MINISTERIO DE SALUD
INSTITUTO NACIONAL DE OFTALMOLOGIA
"Dr. Francisco Contreras Campos"

REPUBLICA DEL PERU

Nº 252-2022-INO-D

Resolución Directoral

Lima, 28 de Noviembre del 2022

VISTOS: La Nota Informativa N° 292-2022-OEI/INO, Informe N° 129-2022-UO-OEPE/INO, Informe Técnico N° 002-2022-OEI/INO, Nota Informativa N° 295-2022/UFGRD-PPR068/INO, Informe Legal N° 033-2022-OAJ/INO, y;

CONSIDERANDO:

Que, mediante Decreto Supremo N° 008-2017-SA, modificado por el Decreto Supremo N° 011-2017-SA, se aprobó el Reglamento de Organización y Funciones del Ministerio de Salud, estableciendo al Instituto Nacional de Oftalmología "*Dr. Francisco Contreras Campos*", como un órgano desconcentrado del Ministerio de Salud, dependiente de la Dirección General de Operaciones en Salud;

Que, mediante Resolución Ministerial N° 447-2009/MINSA, modificado por la Resolución Ministerial N° 660-2010/MINSA, se aprobó el Reglamento de Organización y Funciones del Instituto Nacional de Oftalmología;

Que, mediante Resolución Ministerial N° 388-2022/MINSA, el Ministro de Salud designó temporalmente al señor FELIX ANTONIO TORRES COTRINA, en el puesto de Director de Instituto Especializado (CAP-P N° 001), de la Dirección General del Instituto Nacional de Oftalmología del Ministerio de Salud, en adición a sus funciones de Director Adjunto del citado Instituto;

Que, mediante el artículo 11.1 de la Resolución Ministerial N° 003-2022/MINSA, de fecha 06 de enero de 2022, se delegó a los/las Directores/as Generales de las Direcciones de Redes Integradas de Salud (DIRIS) de Lima Metropolitana, Institutos Nacionales Especializados y Hospitales del Ministerio de Salud, la facultad de emitir actos resolutivos sobre, acciones de personal en sus respectivas instituciones;

Que, la Ley N° 28551, Ley que Establece la Obligación de Elaborar y Presentar Planes de Contingencia, en su artículo 2°, establece que, "*los planes de contingencia son instrumentos de gestión que definen los objetivos, estrategias y programas que orientan las actividades institucionales para la prevención, la reducción de riesgos, la atención de emergencias y la rehabilitación en casos de desastres permitiendo disminuir o minimizar los daños, víctimas y pérdidas que podrían ocurrir a consecuencia de fenómenos naturales, tecnológicos o de la producción industrial, potencialmente dañinos*";

Que, la Ley N° 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD), en su artículo 1°, señala que, *se creó como sistema interinstitucional, sinergético, descentralizado, transversal y participativo, con la finalidad de identificar y reducir los riesgos asociados a peligros o minimizar sus efectos, así como evitar la generación de nuevos riesgos, y preparación y atención ante situaciones de desastre mediante el establecimiento de principios, lineamientos de política, componentes, procesos e instrumentos de la Gestión del Riesgo de Desastres;*

Que, el Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, *"tiene por objeto establecer el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno";*

Que, el Reglamento de la Ley N° 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD), aprobado mediante Decreto Supremo N° 048-2011-PCM, en su numeral 2) del artículo 13° establece que, *"las entidades públicas identifican y priorizan el riesgo en la infraestructura y los procesos económicos, sociales y ambientales, en su ámbito de atribuciones, y establecen un plan de gestión correctiva, tomando en consideración los lineamientos establecidos por el CENEPRED"*;

Que, mediante Decreto Supremo N° 038-2021-PCM, se aprueba la Política Nacional de Gestión del Riesgo de Desastres al 2050, la cual, *"es de aplicación inmediata por todas las entidades de la administración pública señaladas en el artículo I del Título Preliminar del Texto Único Ordenado de la Ley Nº 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo Nº 004-2019-JUS, en el marco de sus competencias. También es de obligatorio cumplimiento para el sector privado y la sociedad civil, en cuanto les sea aplicable";*

Que, mediante Resolución Ministerial N° 643-2019/MINSA, se aprueba la Directiva Administrativa N° 271-MINSA/2019/DIGERD, Directiva Administrativa para la Formulación de Planes de Contingencia de las Entidades e Instituciones del Sector Salud, el cual tiene como objetivo, *"establecer los procedimientos específicos del Sector Salud, para una oportuna y adecuada respuesta, ante la inminencia u ocurrencia de un evento adverso, emergencia o desastre, que pone en riesgo la salud de la población y el funcionamiento de los establecimientos de salud"*;

