives
12	**Portal Web Institucional**	Servidor	Pérdida de conexión con el Servidor en la nube	Servidor en la nube carece de mecanismos clusterización	El portal web deje de funcionar e impida el acceso a cualquier usuario
		Base de datos	Fallo en la unidad de almacenamiento que aloja la Base de Datos	Unidad de almacenamiento en la nube carece de mecanismos clusterización	Unidad de almacenamiento falle, deje de funcionar y haya pérdida de información
		Copia de respaldo de la totalidad del contenido de la página web	Pérdida de la información y la configuración del Portal Web Institucional	Carencia de copias de respaldo que permitan restaurar el portal web	Que el Portal web quede fuera de servicio
		Analista responsable del Desarrollo y Mantenimiento del Portal Web	Ausencia del Analista responsable	Existencia de un único responsable del Desarrollo y Mantenimiento del Portal Web	Ante falla del sistema no hay quien pueda resolver los problemas
		Documentación del Portal Web	Ausencia de manuales o manuales desactualizados	Ausencia de un repositorio que aloje los manuales actualizados	Pérdida de los manuales o no contar con ellos, cuando estos sean necesarios
		Sistema como aplicación	Malware que ataque la aplicación y los datos bajo su administración.	Ausencia de certificados de seguridad tipo SSL para el dominio	Daño al contenido de la página web (Defacement), o caída del portal por ataques DoS o DDoS

Item	Nombre	Activo de Información	Amenaza	Vulnerabilidad	Riesgo
		Acceso a Internet	Falta de conexión a Internet	Carencia de línea de contingencia por parte del proveedor o carencia de un proveedor alterno	Carecer de acceso al Portal Web por parte de los equipos al interior del TC
Servicios ofrecidos por terceros y administrados por la OTI					
13	**Acceso a Internet y Seguridad perimetral de red**	Servicio de acceso a Internet con Firewall en ISP	Servicio Tercerizado		
14	**Herramientas colaborativas**	Servicio provisto por Google Inc.	Servicio Tercerizado		
15	**Alojamiento en la nube**	Alojamiento en la nube	Servicio Tercerizado		

Anexo IV

Cuadro de Probabilidades, Impactos y Nivel de Riesgo para cada uno de los riesgos identificados

Ítem	Nombre	Activo de Información	Amenaza	Vulnerabilidad	Riesgo	Prob.	Imp.	Nivel de Riesgo
Servicios ofrecidos y administrados por la OTI								
1	SIGE	Servidor	Fallo en el servidor que aloja la aplicación	Ausencia de Servicios de Mantenimiento y Garantía de los servidores locales	Servidor falle y deje de funcionar	2	5	Alto
		Base de datos	Fallo en la unidad de almacenamiento que aloja la Base de Datos	Ausencia de Servicios de Mantenimiento y Garantía de las Unidades de Almacenamiento	Unidad de almacenamiento falle, deje de funcionar y haya pérdida de información	2	5	Alto
		Código fuente del SIGE	Pérdida del Código fuente o código desactualizado	Indeterminación de la localización de los programas fuente, carencia de bitácora de modificaciones	Pérdida de los programas fuente del SIGE o contar con versiones desactualizadas de los mismos	2	5	Alto
		Copias de Respaldo de la Base de Datos	Fallo en la unidad de almacenamiento que aloja las copias de respaldo	Ausencia de Servicios de Mantenimiento y Garantía de las Unidades de Almacenamiento	Restricciones o imposibilidad de obtener las copias de respaldo para la restauración del sistema	2	5	Alto
		Analista responsable del SIGE	Ausencia del Analista responsable	Existencia de un único responsable de la administración del SIGE	Ante falla del sistema no hay quien pueda resolver los problemas	2	4	Alto
		Documentación del SIGE	Ausencia de manuales o manuales desactualizados	Ausencia de un repositorio que aloje los manuales actualizados	Pérdida de los manuales o no contar con ellos, cuando estos sean necesarios	2	3	Moderado

Ítem	Nombre	Activo de Información	Amenaza	Vulnerabilidad	Riesgo	Prob.	Imp.	Nivel de Riesgo
		Sistema como aplicación	Malware que ataque la aplicación y los datos bajo su administración.	Ausencia de mecanismos de protección Antimalware en el servidor	Daño a los datos manejados por el sistema o robo de los mismos	3	4	Alto
		Acceso a Internet	Falta de conexión a Internet	Carencia de línea de contingencia por parte del proveedor o carencia de un proveedor alterno	Usuarios fuera de las instalaciones del TC no puedan acceder al SIGE	2	4	Alto
2	STD	Servidor	Pérdida de conexión con el Servidor en la nube	Servidor en la nube carece de mecanismos clusterización	El STD deje de funcionar	2	4	Alto
		Base de datos	Fallo en la unidad de almacenamiento que aloja la Base de Datos	Unidad de almacenamiento en la nube carece de mecanismos clusterización	Unidad de almacenamiento falle, deje de funcionar y haya pérdida de información	2	5	Alto
		Código fuente del STD	Pérdida del Código fuente o código desactualizado	Indeterminación de la localización de los programas fuente, carencia de bitácora de modificaciones	Pérdida de los programas fuente del STD o contar con versiones desactualizadas de los mismos	3	4	Alto
		Analista responsable del STD	Ausencia del Analista responsable	Existencia de un único responsable de la administración del STD	Ante falla del sistema no hay quien pueda resolver los problemas	2	4	Alto
		Documentación del STD	Ausencia de manuales o manuales desactualizados	Ausencia de un repositorio que aloje los manuales actualizados	Pérdida de los manuales o no contar con ellos, cuando estos sean necesarios	2	3	Moderado
		Sistema como aplicación	Malware que ataque la aplicación y los datos bajo su administración.	Ausencia de mecanismos de protección Antimalware en el servidor en la nube	Daño a los datos manejados por el sistema o robo de los mismos	2	4	Alto

Ítem	Nombre	Activo de Información	Amenaza	Vulnerabilidad	Riesgo	Prob.	Imp.	Nivel de Riesgo
		Acceso a Internet	Falta de conexión a Internet	Carencia de línea de contingencia por parte del proveedor o carencia de un proveedor alterno	Carecer de acceso al STD por parte de los equipos al interior del TC	2	3	Moderado
3	SIGA	Servidor	Fallo en el servidor que aloja la aplicación	Ausencia de Servicios de Mantenimiento y Garantía de los servidores locales	Servidor falle y deje de funcionar	2	5	Alto
		Base de datos	Fallo en la unidad de almacenamiento que aloja la Base de Datos	Ausencia de Servicios de Mantenimiento y Garantía de las Unidades de Almacenamiento	Unidad de almacenamiento falle, deje de funcionar y haya pérdida de información	2	5	Alto
		Copias de Respaldo de la Base de Datos	Fallo en la unidad de almacenamiento que aloja las copias de respaldo	Ausencia de Servicios de Mantenimiento y Garantía de las Unidades de Almacenamiento	Restricciones o imposibilidad de obtener las copias de respaldo para la restauración del sistema	2	5	Alto
		Administrador de la Base de Datos	Ausencia del Analista responsable	Existencia de un único responsable de la administración de la B.D.	Ante falla del sistema no hay quien pueda resolver los problemas	2	4	Alto
		Sistema como aplicación	Malware que ataque la aplicación y los datos bajo su administración.	Ausencia de mecanismos de protección Antimalware en el servidor	Daño a los datos manejados por el sistema o robo de los mismos	2	4	Alto
		Acceso a Internet	Falta de conexión a Internet	Carencia de linea de cotingencia por parte del proveedor o carencia de un proveedor alterno	Usuarios no puedan enviar información al MEF	2	4	Alto

Item	Nombre	Activo de Información	Amenaza	Vulnerabilidad	Riesgo	Prob.	Imp.	Nivel de Riesgo
4	SIAF	Servidor	Fallo en el servidor que aloja la aplicación	Ausencia de Servicios de Mantenimiento y Garantía de los servidores locales	Servidor falle y deje de funcionar	2	5	Alto
		Base de datos	Fallo en la unidad de almacenamiento que aloja la Base de Datos	Ausencia de Servicios de Mantenimiento y Garantía de las Unidades de Almacenamiento	Unidad de almacenamiento falle, deje de funcionar y haya pérdida de información	2	5	Alto
		Copias de Respaldo de la Base de Datos	Fallo en la unidad de almacenamiento que aloja las copias de respaldo	Ausencia de Servicios de Mantenimiento y Garantía de las Unidades de Almacenamiento	Restricciones o imposibilidad de obtener las copias de respaldo para la restauración del sistema	2	5	Alto
		Administrador de la Base de Datos	Ausencia del Analista responsable	Existencia de un único responsable de la administración de la B.D.	Ante falla del sistema no hay quien pueda resolver los problemas	2	4	Alto
		Sistema como aplicación	Malware que ataque la aplicación y los datos bajo su administración.	Ausencia de mecanismos de protección Antimalware en el servidor	Daño a los datos manejados por el sistema o robo de los mismos	2	4	Alto
		Acceso a Internet	Falta de conexión a Internet	Carencia de línea de contingencia por parte del proveedor o carencia de un proveedor alterno	Usuarios no puedan enviar información al MEF	2	4	Alto
5	SIAJ	Servidor	Pérdida de conexión con el Servidor en la nube	Servidor en la nube carece de mecanismos clusterización	El SIAJ deje de funcionar	2	4	Alto
		Base de datos	Fallo en la unidad de almacenamiento que aloja la Base de Datos	Unidad de almacenamiento en la nube carece de mecanismos clusterización	Unidad de almacenamiento falle, deje de funcionar y haya pérdida de información	2	5	Alto

