Resolución de Dirección Ejecutiva

RDE N° 00179 -2022-ARCC/DE

Lima, 29 de diciembre de 2022

VISTOS: La Nota de Elevación N° 513-2022-ARCC/GG y el Memorando N° 00609-2022-ARCC/GG de la Gerencia General, el Memorando N° 05589-2022-ARCC/GG/OPP y el Informe N° 00196-2022-ARCC/GG/OPP-JAMP de la Oficina de Planificación y Presupuesto, y el Informe N° 01091-2022-ARCC/GG/OAJ de la Oficina de Asesoría Jurídica;

CONSIDERANDO:

Que, mediante la Ley N° 30556, Ley que aprueba disposiciones de carácter extraordinario para las intervenciones del Gobierno Nacional frente a desastres y que dispone la creación de la Autoridad para la Reconstrucción con Cambios (ARCC), y sus modificatorias, se establece que la ARCC es una entidad adscrita a la Presidencia del Consejo de Ministros, de carácter excepcional y temporal, encargada de liderar, implementar y, cuando corresponda, ejecutar el Plan Integral para la Reconstrucción con Cambios;

Que, la ARCC cuenta con autonomía funcional, administrativa, técnica y económica y está a cargo de un/a Director/a Ejecutivo/a con rango de Ministro para los alcances de la Ley N° 30556;

Que, con la Ley N° 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD), se establece que el SINAGERD es el sistema interinstitucional, sinérgico, descentralizado, transversal y participativo, creado a fin de identificar y reducir los riesgos asociados a peligros o minimizar sus efectos, así como evitar la generación de nuevos riesgos, y preparación y atención ante situaciones de desastre, mediante el establecimiento de principios, lineamientos de política, componentes, procesos e instrumentos de la Gestión del Riesgo de Desastres;

Que, mediante la Resolución Ministerial N° 320-2021-PCM, 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", 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, en los Lineamientos se establece que la "Gestión de la Continuidad Operativa del Estado" es un proceso continuo que forma parte de las operaciones habituales de la Entidad Pública con el objetivo de que siga cumpliendo con su misión, mediante la implementación de mecanismos adecuados, con el fin de continuar brindando servicios necesarios a la población, ante la ocurrencia de un desastre o evento que produzca la interrupción prolongada de sus operaciones;

Que, a través de la Resolución de Dirección Ejecutiva N° 00004-2022-ARCC/DE, se designó a la Gerencia General como unidad orgánica responsable de la Gestión de la

Continuidad Operativa de la Autoridad; asimismo, se dispuso que los funcionarios de la alta dirección participen personalmente en la Gestión de la Continuidad Operativa y asuman responsabilidades directas en su implementación, seguimiento y monitoreo, y que los órganos de línea, órganos de apoyo y órganos de asesoramiento de la ARCC remitan la designación de su representante a la Gerencia General, para efecto de coadyuvar con la implementación de las acciones de la Gestión de la Continuidad Operativa en las distintas áreas de la Entidad;

Que, con la Resolución de Dirección Ejecutiva N° 00143-2022-ARCC/DE, se conformó el Grupo de Comando para la Gestión de la Continuidad Operativa de la Autoridad para la Reconstrucción con Cambios, en concordancia con el literal d) del numeral 6.1.1 de los Lineamientos;

Que, de acuerdo con el literal f) del numeral 6.1.1 de los Lineamientos, corresponde al Titular de la Entidad aprobar el Plan de Continuidad Operativa; así también, de acuerdo al literal c) del numeral 6.3.2 de los Lineamientos, se establece que el Plan de Continuidad Operativa será aprobado mediante Resolución o norma de mayor jerarquía de la entidad;

Que, conforme al artículo 10 del Documento de Organización y Funciones de la Autoridad para la Reconstrucción con Cambios (DOF), aprobado por la Resolución de Dirección Ejecutiva N° 00008-2020-ARCC/DE y su modificatoria, la Dirección Ejecutiva es un órgano de la Alta Dirección y está a cargo del/de la Director/a Ejecutivo/a quien es la máxima autoridad ejecutiva de la ARCC, el cual tiene rango de ministro y representa a la ARCC;

Que, asimismo, de acuerdo a los literales q) y r) del artículo 11 del DOF de la ARCC, la Dirección Ejecutiva tiene como funciones, emitir resoluciones para el cumplimiento de sus funciones y ejercer las demás funciones que le corresponde por norma expresa;

Que, con Memorando N° 00609-2022-ARCC/GG, la Gerencia General remite a la Oficina de Planificación y Presupuesto, el proyecto de Plan de Continuidad Operativa de la ARCC, para su opinión en el marco de sus competencias;

Que, en el Informe N° 00196-2022-ARCC/GG/OPP-JAMP que se acompaña al Memorando N° 05589-2022-ARCC/GG/OPP, la Oficina de Planificación y Presupuesto emite opinión favorable respecto al Plan de Continuidad Operativa de la ARCC y concluye que “3.2. La Propuesta del Plan de Continuidad Operativa de la Autoridad para la Reconstrucción con Cambios ha sido elaborada según la estructura establecida en el numeral 6.2.1 de 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, aprobada por Resolución Ministerial N° 320-2021-PCM. 3.3. De acuerdo con el literal f) del numeral 6.1.1 de los Lineamientos, el mencionado Plan debe ser aprobado por el titular de la entidad, que en el caso de la ARCC corresponde a la Dirección Ejecutiva emitir la Resolución para su aprobación”;

Que, mediante el Informe N° 01091-2022-ARCC/GG/OAJ, la Oficina de Asesoría Jurídica concluye que resulta viable legalmente que se continúe con el trámite de aprobación, a través de Resolución de Dirección Ejecutiva, de la propuesta del “Plan de Continuidad

Firmado digitalmente por: MOSQUEIRA MEDINA Ernesto Enrique FAU 20602114091 soft
Motivo: Soy el autor del documento
Fecha: 29/12/2022 16:53:58-0500

Resolución de Dirección Ejecutiva

RDE N° 00179 -2022-ARCC/DE

Operativa de la Autoridad para la Reconstrucción con Cambios", formulada por el Grupo de Comando para la Gestión de la Continuidad Operativa de la ARCC, en el marco de lo dispuesto en la Resolución Ministerial N° 320-2021-PCM que aprueba los "Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Públicas de los tres niveles de gobierno", el cual cuenta con la opinión favorable de la Oficina de Planificación y Presupuesto, conforme a sus respectivas competencias;

De conformidad con la Resolución Ministerial N° 320-2021-PCM, que aprueba los "Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Públicas de los tres niveles de gobierno", y la Resolución de Dirección Ejecutiva N° 00008-2020-ARCC/DE, que aprueba el Documento de Organización y Funciones de la Autoridad para la Reconstrucción con Cambios, aprobado por Resolución de Dirección Ejecutiva Nº 00008-2020-ARCC/DE y modificado por Resolución de Dirección Ejecutiva Nº 00140-2022-ARCC/DE;

SE RESUELVE:

Artículo 1.- Aprobación

Aprobar el "Plan de Continuidad Operativa de la Autoridad para la Reconstrucción con Cambios", el mismo que como Anexo forma parte integrante de la presente Resolución.

Artículo 2.- Remitir

La Gerencia General como unidad orgánica responsable de la Gestión de la Continuidad Operativa de la Autoridad para la Reconstrucción con Cambios, debe remitir al Instituto Nacional de Defensa Civil – INDECI el "Plan de Continuidad Operativa de la Autoridad para la Reconstrucción con Cambios", aprobado mediante la presente Resolución.

Artículo 3.- Notificación

Encargar a la Gerencia General efectuar la difusión e implementación del presente Plan en coordinación con el Grupo de Comando para la Gestión de la Continuidad Operativa de la Autoridad para la Reconstrucción con Cambios.

Artículo 4.- Publicación

La presente Resolución se publica en el portal institucional de la Autoridad para la Reconstrucción con Cambios (www.rcc.gob.pe).

Regístrese y comuníquese.

DOCUMENTO FIRMADO DIGITALMENTE
ERNESTO ENRIQUE MOSQUEIRA MEDINA
Director Ejecutivo (e)
Autoridad para la Reconstrucción con Cambios
Presidencia del Consejo de Ministros

Firmado digitalmente por: VARAS VELASQUEZ Betsy Edith FAU 20602114091 soft
Motivo: Doy V° B°
Fecha: 28/12/2022 19:49:02-0500

Firmado digitalmente por: MELENDEZ HUASASQUICHE Alexander Octavio FAU 20602114091 hard
Motivo: Doy V° B°
Fecha: 28/12/2022 19:55:29-0500

Firmado digitalmente por: LINDO CARDENAS Angelo Alexis FAU 20602114091 hard
Motivo: Doy V° B°
Fecha: 29/12/2022 10:19:18-0500

PLAN DE CONTINUIDAD OPERATIVA DE LA AUTORIDAD PARA LA RECONSTRUCCIÓN CON CAMBIOS

Firmado digitalmente por: GALVEZ PARDAVE Cesar Edmundo FAU 20602114091 hard
Motivo: Doy V° B°
Fecha: 28/12/2022 20:16:24-0500

Firmado digitalmente por: LINDO CARDENAS Angelo Alexis FAU 20602114091 hard
Motivo: Doy V° B°
Fecha: 29/12/2022 10:02:49-0500

Firmado digitalmente por: CHAVEZ FIGUEROA Segundo Victoriano FAU 20602114091 soft
Motivo: Doy V° B°
Fecha: 29/12/2022 08:19:30-0500

Firmado digitalmente por: MOSQUEIRA MEDINA Ernesto Enrique FAU 20602114091 soft
Motivo: Doy V° B°
Fecha: 28/12/2022 20:35:41-0500

Firmado digitalmente por: REYES VARGAS Carlo Joao FAU 20602114091 hard
Motivo: Doy V° B°
Fecha: 28/12/2022 21:19:30-0500

Firmado digitalmente por: ROJAS VELA Mauro FAU 20602114091 hard
Motivo: Doy V° B°
Fecha: 28/12/2022 21:28:57-0500

I. INFORMACION GENERAL

La Autoridad para la Reconstrucción con Cambios (ARCC) es la entidad encargada de liderar e implementar el Plan Integral de Reconstrucción con Cambios (PIRCC), en coordinación con las entidades ejecutoras de los 3 niveles de gobierno.

En el presente Plan de Continuidad Operativa (PCO) se establecen los procedimientos operativos para mantener las actividades críticas y los criterios para la reactivación de las operaciones indispensables de la ARCC y su principal objetivo es Asegurar que la ARCC pueda seguir cumpliendo su misión, cualquiera que sea el evento de interrupción.

El PCO ha sido elaborado siguiendo los Lineamientos para la Gestión de la Continuidad Operativa de las Entidades Públicas en los Tres Niveles de Gobierno, los que proporcionan una estructura para su formulación y estipula la incorporación del enfoque de continuidad en los planes ante escenarios de emergencia o desastres de las entidades públicas y de instituciones privadas, motivo por el cual es de prioridad contar con un respaldo integral, que permita a la entidad enfrentar cualquier eventualidad.

El PCO constituye la principal herramienta que le permitirá a la ARCC realizar las actividades de preparación y respuesta con la finalidad de minimizar el impacto negativo de un desastre, permitiéndole operar a pesar del escenario que pudiera estar enfrentando.

La implementación de la continuidad operativa requiere de un alto grado de compromiso institucional, voluntad de la Alta Dirección y responsabilidad de cada órgano de la ARCC, debido a que es de gran importancia definir anticipadamente las acciones a realizar para disminuir el factor sorpresa de la emergencia, así como lograr mantener una gran capacidad de respuesta con la finalidad de minimizar los daños productos de los desastres.

