Junta Nacional de Justicia

RESOLUCIÓN N° 031-2022-DG-JNJ

San Isidro, 16 de mayo de 2022

VISTOS:

El Memorando N° 000139-2022-OTIGD y el Informe N° 000037-2022-OTIGD/JNJ de la Oficina de Tecnologías de la Información y Gobierno Digital; y el Informe N° 0063-2022-OPCT/JNJ de la Oficina de Planificación y Cooperación Técnica, referidos a la propuesta de Plan de Contingencia Tecnologico de la Junta Nacional de Justicia; y,

CONSIDERANDO:

Que, el artículo 71 del Reglamento de Organización y Funciones de la Junta establece las funciones de la Oficina de Tecnologías de la Información y Gobierno Digital, siendo una de ellas el planificar y ejecutar medidas de seguridad necesarias que permitan proteger la información,software y hardware, en concordancia con las políticas institucionales; así como de formular, coordinar, ejecutar y evaluar el plan informático institucional;

Que, en el marco de sus funciones, la Oficina de Tecnologías de la Información y Gobierno Digital ha elaborado una propuesta de plan de contingencia tecnológico, el cual está enfocado a establecer procedimientos y acciones de contingencia necesaria para asegurar la continuidad de las operaciones de los sistemas y servicios informáticos de la Junta Nacional de Justicia;

Que, el plan de contingencia tecnológico de la Junta Nacional de Justicia, está diseñado para crear una situación de preparación que proporcione una respuesta inmediata diseñada en función de posibles incidentes tecnológicos que afecten el normal desarrollo de las actividades de la Junta Nacional de Justicia, a efecto de asegurar la continuidad de las operaciones de los sistemas y servicios informáticos, que permiten asegurar una pronta y eficaz recuperación de estos;

Que, la Oficina de Planificación y Cooperación Técnica en atención a sus competencias, a través del Informe de vistos, recomienda la aprobación del referido plan;

De conformidad con lo dispuesto en el Reglamento de Organización y Funciones asi como en la Resolución Nº 003-2022-P-JNJ de delegación de facultades a la Dirección General y con las visaciones de los jefes de las Oficinas de Asesoría Jurídica, Tecnologías de la Información y Gobierno Digital y de Planificación y Cooperación Técnica;

Firma Digital

Firmado digitalmente por SIFUENTES DEL MAR Rafael Nicolas FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 16.05.2022 15:02:13 -05:00

Firma Digital

Firmado digitalmente por PIZARRO ROCA Carlos Alberto FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 13.05.2022 23:39:30 -05:00

Firma Digital

Firmado digitalmente por ALVAREZ QUISPE Mario Alejandro FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 13.05.2022 15:07:51 -05:00

SE RESUELVE:

Artículo 1.- Aprobar el Plan de Contingencia Tecnológico de la Junta Nacional de Justicia, que en anexo forma parte de la presente resolución.

Artículo 2.- Disponer que la Oficina de Planificación y Cooperación Técnica haga de conocimiento de las unidades de organización de la Junta Nacional de Justicia el plan aprobado por la presente resolución.

Artículo 3.- Publicar la presente resolución y su anexo en el portal de transparencia y en el portal institucional de la Junta Nacional de Justicia (www.jnj.gob.pe).

Regístrese, comuníquese y archívese.

Firma Digital

Firmado digitalmente por SIFUENTES DEL MAR Rafael Nicolas FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 16.05.2022 15:02:36 -05:00

Firma Digital

Firmado digitalmente por PIZARRO ROCA Carlos Alberto FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 13.05.2022 23:39:42 -05:00

Firma Digital

Firmado digitalmente por ALVAREZ QUISPE Mario Alejandro FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 13.05.2022 15:08:00 -05:00

Firma Digital

Firmado digitalmente por MARRUJO ASTETE Betty Liliana FAU 20194484365 soft
Motivo: Soy el autor del documento
Fecha: 16.05.2022 18:48:23 -05:00

BETTY LILIANA MARRUJO ASTETE
DIRECTORA GENERAL
JUNTA NACIONAL DE JUSTICIA

JUNTA NACIONAL DE JUSTICIA

PLAN DE CONTINGENCIA TECNOLÓGICO

2022

ÍNDICE

1. INTRODUCCIÓN

El presente documento define el Plan de Contingencia Tecnológico como un proceso continuo de planeación, desarrollo, prueba e implantación de procedimientos y acciones necesarios para asegurar la continuidad de las operaciones de los sistemas y servicios informáticos en caso de posibles eventos negativos que puedan presentarse en la Junta Nacional de Justicia, y de esta manera garantizar la continuidad de los procesos y actividades de la organización a los que soportan dichos sistemas y servicios. Estas acciones buscan asegurar la reanudación eficiente y efectiva de los servicios y operaciones de tecnologías de la información en el menor tiempo e impacto posible.

La Oficina de Tecnologías de la Información y Gobierno Digital de la Junta Nacional de Justicia adopta medidas de seguridad para proteger y estar preparados para afrontar con eficiencia las contingencias tecnológicas y diversos desastres, como por ejemplo; virus informáticos, sismos, incendios, personas mal intencionadas, cortes del fluido eléctrico, instalaciones eléctricas y de transmisión de datos implementadas en la intemperie, uso de pendrives (USB) sin antes escanear con el antivirus correspondiente, escaso personal profesional y técnico, etc., medidas que garanticen el funcionamiento continuo de los sistemas y servicios informáticos de la Junta Nacional de Justicia, restaurándolos de forma eficaz, eficiente y con el menor impacto negativo en caso se produzca un incidente que pudiera alterar su operación.

2. MARCO NORMATIVO

- Ley N° 29733, Ley de Protección de Datos Personales, modificada por Decreto Legislativo N° 1353.
- Decreto Supremo N° 003-2013-JUS, Reglamento de la Ley N° 29733, Ley de Datos Personales.
- Resolución de Contraloría N° 320-2006-CG, “Aprueban Normas de Control Interno”.
- Resolución Comisión de Normalización y de Fiscalización de Barreras Comerciales no arancelarias N° 129-2014/CNB-INDECOPI, que aprueba como Norma Técnica Peruana la “NTP-ISO/IEC 27001:2014 TECNOLOGÍA DE LA INFORMACIÓN, Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos 2° Edición. Reemplaza a la NTP- ISO/IEC 27001:2008”.
- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la “NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2° Edición”, en todas las entidades integrantes del Sistema Nacional de Informática modificada por Resolución Ministerial N° 166-2017-PCM y Resolución Ministerial N° 087-2019-PCM.
- Resolución Ministerial N° 028-2015-PCM que aprueba los Lineamientos para la Gestión de la Continuidad Operativa de las entidades públicas en los tres niveles de Gobierno.

3. METODOLOGÍA PARA LA FORMULACIÓN DEL PLAN DE CONTINGENCIA TECNOLÓGICO

- **Fase 1: Organización.** Definición del objetivo, alcance, participantes y demás aspectos generales del Plan de Contingencia Tecnológico.

- **Fase 2: Análisis de la arquitectura tecnológica.** Identificación de los activos informáticos (servicios digitales y componentes de la infraestructura tecnológica) relevantes para la continuidad de los procesos institucionales y, por lo tanto, para la priorización de su recuperación en el escenario de interrupción. Dicha priorización se realiza de acuerdo con la siguiente valoración:

Prioridad para la recuperación	Descripción	Tiempo de recuperación objetivo (RTO)
Alta	Impacta en servicios al ciudadano y/o a la mayor parte de las unidades de organización de la entidad	Hasta 12 horas
Media	Impacta en servicios internos y/o a unidades de organización particulares de la entidad	Hasta 24 horas
Baja	Impacta en servicios de uso individual por algunos puestos de la entidad	Hasta 72 horas

- **Fase 3: Análisis de riesgos.** Identificación de los riesgos que podrían impactar en la provisión continua de los servicios priorizados en la fase anterior. Incluye la caracterización considerando la probabilidad y el impacto de acuerdo con la siguiente valoración:

Probabilidad de ocurrencia	
Alta	Evento que ocurre 10 o más veces al año
Media	Evento que ocurre entre 3 y 9 veces al año
Baja	Evento que ocurre 2 o menos veces al año

Grado de impacto	
Alto	Puede afectar los niveles de operación y servicio de los procesos de la entidad, incumplimiento metas y objetivos establecidos, pérdidas considerables, demandas legales y daño a la imagen de la institución.
Medio	Afecta a ciertos procesos cuyo impacto es limitado a unidades de organización particulares de la entidad.
Bajo	No causa un efecto considerable en la entidad.

	Impacto		
Probabilidad	**Bajo (1)**	**Medio (2)**	**Alto (3)**
Alta (3)	Riesgo moderado (3)	Riesgo importante (6)	Riesgo importante (9)
Media (2)	Riesgo tolerable (2)	Riesgo moderado (4)	Riesgo importante (6)
Baja (1)	Riesgo tolerable (1)	Riesgo tolerable (2)	Riesgo moderado (3)

- **Fase 4: Definición de las estrategias para la contingencia.** Para cada uno de los riesgos evaluados, se definen los procedimientos necesarios tanto en las etapas de prevención, ejecución y restauración. Se establece, además los lineamientos para la planificación y ejecución de las pruebas del Plan de Contingencia Tecnológico y el entrenamiento a los involucrados.

- **Fase 5: Elaboración del Plan de Contingencia Informático.** Consolidación de la información generada en las fases previas en el documento denominado Plan de Contingencia Informático, el cual será aprobado mediante acto resolutivo de la Dirección General.