Que, mediante Resolución Ministerial N° 320-2021-PCM, se aprueba "Lineamientos para la Gestión de la continuidad operativa y la formulación de los planes de continuidad operativa de las entidades públicas de los tres niveles de Gobierno", cuya finalidad es, *"fortalecer la implementación de la Gestión de la Continuidad Operativa en las entidades públicas de los tres niveles de gobierno, ante la ocurrencia de un desastre o cualquier evento que interrumpa prolongadamente sus operaciones".*

Que, en el literal f) del numeral 5.1 del punto 5 de la norma antes mencionada, en referencia al Plan de Recuperación de los servicios informáticos se señala que es el "Plan que forma parte del Plan de Continuidad Operativa, el cual busca, inicialmente, restaurar los servicios tecnología de información necesarios para ejecutar las actividades críticas identificadas, permitiendo una posterior recuperación de las condiciones previas a la ocurrencia...";

Que, mediante Nota Informativa Nº 295-2022/UFGRD-PPR068/INO, el Coordinador de la Unidad Funcional de Gestión del Riesgo de Desastres, solicitó a la Oficina de Estadística Informática remita el Plan de Recuperación de los servicios informáticos de la Institución, a efectos de disminuir los riesgos frente a diversas situaciones de emergencia y/o desastres;

Que, mediante Nota Informativa Nº 292-2022-OEI/INO, el Jefe de la Oficina de Estadística e Informática, con la finalidad que continúe con las acciones de revisión y aprobación, remite ante el Director General, el Proyecto de Documento Técnico: Plan de recuperación de los servicios Informáticos y de Comunicaciones 2022 del Instituto Nacional de Oftalmología – INO "*Dr. Francisco Contreras Campos*";

MINISTERIO DE SALUD
INSTITUTO NACIONAL DE OFTALMOLOGIA
"Dr. Francisco Contreras Campos"

REPUBLICA DEL PERU

Nº 252-2022-INO-D

Resolución Directoral

Lima, 28 de Noviembre del 2022

Que, con Nota Informativa N° 176-2022-OEPE/INO, la Directora Ejecutiva de la Oficina Ejecutiva de Planeamiento Estratégico, remite ante el Director General, los Informes N° 129-2022-UO-OEPE/INO, N° 047-2022/UPLAN-OEPE/INO y N° 054-2022/UP-OEPE/INO, elaborado por el Responsable de la Unidad de Organización, Planeamiento y Presupuesto, respectivamente, quienes emiten Opinión Favorable a la propuesta de Documento Técnico: Plan de recuperación de los servicios Informáticos y de Comunicaciones 2022 del Instituto Nacional de Oftalmología – INO "*Dr. Francisco Contreras Campos*"; señalando que cumple con los criterios establecidos en la "Norma para la Elaboración de Documentos Normativos del Ministerio de Salud", aprobados mediante Resolución Ministerial N° 826-2021/MINSA;

Que, mediante Informe Técnico N° 002-2022-OEI/INO, el Jefe de la Oficina de Estadística e Informática; luego de haber subsanado las observaciones efectuadas por la Oficina de Asesoría Jurídica, solicita su aprobación inmediata de la propuesta de Documento Técnico: Plan de recuperación de los servicios Informáticos y de Comunicaciones 2022 del Instituto Nacional de Oftalmología – INO "*Dr. Francisco Contreras Campos*";

Que, mediante Informe Legal N° 033-2022-OAJ/INO, el Jefe de la Oficina de Asesoría Jurídica, opina que la referida propuesta del Documento Técnico: Plan de recuperación de los servicios Informáticos y de Comunicaciones 2022 del Instituto Nacional de Oftalmología – INO "*Dr. Francisco Contreras Campos*"; resulta atendible de acuerdo a los criterios establecidos en la norma para la elaboración de Documentos Normativos del Ministerio de Salud, motivo por el cual debe ser aprobado mediante acto resolutivo;

Que, el Documento Técnico: Plan de recuperación de los servicios Informáticos y de Comunicaciones 2022 del Instituto Nacional de Oftalmología – INO "*Dr. Francisco Contreras Campos*"; tiene por finalidad, establecer estándares en la operatividad de todos sus procesos en TI así como la continuidad de todos los servicios informáticos, aplicando una contingencia en casos de cada ocurrencia y/o desastre, priorizando los aspectos críticos para el restablecimiento de todos los aplicativos informáticos, de acuerdo al cuadro de priorizaciones;

