PLAN DE RECUPERACIÓN DE SERVICIOS INFORMÁTICOS

Febrero de 2022

RESPONSABLES

CARGOS	ROLES	FIRMA
Encargado de Infraestructura Tecnológica	**ELABORADO POR**	Firmado digitalmente por FEBRERO CABREJOS Eduardo Alfonso FAU 20131367938 hard Motivo: Soy el autor del documento Fecha: 28.02.2022 19:02:53 -05:00
Encargado de Ciberseguridad	**REVISADO POR**	Firmado digitalmente por CASTILLO YARLEQUE Javier Francisco FAU 20131367938 hard Motivo: Doy V° B° Fecha: 28.02.2022 19:24:48 -05:00
Encargado de Sistemas de Información	**REVISADO POR**	Firmado digitalmente por VARGAS PEREYRA Hernan Ronald FAU 20131367938 hard Motivo: Soy el autor del documento Fecha: 28.02.2022 19:29:52 -05:00
Encargado de Soporte Técnico	**REVISADO POR**	Firmado digitalmente por PORTOCARRERO PELAEZ Irving Raul FAU 20131367938 hard Motivo: Soy el autor del documento Fecha: 28.02.2022 19:15:29 -05:00
Oficial de Seguridad y Confianza Digital	**REVISADO POR**	Firmado digitalmente por GARAY CAMPOS Pedro Benjamin FAU 20131367938 hard Motivo: Doy V° B° Fecha: 28.02.2022 19:07:49 -05:00
Jefe de la Oficina General de Tecnologías de la Información y Estadística.	**APROBADO POR**	Firmado digitalmente por GAITAN CARRANZA Eddi Daniel FAU 20131367938 hard Motivo: Soy el autor del documento Fecha: 28.02.2022 19:53:23 -05:00

HISTORIAL DE CAMBIOS

Nombre del fichero	Versión	Resumen de cambios producidos	Fecha
MINDEF-OGTIE-PRSI	1	Primera versión	24/02/2022

CLASIFICACIÓN DEL DOCUMENTO

COMUN

CONTENIDO

1. INTRODUCCIÓN

La recuperación ante desastres se está convirtiendo en un aspecto cada vez más importante en el mundo de las tecnologías de la información y comunicaciones. Como los dispositivos, sistemas y redes se vuelven cada vez más complejos, simplemente hay más cosas que pueden salir mal.

En ese sentido, la Oficina de Tecnologías de la Información y Estadística (OGTIE) ha formulado un Plan de Recuperación de Servicios Informáticos (PRSI) a fin de estar preparada para actuar de manera ágil y ordenada ante posibles situaciones de contingencia o desastre en los servicios de TI/Red que afecten a los procesos críticos del negocio.

El presente Plan y sus anexos deberán ser tratados como documentos vivos, y cuenta con un Plan de Pruebas anual que permitirá demostrar la eficacia de las estrategias, si son completos, actualizados y exactos, e identificar las oportunidades de mejora en el tiempo.

2. OBJETIVO

Los objetivos del Plan de Recuperación de Servicios Informáticos son los siguientes:

- Salvaguardar los recursos informáticos de la OGITE - MINDEF – Sede Central.
- Garantizar la disponibilidad de los principales servicios de Tecnología de la Información y Comunicaciones del MINDEF – Sede Central.

3. ALCANCE

Plan de Recuperación de los Servicios de TI de la Oficina General de Tecnologías de la Información y Estadística de sede central del Ministerio de Defensa - MINDEF.

4. REVISIÓN DEL DOCUMENTO

El presente plan debe ser revisado y actualizado por lo menos una vez al año de manera ordinaria y de forma extraordinaria en aquellos casos tales como mudanzas, cambios en la infraestructura tecnológica, cambios sustanciales de personal que conforma el Equipo de Recuperación, actualización de las estrategias de recuperación, entre otros, de tal manera que todo cambio que impacte al Plan debe ser incorporado tan pronto como sea posible, sin necesidad de esperar su programación en el programa de mantenimiento anual. El responsable de la revisión, actualización y difusión del presente documento es el Líder de Recuperación de Servicios Informáticos .

5. BASE LEGAL Y TÉCNICA

- Manual de Organización y Funciones del Ministerio de Defensa (MOF), aprobado con Resolución Ministerial N° 601-2011/DE/SG
- Decreto Supremo N° 006-2016-DE que Aprueba el Reglamento de Organización y Funciones (ROF).
- Decreto Supremo N° 016-2014-PCM que aprueba el Reglamento de Decreto Legislativo N° 1141.
- Ley N° 28612, Ley que norma el uso, adquisición y adecuación del software en la Administración Pública y su Reglamento, aprobado por el Decreto Supremo N° 024-2005-PCM.

- Decreto Legislativo N° 822, Ley sobre Derechos de Autor.
- Resolución Ministerial N° 041-2017-PCM, que resuelve el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 12207:2016 – Ingeniería de Software y Sistemas. Procesos del ciclo de vida del software. 3ª Edición"
- Ley Marco de Modernización de la Gestión del Estado - Ley 27658.
- Resolución Ministerial N° 004-2016-PCM, que aprueban el uso obligatorio de la Norma Técnica Peruana "ISO NTP/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Ministerial N° 166-2017-PCM, que aprueban el uso obligatorio de la Norma Técnica Peruana "ISO NTP/IEC 27001:2014 referente al Comité de Gestión de Seguridad de la Información.
- NTP-ISO/IEC 27001:2014 EDI. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos 2° Edición.
- Política de Seguridad de Seguridad de la Información – MINDEF.
- Resolución Ministerial N°320-2021-PCM, que 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.

6. GLOSARIO DE TÉRMINOS

a) Análisis de Impacto al Negocio (BIA): Proceso de análisis de actividades y efecto que una interrupción del negocio podría tener sobre ellos.
b) Análisis de riesgos: Es un proceso que se encarga de la identificación y estimación de las amenazas, vulnerabilidades, riesgos y consecuencia que podrías sobre el elemento analizado.
c) Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de la auditoría y evaluarlas de manera objetiva para determinar el grado en que se cumplen los criterios de auditoría.
d) Conformidad: Cumplimiento de un requisito.
e) Corrección: Acción para eliminar una no conformidad detectada.
f) Documento: Información y su medio de soporte.
g) Evento: Aparición o cambio de un conjunto particular de circunstancias. Un evento a veces puede ser referido como un "incidente" o "accidente".
h) Gestión de Riesgo: Coordina las actividades para dirigir y controlar una organización con respecto al riesgo.
i) Incidente: Situación que podría ser, o podría dar lugar a una alteración, pérdida, emergencia o crisis.
j) Tiempo Objetivo de Recuperación (RTO): Periodo de tiempo después de un incidente en el que el producto o servicio debe reanudarse, o actividad debe reanudarse, o se debe recuperar recursos.
k) Centro de datos principal: Espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización.
l) Centro de datos alterno: conjunto de infraestructuras tecnológica cuyo diseño es importante para lograr la disponibilidad y eficiencia de los recursos que lo contienen.
m) Plan de continuidad del negocio: Procedimientos documentados que guían a las organizaciones para responder, recuperar, reanudar y restaurar a un nivel predefinido de operación luego de una interrupción. Por lo general esto cubre los recursos, servicios y actividades necesarias para garantizar la continuidad de las funciones críticas del negocio.

7. ROLES Y RESPONSABILIDADES

El equipo de recuperación de desastres del MINDEF – Sede Central cuenta con personal involucrado con las tareas asignadas y cumplir con los siguientes requisitos:

- Conformado por un líder y un alterno.
- Conocer las responsabilidades para poder minimizar el impacto de una interrupción.

7.1. Líder de Recuperación de TI

- ✓ Coordinar, dirigir y decidir las acciones a seguir en un escenario de contingencia.
- ✓ Activar el Plan de Recuperación de Servicios Informáticos.

- ✓ Liderar al personal durante la situación de contingencia.
- ✓ Verificar la magnitud del desastre y sus posibles consecuencias.
- ✓ Mantener comunicada a la Alta Dirección del estado del desastre, las fases de recuperación y los posibles problemas a enfrentar.
- ✓ Supervisar la recuperación del Centro de Datos.
- ✓ Contactar con los proveedores si existe daño en la infraestructura tecnológica.

7.2. Líder de Infraestructura Tecnológica y Telecomunicaciones

- ✓ Evaluar los daños de la plataforma tecnológica.
- ✓ Coordinar las actividades para la recuperación del Centro de datos alterno.
- ✓ Recuperar la plataforma que soporta los sistemas críticos del MINDEF.
- ✓ Habilitar los procedimientos de backup y restablecer los controles normales de operación del Centro de Datos.
- ✓ Restaurar los enlaces de red y comunicaciones
- ✓ Evaluar el daño en las redes de comunicaciones de datos.
- ✓ Verificar el funcionamiento de la central telefónica.

7.3. Líder de Sistemas de Información

- ✓ Validar el correcto levantamiento de los servicios de los Sistemas de información.
- ✓ Informar a los usuarios el momento en que estará disponible los sistemas de información.
- ✓ Establecer los requerimientos de los sistemas operativos, base de datos y documentación necesaria para el correcto funcionamiento de los sistemas de información.

7.4. Líder de Ciberseguridad

- ✓ Realizar las configuraciones a los equipos de seguridad, según los procedimientos establecidos por su oficina.

7.5. Oficial de Seguridad y Confianza Digital

- ✓ Coordinar con los encargados de equipos de trabajo de la OGTIE lo relacionado a asegurar la integridad, confidencialidad y disponibilidad de la información del MINDEF.

A continuación, se detallan las personas que asumirán los roles del equipo de recuperación de desastres ante desastres.