- **Fase 6: Implementación del Plan de Contingencia.** Ejecución y puesta en marcha de los controles definidos en el Plan de Contingencia Informático. Incluye la ejecución del Plan de pruebas a fin de verificar la efectividad de los controles definidos en la mitigación de los riesgos identificados, así como la efectividad de los procedimientos ante escenarios simulados de contingencia.

- **Fase 7: Planificación y ejecución de las pruebas.** Definición de las actividades para realizar las pruebas periódicas del Plan de Contingencia Tecnológico, a fin de verificar su efectividad simulando los escenarios de contingencia descritos.

- **Fase 8: Seguimiento y evaluación.** Incluye el monitoreo continuo de la implementación del Plan de Contingencia Tecnológico, identificando mejoras que deben ser evaluadas e incluidas en las actualizaciones anuales que se realicen.

4. GENERALIDADES

4.1. Objetivos

4.1.1. Objetivo general

Establecer los procedimientos y acciones de contingencia necesarias para asegurar la continuidad de las operaciones de los sistemas y servicios informáticos que soportan los procesos institucionales de la Junta Nacional de Justicia, ante situaciones que pongan en riesgo su funcionamiento.

4.1.2. Objetivos específicos

a) Definir y programar las medidas de seguridad que garanticen el funcionamiento continuo de los sistemas y servicios informáticos en base a la identificación y caracterización de los riesgos que impacten en su operatividad.

b) Restaurar el funcionamiento continuo de los sistemas y servicios informáticos de forma eficaz, eficiente y con el menor impacto negativo en caso se produzca un incidente que pudiera alterar su operación.

c) Reducir el tiempo de recuperación, y como consecuencia, las pérdidas económicas, directas e inducidas, como resultado de un desastre.

d) Realizar la recuperación de las funciones críticas, mediante el desarrollo de los procedimientos necesarios para:

- Reducir la duración de la recuperación
- Minimizar el coste de la recuperación
- Evitar la confusión y reducir el riesgo de errores
- Evitar la duplicidad de esfuerzos

4.2. Alcance

El presente Plan abarca la continuidad de los sistemas y servicios informáticos que gestiona la Oficina de Tecnologías de la Información y Gobierno Digital de la Junta Nacional de Justicia.

4.3. Justificación

El Plan de Contingencia Tecnológico de los sistemas y servicios informáticos de la Junta Nacional de Justicia está diseñado para crear una situación de preparación que proporcione una respuesta inmediata diseñada en función de una serie de posibles incidentes tecnológicos que afecten el normal desarrollo de las actividades de la Junta.

Teniendo en cuenta los tipos de incidentes externos o internos que pudieran potencialmente causar interrupción a las actividades de la Junta Nacional de Justicia, tales como la pérdida de los servicios de suministro eléctrico o de telecomunicaciones, o incidentes que afecten el funcionamiento del hardware o del software, o incidentes internos que pudiera potencialmente causar o afectar la interrupción de las operaciones de los sistemas de información, como son la falla en los servidores o puntos de conexión.

Siendo necesario definir a las unidades de organización de la Junta Nacional de Justicia que van a estar relacionadas y deben ser incluidas en el Plan. Adicionalmente se debe distinguir las amenazas más probables y descartar aquellas que, aun siendo posibles, su probabilidad de ocurrencia sea muy bajo.

4.4. Roles y responsabilidades

La organización de la Junta Nacional de Justicia para la actuación ante un escenario de contingencia en los servicios informáticos se detalla a continuación:

4.4.1. Líder de Recuperación de TI

- Representado por el Jefe de la Oficina de Tecnologías de la Información y Gobierno Digital de la Junta Nacional de Justicia
- Se encarga de analizar, definir y tomar decisiones ante incidentes disruptivos de los servicios informáticos considerados como críticos para los procesos institucionales.
- Dirige las acciones mientras dura el incidente e informa a instancias superiores el desarrollo y resultado final de la recuperación.
- Informa a la Dirección General y a quien corresponda los avances, resultados y estrategias adoptadas durante la gestión de la contingencia de TI.

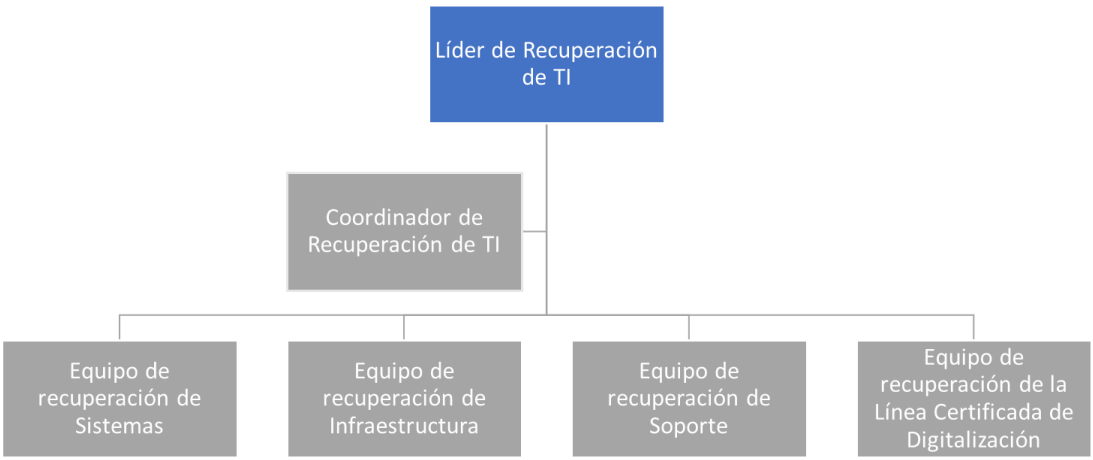
4.4.2. Coordinador de Recuperación de TI

- Representado por el Oficial de Seguridad y Confianza Digital de la Junta Nacional de Justicia
- Responsable de brindar soporte a la continuidad operativa y de contingencia de TI.

- Coordina con los miembros de los equipos de recuperación las actividades de recuperación y la gestión documentaria.

4.4.3. Equipos de Recuperación de TI

- Representado por los especialistas de las áreas de la OTIGD.
- Los equipos de recuperación de TI se encargan de la respuesta al incidente y la recuperación de los servicios de TI que se han visto afectados por la interrupción del servicio.
- Estos equipos se conforman y operan de acuerdo con las indicaciones del Líder de Recuperación de TI y del Coordinador de Recuperación de TI.
- Los miembros de los equipos de recuperación coordinan directamente con sus proveedores de servicios.



De manera adicional:

- La Dirección General es responsable de:
  a) Conducir y coordinar, de requerirse, el involucramiento de las unidades de organización de la entidad ante la ocurrencia de contingencias, en coordinación con la Oficina de Tecnologías de la Información y Gobierno Digital.
  b) Atender los requerimientos de la Oficina de Tecnologías de la Información y Gobierno Digital para la planificación de los medios de prevención, así como durante la ejecución y recuperación ante incidentes tecnológicos o desastres.
- La Oficina de Tecnologías de la Información y Gobierno Digital es responsable de:
  a) Cumplir los procedimientos de respuestas ante cada tipo de los incidentes identificados en el presente Plan.
  b) Actualizar el presente Plan.

4.5. Vinculación con el Plan Estratégico Institucional

El Plan de Contingencia Tecnológico ha sido concebido para establecer procedimientos y acciones de contingencia necesarias para asegurar la continuidad de las operaciones de los sistemas y servicios informáticos, que permiten asegurar una pronta y eficaz recuperación de estos.

En ese sentido, la Oficina de Tecnologías de la Información y Gobierno Digital, tiene como propósito proteger la información, asegurando su procesamiento y desarrollo basándose en los objetivos institucionales definidos en el Plan Estratégico Institucional (PEI), esto es, que coadyuve a la mejora integral de los procesos de soporte administrativo, en el que predomine la automatización, integración, simplicidad y eficacia en su aplicación; y, otro para afrontar la gestión de riesgos en caso de presentarse algún desastre físico.

5. GLOSARIO DE TÉRMINOS Y DEFINICIONES

- **Plan de Contingencia Informático.** Documento de gestión que establece los procedimientos y acciones necesarias para asegurar la continuidad de las operaciones de los sistemas y servicios informáticos que soportan los procesos institucionales de la Junta Nacional de Justicia, ante situaciones que pongan en riesgo su funcionamiento.

- **Incidente (de continuidad).** Situación en la que se interrumpe la provisión de un servicio de TI a los usuarios, impactando en la ejecución de las actividades y/o procesos de las unidades de organización involucradas.

- **Riesgo.** Evento que podría interrumpir la provisión de un servicio de TI a los usuarios, impactando en la ejecución de las actividades y/o procesos de las unidades de organización involucradas.
- **Acciones de prevención.** Actividades, también llamados controles, que tienen la finalidad de evitar o mitigar la materialización de los riesgos identificados en incidentes.

- **Acciones de ejecución.** Actividades que tienen la finalidad de reanudar la provisión de los servicios de TI interrumpidos.

- **Acciones de recuperación.** Actividades que tienen la finalidad de desactivar, una vez superado el incidente de continuidad, las acciones (provisionales) de ejecución que se hayan implementado y retornar a la normalidad los servicios de TI.