II. GLOSARIO

PIRCC	:	Plan Integral de Reconstrucción con Cambios
PCO	:	Plan de Continuidad Operativa
URGCO	:	Unidad orgánica responsable de la Gestión de la Continuidad Operativa
UE	:	Unidad Ejecutora
DE	:	Dirección Ejecutiva
DEA	:	Dirección Ejecutiva Adjunta
GG	:	Gerencia General
OGP	:	Oficina de Gestión de Proyectos
UGMCEE	:	Unidad de Gestión de la Modalidad de Estado a Estado
OAJ	:	Oficina de Asesoría Jurídica
OPP	:	Oficina de Planificación y Presupuesto

OC	:	Oficina de Comunicaciones
OA	:	Oficina de Administración
UL	:	Unidad de Logística
UAF	:	Unidad de Asuntos Financieros
URH	:	Unidad de Recursos Humanos
OTI	:	Oficina de Tecnologías de la Información
DSI	:	Dirección de Soluciones Integrales
DISE	:	Dirección de Intervenciones del Sector Educación
DISS	:	Dirección de Intervenciones del Sector Salud
DISVCS	:	Dirección de Intervenciones del Sector Vivienda, Construcción y Saneamiento
DIST	:	Dirección de Intervenciones del Sector Transporte
DAI	:	Dirección de Articulación de Inversiones
SDR		Subdirección Regional

III. BASE LEGAL

- Ley N° 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres – SINAGERD.
- Ley N° 30787, Ley que incorpora la Aplicación del Enfoque de Derechos en favor de las personas afectadas o damnificadas por Desastres.
- Decreto Supremo N° 048-2011-PCM que aprueba el Reglamento de la Ley N° 29664.
- Decreto Supremo N° 115-2022-PCM que aprueba el Plan Nacional de Gestión del Riesgos de Desastres - PLANAGERD 2022 – 2030.
- Decreto Supremo N° 038-2021-PCM, que aprueba la Política Nacional de Gestión del Riesgo de Desastres al 2050.
- Resolución de Dirección Ejecutiva N° 00008-2020-ARCC/DE que aprueba el Documento de Organización y Funciones de la Autoridad para la Reconstrucción con Cambios.
- Resolución de Dirección Ejecutiva N° 000014-2022-ARCC/DE que aprueba la conformación del Equipo de Respuestas ante Incidentes de Seguridad Digital de la ARCC.
- Resolución de Dirección Ejecutiva N° 0140-2022-ARCC/DE que aprueba la modificación por reasignación de funciones: el artículo 37, los literales a), b) y k) del artículo 38, los artículos 47 y 48 del Documento de Organización y Funciones de la Autoridad para la Reconstrucción con Cambios.
- 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 en los tres niveles de Gobierno, de fecha 30 de diciembre del 2021.
- Resolución de Dirección Ejecutiva N° 004-2022-ARCC/DE, que designa a la Gerencia General como Unidad Orgánica responsable de la Gestión de la Continuidad Operativa de la ARCC.
- Resolución de Dirección Ejecutiva N° 143-2022-ARCC/DE, que designa al Grupo de Comando para la Gestión de la Continuidad Operativa de la ARCC.

IV. OBJETIVOS

4.1 Objetivo General

Garantizar la continuidad operativa de la ARCC, ante la ocurrencia de un desastre de gran magnitud o cualquier evento que interrumpa sus procesos, ejecutando las actividades críticas, hasta lograr su recuperación en el menor plazo posible.

4.2 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 las actividades críticas.
c) Lograr un nivel de preparación que permita, cumplir con las actividades críticas identificadas.

V. IDENTIFICACION DE RIESGOS Y RECURSOS

5.1 Matriz de riesgos

Peligro Muy Alto	Riesgo Alto	Riesgo Alto	Riesgo Muy Alto	Riesgo Muy Alto
Peligro Alto	Riesgo Medio	Riesgo Alto	Riesgo Alto	Riesgo Muy Alto
Peligro Medio	Riesgo Medio	Riesgo Medio	Riesgo Alto	Riesgo Alto
Peligro Bajo	Riesgo Bajo	Riesgo Medio	Riesgo Medio	Riesgo Alto
P / V	**Vulnerabilidad baja**	**Vulnerabilidad media**	**Vulnerabilidad alta**	**Vulnerabilidad muy alta**

En base a la matriz anterior, se han identificado los siguientes niveles de riesgo:

Cuadro N° 1: Identificación de nivel de riesgo

Peligros	Nivel de Peligro	Nivel de Vulnerabilidad	Nivel de Riesgo
Origen natural			
Sismo de gran magnitud	Medio	Medio	Medio
Epidemia - pandemia	Medio	Alto	Alto
Acción humana			
Incendios	Medio	Medio	Medio
Ataque informático	Alto	Medio	Alto
Convulsión social	Alto	Medio	Alto
Atentado Terrorista	Bajo	Bajo	Bajo

Peligros	Nivel de Peligro	Nivel de Vulnerabilidad	Nivel de Riesgo
Actividad criminal	Medio	Medio	Medio
Falla de energía eléctrica	Alto	Alto	Alto
Falla en telecomunicaciones	Medio	Medio	Medio
Aniego	Bajo	Bajo	Bajo
Cierre de carreteras	Medio	Alto	Alto

5.2 Determinación del Nivel de Impacto

De producirse estos hechos, se tendría un impacto negativo que afectaría el cumplimiento de la misión de la ARCC, especialmente en las funciones críticas.

5.3 Identificación de recursos

La Oficina de Administración; a través de la Unidad de Logística, tendrá a su cargo la centralización e implementación de los requerimientos para facilitar la Continuidad de las Operaciones de la ARCC ante un desastre de gran magnitud.

Asimismo, la Oficina de Tecnologías de la Información, pondrá en ejecución el Plan de Recuperación de los servicios informáticos.

VI. ACCIONES PARA LA CONTINUIDAD OPERATIVA

La ARCC cuenta actualmente con 3 órganos de alta dirección, 4 de asesoramiento, 6 de apoyo, 6 de línea y 8 desconcentrados:

Cuadro N° 2: Órganos de la ARCC

Tipo	N°	Órgano
Alta Dirección	1	Dirección Ejecutiva-DE
	2	Dirección Ejecutiva Adjunta-DEA
	3	Gerencia General-GG
Asesoramiento	1	Oficina de Gestión de Proyectos-OGP
	2	Unidad de Gestión de la Modalidad de Estado a Estado-UGMCEE
	3	Oficina de Asesoría Jurídica-OAJ
	4	Oficina de Planificación y Presupuesto-OPP
Apoyo	1	Oficina de Comunicaciones-OC
	2	Oficina de Administración-OA
	3	Unidad de Logística-UL
	4	Unidad de Asuntos Financieros-UAF
	5	Unidad de Recursos Humanos-URH
	6	Oficina de Tecnologías de la Información-OTI
Línea	1	Dirección de Soluciones Integrales-DSI
	2	Dirección de Intervenciones del Sector Educación-DISE

Tipo	N°	Órgano
	3	Dirección de Intervenciones del Sector Salud-DISS
	4	Dirección de Intervenciones del Sector Vivienda, Construcción y Saneamiento-DISVCS
	5	Dirección de Intervenciones del Sector Transporte-DIST
	6	Dirección de Articulación de Inversiones-DAI
Desconcentrados	1	SDR de Ancash
	2	SDR de Arequipa
	3	SDR de Cajamarca
	4	SDR de La Libertad
	5	SDR de Lambayeque
	6	SDR de Lima
	7	SDR de Piura
	8	SDR de Tumbes

6.1 Determinación de las Actividades Criticas

A partir del análisis de actividades críticas de cada órgano de la ARCC, se han identificado las siguientes actividades críticas para la ARCC:

Cuadro N° 3: Actividades críticas y órganos participantes

Actividad critica	Órganos participantes				
	Línea	Alta dirección	Asesoramiento	Apoyo	Desconcentrados
Ejecución y monitoreo de las intervenciones del PIRCC a cargo de la ARCC, durante la fase de pre inversión, inversión y cierre	DSI, DISE, DISS, DISVCS, DIST y DAI	GG	OGP, UGMCEE, OPP y OAJ	OA, UL, UAF, URH, y OTI	-
Asistencia, evaluación y gestión de financiamiento de las intervenciones del PIRCC a cargo de las UE de los 3 niveles de gobierno	DSI, DISE, DISS, DISVCS, DIST y DAI	GG, DEA y DE	OGP, OPP y OAJ	OA, URH, OTI	SDR
Asistencia técnica a las entidades ejecutoras durante la fase de contratación, ejecución y cierre de las intervenciones	DSI, DISE, DISS, DISVCS y DIST	DEA y DE	OGP, OA, UL, UAF, URH	OPP, OTI	SDR

i. Ejecución y monitoreo de las intervenciones del PIRCC a cargo de la ARCC, durante la fase de pre inversión, inversión y cierre

Esta actividad comprende:

- Elaboración y aprobación de los estudios técnicos necesarios para la ejecución de intervenciones, tanto en la fase de preinversión e inversión.
- Seguimiento a la ejecución física y financiera de las intervenciones del PIRCC.
- Realizar los registros correspondientes según la normativa del INVIERTE.
- Evaluación de eventos compensables.

- Gestionar la habilitación presupuestal.
- Evaluación y aprobación de valorizaciones relacionadas a las intervenciones del PIRCC.
- Evaluación y aprobación de modificación contractuales.
- Gestión del Contrato Operativo con el UK Delivery Team – UKDT.
- Gestión de los procesos de Procura en el Marco del Acuerdo Gobierno a Gobierno - G2G.
- Gestión de la Transferencia de Conocimientos en el Marco del Acuerdo G2G.

ii. Asistencia, evaluación y gestión de financiamiento de las intervenciones del PIRCC a cargo de las UE de los 3 niveles de gobierno

Esta actividad comprende:

- Coordinación y/o acompañamiento a las entidades ejecutoras de los Gobiernos Nacionales, Regionales y Locales para la formulación de las solicitudes de financiamiento.
- Evaluación de las solicitudes de financiamiento para el PIRCC.

iii. Asistencia técnica a las entidades ejecutoras durante la fase de contratación, ejecución y cierre de las intervenciones

Esta actividad comprende:

- Evaluación de las solicitudes de modificaciones del PIRCC (precisiones, modificaciones de unidad ejecutora, inclusión y exclusión).
- Seguimiento a la ejecución física y financiera de las intervenciones del PIRCC a cargo de las UE del gobierno nacional, regional y local.

6.2 Aseguramiento del Acervo Documentario

Con el objetivo de conservar y preservar en el acervo documental de la institución, en cumplimiento a lo establecido en la Ley N° 25323, Ley del Sistema Nacional de Archivos, Ley N° 27785, Ley del Sistema Nacional de Control y la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, con Resolución de la Gerencia General N° 00010-2022-ARCC/GG se aprobó el Plan Anual de Trabajo Archivístico de la Autoridad para la Reconstrucción con Cambios para el año 2022, cuyo objetivo es mejorar y actualizar los documentos de gestión archivística, organizar los documentos con el objetivo de mantener su integridad y presérvalos, registrar la información de los documentos en el Inventario de Documentos y digitalizar los documentos organizados con la finalidad de ser accesibles de forma inmediata a los usuarios de institución, servidores públicos de otras instituciones, auditores y ciudadanos.

De acuerdo a lo expuesto se realizará en el cuarto trimestre del 2022 las siguientes actividades:

a) Elaborar el Programa de Control de Documentos Archivísticos (documento de gestión archivística donde se establecen las series

documentales de la una institución), por motivo del cambio de la estructura orgánica de LA AUTORIDAD que fue aprobada por la Resolución de la Dirección Ejecutiva N° 00008-2020-ARCC/DE "Documento de Organización y Funciones de la ARCC".

b) Realizar el control de calidad (nitidez y verificar que sean copias fieles a los originales) del 41 % de imágenes de documentos digitalizados.
c) Migrar la información del Inventario de Documentos a una Base de Datos que mantenga los atributos de seguridad y accesibilidad; asimismo, se deberá realizar el enlace de la información de los documentos con las imágenes de los documentos digitalizados.
d) Continuar con la organización de los documentos de la Gerencia de Planeamiento Estratégico que fue desactivada a fines del mes de enero del 2020 (32% del total de documentos conservados), posteriormente se deberá realizar el registro de la información en la Base de Datos y concluir en la digitalización de los documentos organizados.
e) Evaluar la adquisición de estanterías móviles con el objetivo de racionalizar y aprovechar más los espacios físicos del local del Archivo Central.

En los años posteriores, se realizará las siguientes actividades:

a) Ejecutar el Plan Anual de Trabajo donde se incluirá el cronograma de transferencia de documentos, el cual se iniciará a partir del mes de abril; asimismo, se considerará la transferencia de documentos digitales nativos para su conservación y preservación, en coordinación con la Oficina de Tecnología de la Información.
b) Seguir alimentando la Base de Datos con la información de los documentos digitalizados y enlazar con las imágenes obtenidas por la digitalización; y coordinar con la con la Oficina de Tecnología de la Información para la seguridad de las mismas.
c) Monitorear bimestralmente la creación de nuevas series documentales dentro de la institución.
d) Realizar en el primer trimestre la visita de supervisión y asesoramiento técnico archivístico a las oficinas de provincia que mantengan documentos en físico para realizar la transferencia de documentos.
e) Evaluar en el primer trimestre la implementación de una línea de producción de documentos digitales o la tercerización del proceso de digitalización de documentos con valor legal, enfocado a documentos de valor temporal.

6.3 Aseguramiento de la Base de Datos mediante la ejecución del Plan de Recuperación de los servicios informáticos

La seguridad de la información o protección de bases de datos es fundamental para la continuidad operativa de esta Autoridad, por ello se deben establecer acciones que mitiguen los riesgos de los ciberataques, así como tecnologías que estén protegiendo desde el origen de forma continua.

Es por ello que, debido al incremento de la inseguridad en el ciberespacio, esta Autoridad ha promovido la implementación de sistemas de seguridad informática que brindan contención o mitigación de ataques cibernéticos provenientes de diferentes partes del mundo y de distintos vectores, como

phishing, malware, ransomware, man in the midle, entre otros.