Ítem	Nombre	Activo de Información	Amenaza	Vulnerabilidad	Riesgo	Prob.	Imp.	Nivel de Riesgo
		Código fuente del SIAJ	Pérdida del Código fuente o código desactualizado	Indeterminación de la localización de los programas fuente, carencia de bitácora de modificaciones	Pérdida de los programas fuente del STD o contar con versiones desactualizadas de los mismos	2	4	Alto
		Analista responsable del SIAJ	Ausencia del Analista responsable	Existencia de un único responsable de la administración del SIAJ	Ante falla del sistema no hay quien pueda resolver los problemas	2	4	Alto
		Documentación del SIAJ	Ausencia de manuales o manuales desactualizados	Ausencia de un repositorio que aloje los manuales actualizados	Pérdida de los manuales o no contar con ellos, cuando estos sean necesarios	2	3	Moderado
		Sistema como aplicación	Malware que ataque la aplicación y los datos bajo su administración.	Ausencia de mecanismos de protección Antimalware en el servidor en la nube	Daño a los datos manejados por el sistema o robo de los mismos	2	4	Alto
		Acceso a Internet	Falta de conexión a Internet	Carencia de línea de contingencia por parte del proveedor o carencia de un proveedor alterno	Carecer de acceso al SIAJ por parte de los equipos al interior del TC	2	4	Alto
6	SISPER	Servidor	Fallo en el equipo que aloja la aplicación	Ausencia de Mantenimiento en el equipo que aloja la aplicación	Computadora falle y deje de funcionar	2	5	Alto
		Base de datos	Fallo en la Base de Datos o corrupción de la data	Ausencia de Mantenimiento en el equipo que aloja la aplicación	Unidad de almacenamiento en la nube falle, deje de funcionar y haya pérdida de información	2	5	Alto
		Administrador/operador del Sistema	Ausencia del operador del Sistema	Existencia de una sola de la OGDH encargada de operar el SISPER	Ante ausencia del operador no hay quien pueda ejecutar la planilla	2	3	Moderado

Ítem	Nombre	Activo de Información	Amenaza	Vulnerabilidad	Riesgo	Prob.	Imp.	Nivel de Riesgo
		Sistema como aplicación	Malware que ataque la aplicación y los datos bajo su administración.	Ausencia de mecanismos de protección Antimalware en el equipo en que se ejecuta el SISPER	Daño a los datos manejados por el sistema o robo de los mismos	2	4	Alto
		Acceso a Internet	Falta de conexión a Internet	Carencia de línea de contingencia por parte del proveedor o carencia de un proveedor alterno	No se pueda acceder a la B.D.	2	4	Alto
7	KOHA	Servidor	Fallo en el equipo que aloja la aplicación	Ausencia de Mantenimiento en el equipo que aloja la aplicación	Computadora falle y deje de funcionar	2	5	Alto
		Base de datos	Fallo en la Base de Datos o corrupción de la data	Ausencia de Mantenimiento en el equipo que aloja la aplicación	Unidad de almacenamiento en la nube falle, deje de funcionar y haya pérdida de información	2	5	Alto
		Administrador del Sistema	Ausencia del especialista en la configuración de la aplicación	Existencia de una sola persona capacitada por la BNP en la configuración de la aplicación	Ante ausencia del operador no hay quien pueda ejecutar la planilla	2	3	Moderado
		Sistema como aplicación	Malware que ataque la aplicación y los datos bajo su administración.	Ausencia de mecanismos de protección Antimalware en el servidor que aloja el Koha	Daño a los datos manejados por el sistema o robo de los mismos	2	4	Alto
		Acceso a Internet	Falta de conexión a Internet	Carencia de línea de contingencia por parte del proveedor o carencia de un proveedor alterno	Ausencia del sistema por parte de los usuarios del Koha	2	3	Moderado

Ítem	Nombre	Activo de Información	Amenaza	Vulnerabilidad	Riesgo	Prob.	Imp.	Nivel de Riesgo
8	**Ventanilla Jurisdiccional**	Servidor	Pérdida de conexión con el Servidor en la nube	Servidor en la nube carece de mecanismos clusterización	La Ventanilla Jurisdiccional deje de funcionar e impida el acceso a cualquier usuario	2	4	Alto
		Base de datos	Fallo en la unidad de almacenamiento que aloja la Base de Datos	Unidad de almacenamiento en la nube carece de mecanismos clusterización	Unidad de almacenamiento falle, deje de funcionar y haya pérdida de información	2	5	Alto
		Código fuente de la Ventanilla Jurisdiccional	Pérdida del Código fuente o código desactualizado	Indeterminación de la localización de los programas fuente, carencia de bitácora de modificaciones	Pérdida de los programas fuente de la Ventanilla Jurisdiccional o contar con versiones desactualizadas de los mismos	2	5	Alto
		Analista responsable del Desarrollo y Mantenimiento de la Ventanilla Jurisdiccional	Ausencia del Analista responsable	Existencia de un único responsable del Desarrollo y Mantenimiento de la Ventanilla Jurisdiccional	Ante falla del sistema no hay quien pueda resolver los problemas	2	4	Alto
		Documentación de la Ventanila Jurisdiccional	Ausencia de manuales o manuales desactualizados	Ausencia de un repositorio que aloje los manuales actualizados	Pérdida de los manuales o no contar con ellos, cuando estos sean necesarios	2	3	Moderado
		Sistema como aplicación	Malware que ataque la aplicación y los datos bajo su administración.	Ausencia de mecanismos de protección Antimalware en el servidor en la nube	Daño a los datos manejados por el sistema o robo de los mismos	2	4	Alto
		Acceso a Internet	Falta de conexión a Internet	Carencia de línea de contingencia por parte del proveedor o carencia de un proveedor alterno	Carecer de acceso al STD por parte de los equipos al interior del TC	2	3	Moderado

Ítem	Nombre	Activo de Información	Amenaza	Vulnerabilidad	Riesgo	Prob.	Imp.	Nivel de Riesgo
9	**Jurisprudencia Sistematizada**	Servidor	Pérdida de conexión con el Servidor en la nube	Servidor en la nube carece de mecanismos clusterización	La Jurisprudencia Sistematizada deje de funcionar e impida el acceso a cualquier usuario	2	4	Alto
		Base de datos	Fallo en la unidad de almacenamiento que aloja la Base de Datos	Unidad de almacenamiento en la nube carece de mecanismos clusterización	Unidad de almacenamiento falle, deje de funcionar y haya pérdida de información	2	5	Alto
		Código fuente de la Jurisprudencia Sistematizada	Pérdida del Código fuente o código desactualizado	Indeterminación de la localización de los programas fuente, carencia de bitácora de modificaciones	Pérdida de los programas fuente de la Ventanilla Jurisdiccional o contar con versiones desactualizadas de los mismos	2	5	Alto
		Analista responsable del Desarrollo y Mantenimiento de la Jurisprudencia Sistematizada	Ausencia del Analista responsable	Existencia de un único responsable del Desarrollo y Mantenimiento de la Jurisprudencia Sistematizada	Ante falla del sistema no hay quien pueda resolver los problemas	2	4	Alto
		Documentación de la Jurisprudencia Sistematizada	Ausencia de manuales o manuales desactualizados	Ausencia de un repositorio que aloje los manuales actualizados	Pérdida de los manuales o no contar con ellos, cuando estos sean necesarios	2	3	Moderado
		Sistema como aplicación	Malware que ataque la aplicación y los datos bajo su administración.	Ausencia de mecanismos de protección Antimalware en el servidor en la nube	Daño a los datos manejados por el sistema o robo de los mismos	2	4	Alto
		Acceso a Internet	Falta de conexión a Internet	Carencia de línea de contingencia por parte del proveedor o carencia de un proveedor alterno	Carecer de acceso al STD por parte de los equipos al interior del TC	2	3	Moderado

Ítem	Nombre	Activo de Información	Amenaza	Vulnerabilidad	Riesgo	Prob.	Imp.	Nivel de Riesgo
10	**Correo Electrónico**	Servidor de correo	Pérdida de conexión con el proveedor del Servicio	Pérdida de conexión con el servidor de correos	Los usuarios dejen de tener acceso a sus cuentas de correo electrónico	2	4	Alto
		Analista responsable de la Administración del conjunto de herramientas colaborativas	Ausencia del Analista responsable	Existencia de un único responsable de la Administración del contrato con el distribuidor autorizado	Ante falla del sistema no hay quien pueda resolver los problemas	2	4	Alto
		Acceso a Internet	Falta de conexión a Internet	Carencia de línea de contingencia por parte del proveedor o carencia de un proveedor alterno	Los usuarios que acceden desde el TC no pueden abrir sus respectivos correos electrónicos	2	4	Alto
11	**Drives**	Servidor de alojamiento	Pérdida de conexión con el proveedor del Servicio	Pérdida de conexión con el servidor de almacenamiento de archivos	Los usuarios que acceden desde el TC no pueden abrir sus respectivos Drives	2	4	Alto
		Analista responsable de la Administración del conjunto de herramientas colaborativas	Ausencia del Analista responsable	Existencia de un único responsable de la Administración del contrato con el distribuidor autorizado	Ante falla del sistema no hay quien pueda resolver los problemas	1	4	Moderado
		Acceso a Internet	Falta de conexión a Internet	Carencia de línea de contingencia por parte del proveedor o carencia de un proveedor alterno	Los usuarios que acceden desde el TC no pueden acceder a su información alojada en sus Drives	1	4	Moderado
12	**Portal Web Institucional**	Servidor	Pérdida de conexión con el Servidor en la nube	Servidor en la nube carece de mecanismos clusterización	El portal web deje de funcionar e impida el acceso a cualquier usuario	2	5	Alto

