PERÚ | Ministerio del Interior | Superintendencia Nacional de Migraciones

PLAN DE RECUPERACIÓN DE SERVICIOS DE TECNOLOGÍA DE LA INFORMACIÓN DEL PROCESO DE EMISIÓN DE PASAPORTE ELECTRÓNICO DE LA SUPERINTENDENCIA NACIONAL DE MIGRACIONES

MIGRACIONES Superintendencia Nacional PERÚ FIRMA DIGITAL

Firmado digitalmente por TAIPE DOMINGUEZ Daniel Ivan FAU 20551239692 hard
Motivo: Doy V° B°
Fecha: 13.02.2021 18:21:39 -05:00

MIGRACIONES Superintendencia Nacional PERÚ

MIGRACIONES Superintendencia Nacional PERÚ FIRMA DIGITAL

Firmado digitalmente por TORRES SALAS Maria Martina Cira FAU 20551239692 soft
Motivo: Doy V° B°
Fecha: 13.02.2021 19:45:30 -05:00

MIGRACIONES Superintendencia Nacional PERÚ FIRMA DIGITAL

Firmado digitalmente por PORTOCARRERO PEÑAFIEL Sandra Lucy FAU 20551239692 hard
Motivo: Doy V° B°
Fecha: 13.02.2021 20:10:38 -05:00

OFICINA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES - OTIC

ENERO 2021

CONTENIDO

1. ALCANCE

El presente plan tiene como alcance el Centro de Datos Principal ubicado en las instalaciones que tiene el Proveedor del Servicio de Housing y el Centro de Datos Contingencia ubicado en la Sede Central Breña (primer piso), relacionados al proceso de Emisión de Pasaporte Electrónico de la Superintendencia Nacional de Migraciones.
Es importante precisar que, el Proceso de Emisión de Pasaportes Electrónico cuenta con diferentes Servicios de Tecnología de Información, infraestructura tecnológica y sistemas que residen en los centros de datos mencionados con recursos centralizados y que comparten de manera transversal, tanto los sistemas, equipamiento de plataforma tecnológica, comunicaciones y seguridad.
Este plan brinda las pautas para restablecer los servicios críticos, de esta manera, garantizar la continuidad de las operaciones ante un evento repentino y de emergencia que ocasionen la no disponibilidad.

2. BASE LEGAL

El desarrollo del Plan de Recuperación de Servicios de Tecnología de Información del proceso de Emisión de Pasaporte Electrónico tiene como marco de referencia la siguiente normativa:

- Resolución Ministerial N° 000028-2015-PCM, que aprueba los Lineamientos para la Gestión de la Continuidad Operativa de las entidades públicas en los tres niveles de Gobierno.
- Resolución Ministerial Nº 0188-2015-PCM, que aprueba los Lineamientos para la Formulación y Aprobación de Planes de Contingencia.
- Resolución Ministerial N° 004-2016-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014. Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de Seguridad de la Información. Requisitos. 2ª Edición”.
- Resolución de Contraloría N° 320-2006-CG, que aprueban las Normas de Control Interno.

3. LINEAMIENTOS CON PEI Y POI

El Plan de Recuperación de Servicios de Tecnología de Información del proceso de Emisión de Pasaporte Electrónico está comprendido en el Plan Operativo Institucional - POI 2021 aprobado con Resolución de Superintendencia Nº 000264-2020-MIGRACIONES, con la actividad operativa: “Brindar el servicio de mantenimiento y operatividad del equipamiento informático, comunicaciones y centro de datos de la entidad” y contribuye al desarrollo de la acción estratégica institucional AEI.04.02 “Infraestructura tecnológica moderna con mayores capacidades para la entidad” y cumplimiento de objetivo estratégico institucional OEI.04 “Fortalecer la gestión y transformación digital en la entidad” del Plan Estratégico Institucional 2020-2024 Modificado de MIGRACIONES.

4. PROBLEMÁTICA Y JUSTIFICACIÓN.

Ante la falla no intencional y/o intencional en el Centro de Datos Principal y frente a la criticidad de los servicios de pasaporte electrónico es necesario definir procedimientos, tareas y responsabilidades para mantener la continuidad de los servicios mediante el Centro de Datos Contingencia. En este sentido, es importante determinar los escenarios de riesgo y definir un plan de continuidad que encamine a conseguir la restauración progresiva de los servicios, mitigar el impacto en la operación evitando la paralización parcial o total de la capacidad operativa que afecten en lo económico y en la imagen institucional de la entidad.

Se ha considerado disponer del Plan de Recuperación de Servicios de Tecnología de Información del proceso de Emisión de Pasaporte Electrónico debido a que la

infraestructura tecnológica y el tiempo de recuperación (RTO) son diferentes a los demás procesos de la Superintendencia Nacional de Migraciones, considerando que dicho proceso cuenta con el Sistema de Gestión de Seguridad de la Información Certificado.

Cabe indicar que el presente plan será ejecutado con los recursos asignados a la Oficina de Tecnologías de las Información y Comunicaciones – OTIC, previa autorización por la Dirección de Operaciones y validación de las pruebas funcionales.

5. OBJETIVOS

5.1 Objetivo General

Establecer los lineamientos para restablecer los Servicios de Tecnología de Información, para el sistema de Emisión de Pasaporte Electrónico de la Superintendencia Nacional de Migraciones.

5.2 Objetivos Específicos

- Establecer los escenarios de riesgo.
- Determinar el Análisis de Impacto de Negocio - Tecnologías de Información de la Superintendencia Nacional de Migraciones en el proceso de la Emisión de Pasaporte Electrónico.
- Establecer la cadena funcional de mando para el restablecimiento de los Servicios de TI del Proceso de Emisión de Pasaporte Electrónico, a través del protocolo para la continuidad de los servicios.

6. PLANIFICACIÓN DE LAS ACTIVIDADES PREVIAS, DURANTE Y POST A LA EJECUCIÓN DEL PLAN DE CONTINGENCIA.

El presente plan establece un conjunto de actividades a realizarse durante la ejecución de las pruebas de Recuperación de Servicios de Tecnología de Información, de acuerdo a los procedimientos que se establecen en el “ANEXO N°01: DETERMINACIÓN DE ESCENARIOS DE RIESGO – C. FASE DE PRUEBA”.

Los recursos y responsables se definen en cada una de las fases de prevención, pruebas, corrección y recuperación.

7. SEGUIMIENTO:

La Unidad de Plataforma y Seguridad Tecnológica de la Oficina de Tecnologías de las Información y Comunicaciones – OTIC estará encargada de la revisión del presente plan de manera anual o cada vez que cambie la determinación de los escenarios de riesgo y el informe de seguimiento será remitido a la jefatura de la OTIC con la recomendación de elevar copia a la Oficina de Planeamiento y Presupuesto - OPP.

8. ANEXOS:

ANEXO N°01: DETERMINACIÓN DE ESCENARIOS DE RIESGO.
ANEXO N°02: PROTOCOLO PARA LA CONTINUIDAD DE LOS SERVICIOS.
ANEXO N°03: INFORME ANÁLISIS DE IMPACTO DE NEGOCIO - TECNOLOGÍAS DE INFORMACIÓN DE SUPERINTENDENCIA NACIONAL DE MIGRACIONES.
ANEXO N°04: ABREVIACIONES.

ANEXO N°01: DETERMINACIÓN DE ESCENARIOS DE RIESGO

Los escenarios identificados abarcan la infraestructura y los servicios tecnológicos alojados en el Centro de Datos Principal con el Proveedor del Servicio de Housing y en el Centro de Datos de Contingencia en la Sede Central de Breña (primer piso).

Por lo tanto, se han identificado los siguientes tipos de escenarios cuyo impacto afectaría los servicios de TI en su totalidad y en situaciones puntuales para tomar acciones y respuesta de contingencia según corresponda. A continuación, los escenarios identificados en función a la mayor probabilidad de ocurrencia e impacto:

Escenario N° 01:

Destrucción / Indisponibilidad del Centro de Datos Principal

El Proceso de Emisión de Pasaporte Electrónico está alojado en el Centro de Datos Principal en las instalaciones que tiene el Proveedor del Servicio de Housing, certificado en TIER III Diseño (Uptime Institute) e ISO 27001 con altos estándares de climatización, energía, seguridad, sistemas contra incendios y monitoreo, teniendo una redundancia funcional técnica al Centro de Datos de Contingencia, en casos de problemas críticos no superables.

La indisponibilidad del Centro de Datos Principal, se ha determinado como un escenario crítico debido a la criticidad e importancia de la infraestructura tecnológica, servicios de tecnología de información y las aplicaciones que estas contiene, considerando como amenazas: terremoto devastador, inundación, atentado terrorista e intento de boicot con el uso de bombas; situaciones no controlables de un Centro de Datos con certificación TIER III y sin tiempo estimados de solución, los cuales son descritos como amenazas de mayor impacto que puedan afectar a la institución, procediendo a ejecutar el Plan de Recuperación de Servicios de TI del proceso de Emisión de Pasaporte Electrónico.

Falla de servidores críticos

Se ha determinado también la posibilidad de presentarse fallas de hardware en los servidores donde se alojan las aplicaciones y las bases de datos críticas del Proceso de Emisión de Pasaporte Electrónico, entre las que podemos enumerar:

- Servidores no disponibles, es decir, no se puede tener acceso a aplicaciones interconectadas.
- Falla de discos duros, fuentes o partes del servidor en general, por causas de deterioro o mala manipulación.
- Falla de su conexión a red, por inadecuado cableado en el centro de Datos.
- Falla en la unidad de almacenamiento.
- Corrupción de data.
- Obsolescencia tecnológica y falta de renovación de equipos.
- Falla por errores humanos.

Ataques por Hackers.

Un ataque perpetrado por Hackers a la infraestructura tecnológica, podría afectar la disponibilidad, confidencialidad e integridad de los activos de la Institución.

A continuación, se listan algunos escenarios locales que la Oficina de Tecnologías de Información y Comunicaciones - OTIC podría enfrentar:

- Indisponibilidad de la plataforma virtual que contiene los Servicios Críticos de Tecnología de Información.

- Indisponibilidad de Base de Datos que contiene los Servicios críticos de Tecnología de Información.
- Indisponibilidad del servicio de enlaces de comunicaciones.
- Indisponibilidad por falla de los equipos de comunicaciones o seguridad.
- Ataque por Ransomware.
- Ataque externo por Hackers.
- Falta o corte de fluido eléctrico.
- Sabotaje interno.
- Error involuntario o desconocimiento del usuario

Escenario N° 02:

Equipos de comunicaciones críticos

Dentro de las posibles fallas de equipos de comunicaciones como routers, switches, cableado se considera:

- Fallas por falta de mantenimiento preventivo.
- Falla en el Hardware o Software de los equipos de comunicaciones o seguridad.
- Falla de su conexión a red, por inadecuado cableado en el centro de Datos.
- Fallas por deterioro o tiempo de uso del equipo.
- Obsolescencia tecnológica y renovación de equipos.

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

Enlaces de interconexión entre las sedes remotas y la Sede Central críticos

Entre las posibles causas tenemos:

- Indisponibilidad del servicio de Internet.
- Indisponibilidad de los enlaces de comunicaciones que interconectan las sedes u oficinas descentralizadas con la Sede Central.
- Incidentes ocurridos en el proveedor que afecta el servicio a la Institución.
- Demora en el tiempo de respuesta por el proveedor ante fallas en el servicio.
- Deterioro de equipos de comunicaciones.

Consideramos como críticos los enlaces que permite la interoperabilidad con RENIEC, la Policía Nacional del Perú, Banco de la Nación y las Jefaturas Zonales en todo el país.

ANEXO N°02: PROTOCOLO PARA LA CONTINUIDAD DE LOS SERVICIOS DE TECNOLOGÍAS DE LAS INFORMACIÓN EN EL PROCESO DE EMISIÓN DE PASAPORTE ELECTRÓNICO.

Al producirse una indisponibilidad severa, la continuidad de los servicios, se basa en las políticas de recuperación progresiva que se detallan a continuación.

1. POLÍTICAS DE RECUPERACIÓN DE TECNOLOGÍAS DE INFORMACIÓN.

Las Políticas que rigen el marco a través del cual se desarrollará y ejecutará lo indicado en el Plan de Recuperación de Servicios de TI del proceso de Emisión de Pasaporte Electrónico frente una indisponibilidad, son:

a. Se ejecutará únicamente en última instancia si el centro de datos principal tiene un problema físico, hay un problema crítico no superable en un componente crítico y/o cuando una indisponibilidad severa y por tiempo prolongado afecte negativamente los servicios de Tecnología de Información y como consecuencia afecta la continuidad operativa del Proceso de Emisión de Pasaporte Electrónico.

b. Se ejecuta ante una situación o Incidente Severo de los sistemas informáticos críticos en el Centro de Datos principal.

c. Se conforma una Estructura Organizacional en la Oficina de Tecnologías de Información y Comunicaciones - OTIC, que será conformado por un Líder de Recuperación de las tecnologías de Información y Equipos de Recuperación conformado por personal de Infraestructura de Tecnología de Información.

d. La ejecución es realizada y ejecutada íntegramente por los miembros de cada Equipo de Recuperación, en caso lo requiera se pedirá apoyo a los proveedores de las plataformas y/o servicios tecnológicos previamente identificados.

e. La documentación de la Fase de Ejecución y Recuperación de Servicios de Tecnologías de la Información es un documento dinámico por lo tanto se debe mantener actualizado y vigente, definiendo al responsable de esta función, la desatención de esta función llevará a tener un documento que no asegura la recuperación de los servicios de Tecnología de Información en una situación de contingencia.

f. Los Equipos de Recuperación responsables deberán cumplir estrictamente un programa de pruebas anual indicado en el Plan de Recuperación de Servicios de TI del proceso de Emisión de Pasaporte Electrónico, con la finalidad de identificar desviaciones u observaciones, así mismo las pruebas buscan familiarizar a los Equipos de Recuperación de Tecnología de Información con la ejecución de estos documentos.

g. La estrategia de recuperación permitirá al Proceso de Emisión de Pasaporte Eléctrico recuperar dentro de la ventana de tiempo de recuperación definida por las operaciones de la institución, minimizando el impacto del incidente o problema.

2. FASES DEL PLAN DE CONTINGENCIA Y RECUPERACIÓN ANTE FALLOS DE SERVICIOS DE TECNOLOGÍA DE LA INFORMACIÓN EN EL PROCESO DE EMISIÓN DE PASAPORTE ELECTRÓNICO.