Asimismo, se ha elaborado un Plan de Recuperación de los Servicios Informáticos[1], en el cual se detallan las actividades a desarrollar a fin de garantizar la continuidad de los servicios de informática y telecomunicaciones, con el fin de brindar un servicio eficiente, eficaz y oportuno a la ciudadanía y a todas las entidades que se sirve de los diversos servicios que brinda la Autoridad para la Reconstrucción con Cambios, minimizando el impacto negativo sobre una normal ejecución de los procesos y procedimientos institucionales.

6.4 Roles y Responsabilidades para el desarrollo de las actividades criticas

Se han definido los siguientes roles y responsabilidades a fin de desarrollar las actividades criticas ante situaciones de crisis por eventos adversos:

Cuadro N° 4: Actividad critica 1. Ejecución y monitoreo de las intervenciones del PIRCC a cargo de la ARCC, durante la fase de pre inversión, inversión y cierre

N°	Miembros	Órgano	Responsabilidades
1	Director o representante	DSI	• Elaboración de los estudios técnicos necesarios para la ejecución de intervenciones. • Seguimiento a la ejecución física y financiera de las intervenciones del PIRCC. • Realizar los registros correspondientes según la normativa del INVIERTE (solo DAI). • Evaluación de eventos compensables. • Solicitar la habilitación presupuestal. • Evaluación y aprobación de valorizaciones relacionadas a las intervenciones del PIRCC. • Evaluación de modificaciones contractuales.
2	Director o representante	DISE	
3	Director o representante	DIST	
4	Director o representante	DISVCS	
5	Director o representante	DIST	
6	Director o representante	DAI	
7	Gerente General o representante	GG	• Aprobación de los expedientes técnicos de obra para la ejecución de intervenciones. • Aprobación de modificación contractuales.
8	Jefe o representante	OGP	• Emisión de reportes para el monitoreo y control integral de intervenciones. • Identificar, analizar, gestionar y escalar los riesgos de la ejecución de las intervenciones.
9	Jefe o representante	UGMCEE	• Gestión del Contrato Operativo con

[1] Véase Anexo N° 1

N°	Miembros	Órgano	Responsabilidades
			el UK Delivery Team – UKDT. • Gestión de los procesos de Procura en el Marco del Acuerdo Gobierno a Gobierno - G2G. • Gestión de la Transferencia de Conocimientos en el Marco del Acuerdo G2G.
10	Jefe o representante	OPP	• Revisar y de ser el caso, solicitar la habilitación presupuestal al pliego PCM.

Cuadro N° 2: Actividad critica 2. Asistencia, evaluación y gestión de financiamiento de las intervenciones del PIRCC a cargo de las UE de los 3 niveles de gobierno

N°	Miembros	Órgano	Responsabilidades
1	Director o representante	DSI	• Evaluación de las solicitudes de financiamiento para el PIRCC presentadas por la UE del GN, GR y GL.
2	Director o representante	DISE	
3	Director o representante	DIST	
4	Director o representante	DISVCS	
5	Director o representante	DIST	
6	Director o representante	DAI	
7	Gerente General o representante	GG	• Evaluación de las solicitudes de financiamiento para el PIRCC presentadas por los órganos de asesoramiento.
8	Director o representante	DEA	• Coordinación y/o acompañamiento a las entidades ejecutoras de los Gobiernos Nacionales, Regionales y Locales para la formulación de las solicitudes de financiamiento (Subdirectores Regionales).
9	Jefe o representante	OGP	• Monitorear el avance del PIRCC.
10	Jefe o representante	OPP	• Evaluación de las solicitudes de financiamiento para el PIRCC presentadas por los órganos de línea.

Cuadro N° 5: Actividad critica 3. Asistencia técnica a las entidades ejecutoras durante la fase de contratación, ejecución y cierre de las intervenciones

N°	Miembros	Órgano	Responsabilidades
1	Director o representante	DSI	• Evaluación de las solicitudes de modificaciones del PIRCC (precisiones, modificaciones de unidad ejecutora, inclusión y exclusión).
2	Director o representante	DISE	
3	Director o representante	DIST	
4	Director o representante	DISVCS	
5	Director o representante	DIST	
6	Director o representante	DAI	
7	Gerente General o representante	GG	• Evaluación de las solicitudes de modificaciones del PIRCC presentadas por los órganos de asesoramiento.
8	Director o representante	DEA	• Seguimiento a la ejecución física y financiera de las intervenciones del

N°	Miembros	Órgano	Responsabilidades
			PIRCC a cargo de las UE del GN, GR y GL
9	Jefe o representante	OGP	• Monitorear las modificaciones al PIRCC. • Monitorear el avance del PIRCC.
10	Jefe o representante	OPP	• Evaluación de las solicitudes de modificaciones del PIRCC presentadas por los órganos de línea.

Cuadro N° 6: Actividades transversales a las actividades criticas

N°	Miembros	Órgano	Responsabilidades
1	Jefe o representante	OAJ	• Emitir informes legales. • Proyectar actos resolutivos.
2	Jefe o representante	OA	• Gestionar los recursos materiales y financieros de la ARCC.
3	Jefe o representante	UL	• Gestionar y ejecutar las contrataciones de bienes y servicios en general. • Gestionar, administrar y realizar las actividades relacionadas al control de los bienes patrimoniales y almacén de suministros.
4	Jefe o representante	URH	• Elaboración de Planillas de Remuneración de Personal.
5	Jefe o representante	UAF	• Revisión de Expedientes para su Devengo y Giro.
6	Jefe o representante	OTI	• Requerimientos de atención de soporte técnico de los usuarios de la ARCC. • Requerimientos de la infraestructura tecnológica.

6.5 Requerimientos

Para el desarrollo de las actividades criticas descritas anteriormente, se han identificado los siguientes requerimientos:

6.5.1 Requerimientos de Personal

Cuadro N° 7: Requerimientos de personal

Cargo	Cantidad
Director Ejecutivo	1
Director Ejecutivo Adjunto	1
Director	6
Gerente General	1
Gerente de proyectos	35
Subdirector Regional	8
Experto	11
Asesor	10
Jefe	9

Cargo	Cantidad
Coordinador	30
Especialista	228
Analista	33
Secretaria	5
Asistente	5
Auxiliar	1
Apoyo	8
Total general	**391**

6.5.2 Requerimientos de Material y Equipo

Cuadro N° 8: Requerimientos de materiales y equipo

Material o equipo	Cantidad
Alquiler Vehículo	8
Total general	**8**

6.5.3 Requerimientos de Recursos Informáticos

Cuadro N° 9: Requerimientos de recursos informáticos

Recursos Informático	Cantidad
Alquiler de laptops (mensual)	302
Alquiler de PC (mensual)	62
Alquiler Teléfono satelital	1
Alquiler de Impresora	27
Total general	**392**

6.5.4 Requerimiento Presupuestal

Cuadro N° 10: Requerimiento presupuestal

Rubro	Monto mensual
Equipo	84,850.00
Físico	6,400.00
Humano	4,154,937.50
Financiero	620,520.00
Pago por los servicios del UKDT	430,000.00
Pasajes	66,400.00
Viáticos	124,120.00
Total general	**4,866,707.50**

6.6 Determinación de la Sede Alterna de Trabajo

En relación de las actividades criticas descritas anteriormente, estas serían realizadas en la modalidad remota, en ese sentido, no se requiere contar con una sede alterna de trabajo.

6.7 Activación del Plan de Continuidad Operativa

La activación del PCO es comunicada por la Gerencia General a los jefes de los órganos que conforman el grupo de comando de la ARCC, así como los órganos de asesoramiento y apoyo.

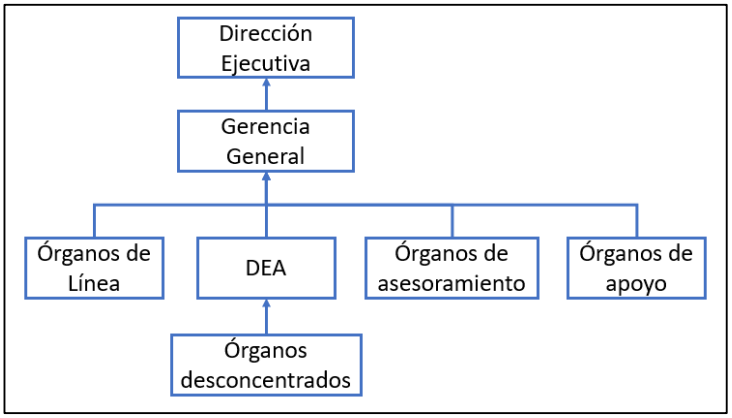
La comunicación realizada por la Gerencia General incluirá la formalización de la activación del PCO.

Asimismo, cada órgano convocara al personal correspondiente para la ejecución de las actividades criticas (véase Anexo 2). El personal deberá informar la condición en que se encuentran, y ponerse a disposición. Esta información debe ser reportada por cada órgano a la GG para su consolidación y reporte a la Dirección Ejecutiva.

Todas comunicaciones realizadas en el marco del PCO serán realizadas por los siguientes medios:

- Vía SMS
- Whatsapp
- Correo institucional y personal

Gráfico N° 1: Árbol de llamadas



a. Procedimiento de reporte inicial. En este procedimiento intervienen:

- GG remitirá comunicado a todo el personal ARCC, indicando la activación del PCO.
- Cada órgano de la ARCC debe trasladar la comunicación al personal a cargo de las actividades críticas.
- La GG elevara el reporte inicial a la Dirección Ejecutiva de la ARCC para conocimiento, acciones y traslado a la Presidencia de Consejo de Ministros.

Para mayor detalle del flujo de comunicación, véase el “Anexo N° 2: Procedimiento para la convocatoria del personal involucrado en la ejecución de las actividades críticas”.

b. Procedimientos de dotación de recursos. Una vez identificado los recursos críticos, la GG remitirá la información a la OA para que, en coordinación con los órganos pertinentes, gestione la dotación de los recursos críticas.

6.8 Activación y desactivación de la Sede Alterna

La ARCC no requiere de una sede alterna, dado que las actividades criticas serán realizadas en un 100% de manera remota.

6.9 Desarrollo de las actividades criticas

El desarrollo de las actividades críticas se realizará de acuerdo al señalado en el numeral 6.4.

Adicionalmente, se realizar las siguientes acciones:

- La OTI pondrán a disposición del personal convocado los canales de soporte técnico.
- La OA remitirá el directorio de sectoristas y coordinadores administrativos para facilitar las coordinaciones correspondientes.
- La URH comunica al personal de manera permanente la situación de operaciones en la entidad.

Sin perjuicio del desarrollo de las actividades críticas, las Unidades Orgánicas de la ARCC pueden disponer el desarrollo de las actividades no criticas mediante la modalidad de trabajo remoto.

VII. CRONOGRAMA DE EJERCICIOS DEL PLAN DE CONTINUIDAD OPERATIVA

A fin de determinar y mejorar el nivel de respuesta para la continuidad operativa de las actividades críticas, se programa ensayos y pruebas del PCO, de acuerdo al siguiente detalle:

Cuadro N° 11: Programación de ensayos y pruebas

N°	Mes	Supuesto	Responsable
1	Mayo	Ataque informático colapso totalmente los sistemas de información de la entidad	OTI
2	Octubre	Sismo de gran magnitud afecto totalmente a las sedes centrales y regionales	OA

VIII. ANEXOS

Anexo N° 1 : Plan de Recuperación de los servicios informáticos
Anexo N° 2 : Procedimiento para la convocatoria del personal involucrado en la ejecución de las actividades criticas
Anexo N° 3 : Directorio
Anexo N° 4 : Organización para el desarrollo de las actividades criticas
Anexo N° 5 : Sistema de Comunicaciones de emergencia
Anexo N° 6 : Cronograma de implementación de la Gestión de la Continuidad Operativa

PLAN DE RECUPERACIÓN DE SERVICIOS INFORMATICOS

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Fortalecimiento de la Soberanía Nacional"
"Año del Bicentenario del Congreso de la República del Perú"

INDICE

INTRODUCCIÓN

El presente documento define el Plan de Contingencia Informático y Recuperación de Servicios de Tecnología de la Información y Comunicaciones como un proceso continuo de planeación, desarrollo, prueba e implantación de procesos y procedimientos de recuperación en caso de una posible incidencia que pueda presentarse en el Centro de Datos de la Autoridad de la Reconstrucción con Cambios (ARCC). Estas acciones buscan asegurar la reanudación eficiente y efectiva de los servicios y operaciones de Tecnologías de la Información y Comunicaciones en el menor tiempo e impacto posible.

El Plan de Recuperación de Servicios de la Oficina de Tecnologías de la Información cuenta con documentos que en conjunto permiten la gestión, ejecución, pruebas y mantenimiento, esta disgregación de documentos permiten una fácil y ágil operación por los responsables a cargo ya que cuentan con un alto nivel de conocimientos para su rápida ejecución, ante situaciones de cualquier desastre que pueda ver afectado el normal funcionamiento de los servicios de la entidad (ARCC).

1. FINALIDAD

Garantizar la continuidad de los servicios de la Oficina de Tecnologías de la Información de la Autoridad de la Reconstrucción con Cambios (ARCC), a fin de que se restablezcan los servicios en el menor tiempo posible, en caso de cualquier ocurrencia o eventualidad que interrumpa el normal funcionamiento de los servicios.