Que, en consecuencia, por convenir a los intereses funcionales que permitan un mejor cumplimiento de los fines y objetivos de la Institución, resulta necesario emitir el correspondiente acto resolutivo, aprobando el Documento Técnico: Plan de recuperación de los servicios Informáticos y de Comunicaciones 2022 del Instituto Nacional de Oftalmología – INO "*Dr. Francisco Contreras Campos*";

Con la visación de la Directora Ejecutiva de la Oficina Ejecutiva de Planeamiento Estratégico, del Jefe de la Oficina de Estadística e Informática, del Coordinador de la Unidad Funcional de Gestión del Riesgo de Desastres, del Jefe de la Oficina de Asesoría Jurídica, y;

De conformidad con las normas contenidas en el Decreto Supremo N° 008-2017-SA, modificado por el Decreto Supremo N° 011-2017-SA que aprobó el Reglamento de Organización y Funciones del Ministerio de Salud; el Reglamento de Organización y Funciones del Instituto Nacional de Oftalmología, aprobado mediante Resolución Ministerial N° 447-2009/MINSA y modificada por Resolución Ministerial N° 660-2021/MINSA; la Resolución Ministerial N° 826-2021/MINSA que aprueba el documento denominado: "Normas para la Elaboración de Documentos Normativos del Ministerio de Salud"; y, el artículo 11.1 de la Resolución Ministerial N° 003-2022/MINSA.

SE RESUELVE:

Artículo 1°. - **APROBAR** el Documento Técnico: Plan de recuperación de los servicios Informáticos y de Comunicaciones 2022 del Instituto Nacional de Oftalmología – INO "*Dr. Francisco Contreras Campos*"; por las consideraciones expuestas, el cual consta de cuarenta (40) folios, que forma parte de la presente Resolución Directoral.

Artículo 2°.- AUTORIZAR al responsable del Portal de Transparencia la publicación de la presente Resolución en el Portal Web del Instituto Nacional de Oftalmología *"Dr. Francisco Contreras Campos"* www.ino.gob.pe.

Regístrese, comuníquese y publíquese

PERÚ Ministerio de Salud INO Instituto Nacional de Oftalmología "Dr. Francisco Contreras Campos"

M.O. FELIX ANTONIO TORRES COTRINA
Director General (e)
CMP.: 38356 RNE.: 17309

PERÚ | Ministerio de Salud

INO INSTITUTO NACIONAL DE OFTALMOLOGÍA
"Dr. Francisco Contreras Campos"

DIRECCION GENERAL

OFICINA DE ESTADISTICA E INFORMATICA

DOCUMENTO TÉCNICO: PLAN DE RECUPERACIÓN DE LOS SERVICIOS INFORMÁTICOS Y DE COMUNICACIONES 2022 DEL INSTITUTO NACIONAL DE OFTALMOLOGÍA – INO "DR. FRANCISCO CONTRERAS CAMPOS"

LIMA – PERU

2022

M.O. FELIX ANTONIO TORRES COTRINA
Director General

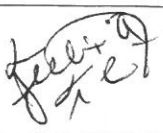
SR. ENRIQUE A. AYALA ALFARO
Jefe de la Oficina de Estadística e Informática

Elaborado por:

LIC. YURI Y. MOLINA OZEJO
Equipo Técnico

Revisado por:

LIC. GADI H. PINTO BACILIO
Equipo Técnico

	Nombre y Apellidos	Órgano / Unidad Orgánica	Firma
Elaborado por:	**Sr. Enrique a. Ayala Alfaro** Jefe de la Oficina de Estadística e Informática	Oficina de Estadística e Informática	
Revisado por:	**Félix Antonio Torres Cotrina** Médico Oftalmólogo Director General	Dirección General	
	Tania Libertad Zapata Orozco Economista Directora Ejecutiva	Oficina Ejecutiva de Planeamiento Estratégico	
Aprobado por:	**Félix Antonio Torres Cotrina** Médico Oftalmólogo Director General	Dirección General	

ÍNDICE

1. INTRODUCCIÓN 5
2. FINALIDAD: 5
4. ÁMBITO DE APLICACIÓN 6
5. BASE LEGAL 6
6. GLOSARIO DE TÉRMINOS 7
7. PRESUPUESTO 9
8. META FISICA 10
9. ANÁLISIS DE IMPACTO DE LA CONTINUIDAD DE LOS SERVICIOS TECNOLÓGICOS 10
10. EVALUACIÓN DE RIESGO 15
11. ESCENARIOS DE RIESGO 25
12. ESTRATEGIAS DE RECUPERACIÓN 26
13. PLAN DE RECUPERACIÓN 30
14. PLAN DE PRUEBAS 33
15. PLAN DE COMUNICACIÓN Y CAPACITACIÓN 36
ANEXO 01 39

1. INTRODUCCIÓN

El Plan de Recuperación de los servicios Informáticos y Comunicaciones 2022, constituye un documento esencial de gestión para la continuidad de los servicios informáticos a través de la organización, planeación constante del equipo de la Oficina de Estadística e Informática, mediante procedimientos de recuperación en caso se presente alguna contingencia de los Servicios de Tecnologías de Información del Instituto Nacional de Oftalmología – INO "Dr. Francisco Contreras Campos".