Ítem	Nombre	Activo de Información	Amenaza	Vulnerabilidad	Riesgo	Prob.	Imp.	Nivel de Riesgo
		Base de datos	Fallo en la unidad de almacenamiento que aloja la Base de Datos	Unidad de almacenamiento en la nube carece de mecanismos clusterización	Unidad de almacenamiento falle, deje de funcionar y haya pérdida de información	2	5	Alto
		Copia de respaldo de la totalidad del contenido de la página web	Pérdida de la información y la configuración del Portal Web Institucional	Carencia de copias de respaldo que permitan restaurar el portal web	Que el Portal web quede fuera de servicio	2	4	Alto
		Analista responsable del Desarrollo y Mantenimiento del Portal Web	Ausencia del Analista responsable	Existencia de un único responsable del Desarrollo y Mantenimiento delPortal Web	Ante falla del sistema no hay quien pueda resolver los problemas	2	4	Alto
		Documentación del Portal Web	Ausencia de manuales o manuales desactualizados	Ausencia de un repositorio que aloje los manuales actualizados	Pérdida de los manuales o no contar con ellos, cuando estos sean necesarios	1	3	Bajo
		Sistema como aplicación	Malware que ataque la aplicación y los datos bajo su administración.	Ausencia de certificados de seguridad tipo SSL para el dominio	Daño al contenido de la página web (Defacement), o caída del portal por ataques DoS o DDoS	2	5	Alto
		Acceso a Internet	Falta de conexión a Internet	Carencia de línea de contingencia por parte del proveedor o carencia de un proveedor alterno	Carecer de acceso al Portal Web por parte de los equipos al interior del TC	2	4	Alto
Servicios ofrecidos por terceros y administrados por la OTI								

Ítem	Nombre	Activo de Información	Amenaza	Vulnerabilidad	Riesgo	Prob.	Imp.	Nivel de Riesgo
13	**Acceso a Internet y Seguridad perimetral de red**	Servicio de acceso a Internet con Firewall en ISP	Servicio Tercerizado	El proveedor no tenga conexiones de contingencia	Carecer de Acceso a Internet y servicios basados en el servicio	1	5	Moderado
14	**Herramientas colaborativas**	Servicio provisto por Google Inc.	Servicio Tercerizado	Haya paralización en los servicios provistos por Google Inc.	Falla en el aprovisionamiento del servicio	1	5	Moderado
15	**Alojamiento en la nube**	Alojamiento en la nube	Servicio Tercerizado	Caída o Ataque a los servidore de alojamiento	Falla en el aprovisionamiento del servicio	2	5	Alto

Anexo V

Aplicación de los controles de la "NTP-ISO/IEC 27001:2014" a los riesgos que están sometidos los activos de Información relacionados con los servicios Críticos del Tribunal Constitucional, que afectaría la continuidad operativa institucional

Ítem	Nombre	Riesgo	Prob.	Imp.	Nivel de Riesgo	Controi	Control NTP-ISO/IEC 27001:2014	Código NTP-ISO-27001
Servicios ofrecidos y administrados por la OTI								
1	SIGE	Servidor falle y deje de funcionar	2	5	Alto	Establecer contratos de mantenimiento y garantía	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
		Unidad de almacenamiento falle, deje de funcionar y haya pérdida de información	2	5	Alto	Establecer contratos de mantenimiento y garantía para las undades de almacenamiento	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
		Pérdida de los programas fuente del SIGE o contar con versiones desactualizadas de los mismos	2	5	Alto	Establecer un repositorio en la nube que aloje las versiones actualizadas de los programas fuente del SIGE	Copias de respaldo de la información, del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.	A.12.3.1
		Restricciones o imposibilidad de obtener las copias de respaldo para la restauración del sistema	2	5	Alto	Establecer contratos de mantenimiento y garantía para las undades de almacenamiento	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3

Ítem	Nombre	Riesgo	Prob.	Imp.	Nivel de Riesgo	Control	Control NTP-ISO/IEC 27001:2014	Código NTP-ISO-27001
		Ante falla del sistema no hay quien pueda resolver los problemas	2	4	Alto	Solicitar a la OGDH la contratación de un analista junior que se encuentre preparado para actuar en ausencia del analista principal	Los acuerdos contractuales con los empleados y contratistas deben estipular responsabilidades de éstos y de la organización respecto de la seguridad de la información.	A.7.1.2
		Pérdida delos manuales o no contar con ellos, cuando estos sean necesarios	2	3	Moderado	Establecer un repositorio en la nube que aloje las versiones actualizadas de los manuales actualizados del SIGE	Los cambios a la provisión de servicios por parte de proveedores, incluyendo el mantenimiento y mejoramiento de políticas, procedimientos y controles existentes de seguridad de la información deben ser gestionados tomando en cuenta la criticidad de la información del negocio, sistemas y procesos involucrados y una reevaluación de riesgos.	A.15.2.2
		Daño a los datos manejados por el sistema o robo de los mismos	3	4	Alto	Disponer la actualización permanente de los "parches" de seguridad de los servidores. Instalar programas antivirales tanto en el servidor como en los End Points	Información sobre vulnerabilidades técnicas de los sistemas de información utilizados debe ser obtenida de manera oportuna, la exposición de la organización a dichas vulnerabilidades debe ser evaluada y las medidas apropiadas deben ser tomadas para resolver el riesgo asociado.	A.12.6.1
		Usuarios fuera de las instalaciones del TC no puedan acceder al SIGE	2	4	Alto	Mejorar los SLAs con el proveedor para evitar ausencia de conexión	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3

Ítem	Nombre	Riesgo	Prob.	Imp.	Nivel de Riesgo	Control	Control NTP-ISO/IEC 27001:2014	Código NTP-ISO-27001
2	STD	El STD deje de funcionar	2	4	Alto	Mejorar los contratos de alojamiento en la nube que caídas en los servidores	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
		Unidad de almacenamiento falle, deje de funcionar y haya pérdida de información	2	5	Alto	Considerar en los contratos de alojamiento en la nube SLAs que mantengan deduplicada la información	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
		Pérdida de los programas fuente del STD o contar con versiones desactualizadas de los mismos	3	4	Alto	Establecer un repositorio en la nube que aloje las versiones actualizadas de los programas fuente del STD	Copias de respaldo de la información, del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.	A.12.3.1
		Ante falla del sistema no hay quien pueda resolver los problemas	2	4	Alto	Solicitar a la OGDH la contratación de un analista junior que se encuentre preparado para actuar en ausencia del analista principal	Los acuerdos contractuales con los empleados y contratistas deben estipular responsabilidades de éstos y de la organización respecto de la seguridad de la información.	A.7.1.2
		Pérdida delos manuales o no contar con ellos, cuando estos sean necesarios	2	3	Moderado	Establecer un repositorio en la nube que aloje las versiones actualizadas de los manuales actualizados del STD	Copias de respaldo de la información, del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.	A.12.3.1

Ítem	Nombre	Riesgo	Prob.	Imp.	Nivel de Riesgo	Control	Control NTP-ISO/IEC 27001:2014	Código NTP-ISO-27001
		Daño a los datos manejados por el sistema o robo de los mismos	2	4	Alto	Considerar en el contrato de alojamiento mecanismos de protección como WAF Y Licencias DAST y SAST para el validación de las aplicaciones que se ejecutarán en esos ambientes	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
		Carecer de acceso al STD por parte de los equipos al interior del TC	2	3	Moderado	Mejorar los SLAs con el proveedor para evitar ausencia de conexión	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
3	SIGA	Servidor falle y deje de funcionar	2	5	Alto	Establecer contratos de mantenimiento y garantía	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
		Unidad de almacenamiento falle, deje de funcionar y haya pérdida de información	2	5	Alto	Establecer contratos de mantenimiento y garantía para las unidades de almacenamiento	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3

Ítem	Nombre	Riesgo	Prob.	Imp.	Nivel de Riesgo	Control	Control NTP-ISO/IEC 27001:2014	Código NTP-ISO-27001
		Restricciones o imposibilidad de obtener las copias de respaldo para la restauración del sistema	2	5	Alto	Establecer contratos de mantenimiento y garantía para las unidades de almacenamiento}	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
		Ante falla del sistema no hay quien pueda resolver los problemas	2	4	Alto	Solicitar a la OGDH la contratación de un analista junior que se encuentre preparado para actuar en ausencia del analista principal	Los acuerdos contractuales con los empleados y contratistas deben estipular responsabilidades de éstos y de la organización respecto de la seguridad de la información.	A.7.1.2
		Daño a los datos manejados por el sistema o robo de los mismos	2	4	Alto	Disponer la actualización permanente de los "parches" de seguridad de los servidores. Instalar programas antivirales tanto en el servidor como en los End Points	Información sobre vulnerabilidades técnicas de los sistemas de información utilizados debe ser obtenida de manera oportuna, la exposición de la organización a dichas vulnerabilidades debe ser evaluada y las medidas apropiadas deben ser tomadas para resolver el riesgo asociado.	A.12.6.1
		Usuarios no puedan enviar información al MEF	2	4	Alto	Mejorar los SLAs con el proveedor para evitar ausencia de conexión	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3

Ítem	Nombre	Riesgo	Prob.	Imp.	Nivel de Riesgo	Control	Control NTP-ISO/IEC 27001:2014	Código NTP-ISO-27001
4	SIAF	Servidor falle y deje de funcionar	2	5	Alto	Establecer contratos de mantenimiento y garantía	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
		Unidad de almacenamiento falle, deje de funcionar y haya pérdida de información	2	5	Alto	Establecer contratos de mantenimiento y garantía para las undades de almacenamiento	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
		Restricciones o imposibilidad de obtener las copias de respaldo para la restauración del sistema	2	5	Alto	Establecer contratos de mantenimiento y garantía para las undades de almacenamiento	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
		Ante falla del sistema no hay quien pueda resolver los problemas	2	4	Alto	Solicitar a la OGDH la contratación de un analista junior que se encuentre preparado para actuar en ausencia del analista principal	Los acuerdos contractuales con los empleados y contratistas deben estipular responsabilidades de éstos y de la organización respecto de la seguridad de la información.	A.7.1.2