2. OBJETIVOS

2.1. OBJETIVO GENERAL:

Definir, establecer los lineamientos y principios básicos para el manejo de incidentes, y garantizar la operatividad de los servicios de la Oficina de Tecnologías de la Información, que afecten la disponibilidad, confidencialidad e integridad de la información, con el fin de brindar un servicio eficiente, eficaz y oportuno a la ciudadanía y a todas las entidades que se sirve de los diversos servicios que brinda la Autoridad para la Reconstrucción con Cambios (ARCC), minimizando el impacto negativo de ocurrencia de un desastre, sea de origen natural o por acción humana.

2.2. OBJETIVOS ESPECIFICOS:

1. Identificar los equipos informáticos y servicios de información, es decir sistemas, aplicaciones o funciones de la red de datos de la ARCC que sean críticos ante cualquier eventualidad o desastre y evaluar de acuerdo al impacto que generen dentro de la Institución.
2. Establecer actividades que permitan evaluar los resultados y retroalimentación del presente plan.
3. Organizar y capacitar constantemente al personal designado en el plan de recuperación de servicios informáticos.

4. Identificar y analizar los riesgos posibles que puedan afectar la funcionalidad de los equipos informáticos.

3. ALCANCE

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

4. EVALUACION Y DIAGNOSTICO

El crecimiento permanente de la ARCC en cuanto a cobertura, ampliación de servicios, ubicación geográfica, aumento de personal, apoyo administrativo, ampliación de servicios y demás ha hecho que la infraestructura tecnológica, se desarrolle con características de alta criticidad para lo cual la OTI como medida de seguridad informática ha desarrollado estrategias de protección de todos los activos informáticos.

5. CONSIDERACIONES (Antes de la Contingencia)

Siempre que exista un fallo o eventualidad en la ARCC, se debe tener en cuenta la seguridad física y lógica del parque informático; por esta razón ante cualquier evento, se debe tener identificados los siguientes aspectos:

Ítem	Actividades	Responsable
1	Ubicación de los edificios donde se encuentran los Data Centers, los cuartos de comunicaciones y los equipos y componentes tecnológicos.	Líder del CSIRT-ARCC
2	Ubicación de los equipos, servidores o componentes de telecomunicaciones que han fallado.	OTI - Infraestructura
3	Identificación de los elementos y materiales de la construcción, para que, en caso de un incidente de mayor magnitud o una catástrofe, poder responder ante la situación.	OTI - Jefatura
4	Identificación de los tableros eléctricos y si se cuenta con acumuladores de energía (UPS) para soporte del equipo afectado y si la Infraestructura cuenta con planta eléctrica que apoye por un tiempo prudencial el funcionamiento de los equipos.	OTI - Infraestructura
5	Identificar el sistema contra incendios y capacitar al personal sobre su uso	OTI - Jefatura
6	Se debe conocer el protocolo de acceso al Data Center ubicados en las demás sedes. (Anexo 8)	Líder del CSIRT-ARCC
7	Solicitar presupuesto para la contingencia de los equipos tecnológicos.	OTI - Jefatura

Ítem	Actividades	Responsable
8	Realizar periódicamente un mantenimiento preventivo de los acumuladores de energía (UPS)	OTI - Infraestructura
9	Contar con equipo contra incendios en los Data Centers de todas sus Subdirecciones Regionales	OTI - Jefatura
10	Contar con acumuladores de energía (UPS) en todos los gabinetes de comunicaciones de las instalaciones de la entidad	OTI - Infraestructura
11	Contar con el procedimiento para reportar los incidentes de las Direcciones u Oficinas involucradas, al igual que los usuarios afectados. (Anexo 9)	OTI - Infraestructura
12	Contar con un plan de ejecución de respaldos de emergencia a la información de base de datos, aplicaciones, tramite documentario, junto a los demás servicios tecnológicos existentes.	OTI - Infraestructura

6. CONSIDERACIONES (Durante la ejecución del plan)

El Plan se basó en los siguientes requerimientos:

- Establecer e informar a la comunidad afectada sobre el periodo crítico de recuperación, en el cual los procesos deben ser recuperados antes de sufrir pérdidas significativas.
- Realizar un listado de las operaciones críticas que deberán ser prioridad en el momento de la recuperación.
- Seguir los procedimientos específicos a cada situación, para aplicarlos al momento de la eventualidad.
- En caso de que se involucren sistemas eléctricos:
    - Comunicarse con la Unidad de Servicios Generales para la supervisión de las plantas eléctricas y realizar las comunicaciones, de ser necesarias, con la entidad encargada del suministro eléctrico en la sede afectada.
    - Monitorear los acumuladores de energía (UPS) cada 10 minutos para activar y realizar las acciones correspondientes.
    - En caso de necesitar más tiempo de recuperación y si no se cuenta con baterías en los acumuladores de energía, apagar los equipos no prioritarios o que no demanden uso mientras se resuelve la contingencia.
- En caso de ser necesario, desactivar o desconectar equipos o servicios, para evitar daños o pérdida de información.
- Asegurar los respaldos (Backups) de los sistemas que atienden servicios críticos, para la posterior recuperación de los mismos.

7. CONSIDERACIONES (Después de la Contingencia)

- Restablecer el funcionamiento de los equipos y servicios críticos.
- Restablecer el funcionamiento de los equipos y servicios que se inactivaron preventivamente, de manera paulatina, supervisada y controlada siguiendo el orden de importancia.
- Validar el correcto funcionamiento de los servicios y equipos afectados.
- Evaluar el impacto y nivel de daño e identificar la cobertura y el costo del impacto.
- Restablecer los respaldos de información (Backups), de ser necesario.
- Cambiar la parte del equipo o del componente afectado o pedir garantía inmediata.
- Actualizar el mapa de riesgos, de ser necesario.
- Notificar a los usuarios afectados sobre el restablecimiento de los servicios y la condición en que quedaron.
- Diligenciar el formato de registro de incidentes, en el cual se anotará lo sucedido, la manera en la que se resolvió el incidente y los tiempos de respuesta aplicados.

8. MATRIZ FODA

Se tomó esta herramienta administrativa como parte de un análisis estratégico para verificar que nos encontramos, cuáles son puntos a favor y en contra y de esta manera podemos identificar los posibles riesgos latentes.

FORTALEZAS	DEBILIDADES
• Contar con una red adecuada para la interconexión que soporta los diferentes procesos administrativos. • Existen planes de adquisición de Tecnología a corto y mediano plazo. • Existe recurso humano capaz de aportar conocimiento y experiencias Informáticas. • Existe una infraestructura de red LAN correctamente segmentada en la ARCC. • Se cuenta con personal capacitado en las diferentes áreas técnicas. • Se cuenta con desarrollos propios que se convierten en servicios que solventan las necesidades del cliente.	• Resistencia al cambio por parte de los trabajadores de la ARCC. • Deficiencia en la cantidad de personal de OTI para realizar las tareas y los proyectos del proceso a tiempo. • Huelgas, protestas, toma de instalaciones que retrasan o interrumpen los servicios (ajenas a la entidad). • Alta rotación de personal que tiene la experiencia y los conocimientos especializadosy cuando realizan estos cambios retrasan los procesos. • Limitada infraestructura física en cuanto a equipos de cómputo, plataforma tecnológica. • Se han desarrollado al interior de la ARCC aplicaciones y/o sistemas de información que no tienen un procedimiento de uso vigente (Sistema Web del Portal Institucional) • Falta de cultura organizacional y un sistema de calidad que permita el flujo de información adecuada entre las áreas de la Entidad.
OPORTUNIDADES	**AMENAZAS**

• Implementar y mejorar la infraestructura física, tecnológica, y de conectividad, para garantizar el desarrollo de las funciones misionales de la ARCC, la comunicación y el bienestar institucional. • Intercambio de conocimiento entre el equipo de OTI, que ayuda a desarrollar nuevas formas de aprendizaje aprovechando la experiencia del día a día generado por el avance vertiginoso de las TIC. • Aplicación de TIC para incrementar la estabilidad de todos los aplicativos de la ARCC. • Creciente dotación y actualización de infraestructura física y lógica. • Vinculación de manera permanente a la institución, de personal técnico calificado.	• Ampliación de cobertura sin el correspondiente crecimiento en recursos humanos, físicos y tecnológicos. • Saturación de la red. • Alta rotación de personal técnico • Cambios tecnológicos acelerados. • No contar con fuentes de financiación de manera permanente y constante • El edificio es alquilado y no permite el uso de grupo electrógeno para casos de corte de fluido eléctrico.

FODA	CAME	CONCEPTOS
DEBILIDADES	**CORREGIR**	• Resistencia al cambio por parte de los trabajadores de la ARCC. Se establecerá un plan de concientización para que los trabajadores en general sean conscientes de la seguridad de la información y la importancia de tener respaldada la información. • Deficiencia de personal para realizar las tareas y los proyectos del proceso a tiempo, falta de personal. Se solicitará la contratación de personal para completar las plazas libres. • Huelgas, protestas, toma de instalaciones que hacen que retrasen o interrumpan los servicios. (toda institución del estado tiene esta debilidad sin embargo como parte del plan se están implementando medidas de contingencia ante este tipo de debilidades). • En un alto porcentaje el proceso cuenta con personal contratado mediante orden de prestación de servicios, esto hace que exista alta rotación de personal que tiene la experiencia y los conocimientos especializados y cuando realizan estos cambios retrasan los procesos. Es una debilidad en la cual ya se viene trabajando mediante las contrataciones bajo el régimen CAS. • Limitada infraestructura física y lógica en cuanto a equipos de cómputo, plataforma tecnológica. (Actualmente se viene solicitando presupuesto para la

FODA	CAME	CONCEPTOS
		adquisición de equipamiento para el site de contingencia en la sede de Camaná). • Se han desarrollado aplicaciones y/o sistemas de información que no tienen un procedimiento de uso vigente. Se desarrollará un manual de procedimiento operativo vigente por cada aplicativo con el que cuenta la ARCC. • Falta de cultura organizacional y un sistema de calidad que permita el flujo de información adecuada entre las áreas de la Entidad. Dado que no existe una cultura de knowledge management donde se establezca un correcto sistema de gestión del conocimiento se viene coordinando con las áreas de la institución para la generación de la misma.
AMENAZAS	**AFRONTAR**	• Ampliación de cobertura sin el correspondiente crecimiento en recursos humanos, físicos y tecnológicos. OTI debe afrontar el alto índice de crecimiento de la entidad, es por ello que es sumamente importante contar con la capacidad tecnológica adecuada con múltiples sistemas de contingencia. • Saturación de la red. Dada la alta demanda en aplicaciones y el crecimiento del consumo por parte de usuarios internos y externos nuestra red tiene un uso actual de solo el 50% y estamos preparados para un crecimiento exponencial de nuestra red a nivel de tráfico WAN y lan. • Alta rotación de personal técnico. La institución viene adoptando sistemas de gestión del conocimiento a fin que el funcionamiento de la OTI no se vea afectada ante la rotación de especialistas. • Cambios tecnológicos acelerados. Como oficina de Tecnología, la OTI debe afrontar el constante crecimiento tecnológico y para ello se debe avanzar a la par. • No contar con fuentes de financiación de manera permanente y constante. La OTI debe afrontar y hacer un constante análisis del crecimiento de la red tecnológica y para ello se debe poder contar con financiamiento en aras del correcto funcionamiento de la ARCC. • El edificio es alquilado y no permite el uso de grupo electrógeno para casos de corte de fluido eléctrico. (por limitaciones propias de la situación del edificio de la

FODA	CAME	CONCEPTOS
		sede principal se debe fortalecer los sistemas UPS de la institución.
FORTALEZAS	**MANTENER**	• Contar con una red adecuada para la interconexión que soporta los diferentes procesos de red. (la red de la institución cuenta con una red completamente segmentada y centralizada todo esto permite una adecuada gestión del tráfico y la adecuada aplicación de las políticas de seguridad. • Existen planes de adquisición de tecnología a corto y mediano plazo. OTI ha solicitado el presupuesto para la adquisición de equipamiento tecnológico para un plan de contingencia tecnológica y de la información, este presupuesto debe ser brindado este año. • Existe recurso humano, capaz de aportar conocimiento y experiencias Informáticas. OTI cuenta con especialistas con una amplia experiencia en sus puestos. • Existe una infraestructura de red LAN correctamente segmentada en la ARCC. La red de la ARCC cuenta con múltiples VLANS que permiten segmentar los dominios de broadcast y de red. • Se cuenta con personal capacitado en áreas técnicas. OTI cuenta con especialistas con una amplia experiencia en sus puestos. • Se cuenta con desarrollos propios que se convierten en servicios que solventan las necesidades del cliente. (La ARCC cuenta con un grupo importante de desarrolladores que constantemente personalizan los aplicativos consumidos por los usuarios internos y externos.
OPORTUNIDADES	**EXPLOTAR**	• Implementar y mejorar la infraestructura física, tecnológica, y de conectividad, para garantizar el desarrollo de las funciones misionales de la ARCC, la comunicación y el bienestar institucional. La red tecnológica de la ARCC tiene una capacidad de crecimiento importante y aún se pueden explotar diferentes aspectos en aras de mejorar la experiencia y la calidad al usuario. • Apoyo en el desarrollo de nuevas formas de aprendizaje y apropiación del conocimiento generado por el avance vertiginoso de las TIC. La ARCC tiene una plataforma llamada "aprendiendo con cambios". Es posible explotar esta aplicación web para ponerlo al alcance de un mayor número de usuarios, así como enriquecer la información que en ella se enseña.