Estos procedimientos permitirán responder de manera eficiente y efectiva minimizando el tiempo de respuesta para reanudar los servicios informáticos y de comunicaciones.

Por lo cual, se realiza el Plan de Recuperación de los servicios Informáticos y Comunicaciones 2022 del Instituto Nacional de Oftalmología - INO "Dr. Francisco Contreras Campos", que está orientado a recuperar la operatividad normal de los servicios críticos de redes y comunicaciones, sistemas de información, aplicaciones y bases de datos en el menor tiempo posible ante la ocurrencia de una falla, minimizando los tiempos de recuperación.

De esta manera, se fortalece la capacidad de respuesta ante todo tipo de evento adverso, permitiendo al Instituto garantizar la continuidad de los Servicios de Tecnologías de Información necesarios para la atención de la salud ocular.

2. FINALIDAD:

El instituto nacional de Oftalmología, tiene por finalidad establecer estándares en la operatividad de todos sus procesos en TI así como la continuidad de todos los servicios informáticos, aplicando una contingencia en casos de cada ocurrencia y/o desastre, priorizando los aspectos críticos para el restablecimiento de todos los aplicativos informáticos, de acuerdo al cuadro de priorizaciones.

INSTITUTO NACIONAL DE OFTALMOLOGIA · Oficina de Estadística e Informática ·

3. OBJETIVOS:

3.1. OBJETIVO GENERAL:

Recuperar la operatividad normal de los servicios críticos de redes y comunicaciones, sistemas de información, aplicaciones y bases de datos en el menor tiempo posible ante la ocurrencia de una contingencia.

3.2. OBJETIVO ESPECÍFICOS

- Asegurar la continuidad de los servicios informáticos priorizando las atenciones de emergencia.
- Minimizar los daños a los servicios informáticos y de comunicaciones del Instituto mediante la protección y conservación de los archivos ante las amenazas internas y externas.

4. ÁMBITO DE APLICACIÓN

El presente plan es de aplicación en el Instituto Nacional de Oftalmología – INO "*Dr. Francisco Contreras Campos*", ubicado en la Av. Tingo María N°398 - Lima.

5. BASE LEGAL

- **Ley N° 29664**, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
- **Decreto Supremo N° 048-2011-PCM**, Decreto Supremo que aprueba el Reglamento de la Ley N° 29664, que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
- **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. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática y modificatoria.
- Resolución Directoral N°019–2013–JUS/DGPDP, que aprueba la Directiva de Seguridad de la información administrada por lo Bancos de Datos Personales.

INSTITUTO NACIONAL DE OFTALMOLOGÍA · REPÚBLICA DEL PERÚ · Oficina de Estadística e Informática

- Decreto Supremo N° 018-2017 –PCM, Decreto Supremo que aprueba medidas para fortalecer la planificación y operatividad del Sistema Nacional de Gestión de Riesgos de Desastres mediante la adscripción y transferencia de funciones al Ministerio de Defensa a través del Instituto Nacional de Defensa Civil–INDECI y otras disposiciones.
- Decreto Supremo N° 029-2021 – PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.
- Decreto Supremo N° 038-2021 – PCM, que aprueba la Política Nacional de Gestión del Riesgo de Desastres al 2050.
- Resolución Ministerial N° 320-2021-PCM, que aprueba los Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las entidades públicas en los tres niveles de gobierno.
- Resolución Ministerial N° 826-2021-MINSA, que aprueba las "Normas para la Elaboración de Documentos Normativos del Ministerio de Salud"
- Resolución de Contraloría N° 146-2019-CG publicada el 15 de mayo de 2019, que aprueba la Directiva N°006-2019-CG/INTEG "Implementación del Sistema de Control Interno en las entidades del Estado".

Las referidas normas incluyen sus respectivas disposiciones ampliatorias, modificatorias y conexas, de ser el caso.

6. GLOSARIO DE TÉRMINOS

Para el propósito de este documento, los siguientes términos y definiciones aplican.