Ítem	Nombre	Riesgo	Prob.	Imp.	Nivel de Riesgo	Control	Control NTP-ISO/IEC 27001:2014	Código NTP-ISO-27001
		Daño a los datos manejados por el sistema o robo de los mismos	2	4	Alto	Disponer la actualización permanente de los "parches" de seguridad de los servidores. Instalar programas antivirales tanto en el servidor como en los End Points	Información sobre vulnerabilidades técnicas de los sistemas de información utilizados debe ser obtenida de manera oportuna, la exposición de la organización a dichas vulnerabilidades debe ser evaluada y las medidas apropiadas deben ser tomadas para resolver el riesgo asociado.	A.12.6.1
		Usuarios no puedan enviar información al MEF	2	4	Alto	Mejorar los SLAs con el proveedor para evitar ausencia de conexión	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
5	SIAJ	El SIAJ deje de funcionar	2	4	Alto	Mejorar los contratos de alojamiento en la nube que caídas en los servidores	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
		Unidad de almacenamiento falle, deje de funcionar y haya pérdida de información	2	5	Alto	Considerar en los contratos de alojamiento en la nube SLAs que mantengan deduplicada la información	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3

Ítem	Nombre	Riesgo	Prob.	Imp.	Nivel de Riesgo	Controi	Control NTP-ISO/IEC 27001:2014	Código NTP-ISO-27001
		Pérdida de los programas fuente del STD o contar con versiones desactualizadas de los mismos	2	4	Alto	Establecer un repositorio en la nube que aloje las versiones actualizadas de los programas fuente del STD	Copias de respaldo de la información, del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.	A.12.3.1
		Ante falla del sistema no hay quien pueda resolver los problemas	2	4	Alto	Solicitar a la OGDH la contratación de un analista junior que se encuentre preparado para actuar en ausencia del analista principal	Los acuerdos contractuales con los empleados y contratistas deben estipular responsabilidades de éstos y de la organización respecto de la seguridad de la información.	A.7.1.2
		Pérdida delos manuales o no contar con ellos, cuando estos sean necesarios	2	3	Moderado	Establecer un repositorio en la nube que aloje las versiones actualizadas de los manuales actualizados del STD	Copias de respaldo de la información, del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.	A.12.3.1
		Daño a los datos manejados por el sistema o robo de los mismos	2	4	Alto	Considerar en el contrato de alojamiento mecanismos de protección como WAF Y Licencias DAST y SAST para el validación de las aplicaciones que se ejecutarán en esos ambientes	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
		Carecer de acceso al SIAJ por parte de los equipos al interior del TC	2	4	Alto	Mejorar los SLAs con el proveedor para evitar ausencia de conexión	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3

Ítem	Nombre	Riesgo	Prob.	Imp.	Nivel de Riesgo	Controi	Control NTP-ISO/IEC 27001:2014	Código NTP-ISO-27001
6	SISPER	Computadora falle y deje de funcionar	2	5	Alto	Establecer contratos de mantenimiento y garantía, tener un equipo disponible de reemplazo	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
		Unidad de almacenamiento en la nube falle, deje de funcionar y haya pérdida de información	2	5	Alto	Mantener copia de la B.D. de planillas en otro respositorio	Copias de respaldo de la información, del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.	A.12.3.1
		Ante ausencia del operador no hay quien pueda ejecutar la planilla	2	3	Moderado	Solicitar a la OGDH la contratación de un analista junior que se encuentre preparado para actuar en ausencia del analista principal	Los acuerdos contractuales con los empleados y contratistas deben estipular responsabilidades de éstos y de la organización respecto de la seguridad de la información.	A.7.1.2
		Daño a los datos manejados por el sistema o robo de los mismos	2	4	Alto	Disponer la actualización permanente de los "parches" de seguridad de los equipos. Instalar programas antivirales en los End Points	Información sobre vulnerabilidades técnicas de los sistemas de información utilizados debe ser obtenida de manera oportuna, la exposición de la organización a dichas vulnerabilidades debe ser evaluada y las medidas apropiadas deben ser tomadas para resolver el riesgo asociado.	A.12.6.1
		No se pueda acceder a la B.D.	2	4	Alto	Mejorar los SLAs con el proveedor para evitar ausencia de conexión	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3

Ítem	Nombre	Riesgo	Prob.	Imp.	Nivel de Riesgo	Control	Control NTP-ISO/IEC 27001:2014	Código NTP-ISO-27001
7	KOHA	Computadora falle y deje de funcionar	2	5	Alto	Establecer contratos de mantenimiento y garantía, tener un equipo disponible de reemplazo	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
		Unidad de almacenamiento en la nube falle, deje de funcionar y haya pérdida de información	2	5	Alto	Mantener copia de la B.D. de planillas en otro respositorio	Copias de respaldo de la información, del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.	A.12.3.1
		Ante ausencia del operador no hay quien pueda ejecutar la planilla	2	3	Moderado	Pedir a la BNP capacitar a otra persona en la configuración y mantenimiento del Koha	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
		Daño a los datos manejados por el sistema o robo de los mismos	2	4	Alto	Disponer la actualización permanente de los "parches" de seguridad de los equipos. Instalar programas antivirales en los End Points	Información sobre vulnerabilidades técnicas de los sistemas de información utilizados debe ser obtenida de manera oportuna, la exposición de la organización a dichas vulnerabilidades debe ser evaluada y las medidas apropiadas deben ser tomadas para resolver el riesgo asociado.	A.12.6.1

Ítem	Nombre	Riesgo	Prob.	Imp.	Nivel de Riesgo	Controi	Control NTP-ISO/IEC 27001:2014	Código NTP-ISO-27001
		Ausencia del sistema por parte de los usuarios del Koha	2	3	Moderado	Mejorar los SLAs con el proveedor para evitar ausencia de conexión	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
8	**Ventanilla Jurisdiccional**	La Ventanilla Jurisdiccional deje de funcionar e impida el acceso a cualquier usuario	2	4	Alto	Mejorar los contratos de alojamiento en la nube que caídas en los servidores	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
		Unidad de almacenamiento falle, deje de funcionar y haya pérdida de información	2	5	Alto	Considerar en los contratos de alojamiento en la nube SLAs que mantengan deduplicada la información	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
		Pérdida de los programas fuente de la Ventanilla Jurisdiccional o contar con versiones desactualizadas de los mismos	2	5	Alto	Establecer un repositorio en la nube que aloje las versiones actualizadas de los programas fuente de la Ventanilla Jurisdiccional	Copias de respaldo de la información, del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.	A.12.3.1
		Ante falla del sistema no hay quien pueda resolver los problemas	2	4	Alto	Solicitar a la OGDH la contratación de un analista junior que se encuentre preparado para actuar en ausencia del analista principal	Los acuerdos contractuales con los empleados y contratistas deben estipular responsabilidades de éstos y de la organización respecto de la seguridad de la información.	A.7.1.2

Ítem	Nombre	Riesgo	Prob.	Imp.	Nivel de Riesgo	Controi	Control NTP-ISO/IEC 27001:2014	Código NTP-ISO-27001
		Pérdida de los manuales o no contar con ellos, cuando estos sean necesarios	2	3	Moderado	Establecer un repositorio en la nube que aloje las versiones actualizadas de los manuales actualizados del STD	Copias de respaldo de la información, del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.	A.12.3.1
		Daño a los datos manejados por el sistema o robo de los mismos	2	4	Alto	Considerar en el contrato de alojamiento mecanismos de protección como WAF Y Licencias DAST y SAST para el validación de las aplicaciones que se ejecutarán en esos ambientes	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
		Carecer de acceso al STD por parte de los equipos al interior del TC	2	3	Moderado	Mejorar los SLAs con el proveedor para evitar ausencia de conexión	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
9	**Jurisprudencia Sistematizada**	La Jurisprudencia Sistematizada deje de funcionar e impida el acceso a cualquier usuario	2	4	Alto	Mejorar los contratos de alojamiento en la nube que caídas en los servidores	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
		Unidad de almacenamiento falle, deje de funcionar y haya pérdida de información	2	5	Alto	Considerar en los contratos de alojamiento en la nube SLAs que mantengan deduplicada la información	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3

Ítem	Nombre	Riesgo	Prob.	Imp.	Nivel de Riesgo	Controi	Control NTP-ISO/IEC 27001:2014	Código NTP-ISO-27001
		Pérdida de los programas fuente de la Ventanilla Jurisdiccional o contar con versiones desactualizadas de los mismos	2	5	Alto	Establecer un repositorio en la nube que aloje las versiones actualizadas de los programas fuente de la Jurisprudencia Sistematizada	Copias de respaldo de la información, del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.	A.12.3.1
		Ante falla del sistema no hay quien pueda resolver los problemas	2	4	Alto	Solicitar a la OGDH la contratación de un analista junior que se encuentre preparado para actuar en ausencia del analista principal	Los acuerdos contractuales con los empleados y contratistas deben estipular responsabilidades de éstos y de la organización respecto de la seguridad de la información.	A.7.1.2
		Pérdida delos manuales o no contar con ellos, cuando estos sean necesarios	2	3	Moderado	Establecer un repositorio en la nube que aloje las versiones actualizadas de los manuales actualizados del STD	Copias de respaldo de la información, del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.	A.12.3.1
		Daño a los datos manejados por el sistema o robo de los mismos	2	4	Alto	Considerar en el contrato de alojamiento mecanismos de protección como WAF Y Licencias DAST y SAST para el validación de las aplicaciones que se ejecutarán en esos ambientes	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
		Carecer de acceso al STD por parte de los equipos al interior del TC	2	3	Moderado	Mejorar los SLAs con el proveedor para evitar ausencia de conexión	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3