Rol	Principal Secundario	Cargo
Líder de Recuperación de TI	Principal	Jefe de la Oficina General de Tecnologías de la Información y Estadística
	Secundario	Encargado de Infraestructura Tecnológica
Líder de Infraestructura Tecnológica	Principal	Responsable del equipo de trabajo de Infraestructura Tecnológica y telecomunicaciones
	Secundario	Responsable servidores del equipo de trabajo Infraestructura Tecnológica y telecomunicaciones
Líder de Sistemas de Información	Principal	Responsable del equipo de Sistemas de Información
	Secundario	Coordinación Alterna
Líder de Ciberseguridad	Principal	Coordinador del equipo de Ciberseguridad
	Secundario	Analista de Ciberseguridad

Oficial de Seguridad de la Información	Principal	Oficial de Seguridad y Confianza Digital
	Secundario	

8. METODOLOGÍA BIA

El análisis de impacto en el negocio (BIA) es un proceso que tiene por objetivo determinar, de acuerdo con la misión del Ministerio ("Garantizar la seguridad y defensa nacional del país de manera permanente y eficaz"), las funciones críticas de la entidad y sus recursos críticos asociados.
Esto se logra:

- Identificar los procesos críticos del MINDEF.
- Identificar todas las aplicaciones que soportan los procesos.
- Estimar la pérdida potencial.
- Estimar el tiempo de recuperación.

9. PRIORIDADES DE RECUPERACIÓN DE LOS SERVICIOS

- Los servicios de Tecnologías de la Información son recuperados según los resultados del análisis de impacto a las aplicaciones realizado con el personal clave del equipo de Sistemas de Información. Los resultados del análisis se muestran a continuación.

Priorización de recuperación	
	Servicios Internos:
1	Servicios WEB en Atención al Ciudadano
2	Servidor Base de Datos (Intranet Sharepoint)
3	Servidor Aplicaciones Sharepoint
4	Servicio de aplicaciones Intranet
5	Servicio de servidor de archivos 1
6	Servicio de servidor de archivos 2
7	Servicio de controlador de dominio principal
8	Servicio de controlador de dominio secundario
9	Servicio de despliegue de IPs
10	Servidor BD (Alta Disp. del Portal Web MySql)
11	Almacenamiento de Archivos del Sistradoc.
12	Servidor de Aplicaciones E-Firma (Sistema Tradoc)
13	Servicio de BD Oracle SIGA_MINDEF,SIGA_DIGEPREV)
14	Servicio de correo Principal
15	Servicio de correo secundario
16	Servicio de aplicación de MEF
17	Servicios de Oracle RAC 1
18	Servicios de Oracle RAC 2
19	Servicio de Aplicaciones Apache TRADOC
20	Servicio réplica de BD y Alta Disp. Sistema Tradoc
21	Servicio de acceso a carpetas y aplicaciones.

22	Servidor de Aplicaciones E-Firma(Sistema Tradoc)
23	Sistema de consultas PIDE

- Los tiempos estimados de recuperación para cada uno de los servicios de Tecnologías de la Información antes mencionados han sido calculados por la OGTIE tomando en consideración los recursos disponibles vigentes (Personal, Infraestructura, tecnología, entre otros).

Priorización de recuperación equipamiento tecnológico	
	Servicio Interno
1	Switch de borde (*)
	Core de datos (*)
	Core de voz (*)
	Central Telefónica (*)
	Antispam
	Firewall de capa 3

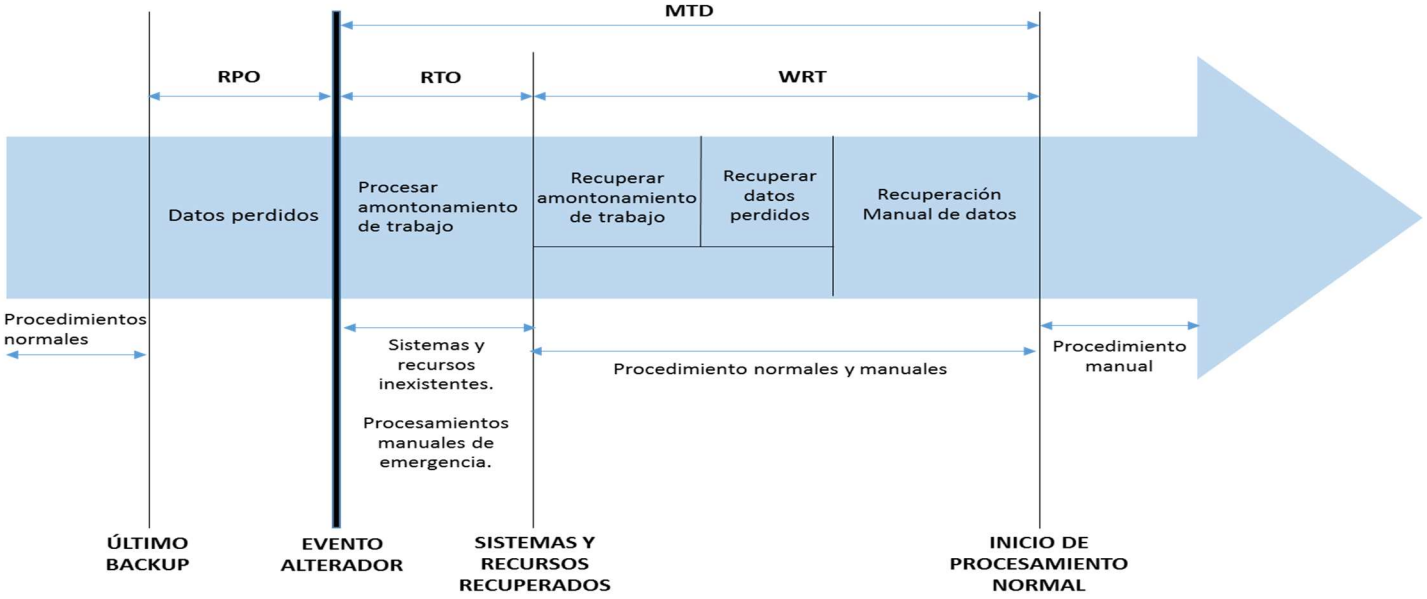
(*) No se cuenta con equipamiento alterno

Recovery Time Objetive (RTO): Representa el tiempo en el que se debe restablecer las operaciones del proceso de negocio para volver a brindar el servicio con normalidad. Para calcular el valor se emplea la siguiente fórmula:
RTO: Tiempo de configuración del hardware + tiempo de iniciación del sistema operativo + tiempo de iniciación de los sistemas de información + tiempo de restablecer los procesos y datos + tiempo de verificación + tiempo de conexión IP.

Recovery Point Objetive (RPO): Representa la cantidad de información que la OGTIE está dispuesta a perder desde su último backup. Para calcular este valor, solo es necesario preguntar la frecuencia con la que se realiza el backup de la información que utiliza el proceso crítico.

Maximun Tolerable Dowtime (MTD): Consiste en el espacio de tiempo durante el cual un proceso puede estar inoperante hasta que el MINDEF empiece a tener pérdidas y colapse.

Work Recovery Time (WRT): Es el tiempo disponible para recuperar datos perdidos una vez que los sistemas están reparados, dentro del MTD. Se calcula como el tiempo entre la recuperación del sistema y la normalización del procesamiento. Es el tiempo invertido en buscar datos perdidos y realizar reparaciones.



		RPO	RTO								
#	Sistemas de Información		Tiempo de iniciación o configuración de hardware	Tiempo de inicio del sistema operativo	Tiempo de inicio de los sistemas de información	Tiempo de restablecer los procesos y datos	Tiempo de verificación	Tiempo de conexión IP	TOTAL	Ubicación	Plataforma
1	Servicios WEB en Atención al Ciudadano	24 horas	2 horas	40 min	30 min	30 min	30 min	10 min	260 min (4.33 horas)	OGTIE	Linux
2	Servidor Base de Datos (Intranet Sharepoint)	24 horas	2 horas	40 min	40 min	30 min	30 min	10 min	270 min (4.33 horas)	OGTIE	W. Server
3	Servidor Aplicaciones Sharepoint	24 horas	2 horas	1 hora	40 min	30 min	45 min	10 min	305 min (5.083 horas)	OGTIE	W. Server
4	Servicio de aplicaciones Intranet	24 horas	2 horas	40 min	40 min	30 min	40 horas	10 min	360 min (6 horas)	OGTIE	W. Server
5	Servicio de servidor de archivos 1	24 horas	2 horas	1 hora	40 min	30 min	40 min	10 min	300 min (5 horas)	OGTIE	W. Server
6	Servicio de servidor de archivos 2	24 horas	2 horas	1 hora	40 min	30 min	40 min	10 min	300 min (5 horas)	OGTIE	W. Server
7	Servicio de controlador de dominio principal	24 horas	2 horas	1 hora	40 min	30 min	5 min	10 min	265 min (4.41 horas)	OGTIE	W. Server
8	Servicio de controlador de dominio secundario	24 horas	2 horas	2 horas	0 horas	0 horas	30 min	10 min	280 min (4.66 horas)	OGTIE	W. Server

#	Sistemas de Información	RPO	RTO						TOTAL	Ubicación	Plataforma
			Tiempo de iniciación o configuración de hardware	Tiempo de inicio del sistema operativo	Tiempo de inicio de los sistemas de información	Tiempo de restablecer los procesos y datos	Tiempo de verificación	Tiempo de conexión IP			
9	Servicio de despliegue de IPs	24 horas	2 horas	2 horas	0 horas	0 horas	30 min	10 min	280 min (4.66 horas)	OGTIE	W. Server
10	Servidor BD WEB	24 horas	2 horas	40 min	30 min	30 min	30 min	10 min	260 min (4.33 horas)	OGTIE	Linux
11	Almacenamiento de Archivos del Sistradoc.	24 horas	2 horas	1 hora	30 min	30 min	30 min	10 min	280 min (4.66 horas)	OGTIE	W. Server
12	Servidor de Aplicaciones E-Firma (Sistema Tradoc)	24 horas	2 horas	1 hora	30 min	30 min	30 min	10 min	280 min (4.66 horas)	OGTIE	W. Server
13	Servicio de BD Oracle SIGA_MINDEF,SIGA_DI GEPREV)	24 horas	2 horas	1 hora	30 min	30 min	30 min	10 min	280 min (4.66 horas)	OGTIE	Linux
14	Servicio de correo Principal	24 horas	2 horas	40 min	30 min	30 min	30 min	10 min	260 min (4.33 horas)	OGTIE	W. Server
15	Servicio de correo secundario	24 horas	2 horas	40 min	30 min	30 min	5 min	10 min	235 min (3.91 horas)	OGTIE	W. Server
16	Servicio de aplicación de MEF	24 horas	2 horas	40 min	30 min	30 min	5 min	10 min	235 min (3.91 horas)	OGTIE	W. Server
17	Servicios de Oracle RAC 1	24 horas	2 horas	40 min	30 min	30 min	5 min	10 min	235 min (3.91 horas)	OGTIE	Linux
18	Servicios de Oracle RAC 2	24 horas	2 horas	40 min	30 min	30 min	5 min	10 min	235 min (3.91 horas)	OGTIE	Linux