- **Plan de Pruebas.** Secuencia de actividades que permiten verificar la efectividad de las acciones de prevención, ejecución y recuperación establecidas en el Plan de Contingencia Informático.

6. ANÁLISIS DE LA ARQUITECTURA TECNOLÓGICA

6.1. Servicios digitales

En la siguiente tabla se presentan los servicios digitales implementados en la Junta Nacional de Justicia. Actualmente se encuentran 25 sistemas de información en producción, encontrándose algunos de ellos en modo de sólo consulta de la información registrada desde julio de 2018. Para ellos, se estima la prioridad para su recuperación y el tiempo objetivo asociado.

N°	Servicio digital (sistema de información y otros)	Tipo	Prioridad para la recuperación	Tiempo de recuperación objetivo (RTO)
1	**Selección y Nombramiento** (para Jefes de la ONPE y RENIEC, para jefes de las ANC)	Orientado al ciudadano	Alta	Hasta 12 horas
2	**Ficha Única**	Orientado al ciudadano	Alta	Hasta 12 horas
3	**Procesos Disciplinarios**	Orientado al ciudadano	Alta	Hasta 12 horas
4	**Registro de Jueces y Fiscales** (Registro de Declaraciones Juradas de Magistrados; Consulta de la Base de Datos de Magistrados)	Orientado al ciudadano	Alta	Hasta 12 horas
5	**Mesa de Partes Virtual**	Orientado al ciudadano	Alta	Hasta 12 horas
6	**Sistema de Administración de Solicitudes de Información Pública**	Orientado al ciudadano	Alta	Hasta 12 horas
7	**Casilla de Notificaciones**	Orientado al ciudadano	Alta	Hasta 12 horas
8	**Recursos Humanos** (SIM-Personal, Legajo de Personal)	Gestión interna	Media	Hasta 24 horas
9	**Tesorería (ESTESO)**	Gestión interna	Media	Hasta 24 horas
10	**BOM (Boletín Oficial de La Magistratura)**	Orientado al ciudadano	Alta	Hasta 12 horas
11	**Asesoría Jurídica** (Compendio Normativo y Resoluciones JNJ)	Gestión interna	Media	Hasta 24 horas
12	**Logística** (SIGA-MEF)	Gestión interna	Media	Hasta 24 horas
13	**Trámite documentario**	Gestión interna	Media	Hasta 24 horas
14	**Registro de envío de documentos externos**	Gestión interna	Media	Hasta 24 horas
15	**Secretaría General** (SG-Web)	Gestión interna	Baja	Hasta 24 horas
16	**SIM - POI**	Gestión interna	Baja	Hasta 24 horas
17	**SIM - Estadística**	Gestión interna	Baja	Hasta 24 horas
18	**Centro de Información Gerencial**	Gestión interna	Baja	Hasta 24 horas
19	**SIM - Imagen**	Gestión interna	Baja	Hasta 24 horas
20	**Página Web Institucional**	Orientado al ciudadano	Alta	Hasta 12 horas
21	**Asignación Aleatoria de Expedientes para Revisión por Miembros de la JNJ**	Gestión interna	Media	Hasta 24 horas
22	**Selección y Nombramiento** (sólo consulta)	Orientado al ciudadano	Alta	Hasta 12 horas
23	**Sistema de Calificación de Documentos de Desempeño Profesional de DSN (Unidad de Calificación)** (sólo consulta)	Gestión interna	Media	Hasta 24 horas
24	**Sistema de Calificación de Documentos de Magistrado - DER (Unidad de Calificación)** (sólo consulta)	Gestión interna	Media	Hasta 24 horas
25	**Evaluación y Ratificación** (sólo consulta)	Orientado al ciudadano	Alta	Hasta 12 horas
26	**Correo electrónico**	Orientado al ciudadano / Gestión interna	Alta	Hasta 12 horas
27	**Producción y almacenamiento de microformas**	Gestión interna	Media	Hasta 24 horas

N°	Servicio digital (sistema de información y otros)	Tipo	Prioridad para la recuperación	Tiempo de recuperación objetivo (RTO)
28	**Atención de consultas, requerimientos e incidentes de TI**	Gestión interna	Media	Hasta 24 horas

6.2. Infraestructura tecnológica

En la siguiente tabla se presentan los componentes de la plataforma tecnológica (incluyendo los servicios base) implementada en la Junta Nacional de Justicia. Para ellos, se estima la prioridad para su recuperación y el tiempo objetivo asociado.

N°	Equipamiento y/o servicio	Tipo	Prioridad para la recuperación	Tiempo de recuperación objetivo (RTO)
1	Servicio de internet de alta velocidad	Gestión interna	Alta	Hasta 12 horas
2	Servicio de seguridad perimetral	Gestión interna	Alta	Hasta 12 horas
3	Sistema de almacenamiento SAN	Gestión interna	Alta	Hasta 4 horas
4	Sistema de almacenamiento NAS	Gestión interna	Alta	Hasta 4 horas
5	Servidor de BD Producción Oracle 12c	Gestión interna	Alta	Hasta 4 horas
6	Equipo servidores de producción (intranet, extranet)	Orientado al ciudadano	Alta	Hasta 6 horas
7	Servidor de correo electrónico	Orientado al ciudadano / Gestión interna	Alta	Hasta 6 horas
8	Servidor de Gestión de contenidos - Alfresco	Gestión interna	Alta	Hasta 4 horas

7. ANÁLISIS DE RIESGOS

Los sistemas y servicios informáticos están expuestos a riesgos de diferente tipo y naturaleza que pueden afectar su normal funcionamiento, razón por la cual los problemas potenciales se han clasificado en grupos de acuerdo con los factores que determinan su origen, los cuales se describen a continuación:

7.1. Factores de recursos humanos

Están relacionados con la ausencia o presencia insuficiente del personal que trabaja en el mantenimiento y operación de las aplicaciones informáticas. Podrían causar demoras en la atención de desperfectos, daños a los archivos, equipos y otros dispositivos que requieren personal entrenado y calificado para su operación.

ID	Riesgo	Probabilidad de ocurrencia	Grado de impacto	Valoración	Efecto
Riesgo 1.1	Ausencia o presencia insuficiente de personal de la Oficina de Tecnología de la Información y	Media	Alto	Riesgo moderado	- Se podría ver afectada la operatividad de los servicios informáticos y la adecuada atención a los usuarios (demoras). - El manejo de los sistemas por personal no capacitado podría causar daños a los archivos,

	Gobierno Digital				equipos informáticos y otros dispositivos que requieren entrenamiento y competencias específicas para su operación.

7.2. Factores de sistemas

Estos riegos están asociados con el funcionamiento de los equipos, cuyo deterioro o mal uso puede implicar lo siguiente:

ID	Riesgo	Probabilidad de ocurrencia	Grado de impacto	Valoración	Efecto
Riesgo 2.1	Fallas en los dispositivos de comunicaciones	Media	Alto	Riesgo importante	- Paralización total de las comunicaciones de toda la red de la Junta Nacional de Justicia o un segmento de esta.
Riesgo 2.2	Fallas en las computadoras de escritorio en las computadoras portátiles	Media	Alto	Riesgo importante	- Imposibilidad de utilización de una computadora de escritorio o de una computadora portátil por un usuario.
Riesgo 2.3	Fallas en los servidores	Media	Alto	Riesgo importante	- Paralización en la atención de usuarios internos que utilicen las aplicaciones de los servidores afectados.
Riesgo 2.4	Daños o perdida de la información en las bases de datos	Media	Alto	Riesgo importante	- La pérdida total o parcial de la información ocasionarla problemas en la atención en línea y en la emisión de resultados.
Riesgo 2.5	Acceso de personas no autorizadas a los sistemas informáticos de la JNJ de manera remota o a través de vulnerabilidades	Media	Alto	Riesgo importante	- Alteración o pérdida de información de los sistemas informáticos. - Difusión de información confidencial en medios públicos. - Ataque de denegación de servicio que, sin vulnerar la confidencialidad de la información interna, haga inaccesible la página web institucional, el correo electrónico o la navegación por internet por parte del personal.
Riesgo 2.6	Infección de virus informáticos en las computadoras	Media	Alto	Riesgo importante	- Lentitud en el funcionamiento de los equipos informáticos. - Modificaciones en los archivos o pérdida de información. - Mensajes de error. - Disminución del espacio en la memoria y el disco duro.
Riesgo 2.7	Fallas en la funcionalidad de los sistemas de información	Media	Alto	Riesgo importante	- Paralización en la ejecución de los procesos institucionales que utilicen los sistemas de información afectados. - Errores en los registros de los datos a través de los sistemas de información

7.3. Factores de servicios

Los riesgos identificados en este grupo pueden generar la interrupción de los sistemas y servicios informáticos, afectando las actividades administrativas y de atención al público. Se considera dentro de este grupo el siguiente factor:

ID	Riesgo	Probabilidad de ocurrencia	Grado de impacto	Valoración	Efecto
Riesgo 3.1	Corte de suministro de energía eléctrica	Media	Alto	Riesgo importante	- Paralización total de las actividades de la Junta Nacional de Justicia. - Servicio restringido, se mantendría la operatividad con equipamiento mínimo.
Riesgo 3.2	Interrupción del servicio de Internet, telefonía y otros provistos por terceros	Media	Alto	Riesgo importante	- Paralización total de las actividades de la Junta Nacional de Justicia.