FODA	CAME	CONCEPTOS
		• Aplicación de TIC y la comunicación para incrementar la estabilidad de todos los aplicativos de la ARCC. Se puede explotar las diferentes tecnologías de la información para incrementar la estabilidad de todos los aplicativos. • Creciente dotación y actualización de infraestructura física y lógica. La ARCC cuenta con tecnología actualizada esta puede ser actualizada y explotada para el bien de la ARCC.

9. PRIORIDAD EN LA RECUPERACIÓN DE SERVICIOS

Sistema	Fecha de Implementación	Herramientas de Desarrollo	Metodología empleadas	Funcionalidades
Portal Institucional	2020	1. Briefing. 2. Sitemap. 3. Diseño de wireframes de baja resolución (estructura). 4. Recopilación de recursos imágenes, información, etc.). 5. Mockup o diseño de alta resolución (imágenes y color). 6. Elección del tema de Wordpress. 7. Prototipo en un servidor local. Instalación de un servidor local (XAMPP) y Wordpress. - Instalación del tema. - Plugins: elección, instalación y testeo. 8. Pruebas UI yUX. 9. Depuración de errores y rediseño de páginas.	1. Sublime Text (edición de código fuente) 2. Workbench (acceso a base de datos) 3. Terminal (Unix access) 4. Putty (Unix access)	Es documento electrónico, accesible desde un navegador web, cuya finalidad es la de difundir información dinámica de nuestra entidad a través de la World Wide Web.
Sistema de Visitas	2018	.Net C# con SQL Server	Orientada a Objetos	Registrar las visitas a la Autoridad
SIGA, SIAF	2017	Desktop		Gestionar los recursos logísticos y financieros de la Autoridad
MONITOR ARCC	2018	PHP 7.3, SQL Server 2017, Zend Framework	Scrum	Sistema de Seguimiento de Análisis de Proyectos, gestionar la Información
sistema de Repositorio Virtual	2020	.Net C# con SQL Server	Orientada a Objetos	Permite la organización de la información de las intervenciones del Plan Integral.
Sistema de Tramite Documentario	2018	PHP con SQL Server	Orientada a Objetos	Organizar, conservar, depurar y custodiar el archivo que corresponde a Trámite Documentario (Resoluciones, Informes, proyectos) y de Actas y Certificados.

Registro de empresas Extranjeras	2019	.Net C# con SQL Server	Orientada a Objetos	Permite a las empresas extranjeras registrarse para poder participar en las procesos de contratación.
Archivo Digital	2019	Net C# con SQL Server	Orientada a Objetos	Permite a las Unidades Ejecutoras obtener un link de los archivos de un proceso para ser publicado en su portal institucional.
Soporte SSAP	2020	PHP, MariaBD	Orientada a Objetos	Sistema para llevar una bitácora de atenciones que se realizan en el sistema de SSAP.
Sistema de Expediciones	2019	Net C# con SQL Server	Orientada a Objetos	Permite llevar un mejor control en la salida de documentos.
OCS	2019	PHP, con MariaBD	Orientada a Objetos	Permite llevar un control del parque informático.
Soporte	2020	PHP, MariaBD	Orientada a Objetos	Permite llevar un control de atenciones de helpdesk de OTI.
Sistema de Convocatorias	2018	.NET, Oracle Express	Orientada a Objetos	Permite llevar el control del proceso de seleccion CAS.
Nuevo Reglamento	2019	PHP	Orientada a Objetos	Portal informativo del nuevo reglamente para el proceso especial de contrataciones.
Sistema de Reclamos	2018	.Net C# con MySQL	Orientada a Objetos	Plataforma que permite a los ciudadanos realizar un reclamo.

El software que soporta toda la plataforma de virtualización está basado en VMWare, líder del sector en virtualización y nube. Dicho software se encuentra instalado en el Data Center de la ARCC.

10. MEDIDAS TOMADAS A PARTIR DEL ESTABLECIMIENTO DEL DATA CENTER DE CONTINGENCIA

- Todos los servidores virtuales serán copiados exactamente en el site de contingencia, para ello se generará un clúster entre cuatro host de Blade para que la sincronización sea constante.
- Redundancia del servicio de internet para el site de contingencia, se contratará un servicio adicional de internet con otro operador para que en caso de que el operador 01 sufra el colapso de su red nuestros servicios pueden seguir activos mediante el operador 02. (Este servicio deberá incluir seguridad gestionada)
- Redundancia de conexión ante la caída del enlace Lan to Lan entre la sede central y la Sede del site de contingencia en Camaná, para lograr ello se desplegará un radioenlace de alto performance entre la sede central en Jr. Santa rosa y la sede de Camaná. Este enlace no debe ser menor a 300 Mbps.

- Todos los servicios externos e internos de la Autoridad para la Reconstrucción con Cambios tendrán una copia de seguridad en alta disponibilidad de tipo activo pasivo, incluyendo el repositorio de archivos general en los servidores de archivos.

11. PANORAMA DE RIESGOS

IDENTIFICACION DEL RIESGO			ANALISIS DEL RIESGO			MANEJO DEL RIESGO
RIESGO	**CAUSAS**	**CONSECUENCIA**	**PROBABILIDAD**	**IMPACTO**	**ZONA DE RIESGO**	**ACCIONES /CONTROLES**
Pérdida de la configuracióndelos equipos telefónico	* Usuarios malintencionados * Falta de capacitación al usuario final * Mal uso de los teléfonos	* Inestabilidad en la continuidad de los servicios * Incomunicación total o con dificultades * Pérdida de tiempo al realizar el desplazamiento hasta el sitio para su reparación	**BAJA**	**ALTO**	**MODERADO**	* Manuales para los usuarios finales
Fallas en la comunicación telefónica IP	* Ancho de banda insuficiente entre lasede central y la sede de contingencia. * Daño en la configuración de los equipos * Retardo entre enlaces	* Deficiencia en el servicio	**BAJA**	**ALTO**	**MODERADO**	* Aumento de ancho de banda * Calidad de servicio en teléfonos y en regiones * Optimización de ancho de banda (compresión de voz)
Errores de configuración ellos aparatos telefónicos	* Falta de capacitación * Falta de conocimiento en el procedimiento de instalación y configuración del aparato telefónico * Errores en el administrador	* Deficiencia en el servicio * Deficiencia en el uso de los aparatos telefónicos	**BAJA**	**BAJO**	**ACEPTABLE**	* Pruebas o laboratorios para aplicar configuración en la plataforma
Uso inadecuado de los códigos de servicios especiales	* Divulgación de claves por parte de losusuarios * Usuarios malintencionados	* Interceptación de la información	**MEDIA**	**ALTO**	**TOLERABLE**	* Cambio de código de servicios especiales según su uso, y validación donde el código tenga un grado alto de complejidad.
Daños a equipos de red	* Fallas eléctricas * Terminación de vida útil * Falta de mantenimientos * Condiciones ambientales inapropiadas	* Caída de la red que atiende el equipo dañado	**MEDIA**	**ALTO**	**IMPORTANTE**	* Instalación de UPS * Mantenimientos programados * Seguimiento de las fechas de vida útil de los equipos. EOS (end of sale),EOL (end of life time) * Adecuación de cuartos de telecomunicaciones
Pérdida de la configuracióndelos equipos	* Fallas de hardware en la memoria no volátil NVRAM * Reinicio inesperado del sistema * Olvido por parte del administrador para salvar la configuración	* Caída de la red que atiende el equipo dañado	**BAJA**	**ALTO**	**MODERADO**	* Adquisición de nuevos equipos * Realización de Backups de los equipos más importantes
Fallas en la certificación del cableado	* EMI y RFI (interferencia electromagnética e interferencia por radiofrecuencia) * Mala instalación de cableado	* Mal desempeño de lospuntos cableados * Existe conectividad limitada o nula	**BAJA**	**MEDIO**	**TOLERABLE**	* entrenamiento en los procesos del cableado * Diseño previo que evite o aislé las fuentes de EMI y RFI
Caída de enlace de datos	* Problemas en la red del proveedor de servicios de telecomunicaciones ISP	* Sedes sin servicio de red	**BAJA**	**ALTO**	**MODERADO**	Exigencia de niveles de servicios ANS comunicación Help Deskcon el proveedor

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Fortalecimiento de la Soberanía Nacional"
"Año del Bicentenario del Congreso de la República del Perú"

IDENTIFICACION DEL RIESGO			ANALISIS DEL RIESGO			MANEJO DEL RIESGO
RIESGO	**CAUSAS**	**CONSECUENCIA**	**PROBABILIDAD**	**IMPACTO**	**ZONA DE RIESGO**	**ACCIONES /CONTROLES**
Problemas con el direccionamiento IP	* Instalación no autorizada de equipos que entregan direcciones IP * Caída de servidor DHCP	* Los equipos que toman IP en un segmento de red equivocado no pueden navegar	**MEDIA**	**ALTO**	**IMPORTANTE**	* Se detectan los equipos y se desactivan * Configuración segura de puntos de red y puertos.
Ataque a los equipos de red	* Equipos de telecomunicaciones desactualizados en hardware y/o software * Sistemas de conexión para la administración no seguros	* Denegación del servicio	**MEDIA**	**ALTO**	**IMPORTANTE**	*Actualización del software d los equipos que se encuentran con tiempo de vida activo * Reemplazo de los equipos cuyo tiempo de vida ya caduco *Monitoreo
Daño en los servidores	* Falta de mantenimiento de losservidores * Instalaciones físicas inadecuadas * Condiciones ambientales inapropiadas	* Interrupción de los servicios que el servidor soporta	**BAJA**	**ALTO**	**MODERADO**	* Mantenimientos programados * Adecuación del espacio físico con estándares internacionales
Pérdida de la informacióndel sistema de almacenamiento masivo	* No aplicar procedimiento adecuadopara apagado del sistema de almacenamiento masivo * Fallas eléctricas * Daño en disco	* Pérdida de información	**BAJA**	**ALTO**	**MODERADO**	* Mantenimientos preventivos * Garantía de los discos * mantenimiento sistema eléctrico.
Daños de sistemas operativos en los servidores	* Mala administración * Daños en disco * Ejecución errónea del mantenimiento	* Interrupción de los servicios que el servidor soporta	**BAJA**	**ALTO**	**MODERADO**	* Actualizaciones – update, upgrade - *Revisión de logs * Supervisión de mantenimientos *monitoreo de desempeño
Demora en los procesos de contratación de aspectos técnicos.	* Demora en los procesos administrativos de contratación * Respuesta baja y lenta deproveedores * Cambio tecnológico acelerado	* Atraso en la contratación de recursos tanto humano como tecnológico provocando un retraso y fallas en las actividades de la red	**BAJA**	**ALTO**	**MODERADO**	Reiteración en el cumplimiento de acciones alos actores involucrados: oficinas de la ARCCy proveedores
Pérdida de contraseñas de administrador	* Robo de contraseñas * Olvido de las contraseñas * Las contraseñas no se encuentran debidamente resguardadas * El administrador se retira y no dejalas contraseñas	* Tomar posesión de los servidores sin autorización * Pérdida de información * Cambio o pérdida de la configuración de los servicios *sin acceso a la administración del equipo involucrado	**BAJA**	**ALTO**	**MODERADO**	* Actualización anual o por inicio de nuevo contrato de sobres cerrados de Contraseñas. * Las contraseñas deben tener una combinación alfanumérica
Ataques a los servidores por medio de software malicioso	* No tenga instalado la licencia deantivirus * No se encuentre debidamente configurado el antivirus * No se encuentre actualizado elantivirus	* Daño en los archivos de configuración del servidor que podría ocasionar fallas en el servicio que se preste * Perdida de información * Daño en el sistemaoperativo	**MEDIA**	**ALTO**	**IMPORTANTE**	* Licenciamiento de antivirus * Backups a la informaciónde los servidores * Monitoreo de red. * Claves de Administración del antivirus diferente al de los servidores
Vulnerabilidades o huecosde seguridad en software	*No contar con actualizaciones, y parches de software, puertos mal administrados, no disponer de firewalladecuado.	* Pérdida de información * Apoderamiento de la máquina por personal no autorizado * Robo de información * Servicios no disponibles	**BAJA**	**ALTO**	**MODERADO**	* Actualizaciones permanentes de los servicios y sistema operativo * Monitoreo de red

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Fortalecimiento de la Soberanía Nacional"
"Año del Bicentenario del Congreso de la República del Perú"