		RPO	RTO								
#	Sistemas de Información		Tiempo de iniciación o configuración de hardware	Tiempo de inicio del sistema operativo	Tiempo de inicio de los sistemas de información	Tiempo de restablecer los procesos y datos	Tiempo de verificación	Tiempo de conexión IP	TOTAL	Ubicación	Plataforma
19	Servicio de Aplicaciones Apache TRADOC	24 horas	2 horas	40 min	30 min	30 min	5 min	10 min	235 min (3.91 horas)	OGTIE	W. Server
20	Servicio réplica de BD y Alta Disp. Sistema Tradoc	24 horas	2 horas	40 min	30 min	30 min	5 min	10 min	235 min (3.91 horas)	OGTIE	W. Server
21	Servicio de acceso a carpetas y aplicaciones.	24 horas	2 horas	40 min	30 min	30 min	5 min	10 min	235 min (3.91 horas)	OGTIE	W. Server
22	Servidor de Aplicaciones E-Firma(Sistema Tradoc)	24 horas	2 horas	40 min	30 min	30 min	5 min	10 min	235 min (3.91 horas)	OGTIE	Linux
23	Sistema de consultas PIDE	24 horas	2 horas	40 min	30 min	30 min	5 min	10 min	235 min (3.91 horas)	OGTIE	Linux

#	Equipo de Infraestructura	RPO	RTO				
			Tiempo de iniciación o configuración de hardware	Tiempo de verificación	Tiempo de conexión IP	TOTAL	Ubicación
01	**Central Telefónica (*)**	0 horas	120 min	10 min	1 min	131 min	OGTIE
02	**Switch de borde(*)**	0 horas	20 min	10 min	1 min	31 min	OGTIE
03	**Core de voz (*)**	0 horas	20 min	10 min	1 min	31 min	OGTIE
04	**Core de datos (*)**	0 horas	20 min	10 min	1 min	31 min	OGTIE
05	**AntiSpam**	4 horas	2 horas	10 min	1 min	6 h. 21 min	OGTIE
06	**Firewall de capa 3**	0 horas	20 min	10 min	1 min	31 min	OGTIE

(*) No se cuenta con equipamiento alterno

Procedimientos de Activación				
Tipo de evento	Descripción del evento	Verde	Amarrillo	Rojo
Sismo	Sacudida violenta de la corteza y manto terrestres, ocasionada por fuerzas que actúan en el interior de la Tierra.	Impacto a todas las oficinas <= 16 horas	Impacto a todas las Oficinas > 16 horas y <= 24 horas	Impacto a todas las Oficinas > 24 horas
Incendio	Fuego de grandes proporciones que arde de forma fortuita o provocada y destruye cosas que no están destinadas a quemarse	Oficina Principal / Parte significativa de la red <= 2 horas	Oficina Principal / Parte significativa de la red > 2 horas y <= 4 horas	Oficina Principal / Parte significativa de la red >4 horas
Ataque Terrorista	Acción deliberada que emplea medios violentos cuyos efectos pueden vulnerar la seguridad y la integridad de las personas, de las cosas o de los servicios públicos	Oficina Principal / Parte significativa de la red <= 2 horas	Oficina Principal / Parte significativa de la red > 2 horas y <= 4 horas	Oficina Principal / Parte significativa de la red >4 horas
Social	✓Huelgas externas ✓Paros ✓Delincuencia ✓Manifestaciones ✓Terrorismo ✓Conflicto bélico	Oficina Principal / Parte significativa de la red <= 2 horas	Oficina Principal / Parte significativa de la red > 2 horas y <= 4 horas	Oficina Principal / Parte significativa de la red >4 horas
Fluido eléctrico	Corte no programado en la zona	Oficina Principal / Parte significativa de la red <= 2 horas	Oficina Principal / Parte significativa de la red > 2 horas y <= 4 horas	Oficina Principal / Parte significativa de la red >4 horas
Telecomunicaciones	Falla en el enlace Principal, equipos de comunicación (Oficina Principal)	Impacto a todas las Oficinas <= 2 horas	Impacto a todas las Oficinas > 2 horas y <= 4 horas	Impacto a todas las Oficinas > 4 horas
	Falla en el enlace de datos (nodo principal)	Impacto a una parte significativa de la red <= 2 horas	Impacto a una parte significativa de la red > 2 horas y <= 4 horas	Impacto a una parte significativa de la red > 4 horas
Hardware	Equipos del Centro de Procesamiento de Datos	Impacto a todas las oficinas <= 2 horas	Impacto a todas las Oficinas > 2 horas y <= 4 horas	Impacto a todas las Oficinas > 4 horas
Software	Aplicaciones y Base de datos de soporte al proceso de trámite documentario, proceso previsional	Impacto a todas las oficinas <= 2 horas	Impacto a todas las Oficinas > 2 horas y <= 4 horas	Impacto a todas las Oficinas > 4 horas

Procedimientos de Activación				
Tipo de evento	Descripción del evento	Verde	Amarrillo	Rojo
Infraestructura	Aire acondicionado, UPS, grupo electrógeno (centro de procesamiento de datos)	Impacto a todas las oficinas <= 2 horas	Impacto a todas las Oficinas > 2 horas y <= 4 horas	Impacto a todas las Oficinas > 4 horas
Ataques cibernéticos	Denegación de servicios, código malicioso, accesos no autorizados, infección por ransomware	Impacto a todas las oficinas <= 2 horas	Impacto a todas las Oficinas > 2 horas y <= 4 horas	Impacto a todas las Oficinas > 4 horas
Proveedores	Proveedores críticos de procesos urgentes	Impacto a todas las oficinas <= 2 horas	Impacto a todas las Oficinas > 2 horas y <= 4 horas	Impacto a todas las Oficinas > 4 horas

10. GESTIÓN DEL RIESGO

Ante la posible materialización de algún evento que ponga en riesgo la operatividad del Centro de Datos y con el fin de establecer prioridades para la mitigación de los riesgos.

Riesgos Tecnológicos

- ✓ Fallas en el Fluido Eléctrico
- ✓ Sabotaje Informático

Riesgos Humanos

- ✓ Robos
- ✓ Artefactos explosivos
- ✓ Problemas con los proveedores de insumo o subproductos

Riesgos Desastres Naturales

- ✓ Sismos
- ✓ Incendios
- ✓ Inundaciones

11. FASES DEL PLAN DE RECUPERACIÓN DE SERVICIOS INFORMÁTICOS

El Plan de Recuperación de Servicios Informáticos tiene las siguientes fases: Antes del Desastre, Alerta de Desastre, Desastre Declarado "Diagnostico", Desastre Controlado "Operación en Contingencia", Fin de Desastre "Cierre" y Retorno a la normalidad "Reserva".

12. PROCEDIMIENTO DE ACTUACIÓN ANTES DEL DESASTRE

Comprende la identificación de las actividades preventivas a realizar, a fin de tomar las acciones correspondientes para los riesgos que puedan afectar a la normal operación de los servicios.

A continuación, se alistan las actividades por cada "rol" del equipo de recuperación:

ROL: Líder de Infraestructura Tecnológica y Telecomunicaciones	
ANTES: ACTIVIDADES DE PREPARACIÓN	
#	Actividades a realizar
1	**Identificación de riesgos:** – Identificar periódicamente (por lo menos una vez al año) los riesgos que puedan afectar la normal operación de la infraestructura del Centro de Datos Principal.
2	**Acciones previsoras** – Conformación de un Equipo de Recuperación de Infraestructura del Centro de Datos Principal, integrado por los principales roles responsables del área. *Ver "ANEXO - 02 - Equipo de Recuperación" y "ANEXO - 03 - Relación de Proveedores"* – Actualizar periódicamente los datos de contacto del personal responsable de las actividades de recuperación del área, en caso de presentarse un evento de desastre. *Ver "ANEXO - 02 - Equipo de Recuperación".* – Ejecutar al menos una vez al año una prueba o ejercicio con la finalidad de probar y reforzar el uso del Plan. Para ello se deberá elaborar un Plan de Pruebas anual indicando el tipo de prueba y su complejidad.
3	**Respecto a la disponibilidad del personal:** – Validar el plan respecto a la vigencia del personal existente en el área. – Validar que titular y alterno de un mismo rol, no estén ausentes en periodos similares.
4	**Respecto al esquema interno de notificación:** – Efectuar pruebas de comunicación entre el personal, a fin de validar la vigencia de la información de contacto registrada en el plan. *Ver "ANEXO - 02 - Equipo de Recuperación".*
5	**Respecto a externos:** – Validar funcionamiento de los números de teléfono de los proveedores externos clave. *Ver "ANEXO - 03 - Relación de Proveedores".*
6	**Identificación de riesgos:** – Identificar periódicamente (por lo menos una vez al año) los riesgos que puedan afectar la normal operación de la conectividad del Centro de Datos Principal.
7	**Acciones previsoras** – Conformación de un Equipo de Recuperación de Conectividad del Centro de Datos Principal, integrado por los principales roles responsables del área y de los proveedores críticos (en caso aplique). *Ver "ANEXO - 02 - Equipo de Recuperación" y "ANEXO - 03 - Relación de Proveedores"* – Actualizar periódicamente los datos de contacto del personal responsable de las actividades de recuperación del área, en caso de presentarse un evento de desastre. *Ver "ANEXO - 02 - Equipo de Recuperación"* – Ejecutar al menos una vez al año un a prueba o ejercicio con la finalidad de probar y reforzar el uso del Plan. Para ello se deberá elaborar un Plan de Pruebas anual indicando el tipo de prueba y su complejidad.