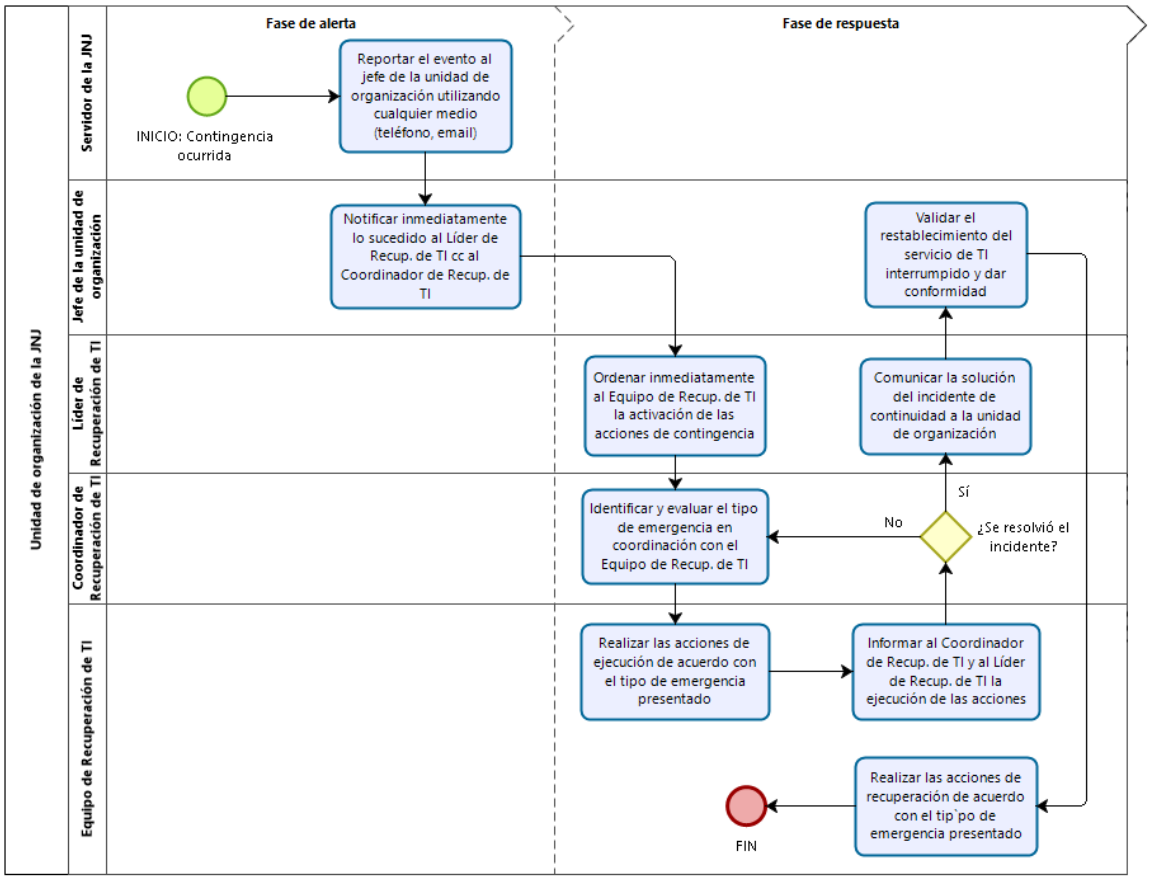
7.4. Factores naturales y artificiales

Son originados por causas externas a la institución y cuyo grado de previsión es muy reducido. Estos percances pueden generar pérdidas o daños físicos en el local de la Junta Nacional de Justicia (equipos, mobiliario, inclusive a las personas). Se consideran dentro de este grupo los siguientes:

ID	Riesgo	Probabilidad de ocurrencia	Grado de impacto	Valoración	Efecto
Riesgo 4.1	Desastres naturales (terremotos, maremotos, entre otros)	Baja	Alto	Riesgo moderado	- Posible deterioro o inutilización parcial de la infraestructura física de los locales de la JNJ. - En casos muy graves, inutilización total de los equipos de uso crítico (servidores y equipos de comunicaciones). - Incapacidad temporal para utilizar servicios de tecnologías de la información.
Riesgo 4.2	Desastres artificiales	Baja	Alto	Riesgo moderado	- Posible deterioro o inutilización parcial de la infraestructura física de los locales de la JNJ. - En casos muy graves, inutilización total de los equipos de uso crítico (servidores y equipos de comunicaciones). - Incapacidad temporal para utilizar servicios de tecnologías de la información.

8. PROCEDIMIENTOS PARA LA CONTINGENCIA

Las actividades para la atención de los escenarios de contingencia se organizan en dos fases: alerta y respuesta.



8.1. Fase de alerta

a. Se produce el incidente o se materializa una contingencia, llámese emergencia.

b. Es responsabilidad del servidor de la JNJ que identificó la emergencia, reportar el evento al jefe de la unidad de organización a la que pertenece utilizando cualquier medio de los que encuentre disponibles (teléfono, correo electrónico o en persona).

c. El responsable de la unidad de organización notifica inmediatamente lo sucedido al Líder de Recuperación de TI con copia al Coordinador de Recuperación de TI.

8.2. Fase de respuesta

a. El Líder de Recuperación de TI ordena inmediatamente al Equipo de Recuperación de TI la activación de las acciones de contingencia de acuerdo con los ámbitos pertinentes.

b. El Coordinador de Recuperación de TI identifica y evalúa el tipo de emergencia a atender (ámbito funcional) en coordinación con el Equipo de Recuperación de TI.

c. El Equipo de Recuperación de TI realiza las acciones de ejecución de acuerdo con el tipo de emergencia presentado para restablecer la continuidad de las operaciones. De

ser necesario se coordinará con empresas, proveedores de servicios, autoridades locales y nacionales y otras instituciones.

d. El Equipo de Recuperación de TI informa al Coordinador de Recuperación de TI y al Líder de Recuperación de TI la ejecución de las acciones de contingencia.

e. De no resolverse el incidente de continuidad de los servicios de TI, se realizan las actividades a partir del inciso b. de la fase de respuesta.

f. De resolverse el incidente de continuidad de los servicios de TI, el Líder de Recuperación de TI comunica a la unidad de organización afectada la solución de dicho incidente.

g. El jefe de la unidad de organización valida el restablecimiento del servicio TI interrumpido y da la conformidad a la solución implementada.

h. El Equipo de Recuperación de TI realiza las acciones de recuperación de acuerdo con el tipo de emergencia presentado para retornar a la normalidad los servicios de TI. De ser necesario se coordinará con empresas, proveedores de servicios, autoridades locales y nacionales y otras instituciones.

Procedimientos para la continuidad de servicios

A continuación, se detallan las medidas preventivas, de ejecución y recuperación, que deberán ser aplicados para minimizar los riesgos de interrupción de los sistemas informáticos; de acuerdo con el grado de impacto de los riesgos, así con su probabilidad de ocurrencia y posibles efectos.

A. Factores de recursos humanos

Riesgo 1.1.	**Ausencia de personal de la Oficina de Tecnología de la Información y Gobierno Digital**		
Probabilidad de ocurrencia	Media	**Grado de impacto**	Alto
Efecto	- Se podría ver afectada la operatividad de los servicios informáticos y la adecuada atención a los usuarios. - El manejo de los sistemas por personal no capacitado podría causar daños a los archivos, equipos informáticos y otros dispositivos que requieren entrenamiento y competencias específicas para su operación.		
Acciones de prevención	- Implementar manuales de operaciones y procedimientos en los que se señale las labores que llevan a cabo por cada proceso crítico de los sistemas informáticos. - Elaborar una lista de los sistemas informáticos críticos, con el nombre y número de teléfono del encargado de cada sistema y el de su reemplazo en caso de emergencia. Esta lista será actualizada cada vez que cambie el personal de la Oficina de Tecnologías de la Información y Gobierno Digital o rote de funciones. - Almacenar las credenciales de acceso (usuarios y claves) con permiso de administrador, de los equipos del Centro de Datos en sobres lacrados, los cuales deberán estar bajo la custodia del Jefe (a) de la Oficina de Tecnologías de la Información y Gobierno Digital.		
Acciones de ejecución	- El personal de reemplazo asume las funciones del personal titular en caso de emergencia. - Brindar al personal de reemplazo todos los accesos necesarios para que cumpla con		

	las labores encargadas. - Brindar al personal de reemplazo los usuarios y claves con permiso de administrador, de ser necesario.
Acciones de recuperación	- Retirar los accesos brindados al personal de reemplazo una vez recuperados los servicios. - Realizar el cambio de las claves y generar nuevos sobres lacrados de credenciales de acceso a los equipos del Centro de Datos, en el caso que los anteriores sobres hayan sido abiertos.