IDENTIFICACION DEL RIESGO			ANALISIS DEL RIESGO			MANEJO DEL RIESGO
RIESGO	**CAUSAS**	**CONSECUENCIA**	**PROBABILIDAD**	**IMPACTO**	**ZONA DE RIESGO**	**ACCIONES /CONTROLES**
Se acabe el espacio en eldisco de los servidores	* No se tenga planeado el crecimiento de la información * Virus * Falta de revisión log	No se puede prestar los servicios que soporta el servidor	**MEDIA**	**ALTO**	**IMPORTANTE**	* Revisión de logs periódicamente * Liberación constante de archivos innecesarios *monitoreo
Falta de acceso físico aestación de trabajo	* Toma o cierre forzoso de sedes de laARCC	* Los usuarios finales no podrán ingresar a sus equipos de trabajo	**MEDIA**	**ALTO**	**IMPORTANTE**	* Identificación de equipos atendidos generando listado de equipos, MAC, nombre de usuarios, funciones de equipo. * Configurar encendido de equipo "wake up on lan" * Configuración de escritorio remoto según serequiera * Configuración acceso externo a la ARCC sise requiere. VPN * Virtualización de escritoriosy aplicaciones requeridas. Habilitación de administración remota deinfraestructura de TI
Publicar en web informaci ón desactuali zada y/o errada.	* No se tienen identificadas o no existen las fuentes de información. * El usuario que publica NO tiene la experticia y conocimiento para hacerlo. * No existe la política institucional de comunicaciones. * El usuario desconoce o no aplica laresolución 711 de 2008 para publicación Web * Descuido del usuario, Errores en la digitalización. * alta rotación del Recurso humano por tipo de vinculación (CPS) * Las oficinas no verifican la veracidad y la pertinencia de la información publicada.	* Generar confusión en la comunidad. * Problemas jurídicos y legales. * Problema de transparencia institucional * Mala imagen institucional	**MEDIA**	**MEDIO**	**MODERADO**	*Adelantar capacitaciones a responsables de publicación en web delas dependencias. *Entregar al líder de comunicaciones institucionales el perfil y clave de autorización de publicación. *Adelantar elaboración de políticas publicaciónweb. *Hacer revisiones y comunicaciones con las dependencias que tienen página
Publicar información malintencionada o falsa	* Acceso no autorizado. * Usuario autorizado publica información no institucional, o confines personales * No se revisa la información a la hora de la activación o la publicación. * Sufrir un ataque al sitio que modifique la información publicada * el usuario publicador no verifica laveracidad de la información *el usuario publica información si solicitar autorización a su jefe directo.	* Daño a la imagen institucional * Generar confusión * Perjudicar el buen nombre de las instituciones y/o personas * filtración de información * Inconsistencia en la información * Problemas legales	**BAJA**	**ALTO**	**MODERADO**	* Realizar capacitaciones * Hacer campañas de responsabilidad en la publicación de información * Revisión periódica de información publicada

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Fortalecimiento de la Soberanía Nacional"
"Año del Bicentenario del Congreso de la República del Perú"

IDENTIFICACION DEL RIESGO			ANALISIS DEL RIESGO			MANEJO DEL RIESGO
RIESGO	**CAUSAS**	**CONSECUENCIA**	**PROBABILIDAD**	**IMPACTO**	**ZONA DE RIESGO**	**ACCIONES /CONTROLES**
Problemas legales	* Utilizar software sin licenciamiento * No respetar las normas y leyes de derechos de autor * Problemas de cultura	*violación a derechos de autor * sanciones al representante legal y los responsables como: Cárcel, Multas. * Desprestigio para la institución	**MEDIA**	**ALTO**	**IMPORTANTE**	* Instalación de software debidamentelicenciado. * Política de administración y uso de equipo de usuario final
No se puede acceder a la información publicada	* Errores en los formatos de la presentación de la información * Errores técnicos que hacen que losservicios fallen * El usuario no tiene las herramientaspara ver la información * Manejo de software incompatible * Incompatibilidad de versiones	* Generar confusión * Problemas legales * Demora en los procesos	**BAJA**	**MEDIO**	**TOLERABLE**	* Capacitación al usuario * Instructivo para acceso * Revisiones y pruebasde versión a los documentos a publicar
No se articule o active el mecanismo para recibir retroalimentación	* Problema de planeación * Problemas técnicos * No se habiliten los canales de comunicación y retroalimentación * No se informa de la habilitación * Problema cultural	* No exista la retroalimentación de la información publicada Comunicación errónea	**BAJA**	**BAJO**	**ACEPTABLE**	* Definir claramente los mecanismos de retroalimentación y determinar si hay viabilidad técnica * Hacer pruebas o simulacros * Hacer capacitaciones Realizar instructivos de uso de los servicios
Mal funcionamiento de unaplicativo	* Deficiencias en el mantenimiento * Mal diagnóstico a la detención de lafalla * Implementación de una solución no adecuada * Uso de actualizaciones y parches de seguridad que producen mal funcionamiento	* No se puede hacer uso correcto del servicio * Demoras en la respuestaa las solicitudes hechas con ese servicio	**BAJA**	**ALTO**	**MODERADO**	* Crear un ambiente de desarrollo por etapas que incluya desarrollo, pruebas y producción *Uso de estándares y procedimiento de detección de fallas * Hacer iteraciones para corregir las publicaciones
Daños en hardware, software o medios	* Fallas en el funcionamiento * Inadecuada manipulación de equiposy medios * Almacenamiento inadecuado demedios * Virus en el sistema	* Caída total o parcial del servicio * * Problemas de actualización del sitio	**BAJA**	**ALTO**	**MODERADO**	* Redundancia de equipos críticos * Cultura en el manejo y almacenamiento de los equipos y medios * Mantenimiento preventivo y correctivo * Manejo de vida útil
Pérdida de la información	* Problema de cultura * Falta de capacitación * Inadecuada o inexistencia realización de copias de seguridad * Ataque informático a los sistemas * Ataques de virus informáticos * Inadecuado manejo de la información y las herramientas de la información * Robo o pérdida de dispositivos de almacenamiento con	* Demora en los procesos * Uso indebido de lainformación Problemas legales	**MEDIA**	**ALTO**	**IMPORTANTE**	* Cultura en el manejo y almacenamiento de los equipos y medios * Concientización al usuario sobre la clasificación y el manejode la información * Definición de roles de usuario de acuerdo a la forma de acceder y hacer uso de la información * Implementación de políticas de copias de seguridad * Implementación de políticas de digitalización de la información

IDENTIFICACION DEL RIESGO			ANALISIS DEL RIESGO			MANEJO DEL RIESGO
RIESGO	**CAUSAS**	**CONSECUENCIA**	**PROBABILIDAD**	**IMPACTO**	**ZONA DE RIESGO**	**ACCIONES /CONTROLES**
	información					
Publicación de información no autorizada	* Falta de responsabilidad y prudencia en el uso de la información * Error humano * Error en la verificación de lainformación * Publicación de información sin autorización del jefe directo	* Robo * Problemas legales * Vulneración de derechos fundamentales	**BAJA**	**ALTO**	**MODERADO**	* Políticas claras de publicación de la información * Sensibilizar al usuario sobre la clasificación de la información * Definición de roles de usuario de acuerdo a la forma de acceder y hacer uso de la información * Cumplimiento de normatividad vigente

12. FASES DEL PLAN DE RECUPERACIÓN DE SERVICIOS INFORMÁTICOS

El Plan de Recuperación de Servicios Informáticos tiene las siguientes fases:

13. ACTIVIDADES DE PREPARACIÓN

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:

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 el 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.
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	**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.
7	**Respecto a la preparación y actualización registros vitales:** ✓ Actualizar los registros de direccionamiento IP. ✓ Revisar la vigencia de los archivos de las topologías. ✓ Revisar y actualizar los archivos de configuración. ✓ Revisar y actualizar scripts de Backups de comunicaciones (en caso sea necesario) ✓ Realizar periódicamente los Backups de comunicaciones. ✓ Respaldar el cliente VPN (software + perfiles)

14. 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.

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.
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 (no mayor a un día, si es factor interno y no hay ningún reemplazo de equipo, pero si es factor externo como la adquisición de algún equipo dañado puede tomar más tiempo), 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 - 01- Ubicación 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" (denominado así al momento del desastre a la "sala de reuniones") 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 o 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/Amarillo "** 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 - 01- Ubicación de Recuperación".
4	Solicitar al equipo de líderes ejecutar las gestiones para movilizar al personal crítico: empresas de taxis movilidad pública y/o transporte particular, que se encuentren disponibles.
5	Coordinar con el equipo de líderes, la entrega y la 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 de Centro de Comando, los desplazamientos del personal correspondiente hacia el Centro de Datos Alterno (en la Nube) 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 la Infraestructura coordinar con el líder de infraestructura del Centro de Datos Alterna.
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	Una vez que el Líder de Sistemas de Información, confirme la recuperación de los servicios críticos en el Centro de Datos alterno, validar el status de los servicios para dar pase al estado **"Desastre Controlado".**
10	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. ✓ Reactivar y ejecutar el Servicio de Aplicaciones Intranet. ✓ Activar ejecutar el Servicio del Servidor de Archivos 1. ✓ Activar y ejecutar el Servicio del Servidor de archivos 2. ✓ Activar y ejecutar el Servicio del Controlador de Dominio Principal. ✓ Activar y ejecutar el Servicio del Controlador de Dominio Secundario. ✓ Activar y ejecutar el Servicio de despliegue de IP's. ✓ Activar y ejecutar el servidor de base de datos Web. ✓ Activar y ejecutar en almacenamiento de archivos del Sistradoc. ✓ Activar y ejecutar el servidor de aplicaciones E-Firma Sistradoc.

	✓ Servicio de base de datos Oracle SIGA_MINDEF, SIGA_DIGEPREV. ✓ Activar y ejecutar el servicio de correo principal. ✓ Activar y ejecutar el servicio de correo secundario. ✓ Activar y ejecutar del servicio de aplicación del MEF. ✓ Activar y ejecutar el servicio de Oracle con RAC 1. ✓ Activar y ejecutar el servicio de Oracle con RAC 2. ✓ Activar y ejecutar el servicio de aplicaciones Apache Sistradoc. ✓ Activar ejecutar el servicio de réplica de base de datos y alta disponibilidad del Sistradoc. ✓ Activar y ejecutar el servicio de acceso a carpetas de aplicaciones. ✓ Activar y ejecutar el sistema de consultas PIDE. Ver "ANEXO - 06 - Procedimientos de Infraestructura ".
11	Según sea el caso, se recopilará información de los recursos adicionales que sean necesarios para que el líder de telecomunicaciones, coordiné la logística adquisición, con el líder de Recuperación.
12	Monitorear los avances en la activación de la contingencia de la red.
13	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 (Líder de recuperación). ✓ Cualquier otro medio de comunicación vía datos. Ver "ANEXO - 01- Ubicación de Recuperación".

15. 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.

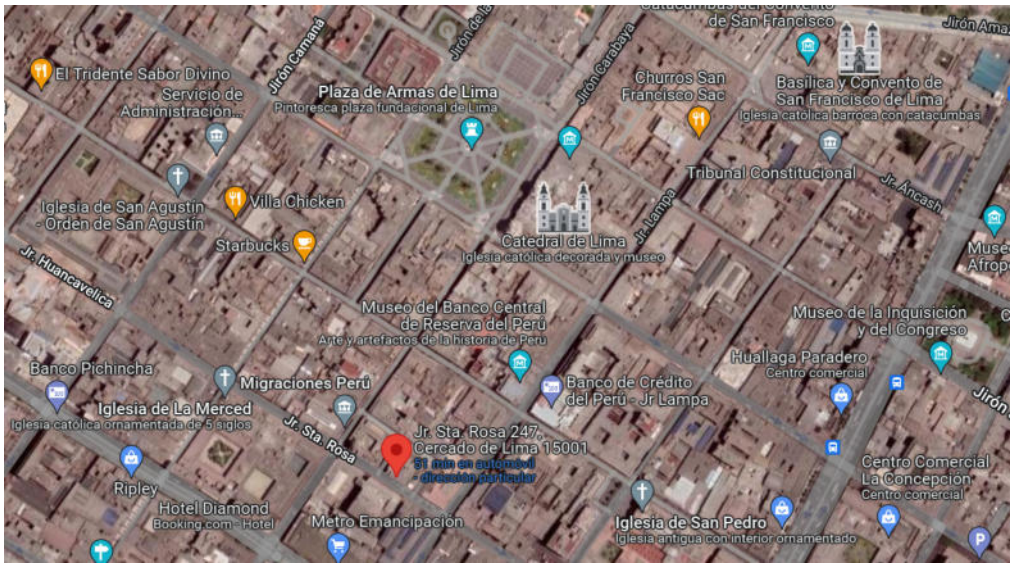
A continuación, se listan las actividades por cada "rol" del equipo de recuperación.

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 Sistema 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 líderes 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 (Líder de recuperación).