Ítem	Nombre	Riesgo	Prob.	Imp.	Nivel de Riesgo	Controi	Control NTP-ISO/IEC 27001:2014	Código NTP-ISO-27001
10	Correo Electrónico	Los usuario dejen de tener acceso a sus cuentas de correo electrónico	2	4	Alto	Mejorar el contrato con el proveedor de las herramientas colaborativas para evitar estas situaciones	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
		Ante falla del sistema no hay quien pueda resolver los problemas	2	4	Alto	Capacitar un administrador alterno	La gerencia debe requerir a todos los empleados y contratistas aplicar la seguridad de la información en concordancia con las políticas y procedimientos establecidos por la organización.	A.7.2.1
		Los usuarios que acceden desde el TC no pueden abrir sus respectivos correso electrónicos	2	4	Alto	Mejorar los SLAs con el proveedor para evitar ausencia de conexión	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
11	Drives	Los usuarios que acceden desde el TC no pueden abrir sus respectivos Drives	2	4	Alto	Mejorar el contrato con el proveedor de las herramientas colaborativas para evitar estas situaciones	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
		Ante falla del sistema no hay quien pueda resolver los problemas	1	4	Moderado	Capacitar un administrador alterno	La gerencia debe requerir a todos los empleados y contratistas aplicar la seguridad de la información en concordancia con las políticas y procedimientos establecidos por la organización.	A.7.2.1

Ítem	Nombre	Riesgo	Prob.	Imp.	Nivel de Riesgo	Control	Control NTP-ISO/IEC 27001:2014	Código NTP-ISO-27001
		Los usuarios que acceden desde el TC no pueden acceder a su información alojada en sus Drives	1	4	Moderado	Mejorar los SLAs con el proveedor para evitar ausencia de conexión	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
12	**Portal Web Institucional**	El portal web deje de funcionar e impida el acceso a cualquier usuario	2	5	Alto	Mejorar los contratos de alojamiento en la nube que caídas en los servidores	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
		Unidad de almacenamiento falle, deje de funcionar y haya pérdida de información	2	5	Alto	Considerar en los contratos de alojamiento en la nube SLAs que mantengan deduplicada la información	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
		Que el Portal web quede fuera de servicio	2	4	Alto	Establecer un repositorio en la nube que aloje copia actualizada de la información suficiente para restaurar el portal	Copias de respaldo de la información, del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.	A.12.3.1
		Ante falla del sistema no hay quien pueda resolver los problemas	2	4	Alto	Solicitar a la OGDH la contratación de un analista junior que se encuentre preparado para actuar en ausencia del analista principal	Los acuerdos contractuales con los empleados y contratistas deben estipular responsabilidades de éstos y de la organización respecto de la seguridad de la información.	A.7.1.2

Ítem	Nombre	Riesgo	Prob.	Imp.	Nivel de Riesgo	Control	Control NTP-ISO/IEC 27001:2014	Código NTP-ISO-27001
		Pérdida delos manuales o no contar con ellos, cuando estos sean necesarios	1	3	Bajo	Establecer un repositorio en la nube que aloje las versiones actualizadas de los manuales actualizados del Portal Web	Copias de respaldo de la información, del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.	A.12.3.1
		Daño al contenido de la página web (Defacement), o caída del portal por ataques DoS o DDoS	2	5	Alto	Considerar en el contrato de alojamiento el uso de certificados SSL para el acceso seguro al Servidor Web, restringir el envío de información vía FTP, enviar información a la página web sólo desde Ips registradas	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
		Carecer de acceso al Portal Web por parte de los equipos al interior del TC	2	4	Alto	Mejorar los SLAs con el proveedor para evitar ausencia de conexión	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
Servicios ofrecidos por terceros y administrados por la OTI								
13	**Acceso a Internet y Seguridad perimetral de red**	Carecer de Acceso a Internet y servicios basados en el servicio	1	5	Moderado	Mejorar los SLAs con el proveedor para evitar ausencia de conexión	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3

Ítem	Nombre	Riesgo	Prob.	Imp.	Nivel de Riesgo	Controi	Control NTP-ISO/IEC 27001:2014	Código NTP-ISO-27001
14	**Herramientas colaborativas**	Falla en el aprovisionamiento del servicio	1	5	Moderado	Mejorar los SLAs con el proveedor para evitar ausencia de conexión	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3
15	**Alojamiento en la nube**	Falla en el aprovisionamiento del servicio	2	5	Alto	Mejorar los SLAs con el proveedor para evitar ausencia de conexión	Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	A.15.1.3

Anexo 2: Procedimiento para la comunicación y convocatoria del personal involucrado en la ejecución de las actividades criticas

Según la disponibilidad técnica y desarrollo de capacidades intervienen tecnología y claves de comunicación establecidas, como "Procedimientos de comunicación", cuando la acción se realiza al interior de la entidad y como "Protocolos de comunicación", cuando se refieren a la acción que se establece con otras entidades y sectores.

Los procedimientos de comunicación a ser considerados, según orden de prioridad, son:

- Mensajes de texto por celular.
- Redes sociales y correos electrónicos.
- Telefonía fija y celular.
- Teléfono satelital y las líneas fijas punto.

Los primeros dos medios de comunicación han de ser usados de manera simultánea; variando para la activación del plan de continuidad operativa, dos procedimientos específicos de comunicación:

1. **Procedimiento de reporte inicial**

   El flujo básico del procedimiento de reporte inicial para la activación del Plan de Continuidad Operativa, donde el operador de turno recepción los mensajes, consolida, analiza y realiza el procedimiento consecutivo de contacto e informan al secretario técnico del GCCO.

   En este procedimiento intervienen:
   1. Secretario general.
   2. Dirección General de Administración.
   3. Oficina de Tecnologías de la Información.

2. **Procedimiento de convocatoria**

   Una vez activado el Plan de Continuidad Operativa, se procede a la convocatoria, mediante radiofonía y mensajes de texto, basados en los mensajes claves preestablecido. "EMERGENCIA URGENTE"

   Como tratamiento específico y por la naturaleza de su función, el Presidente del GCCO, activará su cadena de mando de manera inmediata. Las claves consideradas para el PCO, a ser enviadas por los mensajes de texto (SMS), son las siguientes:

Clave remitido por radio, WhatsApp o SMS	Interpretación de Clave
Clave 0	Mensaje de Prueba
Clave 1: Nombre de la sede alterna.	Suceso o acontecimiento que afecta al Tribunal Constitucional; en este caso: EVACUAR SEDE Se acuerda que al término de la distancia trasladarse a instalaciones de la sede alterna. La sede alterna elegida es emitida en el mensaje seguido de la clave 1
Clave 2	Mensaje enviado con la finalidad de estar en estado de alerta, ante la posible disposición de desplazarse a un determinado lugar.

Para la convocatoria por megáfono, el equipo de emergencias operativas asume la responsabilidad de enviar los mensajes a través del megáfono.

Para la convocatoria por mensaje de texto, el Secretario General del Tribunal Constitucional, a sugerencia del Comando de Continuidad Operativa CCO, trasmite un mensaje de texto a los integrantes del Grupo de Comando de la Continuidad Operativa, quiénes deberán dar la confirmación de recepción de dicho mensaje.

La activación del Plan de Continuidad Operativa debe llevar a cabo el Protocolo de Comunicación esta detallado en el Anexo 3: Sistemas de comunicaciones de emergencia

Para el restablecimiento de los servicios de tecnología de la información, acervo documentario, correos electrónicos, expedientes jurisdiccionales, así como el servicio de telefonía móvil, la Oficina de Tecnologías de la Información gestionará con los proveedores de servicios las garantías de funcionamiento en cualquiera de los servicios que se hayan interrumpido por efectos primarios o secundarios durante la contingencia.

Asimismo, indicar que cada unidad orgánica deberá realizar un flujo de comunicación dentro de su área ante alguna emergencia.

La Oficina de Gestión y Desarrollo Humano es la encargada de realizar la convocatoria a todo el personal de la entidad para lo que debe contar con registros actualizados de contacto del personal.

DIRECCIÓN GENERAL DE ADMINISTRACIÓN
V°B°

TRIBUNAL CONSTITUCIONAL
Tecnologías de la Información

Anexo 3: Sistema de Comunicaciones de emergencia

1. Introducción

De ocurrir una catástrofe de gran magnitud, los canales normales de comunicaciones serán afectados por la falta de energía eléctrica, por la destrucción física de los elementos que los conforman, así como por la saturación de las líneas telefónicas.

El papel de las telecomunicaciones es esencial, porque permite el flujo de información entre los diferentes niveles de la entidad. La información por medio de las telecomunicaciones permitirá conocer rápidamente los peligros o emergencias, tomar conocimiento de las características y medir el alcance de estos eventos para promover las disposiciones para su atención. De esta manera, se podrá coordinar la movilización oportuna y eficiente de recursos económicos, humanos y materiales a favor de la entidad.

2. Objetivo

Regular los procedimientos para la instalación y operación de los Sistemas de comunicaciones durante los procesos de preparación, respuesta yrehabilitación a las emergencias o desastres; a fin de brindar una respuesta rápida y ordenada de las disposiciones ante estos eventos por la Alta Dirección.

3. Concepto de la Operación

a. El empleo de los Sistemas de Comunicaciones Convencionales (Canales Primarios) que brindan las empresas proveedoras de servicio de telecomunicaciones en el país deben ser empleadas permanentemente por todos los miembros del Tribunal Constitucional.
b. Los Sistemas de Comunicaciones de Emergencia (Canales Secundarios) que son independientes de cualquier proveedora de servicios de telecomunicaciones (Radio Comunicaciones) son la segunda opción a falta de los primeros. Los Sistemas de Comunicaciones de Emergencia (Canales Secundarios) que brindan las empresas proveedoras de servicio de telecomunicaciones (Comunicaciones Satelitales) son la tercera opción afalta de los segundos.
c. Se realizará la mayor explotación de los sistemas de comunicaciones existentes empleando los equipos integradores disponibles.