B. Factores de sistemas

Riesgo 2.1.	**Fallas en dispositivos de comunicaciones**		
Probabilidad de ocurrencia	Media	**Grado de impacto**	Alto
Efecto	- Paralización total de las comunicaciones de toda la red de la Junta Nacional de Justicia o un segmento de esta.		
Acciones de prevención	- Realizar el mantenimiento preventivo de los equipos de comunicaciones, de acuerdo con lo establecido por la Oficina de Tecnologías de la Información y Gobierno Digital. - Mantener un stock de reposición de controladores de red y dispositivos de comunicaciones que garanticen su reemplazo inmediato en el caso que sufran fallas. - Capacitar al personal responsable de los equipos de comunicaciones, de la Oficina de Tecnologías de la Información y Gobierno Digital, sobre la configuración de los equipos informáticos. - Elaborar, ejecutar y actualizar el Plan de renovación de los equipos de comunicaciones de acuerdo con su vida útil y grado de uso.		
Acciones de ejecución	- Verificar las conexiones de los hubs, switches y routers, entre otros equipos de comunicaciones. - Reiniciar el equipo de comunicaciones que esté fallando. - Verificar la configuración del equipo de comunicaciones que esté fallando. - Si no se obtiene un funcionamiento óptimo, cambiar el equipo de comunicaciones por el equipo de comunicaciones de respaldo y proceder a efectuar la configuración necesaria.		
Acciones de recuperación	- Verificar las posibles fallas en el equipo de comunicaciones; en el caso de detectarse alguna, coordinar con el proveedor su reparación o adquirir otro equipo de comunicaciones para su reemplazo. - Poner operativo el equipo de comunicaciones de respaldo. - Estabilizar la red de datos de la sede central y restablecer los enlaces con las demás sedes.		

Riesgo 2.2.	**Fallas en las computadoras de escritorio o las computadoras portátiles**		
Probabilidad de ocurrencia	Media	**Grado de impacto**	Alto
Efecto	- Imposibilidad de utilización de una computadora de escritorio o de una computadora portátil por un usuario.		
Acciones de prevención	- Realizar el mantenimiento preventivo de las computadoras de escritorio y computadoras portátiles de la JNJ de acuerdo con Plan de Mantenimiento establecido por la Oficina de Tecnologías de la información y Gobierno Digital.		

	- Instalar y actualizar un antivirus en todas las computadoras de escritorio y computadoras portátiles de la JNJ. - Concientizar a los usuarios sobre las buenas prácticas en el uso de las computadoras de escritorio y computadoras portátiles para minimizar la ocurrencia de posibles fallas en estos equipos, en las capacitaciones realizadas por la Oficina de Tecnologías de la Información y Gobierno Digital. - Elaborar, ejecutar y actualizar el plan de renovación de los equipos de oficina de acuerdo con su vida útil y grado de uso.
Acciones de ejecución	- Verificar el origen de la falla y estimar el tiempo que tomará la reparación; si es menor a una hora, efectuar la reparación en el lugar del usuario, de lo contrario se procede a retirar el equipo para su reparación en la Oficina de Tecnologías de la Información y Gobierno Digital, entregándosele temporalmente al usuario una computadora portátil como equipo de reemplazo hasta que dicho equipo sea separado y devuelto.
Acciones de recuperación	- Analizar las causas de la falta de la computadora de escritorio o computadora portátil para ser reparada y restaurada a su estado operativo, y luego devuelta al usuario asignado. Si no se consigue reparar el equipo, asignar otro con las mismas características al usuario afectado. - Restaurar la información del usuario del correo institucional y aquella respaldada por el usuario.

Riesgo 2.3.	**Fallas en los servidores**		
Probabilidad de ocurrencia	Media	**Grado de impacto**	Alto
Efecto	- Paralización en la atención de usuarios internos que utilicen las aplicaciones de los servidores afectados.		
Acciones de prevención	- Realizar el mantenimiento de hardware y software tanto preventivo como correctivo de acuerdo con el Plan de Mantenimiento establecido por la Oficina de Tecnologías de la Información y Gobierno Digital. - Verificar que los servidores deben contar con un UPS que asegure su operatividad por un tiempo prolongado ante la falla de suministro de energía eléctrica, de mínimo 1 hora. - Realizar un inventario, actualizado anualmente, de todos los programas y archivos de los servidores. - Contar con copias de seguridad actualizadas de los servidores. - Elaborar, ejecutar y actualizar el Plan de renovación de los servidores de acuerdo con su vida útil y grado de uso.		
Acciones de ejecución	- Diagnosticar los inconvenientes presentados en los equipos servidores o virtualizados. - Realizar la captura de datos para determinar las fallas presentadas en los servidores físicos o virtualizados.		
Acciones de recuperación	- Realizar la restauración desde las copias de seguridad. - Realizar la restauración o “snapshot” de los equipos virtualizados. - Realizar las pruebas de restauración de datos en los servidores físicos y virtualizados.		

Riesgo 2.4.	**Daños o pérdida de la información en las bases de datos**		
Probabilidad de ocurrencia	Media	**Grado de impacto**	Alto

Efecto	- La pérdida total o parcial de la información ocasionaría problemas en la atención en línea y en la emisión de resultados. - Paralización temporal a la atención de los usuarios internos y externos de la JNJ.
Acciones de prevención	- Restringir los accesos no autorizados a las bases de datos. - Verificar que los registros (logs) incluyan los cambios realizados a las bases de datos con la finalidad de que sean auditables. - Realizar un inventario anual de las bases de datos y su ubicación en los servidores. - Actualizar la política de respaldo y restauración de información de las bases de datos.
Acciones de ejecución	- Verificar la integridad de los datos realizando una auditoria de la información registrada en los logs.
Acciones de recuperación	- Efectuar la restauración de las copias de seguridad de las bases de datos. - Realizar las pruebas de integridad de la información restaurada y los permisos correspondientes. - Restaurar los accesos y permisos de acceso de los usuarios.

Riesgo 2.5.	**Acceso de personas no autorizadas a los sistemas informáticos de la JNJ de manera remota o a través de vulnerabilidades**		
Probabilidad de ocurrencia	Media	**Grado de impacto**	Alto
Efecto	- Alteración o pérdida de información en los sistemas informáticos. - Difusión de información confidencial en medios públicos. - Ataque de denegación de servicio que, sin vulnerar la confidencialidad de la información interna, hagan inaccesible la página web institucional, el correo electrónico o la navegación por internet por parte del personal.		
Acciones de prevención	- Efectuar charlas de capacitación y concientización sobre seguridad de la información para los usuarios, de acuerdo con el Plan de Capacitaciones de la Oficina de Tecnologías de la Información y Gobierno Digital. - Desactivar de los sistemas informáticos los accesos de los servidores públicos que renuncien o hagan uso de su periodo vacacional, para evitar que, en su ausencia, otra persona acceda con sus credenciales y pueda manipular la información de los sistemas informáticos. - Implementar la política que toda modificación de la estructura de la información en las bases de datos deberá ser autorizada por el Jefe (a) de la Oficina de Tecnologías de la Información y Gobierno Digital de la JNJ con el debido sustento del Responsable del área funcional de desarrollo. - Otorgar el acceso a la sala de servidores de la JNJ solo al personal autorizado por la Jefatura de la Oficina de Tecnologías de la Información y Gobierno Digital. - Elaborar una matriz de control de acceso de los usuarios a los diferentes recursos de la red (archivos, base de datos, impresoras, entre otros) especificando las autorizaciones respectivas sobre cada objeto. - Limitar el número de intentos para el ingreso correcto de las credenciales de acceso a los sistemas, recursos y servicios informáticos, de acuerdo con la política establecida por la Oficina de Tecnologías de la Información y Gobierno Digital. - Forzar a los usuarios a cambiar periódicamente su palabra clave, de acuerdo con la política establecida por la Oficina de Tecnologías de la Información y Gobierno Digital.		
Acciones de ejecución	- Bloquear el acceso de todos los usuarios al sistema informático inmediatamente sea detectada la intrusión.		

	- Cambiar la clave de acceso de los sistemas informáticos afectados. - Realizar una copia de seguridad de los sistemas informáticos afectados para realizar un análisis posterior. - Aislar el sistema informático hasta que las vulnerabilidades sean encontradas y subsanadas.
Acciones de recuperación	- Realizar un análisis exhaustivo para detectar las vulnerabilidades que pudieron ser utilizadas para la intrusión. - Analizar los daños que pudo haber ocasionado la intrusión. - De ser necesario, restaurar una copia de seguridad de los sistemas informáticos y subsanar las vulnerabilidades encontradas.

Riesgo 2.6.	**Infección de virus informáticos en las computadoras**		
Probabilidad de ocurrencia	Media	**Grado de impacto**	Alto
Efecto	- Lentitud en el funcionamiento de los equipos informáticos. - Modificaciones de archivos o pérdida de la información. - Mensajes de error. - Disminución del espacio en la memoria y el disco duro.		
Acciones de prevención	- Brindar charlas de capacitación y concientización para los usuarios sobre el uso de adecuado del internet y los dispositivos informáticos, de acuerdo con el Plan de Capacitaciones de la Oficina de Tecnologías de la Información y Gobierno Digital. - Verificar que se cuente con software antivirus instalado, actualizado y activo en todas las computadoras de la entidad. - Realizar actividades de mantenimiento preventivo a las computadoras.		
Acciones de ejecución	- Realizar un análisis de infección de virus informáticos en las computadoras con un antivirus actualizado y un antimalware.		
Acciones de recuperación	- Analizar los daños que pudo haber ocasionado la infección, de ser necesario aplicar el plan de contingencia para “Daños o pérdidas de la información en las bases de datos”. - Realizar las acciones del plan de recuperación para las “Fallas en las computadoras de escritorio o en las computadoras portátiles”.		