INSTITUTO NACIONAL DE OFTALMOLOGÍA · Oficina de Estadística e Informática · REPÚBLICA DEL PERÚ

a) **Activo de Información**: Cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.
b) **Amenaza**: Cualquier factor que tiene el potencial para explotar una debilidad y dar lugar a algún tipo de daño a la información o a la institución.
c) **Aplicaciones:** Son los archivos y programas con sus correspondientes manuales de usuario y/o técnicos desarrollados o adquiridos por la Entidad.
d) **Base de Datos:** Las bases de datos son conjunto de datos relacionados que se almacenan de forma que se pueda acceder a ellos de manera sencilla, con la posibilidad de relacionarlos, ordenarlos en base a diferentes criterios de selección.
e) **Centro de Datos:** El centro de datos, es un centro de procesamiento para obtener información, en el cual se albergan los sistemas de información, hardware, componentes asociados, como telecomunicaciones y sistemas de almacenamiento.
f) **Confidencialidad:** Propiedad de la información que hace que no esté disponible o que sea revelada a individuos o entidades no autorizados.
g) **Control:** Medio para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la entidad que pueden ser de naturaleza administrativa, técnica, de gestión o legal.
h) **Cortafuego (Firewall):** El Cortafuegos, es un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios y pueden ser implementados en hardware o software, o en una combinación de ambos.
i) **Datos:** en general se consideran datos a todos aquellos elementos por medio de los cuales es posible la generación de información, tales elementos

INSTITUTO NACIONAL DE OFTALMOLOGÍA · Oficina de Estadística e Informática · REPÚBLICA DEL PERÚ

pueden ser estructurados (base de datos) o no estructurados (correos electrónicos) y se presentan en forma de imágenes, sonidos o colección de bits.

j) **Datos Personales:** Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados.

k) **Impacto:** Es el resultado o efecto de un evento, el impacto de un evento puede ser positivo o negativo sobre los objetivos relacionado de la institución.

l) **Incidente:** En este contexto será entendido como la interrupción de las condiciones normales de operación en cualquier proceso informático.

m) **Plan de Recuperación de los servicios Informáticos**: Plan definido y documentado que guían a la organización a responder, recuperar, reanudar los servicios de TI después de una interrupción.

n) **Probabilidad:** Posibilidad que un evento determinado ocurra en un período de tiempo dado.

o) **Riesgo:** El riesgo se define como la posibilidad que ocurra un evento adverso que afecte el logro de los objetivos de la entidad/dependencia.

p) **Sistemas de Información:** Conjunto de elementos relacionados entre sí con un objetivo en común, en el cual se almacenan datos y se genera información relacionada a un tema en particular, para ponerlos a disposición de sus usuarios. Pueden ser registros simples como archivos de Word/Excel, o pueden ser complejos como una aplicación de software con base de datos.

q) **TI:** Servicio de Tecnologías de la Información, responsables de desarrollar, operar y mantener las integraciones entre los sistemas informáticos de la institución, así como con los sistemas y servicios internos de la institución.

7. PRESUPUESTO

El presente Plan de recuperación de los servicios informáticos y de comunicaciones 2022 del Instituto Nacional de Oftalmología – INO "Dr. Francisco

INSTITUTO NACIONAL DE OFTALMOLOGIA · REPUBLICA DEL PERU · Oficina de Estadística e Informática

Contreras Campos", es un documento que en esta versión no emerge presupuesto, por que es organizacional de la Oficina de estadística e Informática

8. META FISICA

OE	AE	CAT. PPTAL.	ACT. PPTAL.	ACT. OPERAT.	U.M.	M.F.	RESP.
04. Fortalecer la rectoría y la gobernanza sobre el sistema de salud; y la gestión institucional; para el desempeño eficiente; ético e íntegro; en el marco de la modernización de la gestión pública	04.02. Gestión orientada a resultados al servicio de la población; con procesos optimizados y procedimientos administrativos simplificados	9901: Acciones Centrales	5000003: Gestión Administrativa	Recuperación de Servicios Informáticos y de Comunicación (Por Considerar en la siguiente modificación del POI)	Plan	1	OEI

9. ANÁLISIS DE IMPACTO DE LA CONTINUIDAD DE LOS SERVICIOS TECNOLÓGICOS

En esta fase se procederá a la identificación de las aplicaciones críticas, los recursos y el periodo máximo de recuperación de los servicios de tecnologías de la información y comunicaciones, para los cuales se considerarán todos los elementos susceptibles de provocar eventos que conlleven a activar la contingencia.