Con la finalidad de asegurar la continuidad de los servicios ante interrupciones fuera de las condiciones normales de operación sobre los servicios tecnológicos y minimizar el impacto en el menor tiempo posible de las operaciones de la Oficina de Tecnologías de Información y Comunicaciones - OTIC se han considerado las siguientes fases:

A. Fase de Prevención (correcciones y mejoras)
B. Fase de Ejecución y Recuperación
C. Fase de Pruebas

Tabla 1 Fases del Plan de Recuperación de Servicios de TI del proceso de Emisión de Pasaporte Electrónico ante los escenarios identificados previamente.

FASES	DESCRIPCIÓN
Fase de Prevención	Describe las acciones preventivas que se deberá ejecutar para mantener el Plan de Contingencia y Recuperación ante fallos de Servicios de Tecnología de la Información sobre el proceso de "Emisión de Pasaporte Electrónico", producto de los cambios y mejoras con el propósito de disminuir y mitigar las probabilidades de ocurrencia del mismo.
Fase de Ejecución y Recuperación	Describe las acciones y estrategias para restablecer la capacidad de las operaciones y recursos de los Servicios de Tecnología de Información luego de un incidente severo y prolongado que afecte el proceso de "Emisión de Pasaporte Electrónico".
Fase de Pruebas	Documenta las consideraciones y resultados de las pruebas de operación en los "Sistemas de Pasaporte Electrónico".

A continuación, se desarrollan las tres (3) fases mencionadas.

A. FASE DE PREVENCIÓN:

En la fase de prevención se identifican los sistemas informáticos críticos a recuperar, los tiempos de recuperación y descripción de la estrategia de ejecución.

A.1 Gerencias u Oficinas Críticas:

A continuación, se menciona la Unidad orgánica, así como las funciones y/o actividades críticas que realiza:

Tabla 2 Gerencias y/o Oficinas críticas

ÍTEM	DIRECCIÓN /OFICINA	FUNCIÓN/ACTIVIDAD CRÍTICAS
1	Dirección de Operaciones[1]	Expedir y anular Pasaportes Electrónicos

Fuente: Esta información fue obtenida en los talleres de Análisis de Impacto al Negocio – Tecnología de Información con las Unidades Orgánicas de la Institución.

A.2 Sistemas de Informáticos Críticos

En el proceso de Emisión de Pasaporte Electrónico, los Sistemas de Información críticos requieren de estrategias de recuperación que cumplan las expectativas de recuperación de los Procesos críticos.

A continuación, los sistemas de información críticos consolidados y priorizados en criticidad e impacto:

[1]Según el ROF durante la recolección de la información en los talleres del Análisis de Impacto al Negocio corresponde a la Gerencia de Registros Migratorios - Subgerencia de Registros Nacionales.

Tabla 3 Tiempo Objetivo de Recuperación.

Prioridad 1	RTOs estimado a 8 horas.
Prioridad 2	RTOs estimado a 10 horas.
Prioridad 3	RTOs estimado a 15 horas.
Prioridad 4	RTOs estimado a 20 horas.

Tabla 4 Sistemas Críticos con su criticidad e impacto.

ÍTEM	SISTEMA/APP	CRITICIDAD	IMPACTO	CONTINGENCIA
1	Enrolamiento	**1**	No se puede emitir pasaportes.	N/A
2	Entrega	**1**	No se puede emitir pasaportes.	N/A
3	Central	**1**	No se puede emitir pasaportes.	N/A
4	Producción	**1**	No se puede emitir pasaportes.	N/A
5	Control de Calidad	**1**	No se puede emitir pasaportes.	N/A
6	Estación de Impresión	**2**	No se puede emitir pasaportes, en las sedes salvo Breña.	Producir en Breña temporalmente.
7	Estación de Impresión de alto volumen	**2**	No se puede emitir pasaportes.	Producir en otras sedes temporalmente / utilizar otra impresora.
8	Autentificación Identity Guard	**3**	No se puede loguear con huellas a las estaciones de trabajo.	Usar tarjetas de coordenadas (Segundo factor).
9	Pasaporte Bloqueados	**4**	No se puede bloquear pasaportes en línea.	Bloquear con el proceso habitual.
10	Inteligencia de Negocios	**4**	Se tiene acceso a la información de inteligencia de producción.	Ver estadísticas en Central.

Fuente: Información proporcionada por el Consorcio (Proveedor del Sistema de Pasaporte Electrónico)

Tabla 5 Descripción según el nivel de Criticidad.

CRITICIDAD	DESCRIPCIÓN
1	El Sistema no puede emitir Pasaportes Electrónicos.
2	El sistema puede emitir Pasaportes Electrónicos, pero no al 100% de su capacidad normal.
3	El sistema no está afectado en su capacidad a producir Pasaportes Electrónicos, sin embargo, hay un servicio ligeramente degradado.
4	Los procesos son auxiliares del sistema y no afectan en nada la Emisión de Pasaportes Electrónicos.

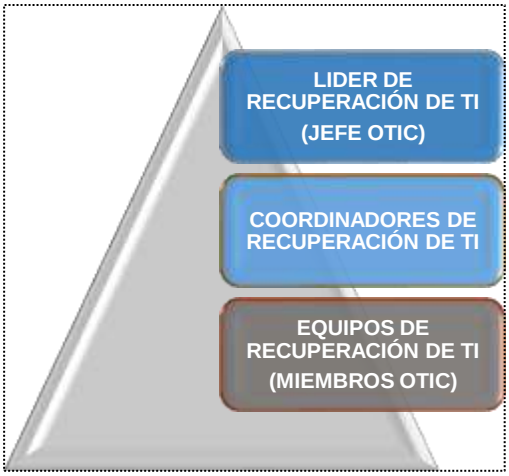
A.3 Organización para la Recuperación de TI

Es responsable de ejecutar actividades correctivas y de recuperación en base a la estrategia de recuperación definida por la Oficina de Tecnologías de Información y Comunicaciones - OTIC, los miembros tomarán acciones y decisiones dependiendo de la situación y tienen como objetivo primordial restablecer la operación normal y toda actividad posterior relativa a la recuperación y minimizar los riesgos e impactos que el evento pudiese causar.

Esta organización se encargará de llevar a cabo la ejecución de lo señalado en la Fase de ejecución y Recuperación con la finalidad de asegurar y cumplir con los tiempos de recuperación de los servicios de Tecnología de Información que la Oficina de Tecnologías de Información y Comunicaciones - OTIC requiere ante un incidente severo.

La estructura organizacional para la recuperación de tecnologías de la información se conforma con los miembros de la Oficina de Tecnologías de Información y Comunicaciones - OTIC, como se muestra en la Figura N°01.

Figura N°01: Estructura Organizacional para la recuperación de Tecnología de Información de MIGRACIONES



La Organización se conformará de un Equipo Técnico de Administración de Crisis de Tecnología de Información y de los Equipos de Recuperación de Tecnologías de Información.
A continuación, la organización del Equipo de Recuperación de Tecnología de Información que se conforma para la recuperación de las operaciones de

Tecnologías de Información que se encuentran afectadas, como se muestra en la Figura N°02.

Figura N°02: Estructura Organizacional de los Equipos de recuperación de la Tecnología de Información de MIGRACIONES

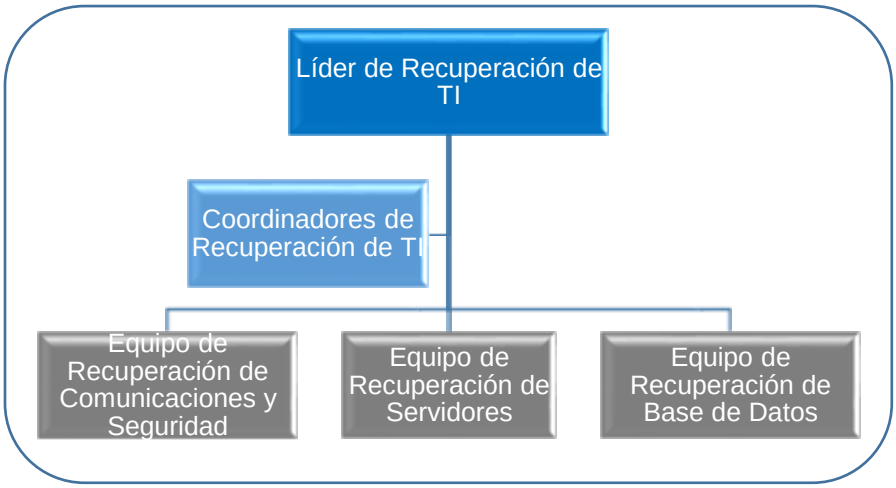


Tabla 6 Equipo Técnico de Recuperación de Tecnología de Información

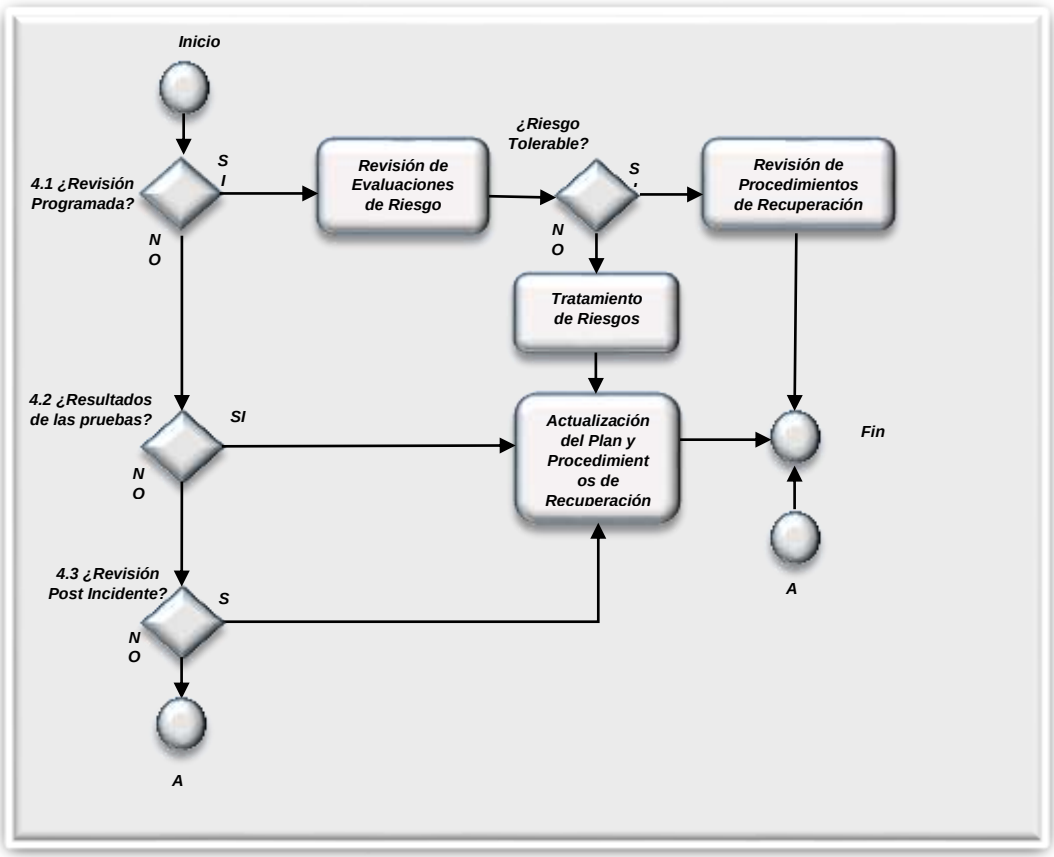
Responsable	Descripción
Líder de Recuperación de Tecnología de Información	• Representado por el jefe de la Oficina de Tecnologías de Información y Comunicaciones - OTIC. • Se encarga de analizar, definir y tomar decisiones ante incidentes disruptivos de los servicios informáticos considerados como críticos por los procesos de negocio. • Dirige las acciones mientras dura el incidente e informa a instancias superiores el desarrollo y resultado final de la recuperación. • Dirige las pruebas de validación de la lista de contactos de los miembros de los equipos de recuperación. • Asegurar la provisión de esquemas de recuperación de los servicios y equipos de Tecnologías de la Información, tales como: ○ Servidores ○ Base de Datos ○ Aplicaciones ○ Comunicaciones y Seguridad. ○ Telecomunicaciones. ○ Servicios ○ Centros de datos.
Coordinadores de Recuperación de Tecnología de Información	• Representado por el jefe de la Unidad de Plataforma y Seguridad Tecnológica – OTIC y el jefe de la Unidad de Soporte Técnico - UST. • Responsable de brindar soporte a la gestión de continuidad operativa de Tecnología de Información. • Coordina con los miembros de los equipos de recuperación las actividades de recuperación y la gestión documentaria.

	• Propiciar las capacitaciones y entrenamientos internos a los distintos equipos de recuperación con respecto a temas de continuidad y recuperación tecnológica.
Equipos de Recuperación de Tecnología de Información	• Representado por los líderes de Comunicaciones y Seguridad (Red de Datos y Telecomunicaciones) y Plataforma (Servidores y Base de Datos), eventualmente el área de Desarrollo actúa como soporte en caso sean requeridos. • Los miembros de los equipos están conformados por todos los especialistas técnicos y analistas de las diferentes áreas. • Los equipos de recuperación de Tecnología de Información, se encargan de la respuesta al incidente y la recuperación de los servicios de Tecnología de Información críticos que se han visto afectados por la interrupción del servicio. • Estos equipos se conforman y operan de acuerdo a las indicaciones del Líder de Recuperación de Tecnología de Información. • Los miembros coordinan directamente con sus Proveedores a través de sus centros de atención y según los procedimientos de escalamiento definido para cada uno de los servicios. **Líder del Equipo de Recuperación de Servidores** • Dirige y coordina la respuesta y recuperación de las plataformas y servicios que soportan los sistemas críticos de la Institución en coordinación con los responsables de comunicaciones y seguridad. • Revisar periódicamente los esquemas de contingencia y disponibilidad de las plataformas de servidores. • Coordinar con proveedores el mantenimiento y soporte en casos de contingencia. • Informa al Líder Recuperación de Tecnología de Información periódicamente el estatus, impacto, actividades y tiempos de recuperación durante un incidente. • Coordinar y supervisar que se cumplan en forma apropiada y completa los procedimientos de respaldo de los sistemas y plataformas tecnológicas. **Líder del Equipo de Recuperación de Base de Datos** • Responsable de asegurar el cumplimiento de la ejecución de los procedimientos de respaldo de las Bases de Datos, configuraciones, esquemas, etc.