Riesgo 2.7.	**Fallas en la funcionalidad de los sistemas de información**		
Probabilidad de ocurrencia	Media	**Grado de impacto**	Alto
Efecto	- Paralización en la ejecución de los procesos institucionales que utilicen los sistemas de información afectados. - Errores en los registros de los datos a través de los sistemas de información		
Acciones de prevención	- Realizar las actividades de QA/QC (aseguramiento y control de calidad) de software y obteniendo la validación del área usuaria, de manera previa al pase a producción.		
Acciones de ejecución	- Realizar un análisis del incidente reportado y definir la acción a tomar: a) caso 1: se conoce el motivo de la falla y la corrección podrá ser realizada en un plazo no mayor a 5 días, b) caso 2: no es posible identificar el motivo de la falla y/o desarrollar la solución se realizará en más de 5 días, en cuyo escenario se desplegará un workaround (solución alternativa) en tanto se defina e implemente una solución definitiva.		
Acciones de recuperación	- Identificar las causas de las fallas y realizar las correcciones necesarias a fin de evitar la recurrencia de los incidentes.		

C. Factores de servicios

Riesgo 3.1.	**Corte de suministro de energía eléctrica**		
Probabilidad de ocurrencia	Media	**Grado de impacto**	Alto
Efecto	- Paralización total de las actividades de la JNJ. - Servicio restringido, se mantendría la operatividad con equipamiento mínimo.		
Acciones de prevención	- Efectuar el mantenimiento preventivo de todo el equipamiento informático. - Realizar pruebas semestrales a los UPS y adquirir nuevos de ser necesario.		
Acciones de ejecución	- Poner en funcionamiento el (los) UPS y/o grupos electrógenos para alimentación de equipos de uso críticos. - Comunicarse con el personal responsable de control de suministro de energía eléctrica, para coordinar con la Oficina de Tecnologías de la Información y Gobierno Digital el restablecimiento de ésta. - En caso de que la falta de energía eléctrica sea mayor a treinta minutos, se deberán apagar los servidores hasta que el servicio sea restablecido.		
Acciones de recuperación	- Verificar si la falta de suministro de energía eléctrica se debe a algún desperfecto ocurrido dentro de la institución, en cuyo caso avisar al personal responsable para que proceda con la reparación del desperfecto; de tratarse de una falta atribuible al proveedor de energía eléctrica, comunicarse con ellos para indicar el problema y solicitar la reposición inmediata del servicio. - Esperar a que el suministro de energía eléctrica se restablezca y luego efectuar el encendido de los equipos informáticos del Centro de Datos y del personal.		

Riesgo 3.2.	**Interrupción del servicio de Internet, telefonía y otros provistos por terceros**		
Probabilidad de ocurrencia	Media	**Grado de impacto**	Alto
Efecto	- Paralización total de las actividades de la Junta Nacional de Justicia.		
Acciones de prevención	- Incluir niveles de servicio en los contratos con los proveedores. - Evaluar el despliegue de servicios alternativos con proveedores diferentes.		
Acciones de ejecución	- Solicitar al proveedor del servicio, la fecha y hora de la restauración del servicio interrumpido (escalar el incidente de ser necesario). - Comunicar a las áreas usuarias del servicio interrumpido, la información proporcionada por el proveedor.		
Acciones de recuperación	- Solicitar al proveedor un reporte detallando las causas de la interrupción, y la planificación de las medidas correctivas/preventivas que implementará.		

D. Factores naturales y artificiales

Riesgo 4.1.	**Desastres naturales (terremotos, maremotos, entre otros)**		
Probabilidad de ocurrencia	Baja	**Grado de impacto**	Alto
Efecto	- Posible deterioro o inutilización parcial de la infraestructura física de los locales de la JNJ. - En casos muy graves, inutilización total de los equipos de uso crítico (servidores y equipos de comunicaciones). - Incapacidad temporal para utilizar servicios de tecnologías de la información.		
Acciones de prevención	- Establecer zonas de seguridad en las cuales se proteja al personal, así como los equipos de uso críticos.		

	- Brindar entrenamiento constante al personal para pueda asumir funciones alternas de apoyo en caso de ocurrir un desastre. - Contar con un grupo electrógeno, en cada sede de la JNJ, que pueda activarse para apoyar a las fuentes de energía alternativa (UPS) en la misión de mantener la operatividad de los sistemas informáticos. - Contar con mobiliario especial (racks) para los equipos informáticos. - Fijar los equipos informáticos mediante mecanismos de anclaje a sus respectivas bases, con la finalidad de que ante un movimiento fuerte no sufran caídas. - Realizar copias de seguridad de los aplicativos y bases de datos más importantes, de acuerdo con la política establecida por la Oficina de Tecnologías de la Información y Gobierno Digital, para asegurar la continuidad de las operaciones.
Acciones de ejecución	- Verificar el estado de la infraestructura del Data Center. - Verificar las conexiones y el adecuado funcionamiento de los equipos de uso crítico. - De encontrarse alguna falla en la infraestructura, en las conexiones, en el funcionamiento de los equipos de uso crítico, falta de energía eléctrica, falta de servidores o de ocurrir un incendio posterior al desastre natural, se deberá tomar en consideración los pasos establecidos en este plan de contingencia como medida de contención para cada uno de los casos.
Acciones de recuperación	- Luego de pasado el desastre natural, evaluar los daños ocasionados a la infraestructura tecnológica y física del centro de datos y a los equipos informáticos asignados al personal de JNJ. - Realizar un inventario general de los sistemas informáticos afectados, indicando el estado de operatividad de los mismos. - Si se han detectado bienes afectados por el evento, evaluar el caso para determinar su reposición o restauración. - Realizar tareas de recuperación de acuerdo con lo establecido por la Oficina de Tecnologías de la Información y Gobierno Digital.

Riesgo 4.2.	**Desastres artificiales**		
Probabilidad de ocurrencia	Baja	**Grado de impacto**	Alto
Efecto	- Posible deterioro de los equipos informáticos de la JNJ. - En casos muy graves, la inutilización total de los equipos de uso crítico. - Incapacidad temporal para utilizar los servicios de tecnología de la información.		
Acciones de prevención	- Mantener operativos los sistemas de detección y extinción de fuego (alarmas de humo y extinguidores de gas) en el Centro de datos. - Mantener operativas las cámaras en el Centro de Datos, para vigilancia y monitoreo de los ingresos a la Sala de Servidores y así evitar sabotajes por ingresos no autorizados que ocasionen un desastre mayor. - Efectuar revisiones anuales del estado de conservación del cableado de energía eléctrica. - Contar con personal o servicio de vigilancia las 24 horas del día, con el fin de garantizar la seguridad en cada sede de la JNJ de los equipos informáticos que procesan y almacenan toda la información de la institución. - Realizar anualmente entrenamiento del personal de la Oficina de Tecnologías de la Información y Gobierno Digital para que pueda asumir funciones alternas de apoyo en caso de ocurrir un desastre. - Brindar mantenimiento y recarga a los extintores de incendios.		
Acciones de	- Si el fuego es controlable, intentar apagado haciendo uso de los extintores		

ejecución	apropiados para cada tipo de incendio. - Retirar todos los objetos inflamables que se encuentren cerca del fuego. - De ser posible, desconectar y retirar los equipos informáticos a un ambiente libre de fuego. - De no extinguirse el fuego, evaluar las instalaciones. - De encontrarse alguna falla en la infraestructura, en las conexiones, en el funcionamiento de los equipos informáticos, falta de energía eléctrica o falla de servidores, tomar en consideración los pasos establecidos en este Plan de contingencia, como medida de contención para cada uno de los casos.
Acciones de recuperación	- Luego de extinguido el incendio, evaluar los daños ocasionados a los sistemas y equipos informáticos. - Realizar un inventario general de los sistemas y equipos informáticos afectados, indicando el estado de operatividad de los mismos. - Si se han detectado bienes afectados por el evento, evaluar el caso para determinar su reposición o restauración. - Efectuar tareas de recuperación, de acuerdo con lo establecido por la Oficina de Tecnologías de la Información y Gobierno Digital.

9. PLAN DE PRUEBAS

Los procedimientos para la contingencia definidos en el presente Plan deben ejecutarse en un ambiente de pruebas que simule los eventos de contingencia establecidos; con la finalidad de verificar su efectividad. Dichas pruebas deben realizarse de manera semestral y será planificada, organizada y realizada por la Oficina de Tecnologías de la Información y Gobierno Digital. La información recolectada debe registrarse en el formato 01 anexo 1.

10. ENTRENAMIENTO

El personal involucrado en las actividades definidas en el presente plan debe ser capacitado de manera anual en los lineamientos y contenido específico del mismo incluyendo: mecanismos de coordinación y comunicación entre equipos, roles y responsabilidades, y procedimientos para la contingencia de acuerdo con los escenarios establecidos; a fin de asegurar las competencias requeridas para su ejecución.

Dicha capacitación será planificada, organizada y realizada por la Oficina de Tecnologías de la Información y Gobierno Digital.

11. CRONOGRAMA DE ACTIVIDADES

A continuación, se presenta la planificación de las actividades del Plan de Contingencia Tecnológico 2022. Se consideran las actividades preventivas que permitan mitigar la probabilidad y el impacto de los riesgos identificados. Las actividades de ejecución y recuperación se ejecutan ante la ocurrencia de alguno de los eventos de contingencia identificados. Todas las actividades descritas en el presente plan están a cargo de la Oficina de Tecnologías de la Información y Gobierno Digital.