9.1 Procesos de Negocio

Para asegurar la continuidad de los servicios oftalmológicos brindando atención al paciente del Instituto Nacional de Oftalmología, mediante la continuidad de los siguientes procesos:

a) Encendido de los sistemas Informáticos.
b) Despliegue para la atención de Emergencia.
c) Despliegue para la atención de Sala de operaciones.
d) Despliegue para la atención de Apoyo al diagnóstico.
e) Despliegue para la atención de consulta externa.

INSTITUTO NACIONAL DE OFTALMOLOGIA · REPÚBLICA DEL PERÚ · Oficina de Informática

f) Despliegue para la atención de los servicios administrativos.

9.2 Aplicaciones y Servicios de Tecnologías de la Información (TI)

Los procesos del Instituto Nacional de Oftalmología están respaldados por los siguientes Servicios de Tecnologías de la Información (TI):

N°	Servicio TI	Descripción	Crítico para operaciones internas	Crítico para servicios externos
1	Internet Corporativo	El servicio de acceso a internet con flujo de carga (publicación) y descarga (navegación)	Alta	Alta
2	Acceso a dominio	Servicio de autenticación en el dominio del INO con el uso de credenciales institucionales.	Alta	Baja
3	Telefonía IP	Servicio de comunicación telefónica por red IP mediante el uso de teléfono físico o teléfonos software.	Baja	Alta
4	Correo electrónico	Servicio de mensajería de correo electrónico bajo el dominio @ino.gob.pe	Media	Media
5	Telefonía móvil	Servicio de comunicación telefónica	Media	Media

		por medio de teléfonos móviles.		
6	Internet inalámbrico	Servicio de acceso a internet mediante conectividad WI-Fi.	Baja	Baja
7	Videoconferencia	Servicio de videoconferencia, conferencia Web y llamadas por internet.	Media	Baja
8	Acceso a Red	El servicio de acceso a red permite la conexión de una computadora a la red de datos institucional.	Alta	Media
9	Firma Digital	Servicio de firma digital mediante el uso de certificados digitales de RENIEC.	Alta	Media
10	Almacenamiento en servidores	Servicio de repositorio digital de archivos generados en las aplicaciones y digitalización de documentos.	Alta	Alta
11	Base de datos	Servicio de repositorio de información indexada en Base de Datos para aplicaciones y servidores del Centro de Datos.	Alta	Alta

INSTITUTO NACIONAL DE OFTALMOLOGIA
Oficina de Estadística e Informática

12	VPN	Servicio de conectividad remota segura para ejecutar trabajo remoto.	Media	Baja
13	Estaciones de trabajo	Equipamiento de cómputo como recurso para el procesamiento de información.	Media	Baja
14	Personal crítico responsable de los procesos TI	Servicios profesionales críticos encargados de procesos de TI de OEI.	Media	Media
15	Sistemas de Información Internos	Aplicaciones disponibles para acceso por personal administrativo de INO.	Alta	Media
16	Sistemas de Información Internos Externos (publicados)	Aplicaciones disponibles para acceso para público en general.	Media	Alta

INSTITUTO NACIONAL DE OFTALMOLOGIA · Oficina de Estadística e Informática ·

9.3 Priorización de restauración de servicios de TI

La priorización de la restauración de los servicios de tecnologías de información serealizará según la siguiente tabla:

Descripción	Prioridad de recuperación
Atención prioritaria:	
Sistemas de información y equipos que requieran alta disponibilidad de atención.	1
Atención estándar:	
Sistemas de información y equipos no relacionados con la atención.	2
Atención baja:	
Sistemas de información de uso interno, uso poco frecuente y/o que manejan bajo volumen de información.	3

Luego del análisis, considerando la criticidad, se determina la priorización de restauración de los servicios de tecnologías de la información:

N°	Servicios TI	Prioridad
1	Internet corporativo	1
2	Transmisión de datos	2
3	Acceso a dominio	1
4	Telefonía IP	1
5	Correo electrónico	2
6	Telefonía móvil	2
7	Internet inalámbrico	3
8	Videoconferencia	2

INSTITUTO NACIONAL DE OFTALMOLOGIA · Oficina de Informática ·

9	Acceso a red	1
10	Firma digital	1
11	Almacenamiento en servidores	1
12	Base de datos	1
13	VPN	2
14	Estaciones de trabajo	2
15	Personal crítico responsable de los procesos TI	2
16	Sistemas de Información Internos	1
17	Sistemas de Información Externos (publicados)	1

10. EVALUACIÓN DE RIESGO

10.1. Identificación de Amenazas

Para determinar el riesgo asociado a cada servicio de TI procederemos a definir las amenazas, la frecuencia o probabilidad de falla o interrupción asociado a éstos.