ROL: Líder de Infraestructura Tecnológica y Telecomunicaciones	
ANTES: ACTIVIDADES DE PREPARACIÓN	
#	Actividades a realizar
8	**Respecto a recursos que soportan el servicio:** Monitorear permanentemente en el Centro de Datos Principal la existencia y funcionamiento de: – Herramientas de trabajo (**Equipos de monitoreo**, puestos de trabajo, teléfonos, etc.) – Servicios de Tecnología que sirven para monitorear los servicios soportados
9	**Respecto a la preparación y actualización de registros vitales:** – Actualizar los registros de Direccionamiento IP – Revisar la vigencia de los archivos de las Topologías – Revisar y actualizar los archivos de Configuraciones – Revisar y actualizar script de backup de comunicaciones (en caso sea necesario) – Realizar periódicamente los backup de comunicaciones – Respaldar el Cliente VPN (software + perfiles)
10	**Respecto a la disponibilidad del personal:** – Validar el plan respecto a la vigencia del personal existente en el área. – Validar que titular y alterno de un mismo rol, no estén ausentes en periodos similares. – Validar que los medios de transporte y los puntos de concentración del personal sean válidos.
11	**Respecto al esquema interno de notificación:** – Efectuar pruebas de comunicación entre el personal, a fin de validar la vigencia de la información de contacto registrada en el plan. *Ver "ANEXO - 02 - Equipo de Recuperación"*
12	**Respecto a externos:** – Validar funcionamiento de los números de teléfono de los proveedores externos clave (en caso aplique). *Ver "ANEXO - 03 - Relación de Proveedores"*

ROL: Líder de Sistemas de Información	
ANTES: ACTIVIDADES DE PREPARACIÓN	
#	Actividades a realizar
1	**Identificación de riesgos:** – Identificar periódicamente (por lo menos una vez al año) los riesgos que puedan afectar la normal operación del Centro de Datos Principal. Asimismo, identificar los riesgos de los ambientes que serán utilizados para activar los procesos de contingencia en el Centro de Datos Alterno. Por ejemplo: Verificación de pruebas de restauración de backups, capacidad de infraestructura en Centro de Datos Alterno (capacidad en disco, memoria RAM, entre otros).
2	**Acciones previsoras** – Conformación de un Equipo de Recuperación de Aplicaciones del Centro de Datos Principal, integrado por los principales roles responsables del área y de los proveedores críticos (en caso aplique).

ROL: Líder de Sistemas de Información	
ANTES: ACTIVIDADES DE PREPARACIÓN	
#	Actividades a realizar
	Ver "ANEXO - 02 - Equipo de Recuperación" y "ANEXO - 03 - Relación de Proveedores" – Actualizar periódicamente los datos de contacto del personal responsable de las actividades de recuperación del área, en caso de presentarse un evento de desastre. *Ver "ANEXO - 02 - Equipo de Recuperación"* – Ejecutar al menos una vez al año un a prueba o ejercicio con la finalidad de probar y reforzar el uso del Plan de recuperación. Para ello se deberá elaborar un Plan de Pruebas anual indicando el tipo de prueba y su complejidad.
3	**Respecto a la preparación y actualización de registros vitales:** – Validar la disponibilidad del código fuente de los sistemas/aplicaciones. – Disponer de un Inventario de sistemas/aplicaciones.
4	**Respecto a la disponibilidad del personal:** – Validar el plan respecto a la vigencia del personal existente en el área. – Validar que titular y alterno de un mismo rol, no estén ausentes en periodos similares. – Validar que los medios de transporte y los puntos de concentración del personal sean válidos.
5	**Respecto al esquema interno de notificación:** – Efectuar pruebas de comunicación entre el personal, a fin de validar la vigencia de la información de contacto registrada en el plan. *Ver "ANEXO - 02 - Equipo de Recuperación"*
6	**Respecto a externos:** – Validar funcionamiento de los números de teléfono de los proveedores externos clave. *Ver "ANEXO - 03 - Relación de Proveedores"*

13. PROCEDIMIENTOS DE RESPUESTA Y OPERACIÓN EN CONTINGENCIA (RECUPERACIÓN)

Comprende las actividades desde el momento de ocurrida la interrupción del servicio hasta el restablecimiento del mismo a un nivel aceptable.
A continuación, se listan las actividades por cada "rol" del equipo de recuperación.

ROL: Líder de Equipo de Recuperación	
DURANTE: PROCEDIMIENTO DE RESPUESTA Y OPERACIÓN EN CONTINGENCIA	
#	Actividades a realizar
1	Ocurrido el evento de desastre, recibirá una notificación de la situación presentada por parte del Líder de Infraestructura. La comunicación se podrá realizar mediante los siguientes medios: • Presencial (si el evento se presentó en horario de oficina o si es viable) • Teléfono Móvil o Fijo • Grupo de Whatsapp (Equipo de Activación Lima) • Buzón de correo (Líder de recuperación) • Cualquier otro medio de comunicación vía datos

ROL: Líder de Equipo de Recuperación	
DURANTE: PROCEDIMIENTO DE RESPUESTA Y OPERACIÓN EN CONTINGENCIA	
#	Actividades a realizar
2	Comunicar la situación y convocar a los Líderes de Infraestructura, Telecomunicaciones y Aplicaciones en el Centro de Comando. Asimismo, solicitará a cada uno de los líderes el cálculo de los tiempos de recuperación y la evaluación de la afectación presentada en el Centro de Datos Principal (afectación de personal, disponibilidad de las instalaciones de trabajo, etc). *Ver "ANEXO - 01 - Ubicación Centro de Comando"* *Ver "ANEXO - 02 - Equipo de Recuperación"* **IMPORTANTE:** El Centro de Comando es el punto de reunión del Líder de Recuperación y su equipo. En caso se hayan caído las comunicaciones o el evento se haya presentado fuera de horario de oficina, el punto de reunión principal de los Líderes será la "Sala de Crisis" o de forma alternativa en el momento del desastre el Líder del Plan definirá una nueva sede, pudiendo ejecutarse la reunión de Líderes en forma remota a través de los mecanismos existentes.
3	Analizar cada uno de los reportes provistos por los líderes y en caso se haya decidido activar el Plan de recuperación, comunicar los Líderes de Infraestructura, Telecomunicaciones y Sistemas de Información, la **"Declaración de desastre" y tipo de alerta "Roja/Amarilla",** La comunicación se podrá realizar mediante los siguientes medios: • Presencial (si el evento se presentó en horario de oficina o si es viable) • Teléfono Móvil o Fijo • Grupo de Whatsapp (Equipo de Activación Lima) • Buzón de correo (Equipo de recuperación) • Cualquier otro medio de comunicación vía datos *Ver "ANEXO - 02 - Equipo de Recuperación"*
4	Solicitar al equipo de líderes ejecutar las gestiones para movilizar al personal crítico: empresas de taxi, movilidad pública y/o transporte particular, que se encuentren disponibles.
5	Coordinar con el equipo de líderes, la entrega y habilitación de los documentos/recursos necesarios para la recuperación de los servicios críticos afectados. *Ver "ANEXO - 04 - Dependencias Internas"* *Ver "ANEXO - 05 - Registros Vitales"* *Ver "ANEXO - 06 – Procedimientos de Infraestructura"* *Ver "ANEXO - 07 - Requerimiento de recursos"*
6	Monitorear desde el Centro de Comando, los desplazamientos del personal correspondiente hacia el Centro de Datos Alterno y el inicio de las tareas de recuperación de los servicios críticos afectados por parte de los Líderes de Telecomunicaciones, Infraestructura y Sistemas de Información. *Ver "ANEXO - 01 - Ubicación Centro de Comando"*
7	En caso de tener dificultades con el acceso a las instalaciones del Centro de Datos Alterno solicitar al Líder de Infraestructura coordinar con el Líder de Infraestructura del Centro de Datos Alterno.
8	Solicitar al Líder de Infraestructura coordinar la logística de adquisición de los recursos adicionales que se puedan requerir por parte de los Líderes de Telecomunicaciones, Infraestructura y Aplicaciones.
9	Monitorear la ejecución de los procedimientos de contingencia contenidos en los Planes de Continuidad de Negocio por cada servicio crítico.