	• Participar en las pruebas de Recuperación validando la operatividad de las Bases de Datos críticas de la Institución. **Líder del Equipo de Recuperación de Comunicaciones y Seguridad** • Verificar la disponibilidad y adecuado funcionamiento del equipamiento de comunicaciones y seguridad y coordinar con el Equipo de Servidores los esquemas y/o procedimientos que faciliten la resolución de incidentes. • Coordinar la recuperación de los equipos e infraestructura de comunicaciones y seguridad con el equipo de servidores y el responsable de los Centros de Datos de la Institución. • Coordina con los proveedores de Telecomunicaciones la recuperación de la disponibilidad de los enlaces a nivel nacional. • Validar, probar y resguardar la configuración de los equipos de comunicaciones y de seguridad perimetral.

A.4 Estrategias de Ejecución

A continuación, se muestra el flujo de la estrategia de ejecución de la Oficina de Tecnologías de Información y Comunicaciones - OTIC durante la Fase de Prevención.



A.4.1 Revisión Programada

Este procedimiento se realizará cuando los Coordinadores de Recuperación de Tecnología de Información hallan culminado con la evaluación de los riesgos de Tecnología de Información según el procedimiento E04.OPP.PR.007-Gestión de Riesgos y Oportunidades y necesita coordinar con los responsables/ especialistas de Tecnología de Información la actualización de lo desarrollado en la Fase de Recuperación de Tecnología de Información - Corrección y Recuperación de Servicios de Tecnología de Información, producto de los resultados obtenidos en la evaluación de riesgos y los cambios en las tecnologías.

No.	Rol	Tarea o actividad
1.	Coordinadores de Recuperación de Tecnología de Información	De acuerdo a la frecuencia definida para la revisión programada del Plan de Recuperación de Servicios de TI del proceso de Emisión de Pasaporte Electrónico y sus Procedimientos de Recuperación • Se revisarán los resultados de las evaluaciones de riesgos de Tecnología de Información realizadas. • En caso que los resultados cuyos riesgos no son aceptables y necesita un tratamiento de los riesgos, los Coordinadores de Recuperación de Tecnología de Información definirán y coordinarán con el Especialista de Tecnologías de Información a cargo el tratamiento a los riesgos de acuerdo al procedimiento E04.OPP.PR.007-Gestión de Riesgos y Oportunidades.
2.	Especialista de Tecnologías de Información	Se encarga de definir la estrategia para el tratamiento de riesgos no aceptables. Luego de la definición de la estrategia del tratamiento, definirá el plan de acción o de trabajo para dicha implementación (técnica o procedimental). Luego de la implementación de controles y/o medidas que minimicen el riesgo, se evaluará nuevamente los riesgos para asegurar que estos se encuentran dentro de la zona de riesgos aceptables por la Institución.
3.	Especialista de Tecnologías de Información	Luego de la evaluación de riesgos, se revisa lo desarrollado en la Fase de Ejecución y Recuperación de Servicios de Tecnología de Información y los Procedimientos de Recuperación. Producto del tratamiento de los riesgos, los activos que fueron afectados con la mejora han sufrido cambios que han afectado lo desarrollado en dicha fase o algún procedimiento asociado a su recuperación. El Especialista procederá a actualizar la documentación correspondiente al activo de Tecnología de Información y solicitaran a los Coordinadores de Recuperación de Tecnología de Información la inclusión de este activo en la programación de las pruebas a fin de asegurar que los cambios realizados funcionen con los cambios realizados producto del tratamiento a los riesgos.

4.	Coordinadores de Recuperación de Tecnologías de Información	Revisar y consolidar todos los cambios que han sufrido el Plan de Recuperación de Servicios de TI del proceso de Emisión de Pasaporte Electrónico y sus Procedimientos de Recuperación. Programa las pruebas de los activos afectados por el cambio. Informa al Líder de Recuperación de Tecnología de Información la actualización de los documentos de recuperación y la programación de las pruebas a ejecutar según cronograma. Se cierran las actividades de la Revisión Programada.

A.4.2 Resultados de las Pruebas

Este procedimiento se realizará toda vez que se han ejecutado pruebas del Plan de Recuperación de Servicios de TI del proceso de Emisión de Pasaporte Electrónico y/o sus Procedimientos de Recuperación y se necesita actualizar la documentación respectiva, producto de los cambios.

No.	Rol	Tarea o actividad
1.	Coordinadores de Recuperación de Tecnología de Información	De acuerdo a las pruebas realizadas en base al Plan de Recuperación de Servicios de TI del proceso de Emisión de Pasaporte Electrónico - Fase de Ejecución y Recuperación de Servicios de Tecnología de Información: • Revisará los resultados de las pruebas, incidiendo en las observaciones que se obtuvieron producto de la ejecución de las pruebas. • Definirá y coordinará con el Especialista de Tecnologías de Información a cargo la resolución de las observaciones emitidas en el informe de la prueba.
2.	Especialista de Tecnologías de Información	Resolverá las observaciones emitidas en el informe de las pruebas. Los cuales pueden involucrar la atención de equipos multidisciplinarios y/o proveedores.
3.	Especialista de Tecnologías de Información	Luego de la resolución de las observaciones revisa y actualiza el Plan de Recuperación de Servicios de TI del proceso de Emisión de Pasaporte Electrónico - Fase de Corrección y Recuperación de Servicios de Tecnología de Información y los Procedimientos de Recuperación asociados.
4.	Coordinadores de Recuperación de Tecnología de Información	Revisar y validar con el Especialista la actualización de los documentos de recuperación del Plan. Informa al Líder de Recuperación de Tecnología de Información la actualización de los documentos de recuperación.

		Se cierra las actividades de los resultados de las pruebas.

A.4.3 Revisión después del incidente

Este procedimiento se ejecuta luego que ha culminado y resuelto un incidente en tecnologías de información y que ha afectado los componentes y/o servicios de Tecnología de Información.

No.	Rol	Tarea o actividad
1.	Líder de Recuperación de Tecnología de Información con los Coordinadores de Recuperación de Tecnología de Información	Revisar el impacto en los procesos de la Institución por la indisponibilidad en los servicios de Tecnología de Información. Revisar los resultados de las actividades que recuperaron los servicios de Tecnología de Información y las oportunidades de mejora a implementar.
2.	Líder de Recuperación de Tecnología de Información	Definir y coordinar con el Especialista de Tecnologías de Información a cargo de la solución del incidente en los componentes y/o Servicios de Tecnología de Información afectados.
3.	Especialista de Tecnologías de Información	Revisar los componentes e implementar las mejoras que se identificaron como oportunidades. Puede involucrar la atención de equipos multidisciplinarios y proveedores. Revisar y actualizar el Plan de Recuperación de Servicios de TI del proceso de Emisión de Pasaporte Electrónico y los Procedimientos asociados.
4.	Coordinadores de Recuperación de Tecnología de Información	Revisar y validar con el Especialista la actualización de los documentos sobre las actividades de recuperación del Plan. Informar al Líder de Recuperación de Tecnología de Información la actualización de los documentos sobre las actividades de recuperación. Se cierra las actividades de Revisión después del incidente.

Los Coordinadores de Recuperación de Tecnología de Información deberán programar las actividades de revisión, evaluación de riesgos de Tecnología de Información y de pruebas anualmente, los mismos que serán validados y aprobados por el Líder de Recuperación de Tecnología de Información.

B. FASE DE EJECUCIÓN Y RECUPERACIÓN:

La Fase de Ejecución y Recuperación del Plan de Recuperación de Servicios de TI del proceso de Emisión de Pasaporte Electrónico, tiene como principal propósito evaluar la información y actuar ante un incidente que ocasione la paralización de las tecnologías de información y afecte a la continuidad operativa de los procesos de MIGRACIONES.

La estrategia de recuperación de Tecnologías de Información representa la preparación y la capacidad para restablecer la operatividad y continuidad de los Servicios de Tecnologías de Información ante la indisponibilidad o interrupción severa por un determinado tiempo definido, a través de una estructura organizacional, procedimientos de recuperación, tecnologías, estrategias y centro de datos, permitiendo de esta manera recuperar la operatividad de los servicios tecnológicos y minimizar el impacto en las operaciones de la Oficina de Tecnologías de Información y Comunicaciones - OTIC de la Superintendencia Nacional de Migraciones.

B.1 Comité ante una Crisis de Tecnología de Información

B.1.1 Objetivo

Establecer las actividades a seguir para declarar la situación de crisis y activar el Plan de Recuperación de Servicios de TI del proceso de Emisión de Pasaporte Electrónico de la Superintendencia Nacional de Migraciones a fin mantener la continuidad del proceso de Emisión de Pasaporte Electrónico luego de una interrupción imprevista o una amenaza inminente que conlleve a una interrupción del proceso.

B.1.2 Alcance

El alcance es a nivel Institucional y aplica para los servidores y terceros involucrados en el proceso de Emisión de Pasaporte Electrónico desde la identificación de una interrupción imprevista o una amenaza inminente que conlleve a una interrupción del proceso hasta el regreso a las operaciones al nivel habitual.

B.1.3 Declaración de la Crisis y Activación de la Ejecución del Plan de Recuperación de Servicios de Tecnologías de Información

N°	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	REGISTRO
1.	Recibir la notificación del incidente que afecte de continuidad del proceso de Emisión de Pasaporte Electrónico	Coordinador de Recuperación ante desastres	Correo Electrónico
2.	Analizar, en coordinación con el equipo técnico de recuperación ante desastres, los servicios y la situación en la zona afectada. Nota: Dependiendo del incidente que interrumpa el proceso se deberá coordinar con los responsables de instituciones como INDECI, Municipalidad del sector afectado, Policía Nacional, Cuerpo General de bomberos, entre otros.	Coordinador de Recuperación ante desastres	--
3.	Informar los resultados del análisis al Comité de Crisis	Coordinador de Recuperación ante desastres	Informe

N°	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	REGISTRO
4.	Evaluar, con los responsables de los órganos especializados, el resultado del Análisis efectuado. Si como resultado de la evaluación, el Comité de Crisis decide declarar formalmente la crisis y a autorizar la activación de Plan de Recuperación de Servicios de TI del proceso de Emisión de Pasaporte Electrónico, comunicando a todos los miembros del Comité de Crisis, así se procede a la inmediata instalación del Comité en mención.	Presidente Comité de Crisis	Correo Electrónico
5.	Comunicar al Equipo de Recuperación la autorización para la activación del Plan de Recuperación de Servicios de TI del proceso de Emisión de Pasaporte Electrónico.	Coordinador de Recuperación ante desastres	Correo Electrónico
6.	Reportar periódicamente al Comité de Crisis el avance en la ejecución del Plan de Recuperación de Servicios de TI del proceso de Emisión de Pasaporte Electrónico hasta el retorno a la normal operación del proceso. Nota: Se podrá establecer mecanismos de comunicación que permitan informar en línea al equipo técnico y al comité de crisis, como conferencias o grupos telefónicos, entre otros.	Coordinador de Recuperación ante desastres	Correo Electrónico
7.	Una vez retornadas las operaciones a la normalidad, comunicar la finalización del Plan de Recuperación de Servicios de TI del proceso de Emisión de Pasaporte Electrónico a los miembros del Comité de Crisis.	Coordinador de Recuperación ante desastres	Correo Electrónico

B.1.4 Roles y Responsabilidades

INTEGRANTE	ROL
Gerente General	Presidente
Director de Operaciones	Presidente (alterno)
Superintendente Nacional	Miembro

Jefe de la Unidad de Imagen y Comunicación	Miembro (Coordinador de la comunicación a partes interesadas externas)
Jefe de la Oficina de Tecnologías de Información y Comunicaciones	Miembro (Coordinador de Recuperación ante desastres)
Jefe de la Oficina de Planeamiento y Presupuesto	Miembro
Jefe de la Oficina de Administración y Finanza	Miembro
Jefe la Oficina de Recursos Humanos	Miembro
Jefe de la Oficina de Asesoría Jurídica	Miembro
Jefe de la Oficina de Integridad Institucional	Miembro
Director de Operaciones	Miembro
Director de Política Migratoria	Miembro

Responsabilidades del Comité

- Evaluar si es necesario declarar la crisis en la Institución.
- Activar, de ser necesario, Plan de Recuperación de Servicios de TI del proceso de Emisión de Pasaporte Electrónico.
- Confirmar quién será el Portavoz oficial de la institución durante y después de la crisis.
- Evaluar si es posible retornar a operación normal.
- Verificar la activación del Procedimiento de Comunicación en Crisis.

Presidente / Presidente alterno

- Evaluar, con los responsables de los órganos especializados, el resultado del Análisis efectuado.
- Comunicar el resultado de la evaluación del Comité de Crisis a todos los miembros de dicho Comité.
- Autorizar la activación del Plan de Recuperación de Servicios de TI del proceso de Emisión de Pasaporte Electrónico.

Coordinador de Recuperación ante desastres

- Solicitar al Presidente /Presidente alterno, la autorización para activar el Plan de Recuperación de Servicios de TI del proceso de Emisión de Pasaporte Electrónico.
- Solicitar al Equipo de Recuperación, la ejecución del Plan de Recuperación de Servicios de TI del proceso de Emisión de Pasaporte Electrónico.
- Mantener comunicación con el Comité de Crisis y el equipo técnico de recuperación ante desastres.
- Asegurar la correcta ejecución del Plan de Recuperación de Servicios de TI del proceso de Emisión de Pasaporte Electrónico.
- Evaluar cualquier eventualidad no contemplada durante la crisis presentada, de acuerdo a las disposiciones internas y/o legales que rijan

sobre el particular y con la opinión favorable y asesoría de la Oficina de Asesoría Jurídica.

Coordinador de la comunicación a partes interesadas externas

- Mantener la comunicación con las partes interesadas externas, incluyendo a los usuarios (comunidad en general), de ser necesario.