N°	Amenaza	Tipo
1	Sismo	**Siniestro Natural**
2	Inundación y aniego en el Centro de Datos	
3	Incendio en el Centro de Datos	
4	Falla en equipos de telecomunicaciones	**Tecnológico**
5	Ciberataque	
6	Falla de hardware o software	
7	Falla de suministro eléctrico en el Centro de Datos y gabinetes de comunicaciones	**Físico y ambiental**
8	Ausencia o no disponibilidad del personal crítico de TI	**Recurso humano**
9	Pandemia y/o Epidemia	**Ambiental**

INSTITUTO NACIONAL DE OFTALMOLOGIA · Oficina de Estadística e Informática

10.2. Probabilidad de ocurrencia

Es la cuantificación de ocurrencia de que una amenaza se produzca realmente. Para el cálculo de probabilidad utilizaremos la siguiente tabla:

Probabilidad	Valor	Descripción
Baja	4	Se puede presentar al menos una vez en 5 años o más.
Media	6	Se puede presentar al menos una vez en 3 años
Alta	8	Se puede presentar al menos una vez al año
Muy Alta	10	Se puede presentar más de 1 vez al año.

A continuación, se muestra la probabilidad estimada de las amenazas a los servicios de TI:

N°	Amenaza (Evento)	Probabilidad de ocurrencia
1	Sismo	6
2	Inundación y aniego en el Centro de Datos	4
3	Incendio en el Centro de Datos	4
4	Falla en equipos de telecomunicaciones	4
5	Ciberataque	8
6	Falla de hardware o software	6
7	Falla de suministro eléctrico en el Centro de Datos y gabinetes de comunicaciones	6
8	Ausencia o no disponibilidad del personal crítico de TI	6
9	Pandemia y/o Epidemia	6

INSTITUTO NACIONAL DE OFTALMOLOGÍA · Oficina de Estadística e Informática ·

10.3. Identificación de Impacto

El impacto del riesgo mide la gravedad o magnitud del efecto adverso a causa de la ocurrencia de la amenaza. Es una calificación aplicada a la amenaza, para describir el grado de afectación. La medición puede ser cualitativa o cuantitativa.

Para nuestro caso la clasificación del impacto será en una escala de 4 al 10, categorizando desde los niveles Bajo hasta Muy Alto, tal como se muestra en la siguiente tabla:

Impacto	valor	Descripción
Bajo	4	No representa un impacto importante. Se cuenta con controles suficientes que responden a un programa de mantenimiento (evaluados y mejorados), se evidencia que han respondido a acontecimientos ocurridos y ejercicios realizados, se puede prescindir del servicio por un tiempo limitado.
Medio	6	El impacto sobre la confidencialidad, integridad y disponibilidad de la información es limitado en tiempo y alcance. Su efecto es para un proceso de soporte o actividad específica que puede subsanarse en corto plazo.
Alto	8	Impacta en forma grave a un área o servicio específico, se puede llegar a comprometer documentos internos clasificados como confidenciales, paralizar o retrasar procesos claves por un tiempo considerable. Su efecto está limitado dentro del INO.
Muy Alto	10	Impacta en forma severa a todo el INO y su efecto no solo se limita a éste. Compromete la confidencialidad o integridad de información crítica o la continuidad de las operaciones por paralización de los servicios más allá de los tiempos tolerables para la institución.

10.4. Cálculo del Nivel de Riesgo

Para determinar el Nivel de Riesgo de un Servicio de TI del INO, se ha considerado los controles existentes que mitigan la afectación de las amenazas y/o el impacto descritas en el punto anterior. Para la identificación del Nivel de Riesgo se considera la siguiente matriz:

Probabilidad de Ocurrencia	Muy Alta	10	40 (Medio)	60 (Alto)	80 (Muy Alto)	100 (Muy Alto)
	Alta	8	32 (Medio)	48 (Alto)	64 (Alto)	80 (Muy Alto)
	Media	6	24 (Bajo)	36 (Medio)	48 (Alto)	60 (Alto)
	Baja	4	16 (Bajo)	24 (Bajo)	32 (Medio)	40 (Medio)
NIVEL DE RIESGO (probabilidad de ocurrencia x impacto)			4	6	8	10
			Bajo	Medio	Alto	Muy Alto
			Impacto			

Interpretación de cada cuadrante de calor o Nivel de Riesgo de la amenaza en evaluación:

Muy Alto	Riesgo no aceptable, se requiere acción correctiva inmediata.
Alto	Riesgo no aceptable, se requiere de una acción correctiva, pero se permite planificar plazos y compromisos.
Medio	Riesgo aceptable con revisión de la dirección, y se evalúa tomar acciones.
Bajo	Riesgo aceptable, sin revisión y no se requieren acciones.