ROL: Líder de Equipo de Recuperación	
DURANTE: PROCEDIMIENTO DE RESPUESTA Y OPERACIÓN EN CONTINGENCIA	
#	Actividades a realizar
10	Una vez que el Líder de Sistemas de Información, confirme la recuperación de los servicios críticos en el Centro de Datos Alterno, validar el estatus de los servicios para dar pase al estado **"Desastre Controlado".**
11	Comunicar a los Líderes de Telecomunicaciones, Infraestructura y Sistemas de Información, el estado **"Desastre Controlado"**. La comunicación se podrá realizar mediante los siguientes medios: • Presencial (si el evento se presentó en horario de oficina o si es viable) • Teléfono Móvil o Fijo • Grupo de Whatsapp (Equipo de Activación Lima) • Buzón de correo (Equipo de recuperación) • Cualquier otro medio de comunicación vía datos *Ver "ANEXO - 02 - Equipo de Recuperación"*

ROL: Líder de Infraestructura	
DURANTE: PROCEDIMIENTO DE RESPUESTA Y OPERACIÓN EN CONTINGENCIA	
#	Actividades a seguir
1	Ocurrido el evento de desastre, el Centro de Control y/o El Proveedor de comunicaciones del Ministerio notifica la situación al Líder de Infraestructura. Seguidamente el Líder de Infraestructura realiza las validaciones correspondientes a través del canal y persona autorizada en Level3 y en caso de confirmar la notificación del evento de desastre, comunicará al Líder de Recuperación lo ocurrido y si se trata de una alerta "Amarilla/Roja". La comunicación se podrá realizar mediante los siguientes medios: • Presencial (si el evento se presentó en horario de oficina o si es viable) • Teléfono Móvil o Fijo • Grupo de Whatsapp (Equipo de Activación Lima) • Buzón de correo (Líder de recuperación) • Cualquier otro medio de comunicación vía datos *Ver "ANEXO - 02 - Equipo de Recuperación"*
2	Gestionar la generación de accesos del personal del equipo de Infraestructura que apoyará en la recuperación de los servicios, a las instalaciones del Centro de Datos Principal (Level 3) en caso de que no dispongan de un acceso preaprobado.
3	En caso de presentarse el evento de desastre cuando se encuentra fuera de horario de oficina o fuera de las instalaciones de trabajo, desplazarse mediante las empresas de taxi, movilidad pública o transporte particular (dependiendo del caso), hacia el Centro de Datos Principal
4	Al llegar al ambiente afectado, el personal del Equipo de Infraestructura debe ingresar a las salas respectivas con los implementos de seguridad correspondientes (si fuese requerido).
5	Solicitar reporte periódico de las condiciones ambientales (energía, climatización) del Centro de Datos Principal e informar sobre la situación al Líder de Recuperación. La comunicación se podrá realizar mediante los siguientes medios: • Presencial (si el evento se presentó en horario de oficina o si es viable) • Teléfono Móvil o Fijo • Grupo de Whatsapp (Equipo de Activación Lima)

ROL: Líder de Infraestructura	
DURANTE: PROCEDIMIENTO DE RESPUESTA Y OPERACIÓN EN CONTINGENCIA	
#	Actividades a seguir
	• Buzón de correo (Líder de recuperación) • Cualquier otro medio de comunicación vía datos *Ver "ANEXO - 02 - Equipo de Recuperación"*
6	El proveedor Level3 deberá realizar las actividades de reparación de daños sobre la infraestructura a fin de evitar otros riesgos según el acuerdo contractual y niveles de servicio para energía y climatización. *Ver "ANEXO - 03 - Relación de Proveedores"*
7	Según los avances realizados y hasta la recuperación de los servicios notificar al Líder de Recuperación la situación. La comunicación se podrá realizar mediante los siguientes medios: • Presencial (si el evento se presentó en horario de oficina o si es viable) • Teléfono Móvil o Fijo • Grupo de Whatsapp (Equipo de Activación Lima) • Buzón de correo (Líder de recuperación) • Cualquier otro medio de comunicación vía datos *Ver "ANEXO - 02 - Equipo de Recuperación"*
8	Ocurrido el evento de desastre, recibe la comunicación del Líder de Recuperación y si aplica, se reúne con él en el Centro de Comando. Seguidamente, notifica la situación a los miembros de su equipo y ejecuta un diagnóstico de la situación presentada. Finalmente, comunica al Líder de Recuperación el cálculo de los tiempos de recuperación y la evaluación de la afectación presentada en el Centro de Datos Principal (afectación de personal, disponibilidad de las instalaciones de trabajo, etc) a nivel de conectividad. *Ver "ANEXO - 01 - Ubicación Centro de Comando"* *Ver "ANEXO - 02 - Equipo de Recuperación"* **IMPORTANTE:** El Centro de Comando es el punto de reunión del Líder de Recuperación y su equipo. En caso se hayan caído las comunicaciones o el evento se haya presentado fuera de horario de oficina, el punto de reunión principal de los Líderes será la "Sala de Crisis" o de forma de alternativa en el momento del desastre el Líder del definirá una nueva sede, pudiendo ejecutarse la reunión de Líderes en forma remota a través de los mecanismos existentes.
9	Recibe la notificación de **"Desastre Declarado"** y tipo de alerta "Amarilla/Roja" del Líder de Recuperación y comunica al personal de su equipo la situación. La comunicación se podrá realizar mediante los siguientes medios: • Presencial (si el evento se presentó en horario de oficina o si es viable) • Teléfono Móvil o Fijo • Grupo de Whatsapp (Equipo de Activación Lima) • Buzón de correo (Equipo de recuperación) • Cualquier otro medio de comunicación vía datos *Ver "ANEXO - 02 - Equipo de Recuperación"*
10	En coordinación con los miembros de su equipo, valorar si es necesario comunicarse con los proveedores externos, a fin de cumplir con la recuperación de los servicios críticos. *Ver "ANEXO - 03 - Relación de Proveedores"*

ROL: Líder de Infraestructura	
DURANTE: PROCEDIMIENTO DE RESPUESTA Y OPERACIÓN EN CONTINGENCIA	
#	Actividades a seguir
11	Luego de que se conozca la magnitud del desastre y que el Líder de Recuperación, haya comunicado **"Desastre declarado"**, coordinar: – Alternativas para movilizar al personal crítico hacia Centro de Datos Principal y/o Centro de Datos Alterno (en caso de que el evento se haya presentado fuera de horario de oficina o sea requerido, para apoyar en la activación de la contingencia en Centro de Datos Alterno: empresas de taxi, movilidad pública y/o transporte particular). – Vía teléfono o correo electrónico, el reporte de la situación operativa en la que se encuentran los servicios críticos (según prioridad de recuperación). – La entrega y/o habilitación de los documentos/recursos necesarios para la ejecución de sus tareas de recuperación. *Ver "ANEXO - 04 - Dependencias Internas"* *Ver "ANEXO - 05 - Registros Vitales"* *Ver "ANEXO - 06 – Procedimientos de Infraestructura"* *Ver "ANEXO - 07 - Requerimiento de recursos"*
12	Activar y ejecutar el **"Plan de Continuidad de los servicios de Red"**. *Ver "ANEXO - 06 - Procedimientos de Infraestructura"*
13	Dar inicio a las actividades de recuperación de las aplicaciones según corresponda: • Activar y ejecutar los Servicios WEB en Atención al Ciudadano • Activar y ejecutar los Servidores de Base de Datos (Intranet Sharepoint) • Activar y ejecutar el Servidor Aplicaciones Sharepoint • Activar y ejecutar el Servicio de aplicaciones Intranet • Activar y ejecutar el Servicio de servidor de archivos 1 • Activar y ejecutar el Servicio de servidor de archivos 2 • Activar y ejecutar el Servicio de controlador de dominio principal • Activar y ejecutar el Servicio de controlador de dominio secundario • Activar y ejecutar el Servicio de despliegue de IPs • Activar y ejecutar el Servidor BD WEB • Activar y ejecutar el Almacenamiento de Archivos del Sistradoc. • Activar y ejecutar el Servidor de Aplicaciones E-Firma (Sistema Tradoc) • Servicio de BD Oracle SIGA_MINDEF, SIGA_DIGEPREV. • Activar y ejecutar el Servicio de correo Principal • Activar y ejecutar el Servicio de correo secundario • Activar y ejecutar el Servicio de aplicación de MEF • Activar y ejecutar el Servicios de Oracle RAC 1 • Activar y ejecutar el Servicios de Oracle RAC 2 • Activar y ejecutar el Servicio de Aplicaciones Apache TRADOC • Activar y ejecutar el Servicio réplica de BD y Alta Disp. Sistema Tradoc • Activar y ejecutar el Servicio de acceso a carpetas y aplicaciones. • Activar y ejecutar el Sistema de consultas PIDE *Ver "ANEXO - 06 - Procedimientos de Infraestructura"*
14	Según sea el caso, se recopilará información de los recursos adicionales que sean necesarios para que el Líder de Telecomunicaciones, coordine la logística de adquisición, con el Líder de Recuperación.
15	Monitorear los avances en la activación de la contingencia de la red.

ROL: Líder de Infraestructura	
DURANTE: PROCEDIMIENTO DE RESPUESTA Y OPERACIÓN EN CONTINGENCIA	
#	Actividades a seguir
16	Una vez que ya se hayan recuperado los servicios a un nivel aceptable, comunicar la situación al Líder de Recuperación para dar pase al estado **"Desastre Controlado".** La comunicación se podrá realizar mediante los siguientes medios: • Presencial (si el evento se presentó en horario de oficina o si es viable) • Teléfono Móvil o Fijo • Grupo de Whatsapp (Equipo de Activación Lima) • Buzón de correo (Líder de recuperación) • Cualquier otro medio de comunicación vía datos *Ver "ANEXO - 02 - Equipo de Recuperación"*

ROL: Líder de Sistemas de Información	
DURANTE: PROCEDIMIENTO DE RESPUESTA Y OPERACIÓN EN CONTINGENCIA	
#	Actividades a seguir
1	Ocurrido el evento de desastre, recibe la comunicación del Líder de Recuperación y si aplica, se reúne con él en el Centro de Comando. Seguidamente, notifica la situación a los miembros de su equipo y ejecuta un diagnóstico de la situación presentada. Finalmente, comunica al Líder de Recuperación el cálculo de los tiempos de recuperación y la evaluación de la afectación presentada en el CPD Principal (afectación de personal, disponibilidad de las instalaciones de trabajo, etc.) a nivel de aplicaciones. *Ver "ANEXO - 01 - Ubicación Centro de Comando"* *Ver "ANEXO - 02 - Equipo de Recuperación"* **IMPORTANTE:** El Centro de Comando es el punto de reunión del Líder de Recuperación y su equipo. En caso se hayan caído las comunicaciones o el evento se haya presentado fuera de horario de oficina, el punto de reunión principal de los Líderes será la "Sala de Crisis" o de forma alternativa en el momento del desastre el Líder del Plan definirá una nueva sede, pudiendo ejecutarse la reunión de Líderes en forma remota a través de los mecanismos existentes.
2	Recibe la notificación de **"Desastre Declarado"** y tipo de alerta "Amarilla/Roja" del Líder de Recuperación y comunica al personal de su equipo la situación. La comunicación se podrá realizar mediante los siguientes medios: • Presencial (si el evento se presentó en horario de oficina o si es viable) • Teléfono Móvil o Fijo • Grupo de Whatsapp (Equipo de Activación Lima) • Buzón de correo (Equipo de recuperación) • Cualquier otro medio de comunicación vía datos *Ver "ANEXO - 02 - Equipo de Recuperación"*
3	En coordinación con los miembros de su equipo, valorar si es necesario comunicarse con los proveedores externos, a fin de cumplir con la recuperación de los servicios críticos. *Ver "ANEXO - 03 - Relación de Proveedores"*
4	Luego de que se conozca la magnitud del desastre y que el Líder de Recuperación, haya comunicado la **"Desastre declarado"**, coordinar:

ROL: Líder de Sistemas de Información	
DURANTE: PROCEDIMIENTO DE RESPUESTA Y OPERACIÓN EN CONTINGENCIA	
#	Actividades a seguir
	– Alternativas para movilizar al personal crítico hacia Centro de Datos Principal Level 3 y/o Centro de Datos Alterno (en caso de que el evento se haya presentado fuera de horario de oficina o sea requerido, para apoyar en la activación de la contingencia en Centro de Datos Alterno): empresas de taxi, movilidad pública y/o transporte particular. – Vía teléfono o correo electrónico, el reporte de la situación operativa en la que se encuentran los servicios críticos (según prioridad de recuperación). – La entrega y/o habilitación de los documentos/recursos necesarios para la ejecución de sus tareas de recuperación. *Ver "ANEXO - 04 - Dependencias Internas"* *Ver "ANEXO - 05 - Registros Vitales"* *Ver "ANEXO - 06 - Procedimientos de Infraestructura"* *Ver "ANEXO - 07 - Requerimiento de recursos"*
5	Iniciar el desplazamiento del personal correspondiente al ambiente destinado para la activación de la contingencia. En caso de tener dificultades con el acceso a las instalaciones coordinar con el Proveedor de Centro de Datos Principal y/o Centro de Datos Alterno. *Ver "ANEXO - 03 - Relación de Proveedores"*
6	Dar inicio a las actividades de validación del funcionamiento de las aplicaciones según corresponda: • Validar el funcionamiento de los Servicios de cara al ciudadano • Validar el funcionamiento de los sistemas de gestión interna • Validar el funcionamiento del Servidor Aplicaciones Sharepoint • Validar el funcionamiento de los Servicios de aplicaciones Intranet • Validar el funcionamiento de los Almacenamiento de Archivos del Sistradoc. • Validar el funcionamiento de las aplicaciones del MEF • Validar el funcionamiento de las Servicio de Aplicaciones Apache TRADOC • Validar el funcionamiento del Servicio de réplica de BD y Alta Disp. Sistema Tradoc • Validar el funcionamiento del Servicio de acceso a carpetas y aplicaciones. • Validar el funcionamiento del Sistema de consultas PIDE La prioridad de recuperación de los servicios de TI se ejecutará tomando en consideración los resultados del "Análisis de Impacto de las Aplicaciones (AIA)" detallados en la sección 8 del presente Plan. *Ver "ANEXO - 06 - Procedimientos de Infraestructura"*
7	Según sea el caso, se recopilará información de los recursos adicionales que sean necesarios para que el Líder de Sistemas de Información, coordine la logística de adquisición, con el Líder de Recuperación.
8	Monitorear los avances en la Activación de la Contingencia en el Centro de Datos Alterno.
9	Una vez que ya se hayan recuperado los servicios a un nivel aceptable, comunicar la situación al Líder de Recuperación para dar pase al estado **"Desastre Controlado".** La comunicación se podrá realizar mediante los siguientes medios: • Presencial (si el evento se presentó en horario de oficina o si es viable) • Teléfono Móvil o Fijo • Grupo de Whatsapp (Equipo de Activación Lima) • Buzón de correo (Líder de recuperación)

ROL: Líder de Sistemas de Información	
DURANTE: PROCEDIMIENTO DE RESPUESTA Y OPERACIÓN EN CONTINGENCIA	
#	Actividades a seguir
	• Cualquier otro medio de comunicación vía datos *Ver "ANEXO - 02 - Equipo de Recuperación"*

14. PROCEDIMIENTO DE RESTAURACIÓN Y RETORNO

Comprende las actividades de restauración, luego de la recuperación de las operaciones a un nivel aceptable para la organización, hasta el retorno a la normalidad de los servicios.

A continuación, se listan las actividades por cada "rol" del equipo de recuperación.

ROL: Líder de Equipo de Recuperación	
DESPUES: PROCEDIMIENTO DE RESTAURACIÓN Y RETORNO	
#	Actividades a realizar
1	En base al monitoreo continuo y a los reportes de avance, respecto a la operación en contingencia (reparación de daños, operatividad de los servicios, entre otros) recibidos periódicamente por parte de los Líderes de Infraestructura, Telecomunicaciones y Sistemas de Información decidir: - Si se ha superado el "**Desastre"** y dar pase al estado **"Fin de Desastre"**
2	Comunicar el estado **"Fin de Desastre"** a los Lideres de Infraestructura, Telecomunicaciones y Sistemas de Información. La comunicación se podrá realizar mediante los siguientes medios: • Presencial (si el evento se presentó en horario de oficina o si es viable) • Teléfono Móvil o Fijo • Grupo de Whatsapp (Equipo de Activación Lima) • Buzón de correo (Equipo de recuperación) • Cualquier otro medio de comunicación vía datos *Ver "ANEXO - 02 - Equipo de Recuperación"*
3	Comunicar a los Líderes de Infraestructura, Conectividad y Aplicaciones el inicio del "**Retorno a la normalidad"**, preparar plan de acción para el retorno a las instalaciones primarias y asignar responsabilidades.
4	Una vez confirmado el fin de **"Retorno a la Normalidad"** y notificar la **"Desactivación del Plan",** solicitar a cada Líder un informe/reporte de las actividades realizadas, problemas, entre otros que se hayan presentado en la recuperación de las operaciones.
5	Participar en el taller de **"Lecciones Aprendidas"** respecto a la situación presentada.
6	Coordinar la actualización del Plan de Recuperación de Servicios Informáticos y documentación relacionada (Planes de Continuidad, anexos, entre otros) según las observaciones y lecciones aprendidas identificadas.

ROL: Líder de Infraestructura	
DESPUES: PROCEDIMIENTO DE RESTAURACIÓN Y RETORNO	
#	Actividades a realizar
1	Informar de manera continua a través de reportes de avance al Líder de Recuperación respecto a la operación en contingencia (reparación de daños, operatividad de los servicios, entre otros) .

ROL: Líder de Infraestructura	
DESPUES: PROCEDIMIENTO DE RESTAURACIÓN Y RETORNO	
#	Actividades a realizar
2	Recibir notificación de **"Fin de Desastre"** por parte del Líder de Recuperación luego de la recuperación total de los servicios afectados.
3	Recibir notificación de **"Retorno a la Normalidad"** y participar del plan de acción para retorno y asignar las responsabilidades al personal de apoyo.
4	Preparar documentación física según los gastos que se hayan incurrido en la recuperación de las operaciones.
5	Participar en el taller de **"Lecciones Aprendidas"** respecto a la situación presentada.
6	Actualizar el Plan de Continuidad del cual es responsable y documentación relacionada, según las observaciones y lecciones aprendidas identificadas.
7	Informar de manera continua a través de reportes de avance al Líder de Recuperación respecto a la operación en contingencia (reparación de daños, operatividad de los servicios, entre otros).
8	Recibir la notificación de "Fin de Desastre" por parte del Líder de Recuperación luego de la recuperación total de los servicios críticos, afectados por el evento de desastre.
9	Recibir notificación de **"Retorno a la Normalidad"** y participar del plan de acción para retorno y asignar las responsabilidades al personal de apoyo.
10	Preparar documentación física según los gastos que se hayan incurrido en la recuperación de las operaciones de Conectividad.
11	Participar en el taller de **"Lecciones Aprendidas"** respecto a la situación presentada.
12	Actualizar el Plan de Continuidad del cual es responsable y documentación relacionada, según las observaciones y lecciones aprendidas identificadas.

ROL: Líder de Sistemas de Información	
DESPUES: PROCEDIMIENTO DE RESTAURACIÓN Y RETORNO	
#	Actividades a realizar
1	Informar de manera continua a través de reportes de avance al Líder de Recuperación respecto a la operación en contingencia (reparación de daños, operatividad de los servicios, entre otros).
2	Recibir la notificación de **"Fin de Desastre"** por parte del Líder de Recuperación luego de la recuperación total de los servicios críticos, afectados por el evento de desastre.
3	Recibir notificación de **"Retorno a la Normalidad"** y participar del plan de acción para retorno y asignar las responsabilidades al personal de apoyo.
4	Preparar documentación física según los gastos que se hayan incurrido en la recuperación de las operaciones de las aplicaciones.
5	Participar en el taller de **"Lecciones Aprendidas"** respecto a la situación presentada.
6	Actualizar el Plan de Continuidad del cual es responsable y documentación relacionada, según las observaciones y lecciones aprendidas identificadas

15. ANEXOS

- 15.1. ANEXO 1 UBICACIÓN CENTRO DE COMANDO
- 15.2. ANEXO 2 EQUIPO DE RECUPERACIÓN
- 15.3. ANEXO 3 RELACIÓN DE PROVEEDORES
- 15.4. ANEXO 4 DEPENDENCIAS INTERNAS
- 15.5. ANEXO 5 REGISTROS VITALES
- 15.6. ANEXO 6 PROCEDIMIENTOS DE INFRAESTUCTURA
- 15.7. ANEXO 7 REQUERIMIENTO DE RECURSOS

ANEXO 1 CENTRO DE COMANDO

El Centro de Comando principal está ubicado en la Av. La Peruanidad S/N, edificio Quiñones (Campo de Marte) - Jesús María - Lima - Perú. Ministerio de Defensa.