4. Sistema de Telecomunicaciones

Los Sistemas de Comunicaciones del Tribunal Constitucional están compuestos por tres elementos básicos:

a. Redes de Comunicaciones

Es el canal por el cual se intercambia mensajes; este canal puede estar contenido en uno del siguiente grupo de medios de comunicaciones: Acústico, Visual, Alámbrico, Inalámbrico o Mensajero.

- **Canales de comunicaciones empleados en el TC son:**

Canales primarios	Canales secundarios
- Telefonía Fija. - Telefonía Celular. - Internet Convencional Fija. - Internet Convencional Móvil.	- Red Especial de Comunicaciones enSituaciones de Emergencia RECSE. - Radio Comunicaciones en la gamaVHF. - Radio Comunicaciones en la gamaUHF. - Radio Comunicaciones en la gamaUHF Troncalizado. - Radio Comunicaciones en la gamaHF. - Telefonía Satelital. - Internet Satelital VSAT. - Internet Satelital BGAN.

- **Estructura de las redes de comunicaciones**

Con la finalidad brindar fluidez de las comunicaciones, las redes están estructuradas de acuerdo a como se realizará el flujo de lasinformaciones

a. Red de Telecomunicaciones Internas
Comprende las comunicaciones al interior del Tribunal Constitucional entre las diferentes unidades orgánicas mediante correos electrónicos y uso de anexos institucionales.

b. Red de Telecomunicaciones Externas
Comprende las comunicaciones al exterior del Tribunal Constitucional entre la Alta Dirección y los diferentes organismos públicos que participan en la gestión de riesgos de desastres (INDECI, CENEPRED, Ministerio de Defensa, Hospitales, etc.), esto será coordinado con la Oficina de Imagen Institucional.

- **Número de abonados, cuentas, indicativos y frecuencias**

A fin de realizar el enlace en cada uno de los canales de comunicaciones es necesario contar entre otros con los números de abonados telefónicos, cuentas correo electrónico, indicativos, frecuencias de radio, etc.

a. Abonados y cuentas
Se cuenta con un listado de los números de anexos, números de telefonía fija y celular del personal que se encuentra en los despachos, oficinas y direcciones la cual se encuentra en posesión de la Oficina de Gestión y Desarrollo Humano, debidamente actualizada.

b. Fuentes de energía
Los equipos de comunicaciones deben contar con un sistema de energía alterna, pudiendo ser la energía fotovoltaica o electrógena, los cuales les permitirá continuar operando a falta del fluido eléctrico convencional.

c. Personal de Comunicaciones
La Oficina de Tecnologías de la Información dispondrá de personalcapacitado y preparado para operar los canales de comunicación primaria y secundaria, los cuales será proveídos previamente por la entidad, en el número suficiente para atender las redes.

El personal participará en los ejercicios y simulacros de comunicacionesa fin de entrenarse en el empleo de los equipos y procedimientos.

d. Procedimientos Operativos Estándar.
Una Red de Comunicaciones está conformada por dos o más estaciones que emplean un mismo canal de comunicaciones, los mismos que son operados por personal de comunicaciones entrenados en explotación de los equipos y el empleo correcto de los Procedimientos Operativos Estándar.

5. Ejecución

La comunicación entre el personal jurisdiccional y administrativos y sus respectivos jefes inmediatos superiores será permanente, por lo que se facilitará todos los canales de comunicaciones disponibles: los canales de comunicaciones convencionales (telefonía fija, telefonía celular, internet) y a falta de estos los canales de comunicaciones de emergencia telefonía e internet satelital coordinado por la oficina de Tecnologías de la Información.

Para facilitar el flujo ordenado de las comunicaciones, los funcionarios y servidores cumplirán con los protocolos y/o procedimientos de comunicaciones que disponga la Oficina de Tecnologías de la información manteniendo la disciplina de red.

6. Instrucciones y coordinaciones

a. Implementación de los Sistemas de Comunicaciones
La implementación de los sistemas de comunicaciones será responsabilidad dela Oficina de Tecnología de la Información y de la Oficina de Imagen Constitucional, quienes gestionarán los Sistemas de Comunicaciones del Tribunal Constitucional.

b. Sistemas de Comunicaciones Alternos
Los sistemas de comunicaciones alternos del Tribunal Constitucional estarán sustentados sobre la base de los canales de comunicaciones normales con equipos propios de cada sede; a falta de éstos se recurrirá al empleo de sistemas de comunicaciones de las Instituciones Públicas según sea el caso; o en caso de saturación de estos sistemas, se recurrirá al empleo de los recursos materiales y humanos de otros operadores de servicio de comunicaciones.

c. Turnos de Atención de las Redes
Las comunicaciones del Tribunal Constitucional son muy importantes cuando se presente una emergencia, lo que implica que el funcionamiento de las Redes de Comunicaciones e Informaciones deben estar disponibles las 24 horas del día; para los cual se establecerán los turnos correspondientes.

d. Pruebas del Sistema de Comunicaciones.
A fin de verificar la operatividad de las redes de comunicaciones, la disponibilidad del personal de operadores y el correcto empleo de los procedimientos operativos estándar, la oficina de Tecnología de la Información realizarán pruebas de los sistemas de comunicaciones.

TRIBUNAL CONSTITUCIONAL - Oficina de Tecnologías de la Información

DIRECCIÓN GENERAL DE ADMINISTRACIÓN V°B°

Anexo 4: Cronograma de la Gestión de la Continuidad Operativa

Actividad / Responsable	2024											
	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sept	Oct	Nov	Dic
Aprobar el Plan de Continuidad Operativa (Grupo de Comando)								X				
Brindar capacitaciones respecto a la continuidad operativa										X		
Dar a conocer el plan de continuidad										X		
Supervisar la implementación de la gestión e la Continuidad Operativa											X	

Actividad / Responsable	2025											
	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sept	Oct	Nov	Dic
Reunión del Grupo de Comando de la Continuidad operativa		X										
Brindar capacitaciones respecto a la continuidad operativa			X						X			
Remitir comunicaciones vía correo electrónico relacionados a la continuidad operativa					X					X		
Supervisar la implementación de la gestión de la Continuidad Operativa						X						X

Anexo 5: Caso especial ante una epidemia -pandemia

Ante la ocurrencia de una epidemia o pandemia, el Tribunal Constitucional regulará suproceder de acuerdo a lo establecido por las políticas de Estado; considerando, las Declaratorias de Estado de Emergencias que disponga el Gobierno Central y las entidades competentes en emergencia sanitaria, como el aislamiento social obligatorio (cuarentena) para evitar la propagación; en ese sentido, suspenderá las labores en la sede de Lima Centro, sede de San Isidro y del Centro de Estudios Constitucionales, para evitar el contagio y la propagación de la enfermedad masiva entre sus trabajadores.

Ante este escenario, se formalizará y otorgará licencias con goce de haber compensable, estableciendo el trabajo remoto, presencial, semipresencial para los funcionarios y servidores/as del Tribunal Constitucional. Se ejecutará la fase C del Plan de Acción del Tribunal Constitucional durante la vigencia de la emergencia sanitaria de acuerdo a lo establecido en la Resolución Administrativa 060-2023- P/TC que aprueba el "Plan de implementación de Teletrabajo en el Tribunal Constitucional"

Se tomará en consideración las siguientes premisas:

1. Los servicios, procedimientos administrativos y/o actividades institucionales enlas sedes del Tribunal Constitucional serán suspendidos en el marco de una declaratoria de Estado de Emergencia.

2. Excepcionalmente y en situaciones de urgencia debidamente justificada, se dispone el desplazamiento de los/las funcionarios/as y servidores/ras a las sedes u otros lugares para el cumplimiento de sus funciones y/o actividades institucionales, realizando trabajo presencial algunos servidores por razones denecesidad institucional.

3. Durante el periodo del Estado de Emergencia Nacional las comunicaciones cursadas mediante correo electrónico estarán autorizadas y tendrán validez para todos los efectos que se requieran.

4. La Oficina de Tecnología de la Información (OTI) del Tribunal Constitucional a pedido de la Alta Dirección, las jefaturas de órganos y unidades orgánicas facilitará el soporte tecnológico, la continuidad de los servicios TI críticos y los accesos remotos que resulten necesarios para el cumplimiento de sus funciones.

5. Durante la vigencia del Estado de Emergencia, solo podrán asistir a las instalaciones del Tribunal Constitucional, las personas debidamente autorizadas y acreditadas, en coordinación con sus respectivos superioresjerárquicos y con conocimiento de la Oficina de Gestión y Desarrollo Humano, según corresponda en cada caso, para garantizar la continuidad operativa de laentidad.