B.1.5 Matriz RACI

Tabla 6 Roles

Abreviatura	Roles
CDR	Coordinador de Recuperación ante desastres
PCC	Presidente Comité de Crisis
CC	Comité de Crisis
CCIE	Coordinador de la comunicación a partes interesadas externas
LRTI	Líder de Recuperación de TI
CRTI	Coordinadores de Recuperación de TI
ERCS	Equipo de Recuperación de Comunicaciones y Seguridad
ERS	Equipo de Recuperación de Servidores
ERBD	Equipo de Recuperación de Base de Datos

Tabla 7 Matriz RACI

Actividades	CRD /LRTI	PCC	CC	CCIE	CRTI	ERCS	ERS	ERBD
Apertura de incidente crítico	I				I	R	R	R
Junta de crisis	C	R	C					
Decisión final de cambiar al sitio de contingencia (DR)	I	A	R	I	I	I	I	I
Plan con acciones técnicas para failover	A	I	I	I	R	C	C	C
Informar los jefes zonales y el público		C		R				
Failover	A	I	I	I	R	R	R	R
Pruebas de validación	I	I	I	I	R	R	R	R
Investigaciones sobre el sitio principal	I	I	I	I	R	R	R	R
Definir la ventana de mantenimiento para el failback	I	A	R	I	I	I	I	I
Plan con acciones técnicas y recursos para failback	A	I	I	I	R	C	C	C
Informar a las sedes					R			
Failback	C				R	R	R	R
Pruebas de validación					R			
Cierre oficial de incidente	A	I	I	I	C	C	C	C
Análisis de la ejecución del plan	A	I	I	I	R	C	C	C

B.1.6 ESQUEMA DE COMUNICACIÓN

Se han definido los siguientes esquemas de comunicación entre los integrantes de los equipos de recuperación de Tecnología de Información:

Tabla 8 Esquema de Comunicación

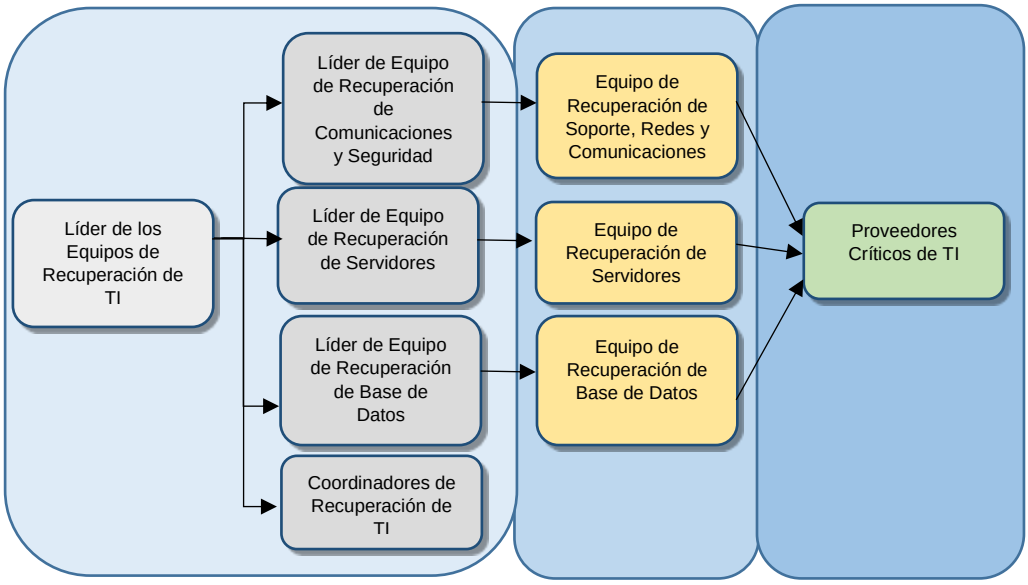
Prioridad	Esquema de comunicación
1	Por llamadas a celular directamente
2	Por chat grupal
3	Por correos electrónicos grupales
4	Por llamadas a teléfonos fijos
5	De manera presencial

Los Coordinadores de Recuperación de Tecnología de Información deberan revisar con una frecuencia anual el esquema de comunicación a fin de mantener la vigencia y actualización de los números celulares, fijos, datos, entre otros.

Árbol de Llamadas

El árbol de llamadas se utilizará para convocar a los Equipos de Recuperación de Tecnología de Información, los líderes de equipos, a sus respectivos equipos de recuperación y a los proveedores de Tecnología de Información en casos sean necesarios utilizando el esquema de comunicación definido por la Oficina de Tecnologías de Información y Comunicaciones - OTIC, como se muestra en la siguiente figura:

Figura N°03: Esquema de Comunicación – Árbol de Llamadas



A continuación, se indica la *lista de contactos* de cada equipo de recuperación de Tecnología de Información.

Equipo de Líderes de los Equipos de Recuperación

Ítem	Rol	Nombre	N° Celular Trabajo
1	Líder de los Equipos de Recuperación de Tecnología de Información	Johny Meregildo Ramos	985022424
2	Líder del Equipo de Recuperación de Comunicaciones y Seguridad	José Carlos Choque Herrera	997490629
3	Líder del Equipo de Recuperación Servidores	Alain Paul Requejo Carrasco	991537757
4	Líder del Equipo de Recuperación de Bases de Datos	Carlos Rodríguez Palacios	977699027
5	Coordinadores de Recuperación de Tecnología de Información	Daniel Iván Taipe Domínguez Javier Aching Acosta	985032866 966353179

Equipo de Recuperación de Comunicaciones y Seguridad

Ítem	Rol	Nombre	N° Celular Trabajo
1	Líder de Equipo de Recuperación de Comunicaciones y Seguridad	José Carlos Choque Herrera	997490629
2	Miembro del Equipo	Deeybe Dávila Villacorta	970593530
3	Miembro del Equipo	Juan Ruiz Rocha	986696504

Equipo de Recuperación de Servidores

Ítem	Rol	Nombre	N° Celular Trabajo
1	Líder de Equipo de Recuperación de Servidores.	Alain Paul Requejo Carrasco	991537757
2	Miembro del Equipo	Jorge Villanueva Loarte	991333830
3	Miembro del Equipo	Ronaldo Soncco Casani	987364583
4	Miembro del Equipo	Reilly Chavez Flores	953256355

Equipo de Recuperación de Bases de Datos

Ítem	Rol	Nombre	N° Celular Trabajo
1	Líder de Equipo de Recuperación de Bases de datos.	Carlos Rodríguez Palacios	977699027
2	Miembro del Equipo	Máximo Rímac Ayala	943412800

B.2 Sistemas de Información Críticos

Los Sistemas de Información Críticos y las prioridades de recuperación requeridos por el área usuaria de MIGRACIONES.

Ítem	Gerencia/Oficina	Función/Actividad Crítica	Sistema/App	Expectativa de Tiempo de Recuperación	Tiempo Máximo Tolerable
1	Dirección de Operaciones[2]	Expedir y anular pasaportes	Sistema de Emisión Descentralizada de Pasaporte Electrónico	En línea	-

Fuente: Esta información fue entregada por las Direcciones/Oficinas en la etapa del Análisis de Impacto al Negocio (BIA – TI)

[2] Según el ROF durante la recolección de la información en los talleres del Análisis de Impacto al Negocio corresponde a la Gerencia de Registros Migratorios - Subgerencia de Registros Nacionales.

A continuación, los sistemas de información críticos consolidados y priorizados en función a los tiempos objetivos de recuperación requeridos por las Gerencias/Oficinas de la Institución:

Prioridad 1	RTOs estimado a 8 horas.
Prioridad 2	RTOs estimado a 10 horas.
Prioridad 3	RTOs estimado a 15 horas.
Prioridad 4	RTOs estimado a 20 horas.

ÍTEM	SISTEMA/APP	CRITICIDAD	IMPACTO	CONTINGENCIA
1	Enrolamiento	**1**	No se puede emitir pasaportes.	N/A
2	Entrega	**1**	No se puede emitir pasaportes.	N/A
3	Central	**1**	No se puede emitir pasaportes.	N/A
4	Producción	**1**	No se puede emitir pasaportes.	N/A
5	Control de Calidad	**1**	No se puede emitir pasaportes.	N/A
6	Estación de Impresión	**2**	No se puede emitir pasaportes, en las sedes salvo Breña.	Producir en Breña temporalmente.
7	Estación de Impresión de alto volumen	**2**	No se puede emitir pasaportes.	Producir en otras sedes temporalmente / utilizar la otra impresora.
8	Autentificación Identity Guard	**3**	No se puede loguear con huellas a las estaciones de trabajo.	Usar tarjetas de coordenadas (Segundo factor).
9	Pasaporte Bloqueados	**4**	No se puede bloquear pasaportes en línea.	Bloquear con el proceso habitual.
10	Inteligencia de Negocios	**4**	Se tiene acceso a la información de inteligencia de producción.	Ver estadísticas en Central.

Ítem	Sistema/Aplicación	Expectativa de Tiempo de Recuperación
1	Sistema de Enrolamiento	En línea
2	Sistema de Entrega	En línea
3	Sistema Central	En línea
4	Sistema de Producción	En línea
5	Estación de Impresión PB500	En línea
6	Estación de Impresión de alto volumen PB6500	En línea
7	Control de Calidad	En línea
8	Pasaporte Bloqueados	En línea
9	Inteligencia de Negocios	En línea
10	Autentificación Identity Guard	En línea

Fuente: Esta información fue entregada por las Direcciones/Oficinas en la etapa del Análisis de Impacto al Negocio (BIA – TI)

B.3 Estrategias de Recuperación De Servicios

A continuación, se detalla las estrategias actuales de recuperación de los servicios de Tecnología de Información en los frentes de comunicaciones y seguridad, servidores y base de datos, tal como se indicó en el numeral “4. DETERMINACIÓN DE ESCENARIOS DE RIESGO”; precisándose que la Oficina de Tecnologías de Información y Comunicaciones - OTIC está solamente preparada a través de las estrategias para eventos locales.

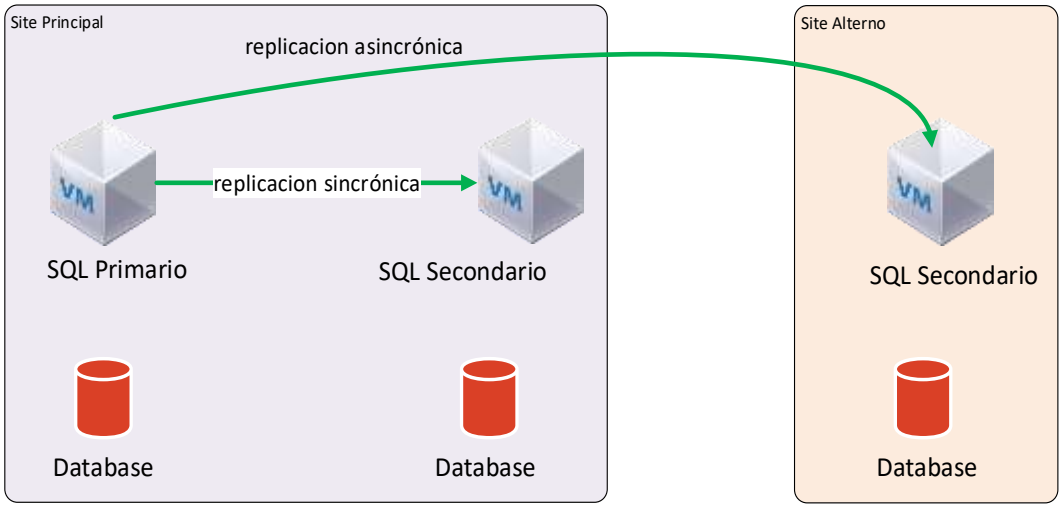
B.3.1 Estrategia de Recuperación ESCENARIO 01

La presente estrategia de recuperación es aplicable para los siguientes escenarios:
1.1 Destrucción / Indisponibilidad del Centro de Datos Principal
1.2 Falla de servidores críticos
1.3 Ataques por Hackers.

A. Clúster Base de Datos SQL

Contamos con 3 clústers SQL, en donde trasladamos los servicios de Centro de Datos Principal al Centro de Datos Contingencia:

SQL Cluster Architecture:



- En el sitio principal, tenemos 2 nodos (replicación síncrona), y un nodo en el Sitio de Contingencia.

Toda aplicación debe utilizar el nombre DNS para comunicarse con la base de datos:

- Base de Datos PM: EPMIGSQLENPM.epmigraciones.gob.pe
- Base de Datos Central: EPMIGSQLCENTRAL.epmigraciones.gob.pe
- Base de Datos BDS: EPMIGSQLBDS.epmigraciones.gob.pe
- Base de Datos Afis: EPMIGSQLAFIS.epmigraciones.gob.pe
- Base de Datos PKI: EPMIGSQLPKI.epmigraciones.gob.pe

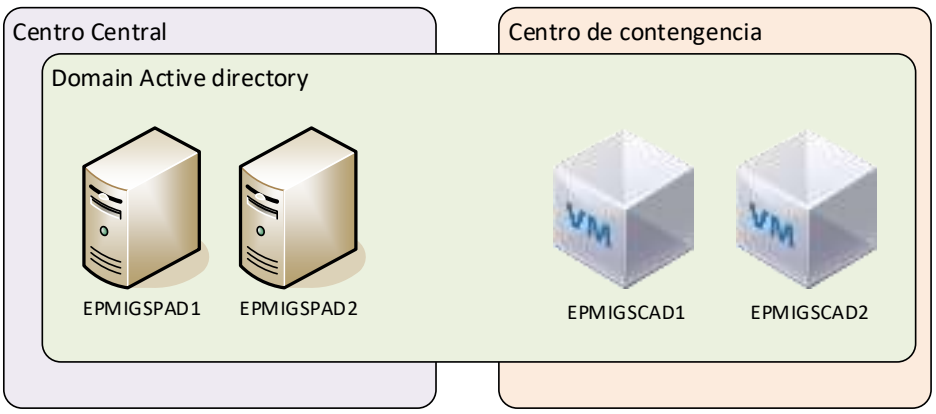
1.1 Servidores AD-DNS

Hay 4 servidores DNS:

- 2 en el sitio principal
- 2 en el sitio de Contingencia

La replicación es automática,

- DNS
- Directorio Activo / Active Directory

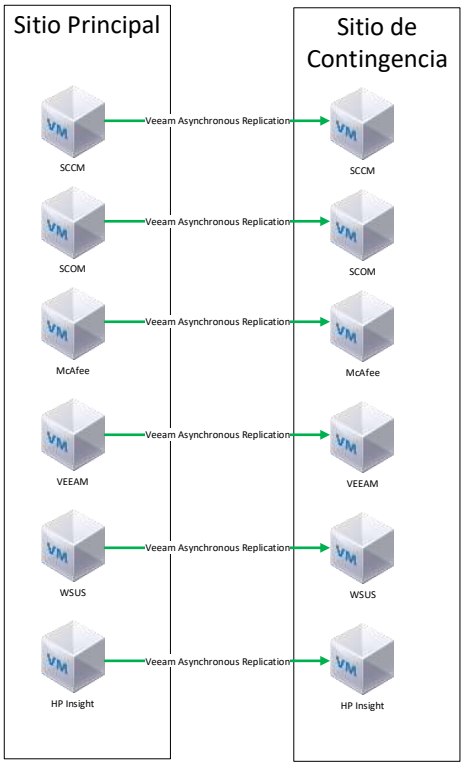


1.2 Servidores de Infraestructura

Todos los servidores de infraestructura son VMs (Máquinas virtuales).
Lista de servidores de infraestructura:

- SCCM (System Center Configuration Manager)

- SCOM (System Center Operation Manager)
- HP Insight (Hardware supervision / Supervisión de hardware)
- McAfee (Antivirus)
- Veeam (Backup)
- WSUS (Windows Server update Services)

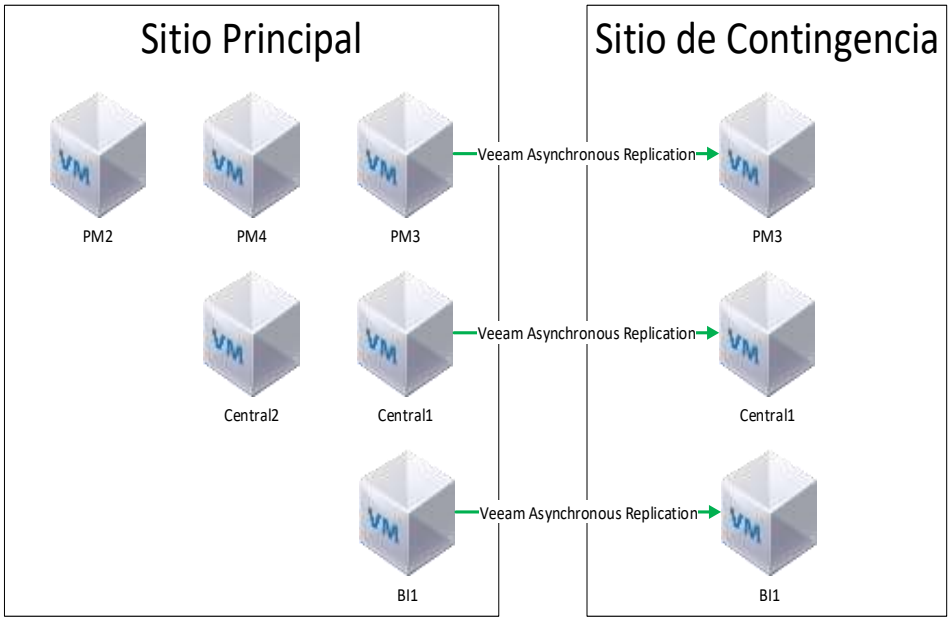


- ✓ Se utiliza el software VEEAM para replicar TODAS las máquinas virtuales en el sitio de Contingencia.
- ✓ Esta replicación es asíncrona.
- ✓ Cuando se reinician las máquinas virtuales (VMs) en el sitio de Contingencia, es con una nueva IP.
- ✓ Este servidor se registra automáticamente en el DNS con la nueva IP.
- ✓ Se usa el DNS para comunicar con cada aplicación.
- ✓ La conmutación por error (failover) es manual.
- ✓ Esas máquinas virtuales (VMs) en el sitio de Contingencia no están disponibles cuando el sitio principal está UP.

1.3 Servidores Principales

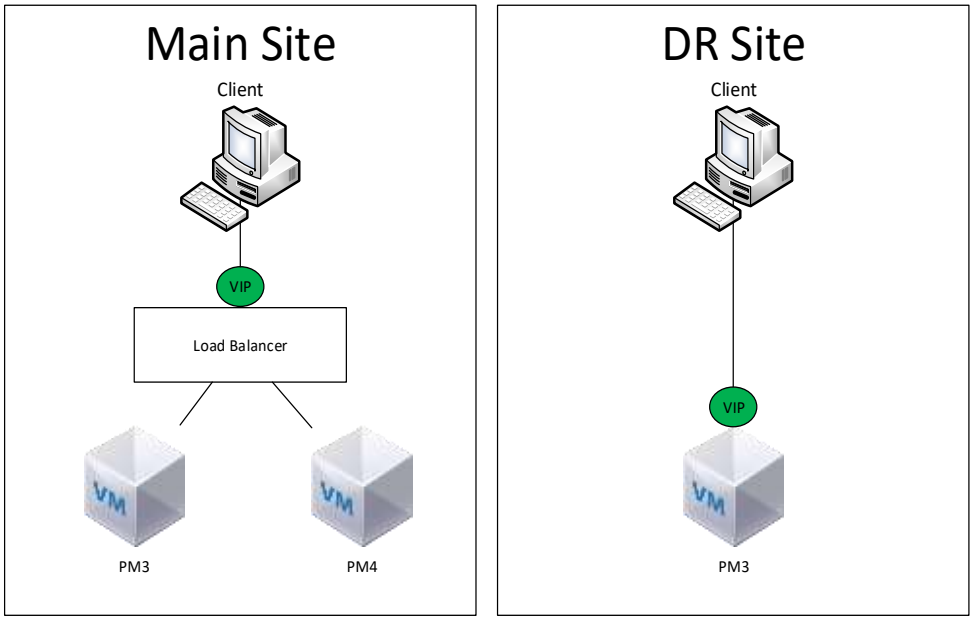
Esos servidores son Máquinas virtuales (VMs).

- PM
  - EPMIGSPPM2.epmigraciones.gob.pe
  - EPMIGSPPM3.epmigraciones.gob.pe
  - EPMIGSPPM4.epmigraciones.gob.pe
- Central
  - EPMIGSPCENTRAL1.epmigraciones.gob.pe
  - EPMIGSPCENTRAL2.epmigraciones.gob.pe
- OPERA
  - EPMIGSPOPERA2.epmigraciones.gob.pe
  - EPMIGSPOPERA3.epmigraciones.gob.pe



- ✓ Se utiliza el software VEEAM para replicar TODAS las máquinas virtuales en el sitio de Contingencia.
- ✓ Esta replicación es asíncrona.
- ✓ Cuando se reinician las máquinas virtuales (VMs) en el sitio de Contingencia, es con una nueva IP.
- ✓ Este servidor se registra automáticamente en el DNS con la nueva IP.
- ✓ Se usa el DNS para comunicar con cada aplicación.
- ✓ La conmutación por error (failover) es manual.
- ✓ Esas máquinas virtuales (VMs) en el sitio de Contingencia no están disponibles cuando el sitio principal está UP.

En el sitio principal existe Alta disponibilidad porque hay un equilibrador de carga (Big-IP de F5), mientras para el sitio de contingencia no se cuenta con una balanceador de carga.



- El equipo cliente envía una solicitud a la dirección IP Virtual (VIP) y el equilibrador de carga envía la solicitud en el EPMIGSPPM3 o EPMIGSPPM4.
- Se utiliza una dirección de DNS para la comunicación con el equilibrador de carga.

  - PM: EPMIGPM.epmigraciones.gob.pe
  - Central: EPMIGCENTRAL.epmigraciones.gob.pe
  - OPERA: EPMIGOPERA.epmigraciones.gob.pe

- Cuando se enciende el sitio de Contingencia, la IP del VIP es el mismo que la del servidor.
- Al poner en marcha el sitio de Contingencia, necesitamos cambiar la IP de DNS para cada IP virtual (VIP).
- El interruptor del DNS no es automático.

B.3.2 Estrategia de Recuperación ESCENARIO 02

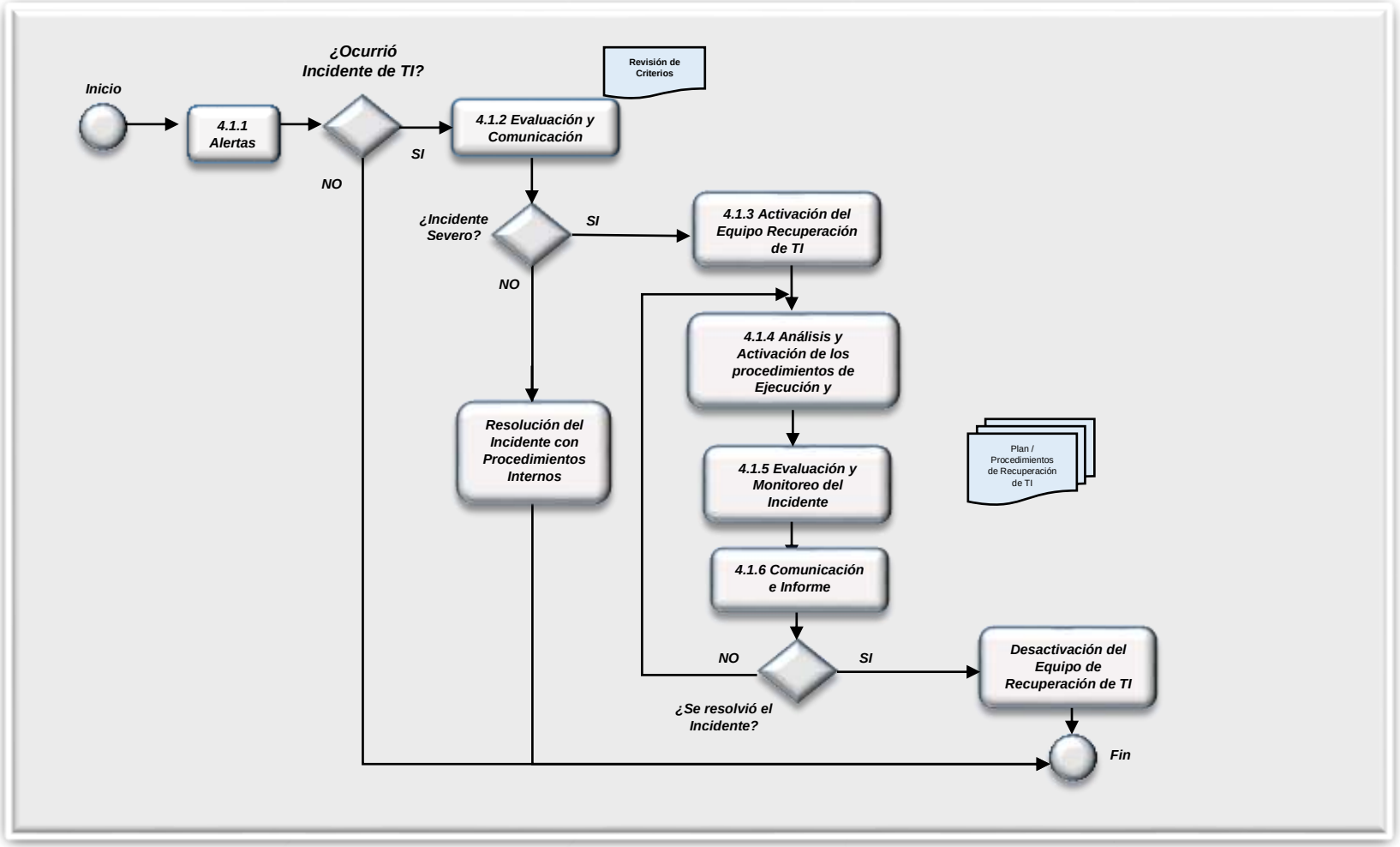
La presente estrategia es aplicable para los siguientes escenarios:
2.1 Equipos de comunicaciones críticos
2.2 Enlaces de interconexión entre las sedes remotas y la Sede Central críticos.

Estrategias actuales de recuperación de Comunicaciones y Seguridad

Servicio TI	*Estrategia*	*Tiempo Rpta.*	*Equipo Respuesta*		*Monitoreo*
			TICE	*Proveedor*	
Enlaces de Comunicaciones	Alta Disponibilidad	Inmediato		□	Ing. Residente (Software de Monitoreo) Especialistas de seguridad y redes. Operadores de Turno (día y noche) Revisiones diarias
Switches Core	Alta Disponibilidad	Inmediato	□	□	
Firewalls	Alta Disponibilidad	Inmediato	□	□	
Balanceadores	Alta Disponibilidad	Inmediato	□	□	
Todos	Respaldo de configuraciones	30 minutos	□		

B.4 Estrategia de Activación De La Recuperación:

A continuación, se muestra el flujo de la estrategia de ejecución y recuperación de las Tecnologías de Información.



B.4.1 Desarrollo de la Estrategia De Recuperación ante un Incidente:

B.4.1.1 Alerta

Identifica y comunica al personal de Tecnología el incidente que interrumpe o reduce la calidad/desempeño del servicio de Tecnología de Información.

No.	Equipo/Rol	Tarea o actividad
1.	Monitor de Alertas	Dependiendo del tipo de evento, los Especialistas de la Oficina de Tecnologías de Información y Comunicaciones - OTIC atenderán inmediatamente la alerta. Estas alertas provienen de: - Los equipos/plataformas tecnológicas. - Sensores de alerta de los Data Center - Llamadas/Avisos de usuarios finales. - Aviso de proveedores, operadores. - Recepción de alertas a través de correos. - Monitoreo de indicadores - Revisión de Logs. *Observación: Los Especialistas de la Oficina de Tecnologías de Información y Comunicaciones - OTIC son miembros de los Equipos de Recuperación de Tecnología de Información (responsable de la solución del incidente).*
2.	Especialista de Tecnología de Información	Atiende de inmediato la alerta y valida que no es un falso positivo, inicia la indagación y evaluación del incidente para determinar el nivel de severidad.

B.4.1.2 Evaluación y Comunicación del Incidente

El objetivo de este procedimiento es evaluar el nivel de afectación de las Tecnologías de Información y de acuerdo a los resultados definir si es necesario o no comunicar al Líder de Recuperación de Tecnología de Información.