	Actividades	Responsable	Fecha de inicio	Fecha de término	T2 2022	T3 2022	T4 2022
Riesgo 1.1	**Ausencia de personal de la Oficina de Tecnologías de la Información y Gobierno Digital**						
1	Desplegar una política interna de rotación del personal dentro de las áreas funcionales de la Oficina de Tecnologías de la Información y Gobierno Digital para que todos conozcan las labores de la Oficina. *Medio de verificación: Comunicación de la política de rotación de personal de la OTIGD*	Jefe de OTIGD	15/05/2022	15/06/2022			
2	Elaborar una lista de los sistemas informáticos críticos, con el nombre y número de teléfono del encargado de cada sistema y el de su reemplazo en caso de emergencia. Esta lista será actualizada cada vez que cambie el personal de la Oficina de Tecnologías de la Información y Gobierno Digital o rote de funciones. *Medio de verificación: Listado de sistemas informáticos con los datos identificados*	Coordinador de Sistemas	15/05/2022	31/05/2022			
3	Almacenar las credenciales de acceso (usuarios y claves) con permiso de administrador, de los equipos del Centro de Datos en sobres lacrados, los cuales deberán estar bajo la custodia del Jefe (a) de la Oficina de Tecnologías de la Información y Gobierno Digital. *Medio de verificación: Comunicación de la política de rotación de personal de la OTIGD*	Coordinador de Infraestructura	15/05/2022	31/05/2022			
Riesgo 2.1	**Fallas en dispositivos de comunicaciones**						
4	Realizar el mantenimiento preventivo de los equipos de comunicaciones, de acuerdo con lo establecido por la Oficina de Tecnologías de la Información y Gobierno Digital. (control existente) *Medio de verificación: Informe de mantenimientos preventivos realizados*	Coordinador de Infraestructura	De acuerdo con el programa de mantenimiento anual				
5	Mantener un stock de reposición de controladores de red y dispositivos de comunicaciones que garanticen su reemplazo inmediato en el caso que sufran fallas. (control existente) *Medio de verificación: Inventario actualizado de equipos y dispositivos*	Coordinador de Infraestructura	Permanente (trimestral)				
6	Capacitar al personal responsable de los equipos de comunicaciones, de la Oficina de Tecnologías de la Información y Gobierno Digital, sobre la configuración de los equipos informáticos. *Medio de verificación: Informe de capacitación realizada*	Coordinador de Infraestructura	15/05/2022	30/06/2022			
7	Elaborar, ejecutar y actualizar el Plan de renovación de los equipos de comunicaciones de acuerdo con su vida útil y grado de uso. (control existente) *Medio de verificación: Informe de renovación de equipos de comunicaciones*	Coordinador de Infraestructura	Permanente (anual)				
Riesgo 2.2	**Fallas en las computadoras de escritorio o las computadoras portátiles**						
8	Realizar el mantenimiento preventivo de las computadoras de escritorio y computadoras portátiles de la JNJ de acuerdo con Plan de Mantenimiento establecido por la Oficina de Tecnologías de la información y Gobierno Digital. (control existente) *Medio de verificación: Informes de mantenimientos preventivos de computadoras*	Coordinador de Soporte	De acuerdo con el programa de mantenimiento anual				
9	Instalar y actualizar un antivirus en todas las computadoras de escritorio y computadoras portátiles de la JNJ. (control existente) *Medio de verificación: Correo con la verificación de los antivirus actualizados*	Coordinador de Soporte	Permanente (ingreso de nuevo colaborador o actualización de versión)				
10	Concientizar a los usuarios sobre las buenas prácticas en el uso de las computadoras de escritorio y computadoras portátiles para minimizar la ocurrencia de posibles fallas en estos equipos, en las capacitaciones realizadas por la Oficina de Tecnologías de la Información y Gobierno Digital. *Medio de verificación: Comunicaciones enviadas al personal de la JNJ*	Coordinador de Soporte	15/05/2022	30/11/2022			

	Actividades	Responsable	Fecha de inicio	Fecha de término	T2 2022	T3 2022	T4 2022
11	Elaborar, ejecutar y actualizar el Plan de renovación de los equipos de oficina de acuerdo con su vida útil y grado de uso. (control existente) *Medio de verificación: Informe de renovación de equipos de oficina*	Coordinador de Soporte	Permanente (anual)				
Riesgo 2.3	**Fallas en los servidores**						
12	Realizar el mantenimiento de hardware y software tanto preventivo como correctivo de acuerdo con el Plan de Mantenimiento establecido por la Oficina de Tecnologías de la Información y Gobierno Digital. (control existente) *Medio de verificación: Informes de los mantenimientos realizados*	Coordinador de Infraestructura	De acuerdo con el programa de mantenimiento anual				
13	Verificar que los servidores deben contar con un UPS que asegure su operatividad por un tiempo prolongado ante la falla de suministro de energía eléctrica, de mínimo 1 hora. (control existente) *Medio de verificación: Correo de verificación de los UPS*	Coordinador de Infraestructura	Permanente (semanal)				
14	Realizar un inventario, actualizado anualmente, de todos los programas y archivos de los servidores. *Medio de verificación: Inventario de programas y archivos de servidores*	Coordinador de Infraestructura	15/05/2022	31/07/2022			
15	Contar con copias de seguridad actualizadas de los servidores. (control existente) *Medio de verificación: Informe de backups realizados*	Coordinador de Infraestructura	Permanente (semanal)				
16	Elaborar, ejecutar y actualizar el plan de renovación de los servidores de acuerdo con su vida útil y grado de uso. (control existente) *Medio de verificación: Informe de renovación de servidores*	Coordinador de Infraestructura	Permanente (anual)				
Riesgo 2.4	**Daños o pérdida de la información en las bases de datos**						
17	Restringir los accesos no autorizados a las bases de datos. *Medio de verificación: Informe de accesos configurados a las bases de datos*	Coordinador de Infraestructura	15/05/2022	30/06/2022			
18	Verificar que los registros (logs) incluyan los cambios realizados a las bases de datos con la finalidad de que sean auditables. (control existente) *Medio de verificación: Correo de verificación de los logs de las bases de datos*	Coordinador de Infraestructura	Permanente (semanal)				
19	Realizar un inventario anual de las bases de datos y su ubicación en los servidores. *Medio de verificación: Inventario de bases de datos*	Coordinador de Infraestructura	01/07/2022	31/07/2022			
20	Actualizar la política de respaldo y restauración de información de las bases de datos. *Medio de verificación: Comunicación de la política de respaldo y restauración de información de las bases de datos*	Coordinador de Infraestructura	01/06/2022	30/06/2022			
Riesgo 2.5	**Acceso de personas no autorizadas a los sistemas informáticos de la JNJ de manera remota o a través de vulnerabilidades**						
21	Efectuar charlas de capacitación y concientización sobre seguridad de la información para los usuarios, de acuerdo con el Plan de Capacitaciones de la Oficina de Tecnologías de la Información y Gobierno Digital. (control existente) *Medio de verificación: Informe de capacitaciones realizadas*	Coordinador de Infraestructura	De acuerdo con el programa de capacitación anual				
22	Desactivar de los sistemas informáticos los accesos de los servidores públicos que renuncien o hagan uso de su periodo vacacional, para evitar que, en su ausencia, otra persona acceda con sus credenciales y pueda manipular la información de los sistemas informáticos. (control existente) *Medio de verificación: Correo con el reporte de inhabilitación de accesos*	Coordinador de Infraestructura	Permanente (al momento de la renuncia o vacaciones)				

	Actividades	Responsable	Fecha de inicio	Fecha de término	T2 2022	T3 2022	T4 2022
23	Implementar la política que toda modificación de la estructura de la información en las bases de datos deberá ser autorizada por el Jefe (a) de la Oficina de Tecnologías de la Información y Gobierno Digital de la JNJ con el debido sustento del Responsable del área funcional de desarrollo. *Medio de verificación: Comunicación de la política de modificación de las BD*	Coordinador de Infraestructura	01/06/2022	30/06/2022			
24	Otorgar el acceso a la sala de servidores de la JNJ solo al personal autorizado por la Jefatura de la Oficina de Tecnologías de la Información y Gobierno Digital. (control existente) *Medio de verificación: Reporte de accesos aceptados a la sala de servidores*	Coordinador de Infraestructura	Permanente				
25	Elaborar una matriz de control de acceso de los usuarios a los diferentes recursos de la red (archivos, base de datos, impresoras, entre otros) especificando las autorizaciones respectivas sobre cada objeto. *Medio de verificación: Informe de control de accesos de los usuarios*	Coordinador de Infraestructura	01/07/2022	30/08/2022			
26	Limitar el número de intentos para el ingreso correcto de las credenciales de acceso a los sistemas, recursos y servicios informáticos, de acuerdo con la política establecida por la Oficina de Tecnologías de la Información y Gobierno Digital. *Medio de verificación: Correo con la comunicación de la implementación*	Coordinador de Infraestructura	01/06/2022	30/06/2022			
27	Forzar a los usuarios a cambiar periódicamente su palabra clave, de acuerdo con la política establecida por la Oficina de Tecnologías de la Información y Gobierno Digital. (control existente) *Medio de verificación: Captura de pantalla con el control implementado*	Coordinador de Infraestructura	Permanente (cada 3 meses)				
Riesgo 2.6	**Infección de virus informáticos en las computadoras**						
28	Brindar charlas de capacitación y concientización para los usuarios sobre el uso de adecuado del internet y los dispositivos informáticos, de acuerdo con el Plan de Capacitaciones de la Oficina de Tecnologías de la Información y Gobierno Digital. (control existente) *Medio de verificación: Informe de capacitaciones realizadas*	Coordinador de Soporte	De acuerdo con el programa de capacitación anual				
29	Verificar que se cuente con software antivirus instalado, actualizado y activo en todas las computadoras de la entidad. (control existente) *Medio de verificación: Informe de verificación de actualización de antivirus*	Coordinador de Soporte	Permanente (mensual)				
30	Realizar actividades de mantenimiento preventivo a las computadoras. (control existente) *Medio de verificación: Informe de mantenimientos preventivos realizados*	Coordinador de Soporte	De acuerdo con el programa de mantenimiento anual				
Riesgo 2.7	**Fallas en la funcionalidad de los sistemas de información**						
31	Realizar las actividades de QA/QC (aseguramiento y control de calidad) de software y obteniendo la validación del área usuaria, de manera previa al pase a producción. (control existente) *Medio de verificación: Conformidades de QA/QC y de las áreas usuarias*	Coordinador de Sistemas	Permanente (en todos los desarrollos o mantenimientos)				
Riesgo 3.1	**Corte de suministro eléctrico**						
32	Efectuar el mantenimiento preventivo de todo el equipamiento informático. *Medio de verificación: Informe de mantenimiento preventivo realizado*	Coordinador de Infraestructura	01/06/2022	30/10/2022			
33	Realizar pruebas semestrales a los UPS y adquirir nuevos de ser necesario. *Medio de verificación: Informe de pruebas a los UPS*	Coordinador de Infraestructura	31/05/2022	30/11/2022			
Riesgo 3.2	**Interrupción del servicio de Internet, telefonía y otros provistos por terceros**						
34	Incluir niveles de servicio en los contratos con los proveedores. *Medio de verificación: Términos de Referencia con los niveles de servicio precisados*	Coordinador de Soporte	01/07/2022	31/08/2022			