ANEXO 2 EQUIPO DE RECUPERACIÓN

Equipo de Ejecución - Infraestructura Tecnológica y soporte	
Cargo	Rol del Equipo
Equipo de recuperación ante desastres	
Jefe de la Oficina General de Tecnologías de la Información y Estadística	Responsable de la coordinación para la recuperación de TI
Responsable del equipo de trabajo de Infraestructura Tecnológica y Telecomunicaciones.	Responsable de la coordinación de la recuperación de la infraestructura tecnológica y telecomunicaciones
Responsable de Soporte Técnico / Mesa de Ayuda	Responsable de brindar soporte técnico durante toda la etapa de recuperación. Revisar los procedimientos de no disponibilidad de la infraestructura tecnológica.

Íter	Principal / Secundario	Correo	Equipo de Trabajo – Infraestructura Tecnológica y telecomunicaciones
Servicios WEB en Atención al Ciudadano			
1	Principal	jpineda@mindef.gob.pe	Especialista de Infraestructura 1
	Secundario	mramirez@mindef.gob.pe	Especialista de Infraestructura 2
Servidor Base de Datos (Intranet Sharepoint)			
2	Principal	jpineda@mindef.gob.pe	Especialista de Infraestructura 1
	Secundario	mramirez@mindef.gob.pe	Especialista de Infraestructura 2
Servidor Aplicaciones Sharepoint			
3	Principal	jpineda@mindef.gob.pe	Especialista de Infraestructura 1
	Secundario	mramirez@mindef.gob.pe	Especialista de Infraestructura 2
Servicio de aplicaciones Intranet			
4	Principal	jpineda@mindef.gob.pe	Especialista de Infraestructura 1
	Secundario	mramirez@mindef.gob.pe	Especialista de Infraestructura 2
Servicio de servidor de archivos 1			
5	Principal	jpineda@mindef.gob.pe	Especialista de Infraestructura 1
	Secundario	mramirez@mindef.gob.pe	Especialista de Infraestructura 2
Servicio de servidor de archivos 2			
6	Principal	jpineda@mindef.gob.pe	Especialista de Infraestructura 1
	Secundario	mramirez@mindef.gob.pe	Especialista de Infraestructura 2
Servicio de controlador de dominio principal			
7	Principal	jpineda@mindef.gob.pe	Especialista de Infraestructura 1
	Secundario	mramirez@mindef.gob.pe	Especialista de Infraestructura 2

Servicio de controlador de dominio secundario			
8	Principal	jpineda@mindef.gob.pe	Especialista de Infraestructura 1
	Secundario	mramirez@mindef.gob.pe	Especialista de Infraestructura 2
Servicio de despliegue de IPs			
9	Principal	jpineda@mindef.gob.pe	Especialista de Infraestructura 1
	Secundario	mramirez@mindef.gob.pe	Especialista de Infraestructura 2
Servidor BD (Alta Disp. del Portal Web MySql)			
10	Principal	jpineda@mindef.gob.pe	Especialista de Infraestructura 1
	Secundario	mramirez@mindef.gob.pe	Especialista de Infraestructura 2
Almacenamiento de Archivos del Sistradoc.			
11	Principal	jpineda@mindef.gob.pe	Especialista de Infraestructura 1
	Secundario	mramirez@mindef.gob.pe	Especialista de Infraestructura 2
Servidor de Aplicaciones E-Firma (Sistema Tradoc)			
12	Principal	jpineda@mindef.gob.pe	Especialista de Infraestructura 1
	Secundario	mramirez@mindef.gob.pe	Especialista de Infraestructura 2
Servicio de BD Oracle SIGA_MINDEF,SIGA_DIGEPREV)			
13	Principal	jpineda@mindef.gob.pe	Especialista de Infraestructura 1
	Secundario	mramirez@mindef.gob.pe	Especialista de Infraestructura 2
Servicio de correo Principal			
14	Principal	jpineda@mindef.gob.pe	Especialista de Infraestructura 1
	Secundario	mramirez@mindef.gob.pe	Especialista de Infraestructura 2
Servicio de correo secundario			
15	Principal	jpineda@mindef.gob.pe	Especialista de Infraestructura 1
	Secundario	mramirez@mindef.gob.pe	Especialista de Infraestructura 2
Servicio de aplicación de MEF			
16	Principal	jpineda@mindef.gob.pe	Especialista de Infraestructura 1
	Secundario	mramirez@mindef.gob.pe	Especialista de Infraestructura 2
Servicios de Oracle RAC 1			
17	Principal	jpineda@mindef.gob.pe	Especialista de Infraestructura 1
	Secundario	mramirez@mindef.gob.pe	Especialista de Infraestructura 2
Servicios de Oracle RAC 2			
18	Principal	jpineda@mindef.gob.pe	Especialista de Infraestructura 1
	Secundario	mramirez@mindef.gob.pe	Especialista de Infraestructura 2
Servicio de Aplicaciones Apache TRADOC			
19	Principal	jpineda@mindef.gob.pe	Especialista de Infraestructura 1
	Secundario	mramirez@mindef.gob.pe	Especialista de Infraestructura 2
Servicio réplica de BD y Alta Disp. Sistema Tradoc			

20	Principal	jpineda@mindef.gob.pe	Especialista de Infraestructura 1
	Secundario	mramirez@mindef.gob.pe	Especialista de Infraestructura 2
Servicio de acceso a carpetas y aplicaciones.			
21	Principal	jpineda@mindef.gob.pe	Especialista de Infraestructura 1
	Secundario	mramirez@mindef.gob.pe	Especialista de Infraestructura 2
Servidor de Aplicaciones E-Firma(Sistema Tradoc)			
22	Principal	jpineda@mindef.gob.pe	Especialista de Infraestructura 1
	Secundario	mramirez@mindef.gob.pe	Especialista de Infraestructura 2
Sistema de consultas PIDE			
23	Principal	jpineda@mindef.gob.pe	Especialista de Infraestructura 1
	Secundario	mramirez@mindef.gob.pe	Especialista de Infraestructura 2
Switch de borde			
24	Principal	No disponible	Especialista en telecomunicaciones

Equipo de Ejecución – Sistemas de Información	
Cargo	Rol del Equipo
Jefe de la Oficina General de Tecnologías de la Información y Estadística	Responsable de la coordinación para la recuperación de TI
Responsable de Sistemas de Información	Responsable de la coordinación sobre los Sistemas de Información
Analista Programador	Revisar los procedimientos de no disponibilidad de los Sistemas de Información

Ítem	**Principal Secundario**	**Correo**	**Equipo de Trabajo – Sistemas de Información**
Página Web Institucional			
1	Principal	jdelacruz@mindef.gob.pe	Especialista de Sistemas 1
	Secundario	hvargas@mindef.gob.pe	Especialista de Sistemas 2
Sistema de Trámite documentario			
2	Principal	accapa@mindef.gob.pe	Especialista de Sistemas 1
	Secundario	wtuco@mindef.gob.pe	Especialista de Sistemas 2
Sistema de Visitas			
3	Principal	jdelacruz@mindef.gob.pe	Especialista de Sistemas 1
	Secundario	wtuco@mindef.gob.pe	Especialista de Sistemas 2
Sistema de Control de Asistencia			
4	Principal	hvargas@mindef.gob.pe	Especialista de Sistemas 1
	Secundario	wtuco@mindef.gob.pe	Especialista de Sistemas 2

Intranet			
5	Principal	hvargas@mindef.gob.pe	Especialista de Sistemas 1
	Secundario	jdelacruz@mindef.gob.pe	Especialista de Sistemas 2
Sistema de Registro Militar			
6	Principal	accapa@mindef.gob.pe	Especialista de Sistemas 1
	Secundario	wtuco@mindef.gob.pe	Especialista de Sistemas 2
Servicio Previsional			
7	Principal	wtuco@mindef.gob.pe	Especialista de Sistemas 1
	Secundario	accapa@mindef.gob.pe	Especialista de Sistemas 2

Equipo de Ejecución - Ciberseguridad	
Cargo	**Rol del Equipo**
Equipo de recuperación ante desastres	
Jefe de la Oficina General de Tecnologías de la Información y Estadística	Responsable de la coordinación para la recuperación de TI
Coordinador de Ciberseguridad	Responsable de la coordinación sobre los Sistemas de seguridad Informática
Analista de Seguridad Informática	Revisar los procedimientos de indisponibilidad de los Sistemas de seguridad Informática

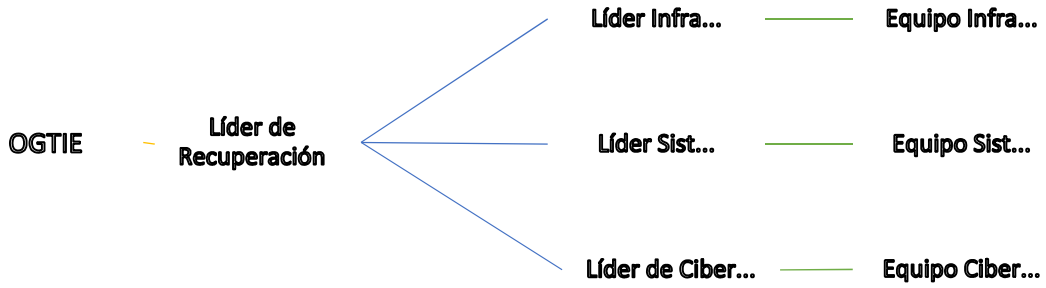
Íter	Principal Secundario	Correo	Equipo de Trabajo - Ciberseguridad
Anti Spam			
1	Principal	ctito@mindef.gob.pe	Especialista en Ciber 1
	Secundario	jcastillo@mindef.gob.pe	Especialista en Ciber 2
Firewall de Capa 3			
2	Principal	jcastillo@mindef.gob.pe	Especialista en Ciber 1
	Secundario	ctito@mindef.gob.pe	Especialista en Ciber 2