Anexo 6: Listado de recursos por sede

- Sede Central - Cercado de Lima

SEDE CERCADO DE LIMA	CANTIDAD
Acumulador de energía - equipo de ups	1
Archivador de melamina	6
Armario archivador de melamina	1
Armario bastidor metálico - rack cabinet	1
Armario de melamina	14
Armario de metal y melamina	3
Aspiradora eléctrica manual para vehículos	2
Balanza de pie con tallímetro	1
Balanza electrónica	1
Banca de madera	1
Banco de condensadores	3
Biombo de metal	1
Bomba (otras)	2
Bomba de succión de agua	2
Cafetera eléctrica	5
Cajonera rodable de melamina	13
Cámara de video	1
Cámara de video ip	11
Cámara domo a color	20
Cámara fotográfica digital	1
Campana extractora eléctrica	1
Capturador de imagen - scanner	17
Carro transportador (otros)	2
Casillero de metal - locker	2
Chasis para servidores tipo hoja/ultradelgados	1
Coche metálico para curaciones	1
Coche transportador de alimento	1
Cocina a gas	1
Cocina eléctrica	1
Compresora de aire	1
Computadora personal portátil	4
Consola de sonido de 16 canales de salida	1
Consola multiplexor kvm	1
Control remoto en general	1
Convertidor hdmi a sdi - sd / hd	1
Credenza de melamina	1
Cuadros en general	7
Cuchillo eléctrico	1
Decodificador codificador de señal de audio	1
Deshumedecedor	3

SEDE CERCADO DE LIMA	CANTIDAD
Destructora de documentos	1
Detector de humo	9
Disco duro externo	4
Electrobomba	1
Engrapador industrial	4
Equipo de aire acondicionado tipo domestico	19
Equipo de alarma y protección	1
Equipo de iluminación de emergencia de 20 w	2
Equipo multifuncional copiadora fax impresora scanner	5
Equipo multifuncional copiadora impresora scanner	12
Equipo multifuncional copiadora impresora scanner laser monocromática 24 ppm	1
Equipo para aire acondicionado tipo domestico	3
Escalera metálica	4
Escritorio de madera	2
Escritorio de melamina	17
Escritorio de melamina en forma de L	5
Escritorio de metal y melamina	12
Estandarte	1
Estante archivador de melamina	2
Estante corredizo - estante móvil	1
Estante de melamina	8
Estante de melamina aéreo	4
Estante de metal	9
Exprimidor eléctrico	3
Extintor de gas carbónico (CO2) DE 10 lb	4
Frigobar 90 l	1
Grabador digital de video y audio	5
Guillotina para 40 hojas	1
Hervidor eléctrico	2
Horno eléctrico	1
Horno microondas	7
Impresora de código de barras	1
Impresora laser	18
Intercomunicador	3
Lectora (otras)	13
Librero de madera	1
Licuadora eléctrica domestica de 2 velocidades	2
Máquina anilladora perforadora	2
Megáfono	2
Mesa de madera	1
Mesa de melamina	2
Micrófono (otros)	8
Micrófono inalámbrico de mano - dual	1

SEDE CERCADO DE LIMA	CANTIDAD
Módulo de melamina para computadora	8
Módulo de melamina para fotocopiadora	1
Módulo de melamina tipo cajonera de 4 gavetas	1
Monitor a color	54
Mostrador de madera	3
Pantalla Ecran eléctrico 3.00 m x 3.00 m	1
Parante ordenador de filas	26
Parlantes en general (mayor a 1/8 uit)	1
Perchero metálico	1
Rack (otros)	6
Reflector	6
Refrigeradora eléctrica domestica	4
Reloj de pared	1
Reloj marcador fechador electrónico	3
Sandwichera	5
Secadora de manos	3
Servidor	6
Servidor blade	1
Silla giratoria de metal	105
Sillón fijo de madera	5
Sillón giratorio de metal	8
Sistema de grabación, verificación y reconocimiento de huella	14
Sistema de protección y seguridad para red - firewall - appliance de filtros de contenido web	1
Sistema de protección y seguridad para red - firewall acceso remoto seguro	1
Sistema de proyección multimedia - proyector multimedia	1
Sofá de madera	1
Solución de almacenamiento externo	1
Surtidor de agua eléctrico - dispensador eléctrico	27
Switch para red	22
Tableta pad	5
Teclado - keyboard	78
Teléfono	36
Teléfono analógico con pantalla	1
Teléfono celular	2
Teléfono inalámbrico	1
Televisor a colores	5
Tensiómetro	1
Termo hervidor eléctrico	7
Termómetro infrarrojo	2
Tótem multimedia	1
Transmisor de tv	1
Unidad central de proceso - CPU	51
Ventilador eléctrico de pie de 3 velocidades	8
Ventilador eléctrico para pared	1

TRIBUNAL CONSTITUCIONAL - Oficina de Tecnologías de la Información

DIRECCIÓN GENERAL DE ADMINISTRACIÓN V°B°

SEDE CERCADO DE LIMA	CANTIDAD
Video cámara para computadora	5
Vitrina de metal	1
Total, general	**866**

- Sede San Isidro

SEDE SAN ISIDRO	CANTIDAD
Acumulador de energía - equipo de ups	6
Amplificador de audio de 2000 w	2
Amplificador mezclador	1
Armario archivador de melamina	6
Armario de melamina	34
Atril de madera	2
Audífonos profesionales	3
Automóvil	5
Biombo de metal	2
Bomba (otras)	1
Cafetera eléctrica	1
Cajonera rodable de melamina	9
Cámara de video de seguridad con audio	3
Cámara de video digital tipo profesional de alta definición	1
Cámara de video ip	24
Cámara domo a color	18
Cámara fotográfica	1
Cámara fotográfica digital	1
Camilla de polietileno	3
Capturador de imagen - scanner	41
Carpeta de metal unipersonal	4
Carro de metal transportador plegable con plataforma de metal	5
Central de comunicaciones	1
Central telefónica	2
Circulina magnética con conector al encendedor del vehículo	2
Cocina eléctrica	1
Compresora de aire	1
Computadora personal portátil	33
Concentrador (otros)	1
Consola para control de audio	2
Conversor analógico digital	3
Convertidor hdmi a sdi - sd / hd	5
Credenza de melamina	3
Decodificador para señales de video vigilancia	1
Deshumedecedor	2
Destructora de documentos	1
Detector de humo	8
Disco duro externo	16

TRIBUNAL CONSTITUCIONAL - Oficina de Tecnologías de la Información

DIRECCIÓN GENERAL DE ADMINISTRACIÓN V°B°

SEDE SAN ISIDRO	CANTIDAD
Engrapador industrial	1
Equipo de iluminación de emergencia de 20 w	2
Equipo de luces portátil	1
Equipo de posicionamiento - GPS	1
Equipo de transmisión de redes	1
Equipo multifuncional copiadora fax impresora scanner	30
Equipo multifuncional copiadora impresora scanner	21
Equipo para aire acondicionado tipo domestico de 24000 btu tipo split pared	21
Equipo para aire acondicionado tipo industrial	2
Escalera de fibra de vidrio tipo tijera	3
Escalera metálica	4
Escritorio de madera	4
Escritorio de melamina	102
Estandarte	22
Estante archivador de melamina	2
Estante corredizo - estante móvil	2
Estante de melamina	20
Estufa eléctrica	1
Etiquetadora - rotuladora	1
Extintor	31
Extractor de aire	2
Filmadora	3
Frigobar 90 l	2
Gabinete de metal	10
Gata en general	1
Generador de tonos y sonda digital	2
Grabador digital de video y audio	2
Grabador digital de video y audio - videograbador digital	1
Grabadora digital	1
Guillotina	1
Horno microondas	13
Impresora de código de barras	1
Impresora laser	38
Intercomunicador	2
Lectora (otras)	21
Lectora de disco compacto externo para computo - cd rom	1
Lectora De Tarjeta Inteligente Portátil	30
Lectora Terminal Portátil De Datos	2
Librero De Madera	3
Licuadora Eléctrica	1
Maletas En General (Mayor A 1/8 Uit)	1
Maletín (Mayor A 1/4 Uit)	5
Mando De Control De Cámaras Domo	1
Máquina Anilladora Perforadora	1
Máquina Espiraladora	1

SEDE SAN ISIDRO	CANTIDAD
Medidor De Temperatura	1
Megáfono	2
Mesa de madera	3
Mesa de melamina	28
Mesa de reuniones	10
Mesita de centro	8
Micrófono	70
Microscanner verificador de cableado para redes	2
Modulador rf video	1
Módulo de melamina	66
Módulo de metal	4
Monitor	311
Oxímetro de pulsos	2
Pantalla Ecran	2
Parlante amplificador portátil	1
Parlantes en general (mayor a 1/8 uit)	4
Parrillero	1
Patch panel - panel de conmutacion	7
Pedestal para micrófono	39
Pinza amperimétrica	1
Pistola para pintar	1
Pizarra digital interactiva	1
Procesador (otros)	2
Proyector	3
Punto de acceso inalámbrico - Access point wireless	6
Rack (otros)	5
Rack móvil modelo pedestal	2
Rack para televisor	4
Radio receptor	1
Reflector	1
Refrigeradora eléctrica domestica	4
Reloj de pared	1
Reloj marcador fechador electrónico	3
Sandwichera	1
Secadora De Manos	2
Servidor	5
Servidor Blade	1
Servidor Tipo Rack	1
Silla De Ruedas Metálica	2
Silla Fija De Madera	9
Silla Fija De Metal	262
Silla Giratoria De Metal	235
Sillón Fijo De Madera	11
Sillón Fijo De Metal	2
Sillón Giratorio De Metal	21
Sillón modular	9

SEDE SAN ISIDRO	CANTIDAD
Sillón modular de cuero de 1 cuerpo	16
Sirena móvil (mayor a 1/4 uit)	1
Sistema de detección contra incendios	1
Sistema de protección y seguridad para red - firewall	2
Sistema de protección y seguridad para red - firewall - appliance de filtros de contenido web	1
Sistema de proyección multimedia - proyector multimedia	2
Sistema de videoconferencia	4
Sistema hibrido telefónico para enlace	1
Sofá de madera	1
Solución de almacenamiento externo	2
Supresor de retroalimentación acústica	3
Surtidor de agua eléctrico - dispensador eléctrico	36
Switch para red	31
Switcher de video digital	2
Tablero digitalizador electrónico	1
Tableta pad	8
Taladro eléctrico portátil atornillador inalámbrico de 18 v	1
Taladro eléctrico portátil percutor	1
Tarima de madera	9
Teclado - keyboard	274
Teleapuntador - teleprompter	1
Teléfono	97
Televisor a colores	12
Tensiómetro digital	2
Termo hervidor eléctrico	5
Termómetro infrarrojo	4
Transformador (mayor a 1/4 uit) de aislamiento monofásico 220/220 10 kva	1
Transmisor de tv	1
Trípode metálico	4
Unidad central de proceso - CPU	271
Vehículo aéreo no tripulado - drone	1
Ventilador eléctrico de pie de 3 velocidades	70
Ventilador eléctrico tipo columna o torre	39
Video cámara para computadora	31
Vitrina de madera	1
Vitrina de metal	1
Voltimetro	1
Total, general	**2751**