No.	Rol	Tarea o actividad
1.	Especialista de Tecnología de Información (A cargo de la solución del Incidente)	Establecer el posible nivel de afectación que ocasiona el equipo/servicio de Tecnología de Información a la Institución: • Afectación de los sistemas informáticos críticos • Afectación de los enlaces de comunicaciones. • Paralización de los servicios críticos de Tecnología de Información. • Afectación parcial o total de las instalaciones de los Centros de Datos. • Afectación parcial o total del servicio del Proveedor Gemalto. Dependiendo del grado de afectación, evaluará si el incidente es severo y decidirá informar al Líder de Recuperación de Tecnología de Información.

No.	Rol	Tarea o actividad
2.	Especialista de Tecnología de Información (A cargo de la solución del Incidente)	Se define como Incidente Severo a la: - Afectación irreversible del Hardware, Software de un equipo o equipos de los sistemas informáticos, de comunicaciones y de seguridad críticos que soportan los procesos de la Institución. - Afectación severa de indisponibilidad de la red de datos. - Indisponibilidad prolongada del servicio de Internet. - Afectación de los Centros de Datos por la materialización de alguna amenaza tales como incendio, inundación, explosión, falta de fluido eléctrico, apagado de los aires acondicionados u otros cuyo efecto es irreversible. - El tiempo de recuperación del incidente sobrepasa los tiempos de indisponibilidad del servicio. Dependiendo de la evaluación y la afectación comunicará al Líder de Recuperación de Tecnología de Información. El tiempo de evaluación no deberá sobrepasar los 20 minutos desde que se atendió/emitió la alerta.
3.	Especialista de Tecnología de Información (A cargo de la solución del Incidente)	En caso determine que el incidente es severo luego de la evaluación, comunica e informa al Líder de Recuperación de Tecnología de Información utilizando el medio de comunicación que se disponga en el momento (llamada, mensaje, presencial, red social, otros) lo siguiente: - Detalle del incidente ocurrido - Afectación a la Institución por indisponibilidad del servicio de Tecnología de Información. - Tiempo aproximado de inoperancia. - Otros de relevancia. En caso el Especialista de Tecnología de Información determine que no es un incidente severo este se resolverá con los procedimientos internos propios del día a día.
4.	Líder de Recuperación de Tecnología de Información	Con la información recibida, decidirá activar a los equipos de recuperación de TI para que en conjunto se defina la solución a seguir. Activa el Árbol de Llamadas para convocar al Equipo.

B.4.1.3 Activación de los Equipos de Recuperación

Este procedimiento se utilizará cuando sea necesario convocar a los miembros de los Equipos de Recuperación, el incidente ha ocurrido y afectó severamente a la Institución.

No.	Rol	Tarea o actividad
1.	Líder de Recuperación de Tecnología de Información	Convoca a los miembros del Equipo Técnico de Administración de Crisis de Tecnología de Información.

No.	Rol	Tarea o actividad
		Activa el Árbol de llamadas del Equipo – Lista de contactos de cada equipo de recuperación de Tecnología de Información, indicados en el numeral "B.1.6 ESQUEMA DE COMUNICACIÓN".
2.	Miembros de los Equipos de Recuperación	Se reúnen de inmediato de manera presencial o virtual (teléfono) para definir los siguientes pasos de la recuperación de los servicios afectados. Según el incidente se convoca a los Equipos de Recuperación de Tecnologías de información involucrados en la respuesta y recuperación. Árbol de Llamadas de Equipos de Recuperación indicados en el numeral "B.1.6 ESQUEMA DE COMUNICACIÓN".

B.4.1.4 Análisis y Activación de la Fase y Procedimientos de Recuperación

Este procedimiento se utilizará tantas veces como se reúna los equipos de recuperación de Tecnología de Información para el análisis, coordinación y toma de decisiones de acuerdo a las soluciones o estrategias de respuesta.

No.	Rol	Tarea o actividad
1.	Especialista de Tecnología de Información (A cargo de la solución del Incidente)	Informa a todos los miembros de los equipos de recuperación de Tecnología de Información la afectación, las actividades ejecutadas, los tiempos de inoperancia e indicando las opciones de respuesta y recuperación de los servicios de Tecnología de Información.
2.	Miembros de los Equipos de Recuperación	Analizarán la información recibida y definirán las acciones o actividades a ejecutar. Este análisis puede involucrar la presencia de proveedores de Tecnología de Información para el soporte respectivo.
3.	Líder de Recuperación de Tecnología de Información	Con la información recabada, el líder tomará la decisión de activar y/o ejecutar las estrategias de recuperación local (instructivos, manuales, de proveedores, otros).
4.	Miembros de los Equipos de Recuperación	Dependiendo de la estrategia de recuperación, se inicia la ejecución de las actividades plasmadas tomando en cuenta los requerimientos previos y los tiempos asignados para la realización de la actividad.
5.	Líder de Recuperación de Tecnología de Información	Informará a la Gerencia General las acciones y decisiones tomadas, así como la expectativa de tiempo de recuperación de los servicios.

B.4.1.5 Evaluación y Monitoreo del Incidente

Este procedimiento se utilizará tantas veces como sea necesario para monitorear y coordinar las estrategias y acciones propuestas para resolver el incidente.

No.	Rol	Tarea o actividad
1.	Especialista de Tecnología de Información (A cargo de la solución del Incidente)	Ejecuta las estrategias de recuperación local identificadas para el escenario. De ser necesario estarán presentes los proveedores que considere necesario para la ejecución de las actividades de recuperación. Monitorear permanentemente el avance de la ejecución de las estrategias y acciones. Informa el alcance y las acciones ejecutadas en respuesta al Líder de Recuperación de Tecnología de Información y a los responsables de los otros equipos vía comunicación elegida (llamada, mensaje, red social, presencial, otros).
2.	Especialista de Tecnología de Información (A cargo de la solución del Incidente o problema)	Evalúa las acciones ejecutadas y determina el tiempo aproximado de recuperación e informa al Líder de Recuperación de Tecnología de Información.

B.4.1.6 Comunicación e Informe.

Este procedimiento se utilizará tantas veces como sea necesario comunicar e informar el estatus del incidente o problema.

No.	Rol	Tarea o actividad
1	Líder de Recuperación de Tecnología de Información	Con el resultado de la evaluación del procedimiento anterior recaba toda la información necesaria para comunicar e informar a la Gerencia General la situación de incidente o problema. En caso que las acciones tomadas no son efectivas y va demandar más tiempo de lo definido, entonces los Equipos volverán a reunirse y analizar las nuevas acciones de recuperación del servicio o servicios de Tecnología de Información afectados. Ir a la Sección B.4.1.4 En caso se determina que la ejecución de las actividades de recuperación resulta efectiva y se culmina en los tiempos definidos se da por terminado la recuperación.

B.4.1.7 Desactivación de los Equipos de Recuperación.

Este procedimiento se utilizará cuando se culminen las actividades de recuperación

No.	Rol	Tarea o actividad
1.	Líder de Recuperación de Tecnología de Información	Declara el fin del incidente y desactiva a los Equipos de Recuperación que participaron en la respuesta y recuperación del incidente, esto incluye el cierre de atención de soporte de los proveedores que apoyaron en la solución.
2.	Especialista de Tecnología de Información (A cargo de la solución del Incidente o problema)	Con los Coordinadores de Recuperación de Tecnología de Información, elaboran el informe de la respuesta y recuperación del Incidente o problema.
3.	Líder de Recuperación de Tecnología de Información y miembros de los equipos de recuperación.	Se reúnen en sesión de trabajo para: - Coordinar próximas actividades. - Evaluar la efectividad de las estrategias adoptadas para la solución - Actualizar el Plan de Recuperación de Servicios de TI del proceso de Emisión de Pasaporte Electrónico. - Lecciones aprendidas. - Coordinar los trabajos a ejecutar con los proveedores que se requieran después del incidente.
4.	Líder de Recuperación de Tecnología de Información	Informa a la Gerencia General, y a las instancias que correspondan las acciones, resultados y próximos pasos.
5	Coordinadores de Recuperación de Tecnología de Información	Coordinar y supervisar la actualización de toda la documentación que requiere oportunidades de mejora producto del incidente y actualiza el cronograma de pruebas.

C. FASE DE PRUEBAS:

Las pruebas a realizar constituyen en todo aspecto el método de asegurar que el Plan de Recuperación de Servicios de TI del proceso de Emisión de Pasaporte Electrónico definido servirá en un escenario real de incidente severo en las operaciones de Tecnología de Información, por lo que se desarrollaran de manera periódica, con los recursos y alcances definidos para la ejecución del mismo. La ejecución de pruebas será realizada después de terminar las actividades de conmutación por error (fail-over) al Centro de Datos de Contingencia y después de las actividades de conmutación de recuperación (fail-back) al Centro de Datos Principal.

El área usuaria es quien determina la ejecución de un escenario o de ambos escenarios durante el año descrito en el "**ANEXO N°01: DETERMINACIÓN DE ESCENARIOS DE RIESGO** ", de acuerdo a la disponibilidad y demanda del servicio de emisión de Pasaporte Electrónico.

C.1 Política de Pruebas Funcionales.

Establece la pauta para validar la ejecución del Plan de Recuperación de Servicios de TI del proceso de Emisión de Pasaporte Electrónico. La política de pruebas funcionales establece que:

- Las Pruebas serán realizadas de manera controlada con los operadores del Sistema Pasaporte Electrónico.
- Todas las pruebas deberán calificarse en función a los resultados obtenidos y el cumplimiento de los objetivos planteados para cada una de ellas.
- Los resultados de las pruebas funcionales permiten analizar los incidentes ocurridos y sustentar la ejecución del Plan de Recuperación de Servicios de TI del proceso de Emisión de Pasaporte Electrónico.
- Luego de la ejecución de cada prueba funcional o cuando exista un cambio significativo en la Institución o Tecnología de Información el Plan de Recuperación de Servicios de TI del proceso de Emisión de Pasaporte Electrónico debe ser actualizado acorde a los cambios identificados.
- Las pruebas ejecutadas deben contar con los formatos registrados, incidentes presentados, oportunidad de mejora y los resultados obtenidos.

C.2 Objetivo de las Pruebas Funcionales

Es la identificación de los incidentes durante las pruebas funcionales al “Sistema de Pasaporte Electrónico” con el fin de aumentar su capacidad de respuesta adecuada a las expectativas establecidas ante la ocurrencia de un evento que origine una contingencia tecnológica.

Objetivos de las Pruebas:

- Identificar posibles eventos que representarían riesgos, con la finalidad de minimizar los riesgos y el impacto que pudiera causar a la entidad.
- Demostrar la viabilidad del Plan de Recuperación de Servicios de TI del proceso de Emisión de Pasaporte Electrónico y de la estrategia de recuperación actuales.
- Simular condiciones similares a una situación real de recuperación.
- Detectar posibles desviaciones o modificaciones en el hardware y/o en el “Sistema de Pasaporte Electrónico” que afecten los procedimientos desarrollados en la Recuperación de Servicios de Tecnología de Información.

C.3 Alcance de las Pruebas Funcionales

Las pruebas funcionales se programan para realizarse en dos sedes de LIMA y una sede en PROVINCIA, en la siguiente tabla se detallan las funcionalidades a revisar por sistema y el personal responsable por cada una de las sedes seleccionada.
La realización de las pruebas funcionales consiste en validar las operaciones a nivel del Sistema de Pasaporte Electrónico que comprende:

SISTEMA	FUNCIONALIDADES A PROBAR	RESPONSABLE
Sistema de Enrolamiento	Acceso a la Estación de Trabajo de Enrolamiento.	Personal de Enrolamiento
	Acceso al Sistema de Enrolamiento.	
	Enrolamiento a mayor de edad por primera vez.	
	Enrolamiento a mayor de edad por segunda vez	
Sistema Central	Acceso al Sistema Central	Supervisor de Pasaporte Electrónico
	Verificación de los Tableros de Gestión	
	Consultar Personas	
	Exportar Lista de Personas	

	Consultar Policía - RQ	
Sistema de Producción	Acceso al Sistema Producción	Supervisor de Pasaporte Electrónico
	Consultar Peticiones	
Sistema de Impresión PB6500/PB500	Acceso al Sistema de Impresión	Personal de Impresión: - PB6500 (Breña) - PB500 (Otras sedes)
	Impresión de Pasaportes	
Sistema de Control de Calidad	Acceso a la Estación de Trabajo de Control de Calidad	Personal de Control de Calidad
	Acceso al Sistema de Control de Calidad	
	Control de calidad del Pasaporte Electrónico.	
Sistema de Entrega	Acceso a la Estación de Trabajo de Entrega	Personal de Entrega
	Acceso al Sistema de Entrega	
	Verificación de datos y entrega de Pasaporte	
Sistema de Bloqueo de Pasaporte Web	Acceso al Sistema de Bloqueo de Pasaporte	Supervisor de Pasaporte Electrónico
	Generar código de bloqueo	
	Bloqueo de Pasaporte	

Nota: El área usuaria es quien define la cantidad de participantes y realiza las actividades con seguimiento de un supervisor técnico de OTIC.

C.4 Actividades de las Pruebas Funcionales

Las pruebas funcionales deben documentar los resultados de la ejecución del Plan de Recuperación de Servicios de TI del proceso de Emisión de Pasaporte Electrónico. Los tipos de pruebas de acuerdo a su naturaleza se definen como:

A. Pruebas Operacionales.
B. Pruebas de Comunicación y Enlaces.

Prueba	Descripción
A. Operacionales	• Este tipo de prueba permite verificar la viabilidad de la habilitación de los Servicios de Tecnología de Información, sistemas y aplicaciones críticas de la Institución. • Consiste en validar la ejecución del Plan de Recuperación de Servicios de TI del proceso de Emisión de Pasaporte Electrónico. Su alcance podrá ser: - Total: Cuando la prueba incluye la totalidad de los componentes involucrados del proceso de Emisión de Pasaporte Electrónico. • Duración 8 horas
B. Comunicación y Enlaces	• Este tipo de prueba permite verificar las comunicaciones y las conexiones entre las sedes descentralizadas y entidades externas. • Duración 3 horas

Es posible también aplicar una combinación de estas categorías para lograr un ejercicio más completo de las pruebas que se realicen en la Fase de Ejecución y Recuperación, con aprobación del área usuaria.