	✓ Cualquier otro medio de comunicación vía datos. Ver "ANEXO - 01- Ubicación 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",** 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	De ser el caso, gestionar un taller de las "L**ecciones Aprendidas"** respecto a la situación presentada.
6	Coordinar la actualización del Plan de Recuperación de Servicios Informáticos y documentación realizada (Planes de continuidad, anexos entre otros) según las observaciones y lecciones aprendidas identificadas.

16. ANEXOS

ANEXO 1: UBICACIÓN DE RECUPERACIÓN SEDE CENTRAL



ANEXO 2: EQUIPO DE RECUPERACIÓN

EQUIPO DE RESPUESTAS	
CARGO	**ROL DE EQUIPO**
JEFE DE LA OFICINA DE OTI	RESPONSABLE DE LA DIRECCIÓN Y COORDINACION PARA LA RECUPERACION DE TI
ESPECIALISTA II DE INFRAESTRUCTURA TECNOLOGICA	RESPONSABLE DE LA COORDINACION PARA LA PUESTA EN MARCHA DE LA RECUPERACIÓN
RESPONSABLE DE INFRAESTRUCTURA	EJECUTOR DE TAREAS DE RECUPERACIÓN

N°	ORDEN	CORREO	EQUIPO DE TRABAJO	NOMBRES Y APELLIDOS
1	PRINCIPAL	VCORIGLIANO@RCC.GOB.PE	ESPECIALISTA	VICTORIO DANIEL CORIGLIANO ZEGARRA
2	SECUNDARIO	SALVITRES@RCC.GOB.PE	ANALISTA	SEGUNDO SERGIO ALVITRES TORRES
SERVIDORES DE BASE DE DATOS				
1	PRINCIPAL	OTI_18@RCC.GOB.PE	ESPECIALISTA	ALFONSO JAIR DENEGRI SAYRITUPAC
2	SECUNDARIO	JRAMIREZB@RCC.GOB.PE	ANALISTA	JUAN CARLOS RAMIREZ BRUNO
SERVIDORES DE APLICACIONES				
1		CRODRIGUEZ@RCC.GOB.PE	ESPECIALISTA	SEGUNDO SERGIO ALVITRES TORRES
2		OTI_27@RCC.GOB.PE	ANALISTA	

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Fortalecimiento de la Soberanía Nacional"
"Año del Bicentenario del Congreso de la República del Perú"

SERVIDORES DE INFRAESTRUTURA				
1	PRINCIPAL	VCORIGLIANO@RCC.GOB.PE	ESPECIALISTA	VICTORIO DANIEL CORIGLIANO ZEGARRA
2	SECUNDARIO	OTI_18@RCC.GOB.PE	ANALISTA	ALFONSO JAIR DENEGRI SAYRITUPAC
	EQUIPAMIENTO DE RED			
1	PRINCIPAL	VCORIGLIANO@RCC.GOB.PE	ESPECIALISTA	VICTORIO DANIEL CORIGLIANO ZEGARRA
2	SECUNDARIO	VCORIGLIANO@RCC.GOB.PE	ANALISTA	VICTORIO DANIEL CORIGLIANO ZEGARRA

ANEXO 3: RELACIÓN DE PROVEEDORES

RELACIÓN DE PROVEEDORES						
N°	**NOMBRES Y APELLIDOS**	**RUC**	**DIRECCIÓN**	**TELÉFONO**	**EMAIL**	**EMPRESA**
1	Barriga Chávez Lisbeth	20546371108	Jr. Rio Chicama N°5662 Urb. Villa del Norte – Los Olivos - Lima	999 867 210 / (01) 528-6439	Lbarriga@jlsoftsoluciones.com.pe	JL SOFT SOLUCIONES INTEGRALES S.A.C
2	Claudio Fernando Arce Ticona	20601858615	Ca. Enrique Palacios 420, Miraflores	980043058	c.guillen@aggity.pe	AGGITY PERU S.A.C.
3	Javier Condori Bayona	20250323221	Jirón Rebeca Oquendo 409, BREÑA,LIMA	934 921 523	ventas@tecnoldata.com.pe	TECNOL DATA S.R.LTDA.
4	RODRIGUEZ MACASSI	20609755751	Calle Mollocmarca Nro 371 – Of 503 – San Miguel	(01)7582951	hardsecur@hardsecur.net	HARDSECUR EIRL
5	Sofía Montesinos Huaman	20601618584	Calle Luther King Nro. 181, Surquillo	956189941	ventas@securetechnologies.com.pe	SECURE TECHNOLOGIES S.A.C.

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.

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Fortalecimiento de la Soberanía Nacional"
"Año del Bicentenario del Congreso de la República del Perú"

						ESPECIALISTA 1
						ESPECIALISTA 2
OTI	JEFE DE LA OFICINA DE OTI	COORDINADOR DE OTI	RESPONSABLE DE INFRAESTRUCTURA			ESPECIALISTA 3
						ESPECIALISTA 4
						ESPECIALISTA 5
						ESPECIALISTA 6

ANEXO 5: REGISTROS VITALES

PERÚ | Presidencia del Consejo de Ministros | Autoridad para la Reconstrucción con Cambios | Equipo de Respuesta ante Incidentes Digitales - CSIRT
RECONSTRUCCIÓN CON CAMBIOS

"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año del Bicentenario del Perú: 200 años de Independencia"

FECHA:

HORA INICIO:

RESPONSABLE DEL REGISTRO:

REGISTROS VITALES DEL DESASTRE

FIRMA

DNI:

HORA FIN:

ANEXO 6: PROCEDIMIENTOS DE INFRAESTRUCTURA

Procedimiento 1	PLAN DE RECUPERACION DE SISTEMA ELECTRICO
Procedimiento 2	PLAN DE ENLACES WAN
Procedimiento 3	PLAN DE TELEFONIA FIJA
Procedimiento 4	PLAN DE RECUPERACION DE SERVIDORES
Procedimiento 5	PLAN DE RECUPERACIONES DE APLICACIONES WEB
Procedimiento 6	PLAN DE RECUPERACION DE BASE DE DATOS
Procedimiento 7	PLAN DE RECUPERACION SISTEMA DE CAMARAS
Procedimiento 8	PLAN DE RECUPERACION DE SISTEMAS EN NUBE

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 para respaldar todas nuestras máquinas virtuales.

Las máquinas virtuales que requerimos sacar a la nube son las siguientes:

VM	CPUs	Memory	NICs	Disks	min Required EVC Mode Key	Video Ram KiB	Provisioned MiB	In Use MiB	Unshared MiB	Datacenter	OS according to the configuration file
IPAM	2	4,096	4	1		4,096	260,476	256,000	256,000	ha-datacenter	Other (64-bit)
SRV-BD	8	8,000	1	2		4,096	316,475	177,717	177,717	ha-datacenter	Microsoft Windows Server 2016 or later (64-bit)
SRV-BD-MSSQL	20	32,768	1	1		8,192	647,309	647,309	647,309	ha-datacenter	Microsoft Windows Server 2016 (64-bit)
SRV-BD-RRHH	4	8,192	1	1		4,096	162,981	132,447	132,447	ha-datacenter	Microsoft Windows Server 2016 or later (64-bit)
SRV-DL	4	6,144	1	2		4,096	477,565	372,250	372,250	ha-datacenter	Microsoft Windows Server 2016 or later (64-bit)
SRV-FILE01	8	6,144	2	4		4,096	11,548,139	11,503,916	11,503,916	ha-datacenter	Microsoft Windows Server 2016 or later (64-bit)
SRV-GLPI	2	2,048	1	1		131,072	97,131	19,130	19,130	ha-datacenter	CentOS 4/5/6 (64-bit)
SRV-OMEDELL	4	16,384	1	1		4,096	233,883	26,482	26,482	ha-datacenter	Other (32-bit)
SRV-SAEDELL	4	16,384	1	1		4,096	159,830	50,675	50,675	ha-datacenter	Other (32-bit)
SRV-SIAF	6	8,000	1	3		4,096	1,149,020	708,931	708,931	ha-datacenter	Microsoft Windows Server 2016 or later (64-bit)
SRV-SIGA	4	10,240	1	1		4,096	391,205	186,033	186,033	ha-datacenter	Microsoft Windows Server 2016 or later (64-bit)
SRV-SPIJ	1	4,000	1	1		4,096	312,426	77,361	77,361	ha-datacenter	Microsoft Windows Server 2016 or later (64-bit)
SRV-SSAP	8	12,288	1	2		4,096	596,370	493,903	493,903	ha-datacenter	Microsoft Windows Server 2016 or later (64-bit)
srv-vcenter01	2	12,288	1	16		4,096	456,785	158,769	158,769	ha-datacenter	Other 3.x or later Linux (64-bit)
SRV-WIFI	1	8,000	1	1		4,096	121,333	94,555	94,555	ha-datacenter	Microsoft Windows Server 2016 or later (64-bit)
SSAP-PRUEBA	4	10,240	2	2		4,096	450,711	312,272	312,272	ha-datacenter	Microsoft Windows Server 2012 (64-bit)
vCLS (4)	1	128	0	1		4,096	2,256	1,216	1,216	ha-datacenter	Other 3.x or later Linux (64-bit)
vCLS (6)	1	128	0	1		4,096	2,256	1,259	1,259	ha-datacenter	Other 3.x or later Linux (64-bit)

ANEXO 8: PROTOCOLO DE ACCESO AL CENTRO DE DATOS DE ARCC

1.- Pedir Acceso al encargado del centro de datos, llenando el formato de Acceso al Centro de Datos del ARCC.
2.- El encargado revisa y analiza el formato de Acceso al Centro de Datos del ARCC, y responde en el plazo establecido sobre dicho acceso, si es aprobado se acuerda fecha y hora del acceso.
3.- El encargado acompaña en todo momento a la persona que pidió el acceso hasta el momento de su retiro del centro de datos.
4.- El encargado registra la actividad que se realizó dentro del centro de datos, tiempo inicio y tiempo fin.

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Fortalecimiento de la Soberanía Nacional"
"Año del Bicentenario del Congreso de la República del Perú"

ANEXO 8.1: FORMATO DE ACCESO AL CENTRO DE DATOS

PERÚ | Presidencia del Consejo de Ministros | Autoridad para la Reconstrucción con Cambios | Equipo de Respuesta ante Incidentes Digitales - CSIRT
RECONSTRUCCIÓN CON CAMBIOS

"Decenio de la igualdad de oportunidades para mujeres y hombres"
"Año del Bicentenario del Perú: 200 años de Independencia"

FORMATO DE ACCESO AL CENTRO DE DATOS DE LA ARCC

Datos Personales:

NOMBRES: _____

APELLIDOS: _____

CORREO: _____

DNI ☐ PASAPORTE ☐ CE ☐ N° _____

ENTIDAD ☐ EMPRESA ☐ NOMBRE: _____

FECHA: _____

Acciones a realizar: _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____ _____

FIRMA DEL SOLICITANTE FIRMA DE LA ENTIDA / EMPRESA

ANEXO 9: PROCEDIMIENTO PARA EL REPORTE DE INCIDENCIAS.

1.- El usuario envía correo a soporte@rcc.gob.pe detallando la incidencia o requerimiento (debe detallar si esta de forma presencial o remota, facilitando número de celular)

2.- Se registra solicitud en el sistema de mesa de ayuda GLPi (acrónimo: en francés, Gestionnaire Libre de Parc Informatique).

3.- El encargado del Sistema de Mesa de Ayuda GLPi, asigna al responsable del área de Soporte Técnico que atenderá dicha incidencia reportada.

4.- El técnico se comunica con el usuario y procede a dar la atención a lo solicitado en el registro del correo (de acuerdo a la complejidad de la incidencia reportada se registra como se encuentra la atención).

5.- Después de culminar la atención el técnico procede a cerrar el ticket indicando que la incidencia o requerimiento fue atendido satisfactoriamente.