- Sede Centro de Estudios Constitucionales

SEDE CENTRO DE ESTUDIOS CONSTITUCIONALES	CANTIDAD
Armario de melamina 35 cm X 1.60 m X 1.75 m	1

SEDE CENTRO DE ESTUDIOS CONSTITUCIONALES	CANTIDAD
Atril de madera	2
Biblioteca de melamina	2
Cabina - caseta	1
Cámara de video de seguridad con audio	4
Cámara domo a color	5
Capturador de imagen - scanner	3
Carpeta de metal unipersonal	46
Carro transportador (otros)	1
Computadora personal portátil	2
Consola para control de audio	1
Deshumedecedor	2
Detector de humo	2
Disco duro externo de 1 tb	1
Equipo de aire acondicionado tipo domestico	7
Equipo de iluminación de emergencia de 20 w	8
Equipo multifuncional copiadora fax impresora scanner	4
Equipo para aire acondicionado	3
Escritorio de melamina	4
Escritorio de metal y melamina	1
Estandarte	6
Estante archivador de melamina	2
Estante de melamina	7
Estante escritorio	1
Estufa eléctrica	1
Exprimidor Eléctrico	1
Extintor	5
Horno Microondas	1
Impresora Laser	6
Intercomunicador	1
Lectora (Otras)	1
Librero De Melamina	22
Licuadora Eléctrica Doméstica De 3 Velocidades	2
Megáfono	1
Mesa De Melamina	2
Mesa Plegable De Melamina	2
Mesita De Centro	1
Micrófono Inalámbrico	2
Monitor a color de 20 In	12
Oxímetro De Pulsos	1
Pantalla Ecran	3
Parlantes En General (Mayor A 1/8 Uit)	4
Proyector	3
Rack (otros)	1
Rack móvil modelo pedestal	1
Reflector	2
Reloj marcador fechador electrónico con lector de tarjeta de proximidad	1
Repostero de melamina	1
Sandwichera	1

SEDE CENTRO DE ESTUDIOS CONSTITUCIONALES	CANTIDAD
Secadora de manos	1
Silla fija de metal	7
Silla giratoria de metal	13
Surtidor de agua eléctrico - dispensador eléctrico	3
Teclado - keyboard	9
Teléfono	11
Televisor LED 43 in	2
Tensiómetro digital	1
Trípode metálico	1
Unidad central de proceso - cpu	13
Ventilador eléctrico de pie de 3 velocidades	1
Total general	**259**

Anexo 7: Listado de personal

UNIDADES ORGÁNICAS	SEDE LIMA			SEDE SAN ISIDRO		
	DL 728 CAP	DL 1057 CAS	Practicantes	DL 728 CAP	DL 1057 CAS	Practicantes
Pleno del Tribunal Constitucional	7					
Secretaría General				27	7	13
Oficina de Trámite Documentario y Archivo	6	7				
Oficina de Control Institucional		3				
Oficina de Procuraduría Pública				1		
Oficina de Planeamiento y Desarrollo				3		
Oficina de Asesoría Jurídica				1		1
Oficina de Presupuesto				3		
Dirección General de Administración	4					
Oficina de Gestión y Desarrollo Humano				9	8	2
Oficina de Contabilidad y Tesorería				5		
Oficina de Logística				5	4	
Oficina de Servicios Generales				15	4	
Oficina de Tecnologías de la Información				3	3	2
Gabinete de Asesores Jurisdiccionales				35	6	8
Secretaría Relatoría				18	11	1
Centro de Estudios Constitucionales				8	6	5
Oficina de Imagen Institucional				6	4	
Total	**17**	**10**	**0**	**139**	**53**	**32**

DIRECCIÓN GENERAL DE ADMINISTRACIÓN V°B°

TRIBUNAL CONSTITUCIONAL

SGD 2449-2024-I

Tribunal Constitucional

"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

Lima, 12 de agosto de 2024

OFICIO N.° 240-2024-DIGA/TC

Señor
ALBERTO BORIS CHE-PIU CARPIO
Secretario General
Tribunal Constitucional
Presente.-

Asunto : Plan de continuidad operativa 2024-2025

Referencia : a) Resolución Ministerial N.° 320-2021-PCM
b) Resolución Administrativa N.° 054-2024-P/TC
c) Resolución Administrativa N.° 095-2023-P/TC

De mi especial consideración:

Me dirijo a usted en relación a la norma de referencia a) mediante la cual se aprueban 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".

Al respecto, mediante resolución de referencia b) se designó el Grupo de Comando para la continuidad operativa quienes han elaborado el proyecto del "Plan de Continuidad Operativa 2024-2025" el cual cuenta con la aprobación del Instituto Instituto Nacional de Defensa Civil, que se adjunta al presente.

En este sentido, traslado para su aprobación mediante resolución administrativa; el Plan de Continuidad Operativa 2024-2025 y el Plan de recuperación de los servicios informáticos; asimismo se solicita dejar sin efecto la resolución de referencia c) en la que se aprobó el plan de continuidad operativa.

Sin otro particular, quedo de usted.

Atentamente,

LAURA PILAR DIAZ UGAS
Directora General de Administración
TRIBUNAL CONSTITUCIONAL

Tribunal Constitucional

RESOLUCIÓN ADMINISTRATIVA 131-2024-P/TC

Lima, 15 de agosto de 2024

VISTA

La comunicación de la Secretaría General de la fecha; y,

CONSIDERANDO

Que, mediante la Ley 29664, se crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD) como sistema interinstitucional, sinérgico, riesgos asociados a peligros o minimizar sus efectos, así como evitar la generación de nuevos riesgos, preparación y atención ante situaciones de desastre mediante el establecimiento de principios, lineamientos de política, componentes, procesos e instrumentos de la Gestión de Desastres;

Que, con el Decreto Supremo 038-2021-PCM se aprueba la Política Nacional de Gestión del Riesgo de Desastres al 2050, en el que se establece que "las entidades públicas en todos los niveles de gobierno, en el marco del proceso de preparación, deben formular e implementar un conjunto de acciones estratégicas que, además, deber ser de carácter nacional, sectorial regional y local. Como parte de ellas, las entidades deben formular e implementar, entre otros instrumentos de importancia, sus Planes de contingencia y planes de continuidad operativa";

Que, la Política Nacional de Gestión del Riesgo de Desastres al 2050 define al Plan de Continuidad Operativa como "el instrumento que incluye la identificación de las actividades y servicios críticos que requieren ser ejecutados y prestados de manera interrumpida, y la determinación de las medidas y acciones que permitan que la entidad de manera eficiente y eficaz siga cumpliendo con sus objetivos", ante la ocurrencia de un desastre o cualquier evento que interrumpa prolongadamente sus operaciones;

Que, con la Resolución Ministerial 320-2021-PCM, se aprueba el documento técnico denominado "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", en adelante los lineamientos, que tienen por finalidad fortalecer la implementación de la Gestión de la Continuidad Operativa en las entidades públicas de los tres niveles de gobierno, ante la ocurrencia de un desastre o cualquier evento que interrumpa prolongadamente sus operaciones;

Que, mediante la Resolución Administrativa 095-2023-P/TC, de fecha 02 de junio de 2023, se aprueba el Plan de Continuidad Operativa del Tribunal Constitucional;

Que, con la Resolución Administrativa 054-2024-P/TC, del 5 de marzo de 2024, se designa a la Dirección General de Administración como unidad orgánica responsable de implementar en la entidad el proceso de la gestión de la continuidad operativa, y al Grupo de Comando (GCCO) para la continuidad operativa del Tribunal Constitucional, conformado por servidores que se encargan de la elaboración del Plan de Continuidad Operativa de la entidad;

Que, a través del Oficio 240-2024-DIGA/TC, de fecha 12 de agosto de 2024, la directora general de administración, en calidad de titular de la unidad orgánica responsable de implementar en la entidad el proceso de la gestión de la continuidad operativa, presenta el Plan de Continuidad Operativa 2024-2025, elaborado por el Grupo de Comando para la Continuidad Operativa (GCCO), validado por el Instituto Nacional de Defensa Civil;

Que, en consecuencia, corresponde a esta Presidencia emitir el presente acto administrativo que materialice la aprobación del Plan de Continuidad Operativa 2024-205 del Tribunal Constitucional;

En uso de las facultades conferidas a esta Presidencia por la Ley Orgánica del Tribunal Constitucional, el Reglamento Normativo; Reglamento de Organización y Funciones; y, la Resolución Ministerial 320-2021-PCM, que aprueba el documento técnico denominado "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";

SE RESUELVE

ARTÍCULO PRIMERO. – DEJAR SIN EFECTO la resolución Administrativa 095-2023-P/TC, de fecha 02 de junio de 2023.

ARTÍCULO SEGUNDO. – APROBAR el Plan de Continuidad Operativa 2024-2025 del Tribunal Constitucional, que en anexo forma parte integrante de la presente resolución

ARTÍCULO TERCERO. – DISPONER la publicación de la presente resolución y su anexo en el Portal Institucional del Tribunal Constitucional (www.tc.gob.pe).

Regístrese, comuníquese y publíquese.

FRANCISCO MORALES SARAVIA
Presidente
TRIBUNAL CONSTITUCIONAL