C.4.1 Actividades Previas a las Pruebas Funcionales

a) Consiste en validar los accesos a los siguientes sistemas como parte del Proceso de Emisión de Pasaporte Electrónico:
   - Sistema de Enrolamiento (EMS)
   - Sistema Central
   - Sistema de Producción (PM)
   - Sistema de Impresión (PB6500, PB500)
   - Sistema de Control de Calidad
   - Sistema de Entrega
   - Sistema de Bloqueo de Pasaportes

b) Disponer de los siguientes planes de ejecución de pruebas funcionales (08 documentos)
   - Prueba Funcional del Sistema de Enrolamiento
   - Prueba Funcional del Sistema Central
   - Prueba Funcional del Sistema de Producción
   - Prueba Funcional del Sistema de Impresión PB6500
   - Prueba Funcional del Sistema de Impresión PB500
   - Prueba Funcional del Sistema de Control de Calidad
   - Prueba Funcional del Sistema de Entrega
   - Prueba Funcional del Sistema de Bloqueo de Pasaporte

c) Disponer de uno o varios recibos del Banco de la Nación para utilizarlos durante las pruebas funcionales en la etapa de enrolamiento. Escenario para el uso de los recibos de pago:

OPERADOR	ACTIVIDAD	RECIBO UTILIZADO
Operador 1	Realizar el proceso de Emisión de Pasaporte Electrónico y rechazar desde el Sistema de Entrega	Recibo 01
Operador 2	Realizar el proceso de Emisión de Pasaporte Electrónico hasta la entrega del Pasaporte al ciudadano.	Recibo 02

Consideraciones:

- **La persona que se enrolan con el Operador 1, puede o no tener pasaportes activos en el Sistema.**
- **La persona que se enrola con el Operador 2 NO debe tener pasaportes activos en el Sistema, esto debido a que se realizará la entrega del pasaporte y anulará sus pasaportes activos.**

C.4.2 Actividades Durante las Pruebas Funcionales

a) Iniciar la ejecución de las pruebas funcionales, haciendo uso de los planes mencionados en el ítem b) del numeral C.4.1, en el mismo orden indicado.
b) Cada operador debe registrar las evidencias capturando las imágenes de las pruebas funcionales y adjuntarlo en cada uno de los planes.
c) En caso de existir incidencias, estas evidencias también deben ser documentadas y reportadas por el operador a la cuenta de correo electrónico de staffti-epassport@migraciones.gob.pe de OTIC para su atención.
d) Para los casos donde la persona que se enrola tiene pasaportes activos en el Sistema, el pasaporte debe rechazarse en la etapa de entrega, si se realiza la entrega anulará el pasaporte activo del ciudadano y no podrá utilizarlo.
e) Finalmente se realizará la anulación del pasaporte entregado, ya que sólo es un documento impreso para el flujo de las pruebas. Para los pasaportes donde se realizó la entrega, estos deben ser bloqueados desde el sistema

de bloqueo de pasaporte electrónico, que se encuentra en la web de Migraciones.

C.4.3 Actividades Después de las Pruebas Funcionales

a) Revisar los formatos de las pruebas funcionales y verificar que en todos los casos contengan los resultados de las pruebas funcionales realizadas.
b) Remitir los resultados de las pruebas funcionales a las cuentas de correo del personal designado. El resultado debe contener los siguientes documentos:
   - Los ochos (08) formatos de las pruebas funcionales.
   - Evidencias de las pruebas funcionales
   - Bitácora de los incidentes con las evidencias
   - Acta de culminación de pruebas funcionales
   - Informe Técnico de la OTIC sobre la ejecución y recuperación del servicio de TI.

C.4.4 Parámetros Generales de las Pruebas

Con el fin de realizar una prueba en forma efectiva, es necesario tener en cuenta los siguientes parámetros para la planificación:

Alcance de la Prueba

- Equipos a realizar las pruebas funcionales: estarán involucrados y presentes los miembros de los equipos que ejecutan las pruebas y los que brindan el soporte a los servicios y aplicaciones.
- Notificación
- Infraestructura
- Sistemas/ aplicaciones
- Comunicaciones

Definición de los Objetivos de la Prueba

- Objetivos y resultados esperados
- Responsables del logro de objetivos.

Medición de la Prueba

- Definir las variables de medición de la prueba.
- Registro de tiempo durante la prueba (puntos de inflexión o puntos críticos).
- Documentar problema/desviación de la prueba.

Evaluación de la Prueba

- Cumplimiento de Objetivos (alcance y tiempos establecidos de recuperación)
- Evaluación del personal que participó en la prueba.
- Evaluación de proveedores que participaron en la prueba según corresponda.
- Identificar y documentar los problemas/fortalezas.

Riesgos de la Prueba

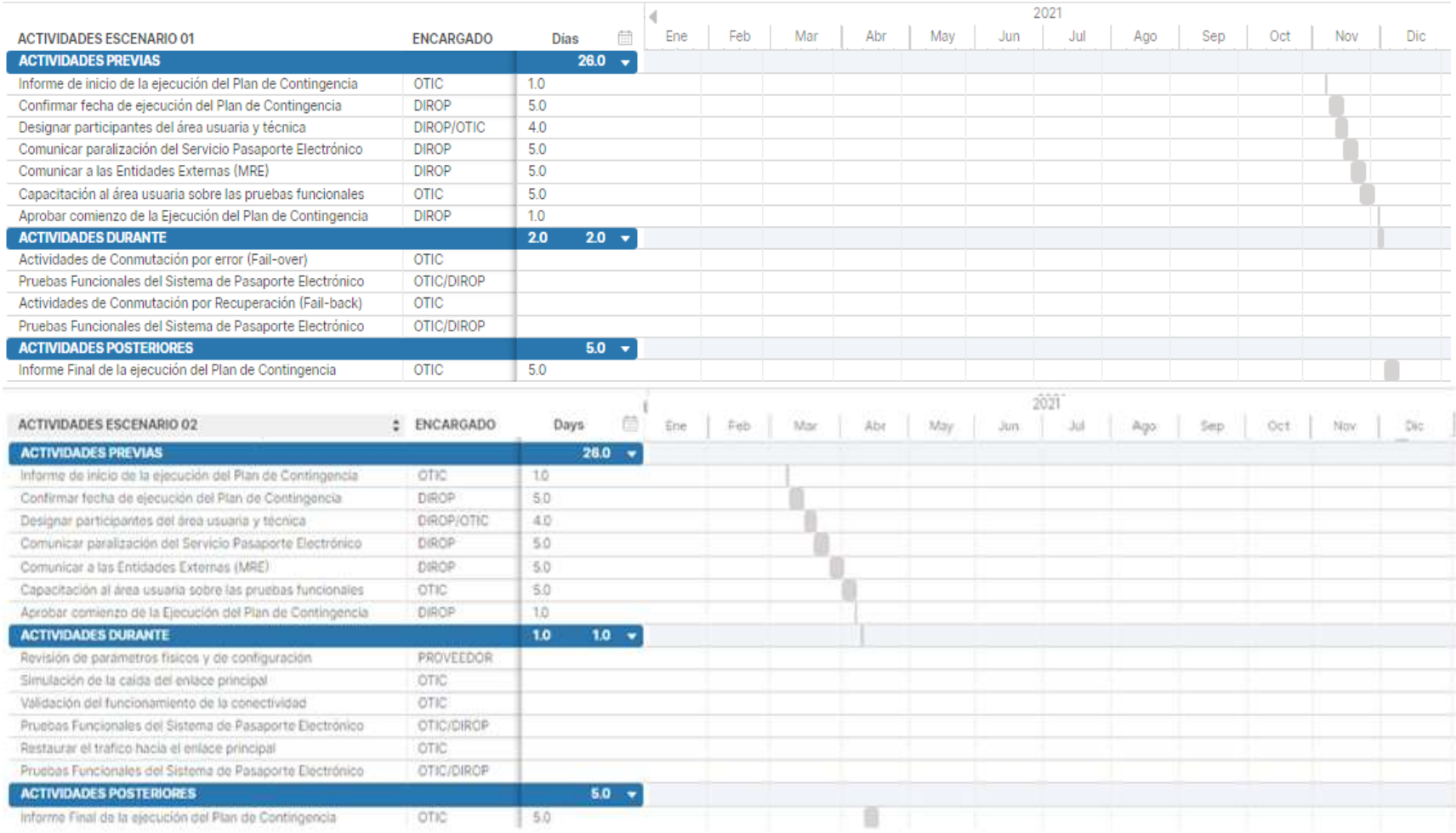
El riesgo de que la ejecución de la prueba falle está siempre latente en toda prueba. Es por ello que se deberá tener en cuenta lo siguiente:

- Identificar previamente todos los componentes de Tecnología de Información que serán probados.
- Identificar las dependencias tecnológicas de los componentes que serán probados, es decir de que otras plataformas o aplicaciones depende para el funcionamiento o procesamiento del componente a probar.
- Evaluar todos los riesgos de falla de la prueba según el procedimiento E04.OPP.PR.007-Gestión de Riesgos y Oportunidades.
- Todos aquellos resultados que poseen un riesgo no aceptable deberán tener su tratamiento al riesgo, es decir identificar y contar con los controles que permita no impactar el resultado de la prueba a los ambientes productivos.

Se debe establecer el límite de tiempo para la prueba, dado que las diversas variantes o variables que se puede presentar en su desarrollo deben estar parametrizadas y limitadas de acuerdo al tiempo previsto de inactividad del servicio Tecnología de Información en producción.

La documentación de la prueba estará enfocada a registrar los problemas y desviaciones presentadas en su ejecución, refiriéndose a problemas como los factores no previstos presentados en el desarrollo de la actividad que afectan el cumplimiento de los objetivos de la misma; y a desviaciones como las actividades no planificadas pero ejecutadas para mejorar el desempeño general y las consideraciones sobre el mismo.

C.5 Cronograma para la ejecución de las Pruebas funcionales



ACTIVIDADES ESCENARIO 01	ENCARGADO	Dias
ACTIVIDADES PREVIAS		**26.0**
Informe de inicio de la ejecución del Plan de Contingencia	OTIC	1.0
Confirmar fecha de ejecución del Plan de Contingencia	DIROP	5.0
Designar participantes del área usuaria y técnica	DIROP/OTIC	4.0
Comunicar paralización del Servicio Pasaporte Electrónico	DIROP	5.0
Comunicar a las Entidades Externas (MRE)	DIROP	5.0
Capacitación al área usuaria sobre las pruebas funcionales	OTIC	5.0
Aprobar comienzo de la Ejecución del Plan de Contingencia	DIROP	1.0
ACTIVIDADES DURANTE		**2.0** **2.0**
Actividades de Conmutación por error (Fail-over)	OTIC	
Pruebas Funcionales del Sistema de Pasaporte Electrónico	OTIC/DIROP	
Actividades de Conmutación por Recuperación (Fail-back)	OTIC	
Pruebas Funcionales del Sistema de Pasaporte Electrónico	OTIC/DIROP	
ACTIVIDADES POSTERIORES		**5.0**
Informe Final de la ejecución del Plan de Contingencia	OTIC	5.0

ACTIVIDADES ESCENARIO 02	ENCARGADO	Days
ACTIVIDADES PREVIAS		**26.0**
Informe de inicio de la ejecución del Plan de Contingencia	OTIC	1.0
Confirmar fecha de ejecución del Plan de Contingencia	DIROP	5.0
Designar participantes del área usuaria y técnica	DIROP/OTIC	4.0
Comunicar paralización del Servicio Pasaporte Electrónico	DIROP	5.0
Comunicar a las Entidades Externas (MRE)	DIROP	5.0
Capacitación al área usuaria sobre las pruebas funcionales	OTIC	5.0
Aprobar comienzo de la Ejecución del Plan de Contingencia	DIROP	1.0
ACTIVIDADES DURANTE		**1.0** **1.0**
Revisión de parametros fisicos y de configuración	PROVEEDOR	
Simulación de la caida del enlace principal	OTIC	
Validación del funcionamiento de la conectividad	OTIC	
Pruebas Funcionales del Sistema de Pasaporte Electrónico	OTIC/DIROP	
Restaurar el trafico hacia el enlace principal	OTIC	
Pruebas Funcionales del Sistema de Pasaporte Electrónico	OTIC/DIROP	
ACTIVIDADES POSTERIORES		**5.0**
Informe Final de la ejecución del Plan de Contingencia	OTIC	5.0

Nota: Cabe indicar que las fechas son propuestas por la OTIC, sin embargo, la Dirección de Operaciones como responsable del servicio, es quien determina y aprueba las fechas de ejecución.

ANEXO N°03: INFORME ANÁLISIS DE IMPACTO DE NEGOCIO - TECNOLOGÍAS DE INFORMACIÓN DE SUPERINTENDENCIA NACIONAL DE MIGRACIONES

Informe Análisis de Impacto de Negocio - Tecnologías de Información de SUPERINTENDENCIA NACIONAL DE MIGRACIONES

Diciembre 2018

Contenido

1. Introducción

En el marco de la ejecución del proyecto para la elaboración del Plan de Recuperación de Servicios de TI del proceso de Emisión de Pasaporte Electrónico, se realizó el Análisis de Impacto al Negocio (BIA) de Tecnologías de Información (TI). Esta etapa es importante debido a que permite identificar, cuantificar y calificar los impactos al negocio ocasionados por la interrupción de las funciones críticas de la Institución producto de la interrupción de los servicios tecnológicos, provee información para una apropiada definición de las estrategias de recuperación de los sistemas de información.

Por ello, el principal objetivo del presente informe es el de identificar las urgencias de recuperación de los procesos críticos y lo servicios informáticos que las soportan.

El enfoque metodológico empleado se desarrolló considerando como base principal el estándar internacional ISO 22301 sobre Gestión de Continuidad de Negocios y los lineamientos para la gestión de continuidad operativa de las entidades públicas en los tres niveles de gobierno como lo indica la RM 028-2015 PCM y otros.

Esta información constituye un punto de partida y un insumo primario, para luego definir cómo se orientará las estrategias de recuperación tecnológica y los planes de prevención, corrección y recuperación de desastres de Tecnologías de la Información en caso de eventos disruptivos.

El informe del Análisis de Impacto consta del presente documento y de todos los cuestionarios de relevamiento de información resueltos con los responsables de las Gerencias y Oficinas de la Institución.