ANEXO 3 RELACIÓN DE PROVEEDORES

Nombre	Servicio	Correo
Infraestructura Tecnológica y Telecomunicaciones		
JWDIT (Ruben Guerrero)	-VIRTUALIZACIÓN -BACKUP	ruben.guerrero@jwdits.com
CLASTEC (Lorena Quispe)	-Servicio de Impresora	lorena.quispe@clastec.com
ITG SOLUTION	-MICROSOFT	administracion@itgsolutions.com.pe
SOFTLINE GROUP (Javier Lara)	-MICROSOFT	javier.lara@softlinegroup.com
SECURESOFT	McAfee	soporte@securesoftcorp.com
Emilio Hernan Garcia Gutierrez	Apoyo informático a los servicios de comunicación	egotierrez@gmail.com
ITALTEL	Switch de Core / Switch de Borde / Central Telefónica	silvia.ricaldi@italtel.com
VALTOM INGENIEROS	Ups / Aire Acondicionado De Precision	implementacion@valtom.com.pe
TELEFONICA S.A.A	Internet / Telefonia Fija / Telefonia Movil	alberto.morales@telefonica.com
Goals S.A.	PCA	lchiappe@goalsnet.net
Sistemas de Información		
Elizabeth Atahua Flores	Pruebas de funcionamiento de las aplicaciones	Systematahua22@gmail.com
Jesús Mariaca Mamani	Sistema de Planificación y Presupuesto	javatar.dev@gmail.com
Ciberseguridad		
AntiSpam	Filtro de correos Spam	soporte@securesoft.com.pe
Firewall de capa 3	Firewall perimetral	soporte@securesoft.com.pe

ANEXO 4 DEPENDENCIAS INTERNAS

En esta sección se presenta el escalamiento de la situación presentada. Esto permitirá gestionar la movilización de los roles al Centro de Comando u otro punto de concentración definido en el momento de la contingencia o desastre.



ANEXO 6 PROCEDIMIENTOS DE INFRAESTRUCTURA

- Procedimiento A – Plan de Continuidad de enlaces de red e internet
  (*) Se requiere un switch de core de contingencia para la implementación del Plan de Recuperación de Servicios Informáticos.
- Procedimiento B – Plan de Continuidad de la Central Telefónica
- Procedimiento 01 – Servicios WEB en Atención al Ciudadano
- Procedimiento 02 – Servidor Base de Datos (Intranet Sharepoint)
- Procedimiento 03 - Servidor Aplicaciones Sharepoint.
- Procedimiento 04 - Servicio de aplicaciones Intranet.
- Procedimiento 05 - Servicio de servidor de archivos 1.
- Procedimiento 06 - Servicio de servidor de archivos 2.
- Procedimiento 07 - Servicio de controlador de dominio principal
- Procedimiento 08 - Servicio de controlador de dominio secundario
- Procedimiento 09 Servicio de despliegue de IPs
- Procedimiento 10 - Servidor BD (Alta Disp. del Portal Web MySql)
- Procedimiento 11 - Almacenamiento de Archivos del Sistradoc
- Procedimiento 12 - Servidor de Aplicaciones E-Firma (Sistema Tradoc)
- Procedimiento 13 - Servicio de BD Oracle SIGA_MINDEF, SIGA_DIGEPREV
- Procedimiento 14 - Servicio de correo Principal
- Procedimiento 15 - Servicio de correo Secundario
- Procedimiento 16 - Servicio de aplicación de MEF
- Procedimiento 17 y 18 - Servicios de Oracle RAC 1 y RAC 2
- Procedimiento 19 - Servicio de Aplicaciones Apache TRADOC
- Procedimiento 20 - Servicio réplica de BD y Alta Disp. Sistema Tradoc
- Procedimiento 21 - Servicio de acceso a carpetas y aplicaciones.
- Procedimiento 22 - Servidor de Aplicaciones E-Firma (Sistema Tradoc).
- Procedimiento 23 - Sistema de consultas PIDE
- Procedimiento 24 – Servicio de SW de Borde
- Procedimiento 25 – Servicio de Core de Datos
- Procedimiento 26 Servicios de Core de Voz
- Procedimiento 26 Servicio de la Central Telefónica

Procedimiento F –Plan de Continuidad de Equipos de Ciberseguridad

Ejecución del procedimiento general de recuperación							
Act.	Descripción	Resultado		Observaciones	Hora de Inicio	Hora de Fin	Check
		OK	FALLO				
1	Activar y ejecutar el Plan de Continuidad Enlace de red e internet.						
2	Activar y ejecutar el Plan de Continuidad Central Telefónica.						
3	Activar y ejecutar el Plan de Continuidad Plataforma de Correo electrónico.						
4	Activar y ejecutar el Plan de Continuidad File Sistema de Trámite Documentario.						
5	Activar y ejecutar el Plan de Continuidad Sistema de Visitas.						
6	Activar y ejecutar el Plan de Continuidad Página Web.						
7	Activar y ejecutar el Plan de Continuidad Intranet.						
8	Activar y ejecutar el Plan de Continuidad Firewall						

ANEXO 7 REQUERIMIENTO DE RECURSOS

De acuerdo a lo evaluado con el Equipo de trabajo de Infraestructura tecnológica y Telecomunicaciones, se necesitará el sistema convergente de nube privada de contingencia y equipos de comunicaciones:

Teniendo estas consideraciones el Centro de Datos alterno contaría:

N°	Servidor	Aplicativos
1	Centro de datos alterno	Servicios WEB en Atención al Ciudadano Servidor Base de Datos (Intranet Sharepoint) Servidor Aplicaciones Sharepoint Servicio de aplicaciones Intranet Servicio de servidor de archivos 1 Servicio de servidor de archivos 2 Servicio de controlador de dominio principal Servicio de controlador de dominio secundario Servicio de despliegue de IPs Servidor BD WEB Almacenamiento de Archivos del Sistradoc. Servidor de Aplicaciones E-Firma (Sistema Tradoc) Servicio de BD Oracle SIGA_MINDEF,SIGA_DIGEPREV) Servicio de correo Principal Servicio de correo secundario Servicio de aplicación de MEF Servicios de Oracle RAC 1 Servicios de Oracle RAC 2 Servicio de Aplicaciones Apache TRADOC Servicio réplica de BD y Alta Disp. Sistema Tradoc Servicio de acceso a carpetas y aplicaciones. Servidor de Aplicaciones E-Firma(Sistema Tradoc) Sistema de consultas PIDE

N°	Servidor	Características	
1	Centro de datos alterno	Cantidad	Dos (02) Nodos o servidores
		Modelo de Procesador	Intel Xeon 8260 o superior
		Cantidad de Cores por nodo	48 Cores
		Velocidad de Procesador	Velocidad de Reloj de procesador, por lo menos 2.4 GHz como mínimo
		Cantidad de memoria RAM instalada	384 GB RAM con capacidad de crecimiento hasta 1.5TB por nodo.
		Almacenamiento Local por nodo	Por lo menos dos (02) discos de 1.2 TB cada uno.
		Almacenamiento Local, Protección RAID	Configurados en Raid 1 o equivalente.
		Conectividad	● (02) Dos puertos de una velocidad 10Gb SFP+ ● (02) Dos puertos convergentes a una velocidad de 100Gb por cada nodo ó (06) Seis puertos de una velocidad 32Gb FC por cada nodo.
		Conectividad Administración	(01) Un puerto de una velocidad 1GbE (BASE-T)
		Fuentes de Poder	Fuentes de Poder redundantes, hot-swap.
		Ventiladores	Ventiladores redundantes

N°	Equipamiento	Características
1	SW de Borde	- Marca: CISCO - Modelo: C9200L-48P-4X **Software** - Cisco IOS XE Software, Version 16.09.03 - Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_LITE_IOSXE), Version 16.9.3, RELEASE SOFTWARE (fc2) **Hardware** - 48 interfaces Gigabit Ethernet interfaces - 4 interface Ten Gigabit Ethernet interfaces - Procesador: Processor board ID JAE233311RJ - - 2048K bytes of non-volatile configuration memory. - 1998932K bytes of physical memory. - 819200K bytes of Crash Files at crashinfo - 1941504K bytes of Flash at flash - 01 Fuente de Power
2	Core de Datos	- Marca: CISCO - Modelo: CISCO NEXUS C9504 **Software** - BIOS: versión 08.36 - NXOS: versión 7.0(3)I7(9) - BIOS compile time: 06/07/2019 - NXOS image file is: bootflash:///nxos.7.0.3.I7.9.bin - NXOS compile time: 8/27/2020 5:00:00 [08/27/2020 06:11:00] **Hardware**

		- 52 interfaces 10Gbase-SR-S - Cisco Nexus9000 C9504 (4 Slot) Chassis ("Supervisor Module") - Procesador: Xeon 1.80Ghz - Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 16400868 kB of memory. - Processor Board ID FOC2142551Q - Device name: N9K-Mindef - bootflash: 21693714 kB - Memoria Ram: 16400868 kB - Fuentes de Power Cant.04
3	Core de Voz	- Marca: CISCO - Modelo: CISCO WS-C3850-24S - Procesador: ID FJB2328H0L6 **Software** - Cisco IOS XE Software, Version 16.09.03a - Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version 16.9.3a, RELEASE SOFTWARE (fc2) **Hardware** - 24 interfaces de a-1000 10/100/1000BaseTX SFP - 04 interfaces Ten Gigabit Ethernet interfaces - Motherboard Assembly Number : 73-14445-07 - Motherboard Serial Number : FJZ232800UC - Model Revision Number : M0 - Motherboard Revision Number : B0 - Model Number : WS-C3850-24S - System Serial Number : FJB2328H0L6
4	Central Telefónica	- Marca CISCO - Modelo: BE6000M (USC C220 M4S) **Software** - Cisco Unity Connection Administration Version 10.5.2.10000-5 **Hardware** - Procesador: Intel(R) Xeon(R) CPU E5-2630 v3 @ 2.40GHz

(*) Requerimiento de equipo de comunicaciones de contingencia para la ejecución del Plan de Continuidad de Servicios Informáticos.