	Actividades	Responsable	Fecha de inicio	Fecha de término	T2 2022	T3 2022	T4 2022
35	Evaluar el despliegue de servicios alternativos con proveedores diferentes. *Medio de verificación: Informe de evaluación de servicios alternativos*	Coordinador de Soporte	01/07/2022	31/08/2022			
Riesgo 4.1	**Desastres naturales (terremotos, maremotos, entre otros)**						
36	Establecer zonas de seguridad en las cuales se proteja al personal, así como los equipos de uso críticos. *Medio de verificación: Comunicación de las zonas de seguridad*	Coordinador de Infraestructura	15/05/2022	30/06/2022			
37	Brindar entrenamiento constante al personal para pueda asumir funciones alternas de apoyo en caso de ocurrir un desastre. (control existente) *Medio de verificación: Correo de entrenamiento programado y realizado*	Jefe de OTIGD	Permanente				
38	Contar con un grupo electrógeno que pueda activarse para apoyar a las fuentes de energía alternativa (UPS) en la misión de mantener la operatividad de los sistemas informáticos. (control existente) *Medio de verificación: Informe de verificación de UPS*	Coordinador de Infraestructura	Permanente				
39	Contar con mobiliario especial (racks) para los equipos informáticos. (control existente) *Medio de verificación: Fotografías del mobiliario*	Coordinador de Infraestructura	Permanente				
40	Fijar los equipos informáticos mediante mecanismos de anclaje a sus respectivas bases, con la finalidad de que ante un movimiento fuerte no sufran caídas. *Medio de verificación: Fotografías de los mecanismos de anclaje*	Coordinador de Infraestructura	15/05/2022	15/07/2022			
41	Realizar copias de seguridad de los aplicativos y bases de datos más importantes, de acuerdo con la política establecida por la Oficina de Tecnologías de la Información y Gobierno Digital, para asegurar la continuidad de las operaciones. (control existente) *Medio de verificación: Informe mensual de backups realizados*	Coordinador de Infraestructura	Permanente (semanal)				
Riesgo 4.2	**Desastres artificiales**						
42	Mantener operativos los sistemas de detección y extinción de fuego (alarmas de humo y extinguidores de gas) en el Centro de datos. *Medio de verificación: Informe de verificación de los sistemas contra incendios*	Coordinador de Infraestructura	Permanente				
43	Mantener operativas las cámaras en el Centro de Datos, para vigilancia y monitoreo de los ingresos a la Sala de Servidores y así evitar sabotajes por ingresos no autorizados que ocasionen un desastre mayor. *Medio de verificación: Informe de verificación de las cámaras*	Coordinador de Infraestructura	Permanente				
44	Efectuar revisiones anuales del estado de conservación del cableado de energía eléctrica. *Medio de verificación: Informe de verificación del cableado de energía eléctrica*	Coordinador de Infraestructura	01/09/2022	30/09/2022			
45	Contar con personal o servicio de vigilancia las 24 horas del día, con el fin de garantizar la seguridad en cada sede de la JNJ de los equipos informáticos que procesan y almacenan toda la información de la institución. (control existente) *Medio de verificación: Informe de verificación del servicio de vigilancia*	Coordinador de Infraestructura	Permanente				
46	Realizar anualmente entrenamiento del personal de la Oficina de Tecnologías de la Información y Gobierno Digital para que pueda asumir funciones alternas de apoyo en caso de ocurrir un desastre. *Medio de verificación: Correo de entrenamiento programado y realizado*	Jefe de OTIGD	01/07/2022	31/07/2022			
47	Brindar mantenimiento y recarga a los extintores de incendios. *Medio de verificación: Informe de mantenimientos realizados*	Coordinador de Infraestructura	01/07/2022	31/07/2022			

12. RECURSOS

12.1. Personal

Conforme lo dispone el numeral 4.4. del presente Plan, para la recuperación y/o mantenimiento de la operatividad de los servicios y aplicaciones en la Junta Nacional de Justicia, la Oficina de Tecnologías de la Información y Gobierno Digital debe contar con el equipo operativo calificado, conforme se especifica a continuación:

a) El Jefe de la Oficina de Tecnologías de la Información y Gobierno Digital quien lo preside.

b) Oficial de Seguridad Digital y Confianza Digital de la JNJ.

c) Equipo de Recuperación de TI
- Coordinador de sistemas de información
- Coordinador de infraestructura y seguridad
- Coordinador de soporte informático
- Coordinador de la Línea Certificada de Digitalización
- Especialista / analista en sistemas de información
- Especialista / analista en redes y comunicaciones.
- Especialista en administración de base de datos.
- Técnico de soporte informático.

12.2. Presupuesto

Las actividades descritas en el presente Plan se financian con el presupuesto institucional asignado a la Oficina de Tecnologías de la Información y Gobierno Digital.

13. SEGUIMIENTO Y EVALUACIÓN

La Oficina de Tecnologías de la Información y Gobierno Digital realiza el seguimiento constante y continuo del Plan de Contingencia Tecnológico, para ello se evalúa anualmente cada contingencia, considerando la siguiente información:

- Fecha exacta.
- Lugar.
- Descripción.
- Personal involucrado.
- Dificultades encontradas.
- Recomendaciones.

Se consideran los siguientes indicadores (métricas) para evaluar el avance de la implementación del Plan:

- Porcentaje de cumplimiento de plazos para la implementación de las acciones preventivas
- Eficacia de las acciones preventivas en la mitigación de riesgos
- Eficacia de las acciones de ejecución y de recuperación

La Oficina de Planificación y Cooperación Técnica es el órgano encargado de realizar el seguimiento y monitoreo del cumplimiento de las actividades establecidas en el presente Plan, el cual se realizará con periodicidad trimestral.

El Plan de Contingencia Tecnológico será actualizado según el marco legal vigente, pudiéndose recomendar ajustes que permitan una mejor aplicación del Plan. Cualquier cambio realizado al presente Plan es sustentado con la documentación respectiva.

14. ANEXOS

14.1. Anexo 1. Formatos

Formato de control y certificación de las Pruebas del Plan de Contingencia Tecnológico

PRUEBA N° _____

Escenario de Prueba: (Descripción del escenario a probar/certificar)

Área Responsable: (Área responsable del escenario de prueba a probar/certificar)

INFORMACION DEL PROCESO

Metodología: (Detallar lo que se va a hacer en la prueba)

Alcance: (Definir hasta donde va a abarcar)

Condiciones de Ejecución

Equipo: Nombre Servidor/PC de prueba

Aplicación/Software: _____

Ubicación: Lugar de prueba

Fecha de Backup: / /

RESULTADO DE LA PRUEBA

Resultado: Satisfactorio: ☐ Satisfactorio con Observaciones: ☐ Deficiente: ☐

Observaciones: (En el caso de haber observaciones o que la prueba haya sido deficiente, se indicarán los motivos, y resultados)

ACTUALIZACION EN EL PLAN DE CONTINGENCIA

Cambios o actualizaciones en el Plan de Contingencia: (Se indicarán los cambios que se deben realizar al Plan de Contingencia como consecuencia de las observaciones detectadas en las pruebas correspondientes)

ACTUALIZACION PARTICIPANTES

Participante	Cargo	Firma

14.2. Anexo 2. Programa de mantenimiento 2022

Mantenimientos preventivos		Responsable	Mes de ejecución
1	Mantenimiento de UPS	Coordinador de Infraestructura	Mayo
2	Mantenimiento de antenas de radioenlace	Coordinador de Infraestructura	Octubre
3	Mantenimiento de servidores del Data Center	Coordinador de Infraestructura	Noviembre
4	Mantenimiento de aire acondicionado de Data Center	Coordinador de Infraestructura	Noviembre
5	Mantenimiento de equipos de la Línea Certificada de Digitalización	Coordinador de la Línea Certificada	Noviembre