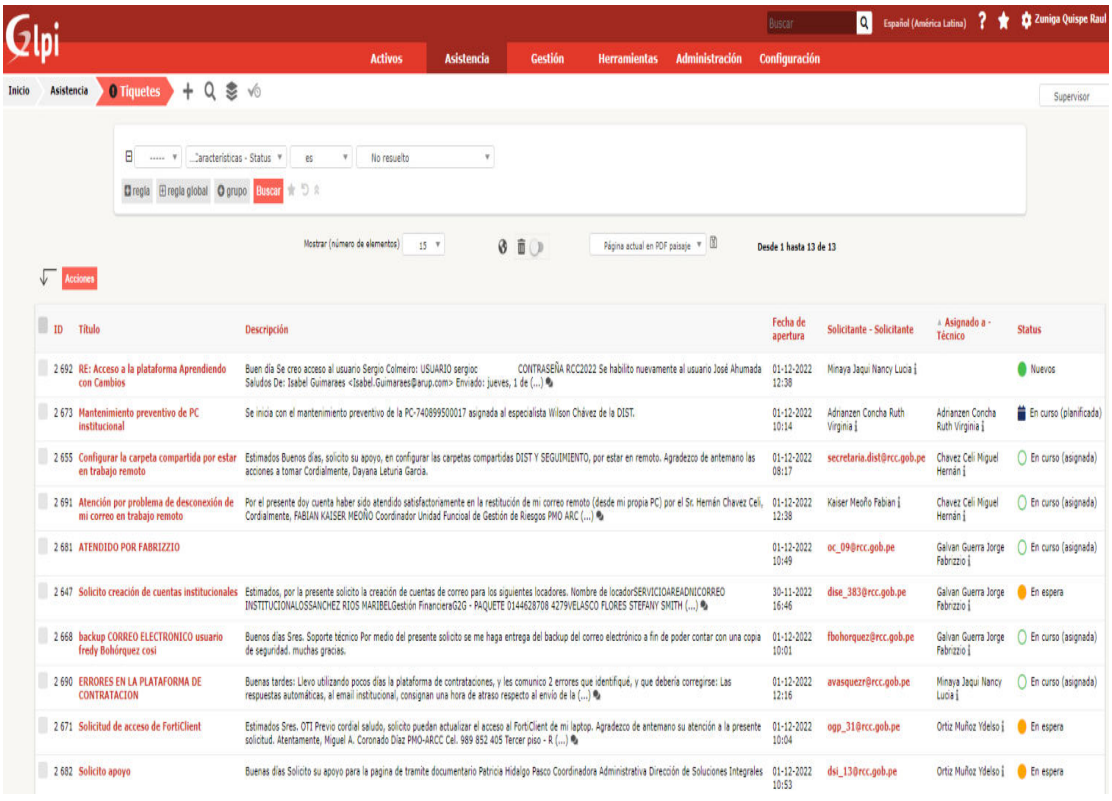


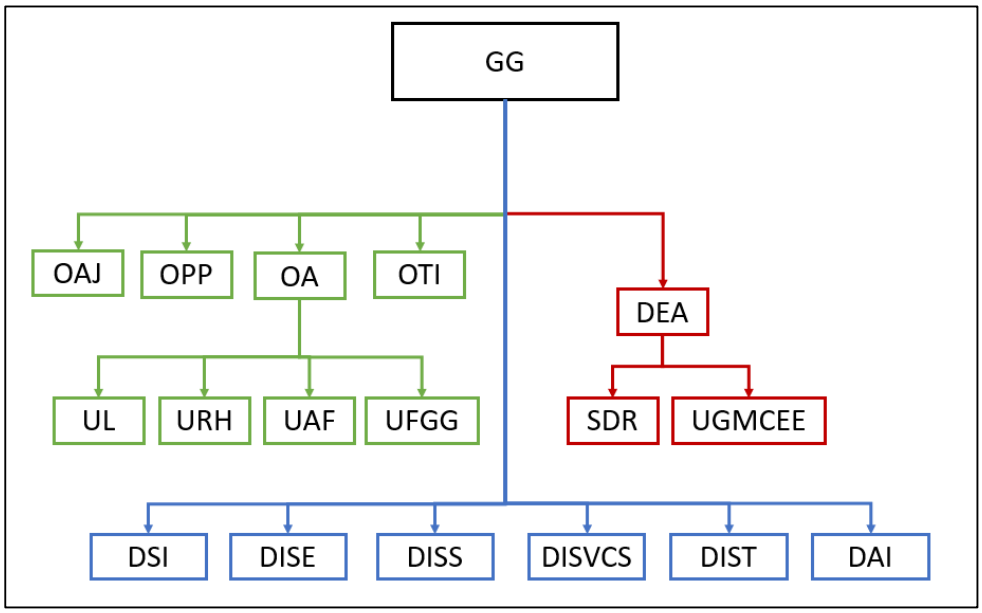
Imagen del Sistema de mesa de ayuda.

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Fortalecimiento de la Soberanía Nacional"
"Año del Bicentenario del Congreso de la República del Perú"

ANEXO 10: PERFILES DE OTIC DE LA ARCC

N°	PERFILES DE LA OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN	PERFILES FALTANTES
1	ANALISTA DE SISTEMAS DE INFORMACIÓN	X
2	ANALISTA I DE MESA DE AYUDA Y SOPORTE TÉCNICO	X
3	ANALISTA I EN SISTEMA DE GESTIÓN DE CALIDAD DE TECNOLOGÍA DE LA INFORMACIÓN	
4	ESPECIALISTA II DE INFRAESTRUCTURA TECNOLOGICA	
5	ESPECIALISTA II EN PROYECTOS TECNOLOGICOS	
6	ANALISTA I PROGRAMADOR DE SISTEMAS DE INFORMACION	X
7	ANALISTA I DE SOPORTE TÉCNICO	x
8	ANALISTA I DE SOPORTE TÉCNICO	x
9	ANALISTA I DE SOPORTE TÉCNICO	
10	ANALISTA I DE SOPORTE TÉCNICO	
11	ANALISTA I DE SOPORTE TÉCNICO	
12	JEFE DE LA OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN	
13	ANALISTA II EN SEGURIDAD INFORMÁTICA	
14	ANALISTA II DE SOPORTE TÉCNICO	
15	ANALISTA II DE SOPORTE TÉCNICO	
16	CONTRATACIÓN ADMINISTRATIVA DE SERVICIOS DE UN ESPECIALISTA II EN SEGUIMIENTO Y MONITOREO DE APLICATIVOS SEDE LIMA	
17	CONTRATACIÓN ADMINISTRATIVA DE SERVICIOS DE UN ESPECIALISTA II EN SISTEMAS DE LA INFORMACIÓN SEDE LIMA	
18	CONTRATACIÓN ADMINISTRATIVA DE SERVICIOS DE UN ANALISTA III EN BASE DE DATOS SEDE LIMA	
19	CONTRATACIÓN ADMINISTRATIVA DE SERVICIOS DE UN ANALISTA III	

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



Elaboración propia

Anexo 3: Directorio

Integrantes	Nombres y Apellidos	Cargo	Celular	Correo
Titular de la UO	Angelo Alexis Lindo Cardenas	Gerente General	947436479	alindo@rcc.gob.pe
Representante de la UO	Martin Jose Valverde Morante	Asesor III	999437982	mvalverde@rcc.gob.pe
DSI	Cesar Nelson Rafael Cusma	Especialista en Evaluación de Proyectos	914467922	crafael@rcc.gob.pe
DISE	Lister Darío Perales Sánchez	Gerente de evaluación (e) - DISE	998730454	lperales@rcc.gob.pe
DISS	Vilca Ferrer Waldir Richard	Coordinador de Estudios	955483931	wvilca@rcc.gob.pe
DISVCS	Sylvia Huari Gonzáles	Coordinadora de Inversión	993612642	shuari@rcc.gob.pe
DIST	Irene Castro Lostaunau	Asesora	943942952	icastro@rcc.gob.pe
DAI	Luis Carlos Gutierrez Ramos	Especialista I en Inversiones	997213477	lgutierrez@rcc.gob.pe
UGMCE	Gladys Salas Marcelo	Analista II Administrativo	948061259	gsalas@rcc.gob.pe
DEA	Salinas Quintana Luis Francisco	Experto en inversiones	949337999	lsalinas@rcc.gob.pe
OA	Mauro Rojas Vela	Jefe de la Oficina de Administración	998091196	mrojas@rcc.gob.pe
URH	Iván Eduardo Goytizolo Villanueva	Analista III en Seguridad	949369301	igoytizolo@rcc.gob.pe
OTI	Nils Joans Zegarra Castillo	Especialista II en seguimiento	948547450	nzegarra@rcc.gob.pe

Elaboración propia.

Anexo 4: Organización para el desarrollo de las actividades criticas

N°	Miembros	Órgano	Responsabilidades
1	Alta Dirección	DE	Asegurar los recursos para la implementación de la PCO.
		GG	Activar el PCO ante una situación de crisis operativa o ante cualquier evento que afecte seriamente las instalaciones de la entidad.
			Aprobar las actividades de ajuste del plan
			Liderar las pruebas y simulacros y revisar los resultados obtenidos.
2	Órganos de Asesoramiento	OPP	Coordinar ejecutar y supervisar la gestión de los recursos presupuestales asignados al pliego.
			Conducir, coordinar y supervisar la programación, formulación, seguimiento y evaluación del Sistema Nacional de Presupuesto en el pliego, en concordancia con las leyes y disposiciones vigentes sobre la materia.
			Establecer las modificaciones del presupuesto para responder a las necesidades de la crisis operativa.
		OAJ	Asesorar a la Alta Dirección y los Órganos del MINDEF sobre asuntos jurídicos relacionados con las competencias del sector, debiendo ser necesario, contar previamente con los informes técnicos elaborados por el órgano o entidad correspondiente.
			Proyectar y visar los dispositivos legales que expida la Alta Dirección de la entidad.
3	Órganos de Apoyo	OA	Formular, coordinar, ejecutar y supervisar la política de recursos humanos, materiales, presupuestales, previsionales y de gestión administrativa.
			Supervisar la atención de las necesidades de recursos materiales y servicios de los órganos del Ministerio, en forma racional, eficiente y oportuna, con la finalidad de coadyuvar al cumplimiento de sus metas.
			Coordinar la seguridad de las informaciones e instalaciones, así como la protección de los funcionarios.
			Planificar y supervisar el mantenimiento preventivo y correctivo de los bienes inmuebles, actualizando sus registros contables y Patrimoniales del Ministerio; así como, consolidar y controlar la información de bienes inmuebles.
		OTI	Supervisar y coordinar las telecomunicaciones, así como los sistemas informáticos y estadísticos.
			Monitorear las amenazas de ciberseguridad, mediante el uso de los sistemas preventivos y defensivos.
			Resguardar la información para su disponibilidad, integridad y confidencialidad.
			Administrar los recursos informáticos, así como el servicio de tecnología de la información.
			Realizar el inventario de los activos informáticos.
			Activar el Plan de Recuperación de los servicios informáticos.
			Coordinar el soporte técnico correspondiente a los usuarios que lo soliciten.

Elaboración: propia.

Anexo 5: Sistema de Comunicaciones de emergencia

1. Introducción

   Ante la ocurrencia de una catástrofe de gran magnitud, los canales normales de comunicaciones serian afectados por la falta de energía eléctrica, por la destrucción física de los elementos que los conforman o por la saturación producto de la desesperación de comunicarse con los familiares haciendo necesario prever otras formas de comunicación, a fin de asegurar el flujo de información entre los diversos órganos de la ARCC.

2. Objeto

   Regular los procedimientos para la implementación y operación de los sistemas de comunicaciones durante los procesos de preparación, respuesta y rehabilitación a las emergencias o desastres; a fin de brindar el flujo rápido y ordenado de las informaciones y comunicaciones de los órganos de la ARCC.

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 órganos de la ARCC.

   b. Los Sistemas de Comunicaciones de Emergencia (Canales Secundarios): Radio Comunicaciones y Comunicaciones Satelitales.

4. Sistema de Comunicaciones

   Los Sistemas de Comunicaciones están compuestos por 3 elementos básicos:

   a. Redes de Comunicaciones.

      Canales Primarios:

      - Telefonía Fija.
      - Telefonía Celular.
      - Internet Convencional Fija.
      - Internet Convencional Móvil.

      Canales Secundarios:

      - Telefonía Satelital.
      - Internet Satelital VSAT.
      - Internet Satelital BGAN.

   b. Personal de Comunicaciones.

      Los Módulos de Comunicaciones de la OTI de la ARCC dispondrán de personal capacitado 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 comunicaciones a fin de entrenarse en el empleo de los equipos y procedimientos.

c. Procedimientos Operativos Estándar.

- Implementación de los Sistemas de Comunicaciones.
  Es responsabilidad de la OTI, gestionar e implementar los Sistemas de Comunicaciones (Redes, Personal y Procedimientos) de la ARCC.

- Sistemas de Comunicaciones Alternos.
  Como norma general y en cuanto sea posible, los sistemas de comunicaciones del ARCC estarán sustentados sobre la base de los canales de comunicaciones normales con equipos propios de cada entidad y a falta de estos se recurrirá al empleo de los sistemas de comunicaciones de las Instituciones Públicas según sea el caso y a falta o saturación de estos sistemas, se recurrirá al empleo de los recursos materiales y humanos de las instituciones privadas y los operadores de servicio de comunicaciones.

- Turnos de Atención de las Redes.
  Las comunicaciones de la ARCC 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.

- Pruebas del Sistema de Comunicaciones.
  A fin de verificar la operatividad de las Redes de Comunicaciones, disponibilidad del Personal de Operadores y el correcto empleo de los Procedimientos Operativos Estándar, se realizarán pruebas de los Sistemas de Comunicaciones.

Anexo 6: Cronograma de implementación de la Gestión de la Continuidad Operativa

N°	Componentes de Gestión	Actividad	Frecuencia	Responsable
1	Elaborar o actualizar los planes de emergencia o contingencia de las sedes regionales y sede central	Informe	Anual	OA
2	Evaluación del grado de conocimiento sobre la gestión de continuidad.	Encuestas	Junio y Noviembre	GG
3	Desarrollo y mejora de la cultura de continuidad.	Mailing	Mensual	OC
4	Monitoreo permanente de las condiciones tecnológicas	Inspección	Trimestral	OA y OTI