2. Objetivos

Los objetivos a obtener en el presente análisis de impacto son los siguientes:

- Identificar las urgencias de recuperación de los servicios informáticos que brindan el soporte a las actividades críticas del proceso de Emisión de Pasaporte Electrónico.
- Identificar los impactos que ocasionaría a la Institución la interrupción de sus operaciones y/o funciones críticas producto de la falta del servicio de las tecnologías de información.
- Identificar las expectativas de tiempos de recuperación que la Institución necesita, tales como el tiempo objetivo de recuperación (RTO por sus siglas en inglés Recovery Time Objective), tiempo máximo tolerable de indisponibilidad (MTPD por sus siglas en inglés Maximum Tolerable Period of Disruption) y el Punto Objetivo de Recuperación (RPO por sus siglas en inglés) asociado a la necesidad de respaldos de información.
- Identificar la información crítica digital del proceso de Emisión de Pasaporte Electrónico consideran como recursos/registros vitales para su operación y que requieren de asegurar mediante una estrategia adecuada de respaldo la disponibilidad de esta información.

3. Alcance

El alcance del análisis de impacto, comprende la identificación y análisis de las necesidades informáticas del proceso de Emisión de Pasaporte Electrónico ante un evento disruptivo de los servicios tecnológicos.

A continuación, las personas responsables que participaron en el desarrollo de los talleres del Análisis de Impacto al Negocio asociado a los requerimientos de Tecnología de Información:

Ítem	Gerencia/Oficina	Entrevistado
1	Gerencia de Registro Migratorio[3]	LIUBEN DEL PILAR CELI SILVA

El Sr. José Luís Uscuvilca de la Oficina de Tecnologías de Información y Comunicaciones - OTIC facilitó y acompaño en todas las entrevistas realizadas.

4. Premisas

Los siguientes supuestos fueron utilizados durante el desarrollo de este análisis:

a) El análisis supone que la situación de interrupción afecta la disponibilidad de alguno de los servicios críticos de Tecnología de Información y/o desastre total en la provisión de servicios de MIGRACIONES, afectando severamente las operaciones de la Institución.

b) El análisis se apoya y sustenta en la información obtenida del personal asignado por la Institución, asumiendo que toda la información es veraz y confiable.

5. Metodología

En el diagrama adjunto se muestran las macro actividades realizadas para el Análisis de Impacto.

Macro actividades del Análisis de Impacto - Tecnología de Información

Planificación

- Coordinación con la Gerencia de Registro Migratorio[4] para la elaboración del Análisis de Impacto al Negocio.
- Identificación del personal de Gerencia de Registro Migratorio participante para el desarrollo de los talleres.
- Elaboración del material de trabajo para los talleres de Análisis de Impacto.
- Programación de las reuniones de trabajo con los responsables asignados por MIGRACIONES.

Ejecución de Talleres

- Ejecución de las entrevistas - talleres de trabajo con el personal responsable de las Gerencias[5] y Oficinas de manera presencial, con material de apoyo para la evaluación, llenado directo de los formatos del análisis de impacto al negocio, fomentando el debate y ajuste de la información proporcionada.

Análisis de Información

- Revisión y consulta de los datos obtenidos en los talleres
- Consolidación de los datos
- Análisis de la información
- Evaluar y analizar los resultados.

[3] De acuerdo con el nuevo ROF corresponde a la oficina Dirección de Operaciones.
[4] De acuerdo al nuevo ROF corresponde a la Dirección de Operaciones.
[5] De acuerdo al nuevo ROF corresponde a Direcciones.

Informe

- Elaboración del Informe Final del Análisis de Impacto.
- Entrega del Informe final del Análisis de Impacto.

Los estándares y guías que han servido para la elaboración del análisis y del informe se basa en:

- Las prácticas profesionales del Business Continuity Institute (BCI) (www.thebci.org) y del Disaster Recovery Institute International (DRII) (www.drii.org)
- Organización de estándar internacional de Normalización (ISO - www.iso.org) que provee el estándar Internacional ISO/IEC 22301 referido al Sistema de Gestión de Continuidad de Negocios y el ISO/IEC 22317 referido al Análisis de Impacto al Negocio.
- ISO 27031 Tecnología de la Información -Técnicas de seguridad – Directrices para la adecuación de las tecnologías de la información y las comunicaciones para la continuidad del negocio.
- ISO 27001:2013, dominio A.17 Aspectos de seguridad de la información de gestión de la continuidad del negocio, controles:
  - A.17.1.1 Planeando la continuidad de seguridad de información.
  - A.17.1.2 Implementación de la continuidad de seguridad de información.
  - A.17.1.3 Verificar, revisar y evaluar la continuidad de seguridad de información.
  - A.17.2.1 Planeando la continuidad de seguridad de información.
- Lineamientos para la gestión de continuidad operativa de las entidades públicas en los tres niveles de gobierno como lo indica la RM 028-2015 PCM.

6. Actividades Críticas de la Gerencia de Registro Migratorio

A continuación, se muestran las funciones/actividades críticas identificados por sus responsables, estas funciones/actividades críticas dependen de las tecnologías de información y son las que se verían severamente afectadas ante una interrupción prolongada de los servicios informáticos que los soportan.

Ítem	Gerencia/Oficina	Función/Actividad Críticas
1	Gerencia de Registros Migratorios - Subgerencia de Registros Nacionales [6]	1.1 Expedir y anular pasaportes

Fuente: Información obtenida de las entrevistas con la Gerencia de Registro Migratorio de MIGRACIONES y del Reglamento de Organización y Funciones de la Superintendencia Nacional de Migraciones

Se ha identificado 01 función y/o actividad crítica de la Oficina evaluada.

7. Análisis de Impacto -TI

En esta sección se analiza el impacto en la organización producto de una paralización severa y prolongada de los servicios informáticos y las necesidades de los recursos de tecnologías de información que requieren las funciones/actividades críticas de las Gerencias y Oficinas de MIGRACIONES

7.1 Análisis de Impacto al Negocio – Impactos

En esta sección se analiza el impacto y el nivel de severidad en los ámbitos económicos, imagen, legal, operación y de Seguridad Nacional y Jurídica de la institución, producto de la no ejecución de la función y/o actividad crítica ante una paralización o interrupción de los servicios de Tecnología de Información que los

[6] De acuerdo al nuevo ROF corresponde a Dirección de Operaciones.

soportan el proceso de Emisión de Pasaporte electrónico. Se procede a identificar los Impactos que han sido definidos con los siguientes criterios:

Ítem	Impacto	Descripción
1	Económico	Pérdidas económicas de la Institución por tiempos vencidos de atención, sanciones, multas, otros.
2	Imagen/Reputación	Impacto en la imagen de la Institución o en sus funcionarios por reclamos, denuncias, falta de información, falta de atención, otros
3	Legal	Impacto por contingencia de procesos legales que afectan a la Institución o la Alta Dirección.
4	Operacional	Impacto que ocasiona a la Institución producto de la pérdida de horas/hombre por trabajos truncados, perdidos, re trabajos y como consecuencia atraso en la atención y los tiempos establecidos.
5	Seguridad Nacional y Jurídica	Impacto que ocasiona la emisión de un documento internacional reconocido por el ordenamiento migratorio internacional.

Nivel	Descripción de los niveles de impacto
Muy Alta (5)	Puede afectar seriamente a la institución, en términos de paralización de las operaciones/actividades más allá del tiempo tolerable, pérdidas considerables, demandas legales y daño considerable a la imagen de la institución.
Alta (4)	Puede afectar los niveles de operación/actividades y servicio del Procesos de la institución, incumplimiento metas y objetivos trazados.
Moderada (3)	Afecta a ciertas operaciones/actividades cuyo impacto es limitado a áreas y/o procesos específicos de la institución por lo que puede ser solucionado sin afectación de la Institución.
Baja (2)	No causa un efecto considerable en la institución.
Muy Baja (1)	El efecto en la institución es insignificante.

A continuación, se muestran los resultados de los impactos en la Institución por la interrupción de las funciones/actividades críticas de las Gerencias y Oficinas.

Ítem	Gerencia/Oficina	Función/Actividad Críticas	Económico	Imagen	Legal	Operacional	Seguridad Nacional y Jurídica
1	Gerencia de Registro Migratorio - Subgerencia de Registros Nacionales [7]	1.1 Expedir y anular pasaportes	N.A.	N.A.	N.A.	N.A.	Muy Alta

Fuente: Información obtenida de las entrevistas con las Gerencias y Oficinas de MIGRACIONES.
NA: No Aplica, la función/actividad no impacta en MIGRACIONES si estas se interrumpen producto de la paralización de los Sistemas Informáticos.

Del análisis de la información se determinó que el Impacto que ocasiona la indisponibilidad de los servicios tecnológicos a nivel Institucional se presenta con mayor severidad en el ámbito de Seguridad Nacional.

[7] De acuerdo al nuevo ROF corresponde a Dirección de Operaciones

7.2 Análisis de Impacto al Negocio – Tiempos de Recuperación Tecnología de Información

En esta sección, el análisis se centra en la identificación de las expectativas de tiempos de recuperación de los sistemas/aplicaciones que requiere la Gerencia de Registro Migratorio de MIGRACIONES ante la interrupción de estos servicios informáticos que lo soportan.

Se establece como expectativa de tiempo recuperación al Tiempo Objetivo de Recuperación (RTO siglas en inglés) que la función y/o actividad crítica requiere tener los servicios informáticos activos y listos para operar luego de una interrupción, el tiempo máximo tolerable refiere al Periodo Máximo Tolerable de Disrupción (MTPD siglas en inglés), tiempo máximo de inoperancia de la función y/o actividad crítica sin los servicios informáticos, asimismo se relevó el tiempo mínimo que la información crítica de las funciones y/o actividad crítica que usan para su operación necesitan estar respaldados es decir el Punto Objetivo de Recuperación (RPO siglas en inglés). A continuación, la lista de sistemas/aplicaciones con los tiempos requeridos por cada Gerencia y Oficina de la Institución.

Ítem	Gerencia/Oficina	Función/Actividad Críticas	Sistema/App	Expectativa de Tiempo de Recuperación	Tiempo Máximo Tolerable	Frecuencia de Respaldo
1	Gerencia de Registros Migratorios - Subgerencia de Registros Nacionales[8]	Expedir y anular pasaportes	Sistema de Emisión Descentralizada de Pasaporte Electrónico	En línea		En Línea

Fuente: Información obtenida de las entrevistas con la Gerencia de Registro Migratorio de MIGRACIONES

8. Priorización de Recuperación de las Tecnología de Información

Teniendo como base los tiempos objetivos de recuperación (RTOs) se establece la priorización de recuperación de las Tecnologías de Información. Para ello se elaboró la siguiente matriz de priorización, el cual nos permite priorizar la recuperación de los servicios de Tecnología de Información.

Prioridad 1	RTOs hasta 8 horas.
Prioridad 2	RTOs hasta 10 horas.
Prioridad 3	RTOs hasta 15 horas.
Prioridad 4	RTOs hasta 20 horas.

Los Servicios de Tecnología de Información que son identificados con Prioridad 1 (RTOs hasta 8 horas) son consideradas servicios informáticos muy críticos para la Institución y que necesitarán de respuesta y recuperación inmediata ante un evento disruptivo, Tecnología de Información deberá tomar acción en la implementación, mejora y mantenimiento de las estrategias de recuperación.

[8] De acuerdo al nuevo ROF corresponde a Dirección de Operaciones

A continuación, la lista priorizada de recuperación de los servicios informáticos:

Ítem	Sistema/App	Expectativa de Tiempo de Recuperación
1	Sistema de Emisión Descentralizada de Pasaporte Electrónico	En línea

Fuente: Información obtenida de las entrevistas con las Gerencias y Oficinas de MIGRACIONES

Es preciso indicar que los servicios de Tecnología de Información a recuperar en base a los tiempos de recuperación y requeridas por la Institución, involucra también recuperar e implementar estrategias a aquellos servicios de Tecnología de Información que brindan el soporte tales como Base de Datos, Directorio Activo, DNS, Seguridad Perimetral, comunicaciones LAN, WAN, Storage y otros que hacen posible la entrega de servicios informáticos a la Institución.

ANEXO N° 04: DEFINICIONES Y ABREVIATURAS

- **BD:** Base de datos
- **CEPLAN:** Centro Nacional de Planeamiento Estratégico
- **Cintas de Backup:** es el tipo de dispositivo de almacenamiento de datos que lee o graba en el soporte de almacenamiento de datos de tipo cinta magnética.
- **Ransomware:** en español "secuestro de datos", es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado, y pide un rescate a cambio de quitar esta restricción.
- **RTO:** en inglés son las iniciales de “Recovery Time Objetive” es el tiempo que un negocio necesita para recuperar sus sistemas después de inactividad producida por un incidente (desastre), es decir, la cantidad de datos que se pierden y se tienen que volver a ingresar durante el tiempo de inactividad de la red.
- **TI:** Tecnología de Información
- **Vcenter:** Software de administración de servidores en entornos virtuales.
- **Veeam Backup & Replication: S**oftware de protección de datos que ofrece backup, replicación y opciones de recuperación.
- **PEI:** Plan Estratégico institucional
- **POI:** Plan Operativo institucional
- **OTIC:** Oficina de Tecnologías de Información y Comunicaciones
- **PNP:** Policia Nacional del Perú
- **RENIEC:** Registro Nacional de identificación y Estado Civil
- **MRE:** Ministerio de Relaciones Exteriores
- **Fail Over:** o conmutación por error es un modo de funcionamiento de respaldo en el que las funciones de un componente de un sistema primario, como el procesador, un servidor, la red o una base de datos, por ejemplo, son asumidos por componentes de un sistema secundario.
- **Fail Back:** o conmutación por recuperación es un modo de devolver el cambio realizado luego de restaurar los servicios.
- **OPP:** Oficina de Planeamiento y Presupuesto
- **TIER III:** Mantenimiento Concurrente. Un centro de datos de esta categoría no permite ningún evento de apagado o desconexión de la energía eléctrica. No deben ocurrir eventos de interrupción de procesos y operaciones, si es que hay que hacer mantenimiento o cambio de equipos
- **ISO:** Organismo Internacional de Normalización
- **MTPD:** Máximum Tolerable Period of Disruption – Tiempo Máximo Tolerable de Indisponibilidad define el tiempo máximo tolerable de la indisponibilidad debido a una interrupción
- **RPO**: Recovery Point Objective – Punt objetivo de Recuperación
- **PKI:** Infraestructura de clave pública.
- **RQ:** Requisitorias
- **ROF:** Reglamento de Organización y Funciones