Listado de riesgos considerando las amenazas existentes a los servicios de TI

N°	Amenaza	Riesgo	Probabilidad	Impacto	Nivel de riesgo
1	Falla de Hardware o Software	Inexistencia del acceso al dominio del INO o por falla de hardware	6	10	60
2	Falla de Hardware o Software	Exposición de información por acceso electrónico no autorizado a sistemas internos	6	10	60
3	Falla de Hardware o Software	Exposición de información por acceso electrónico no	6	8	60

		autorizado a sistemas externos			
5	Falla de suministro eléctrico en el Centro de Datos y gabinetes de comunicaciones	Daño en los discos duros o componentes de los servidores, controladores de red, equipamiento de infraestructura, etc.	6	8	48
6	Inundación y aniego en el Centro de Datos	Centro de datos por inundación o aniego en las instalaciones de INO.	4	10	40
7	Falla de suministro eléctrico en el Centro de Datos y gabinetes de comunicaciones	Daño en el equipamiento del Centro de Datos por corte no programado de energía.	6	8	48
8	Ciberataque	Daño o pérdida de equipo, unidades de almacenamiento, etc.	8	8	64
9	Ciberataque	Imposibilidad de acceso a los recursos informáticos, sean estos por cambios voluntarios o involuntarios, tales como cambio de claves de acceso, eliminación de los	8	6	48

		archivos o proceso de información no deseado.			
11	Ciberataque	Exposición de información por suplantación de identidad a través de técnicas de ingeniería social	8	8	64
12	Falla en equipos de telecomunicaciones	Dificultad para acceder a los servicios de internet e intranet	4	8	32
13	Ciberataque	Pérdida o alteración de información institucional, por intromisión de agentes externos y/o inescrupulosos, los cuales pueden generar daño y pérdida de información institucional	8	10	80
14	Ausencia o no disponibilidad del personal crítico de TI	Pérdida de datos por error de personal no especializado	6	6	36
15	Falla de Hardware o Software	Falta de actualización de software y	6	6	36

		hardware (procesos y recursos)			
16	Falla de Hardware o Software	Daño físico por cableado de red expuesta o en mal estado en las instalaciones de la institución	6	6	36
17	Ausencia o no disponibilidad del personal crítico de TI	Indisponibilidad de los sistemas de información por error en la ejecución de procedimientos no documentados.	6	6	36
18	Falla en equipos de telecomunicaciones	Saturación del servicio de red inalámbrica por acceso no autorizado	4	4	16
19	Inundación y aniego en el Centro de Datos	Daño del centro de datos por falla en el equipo de aire acondicionado o ventilación del centro de datos.	4	8	32
20	Ciberataque	Alteraciones de la información por manejo inadecuado de contraseñas (inseguras, compartidas).	8	8	64

21	Falla en equipos de telecomunicaciones	Desconexión de la red corporativa por falla en los enlaces de comunicación	4	8	32
22	Falla en equipos de telecomunicaciones	Suplantación de identidad o acceso no autorizado por desprotección de equipos móviles corporativos	4	4	16
23	Ausencia o no disponibilidad del personal crítico de TI	Pérdida de información por falta de traslado de copias de seguridad hacia el servicio de custodia.	6	8	48
24	Ciberataque	Indisponibilidad de los Sistemas por ataques de denegación de servicio (DDoS) a aplicaciones críticas	8	8	64
25	Falla de Hardware o Software	Pérdida de información por uso de software sin soporte del fabricante	6	8	48
26	Pandemia y/o Epidemia	Indisponibilidad de los servicios por falta de personal técnico	6	6	36

INSTITUTO NACIONAL DE OFTALMOLOGÍA · Oficina de Estadística e Informática ·

10.5. Identificación de controles existentes

La identificación de controles existentes, permiten conocer que tan protegidos están los servicios de TI del INO frente a cada amenaza.

Los controles existentes son:

- Acuerdos de niveles de servicio con proveedor de servicio de internet.
- Sistema de control de acceso al Centro de Datos
- Mantenimiento de Tableros eléctrico y UPS. El mantenimiento de los tableros eléctricos está a cargo de Servicios Generales de la Oficina de Administración
- Mantenimiento para equipos de aire acondicionado del Centro de Datos. El mantenimiento está a cargo de Servicios Generales de la Oficina de Administración.
- Alarma contra incendios en el Centro de Datos.
- Respaldo de información en cintas almacenadas en el Centro de Datos.
- Solución antivirus instalada en los servidores de red y computadoras.
- Actualización mensual de parches de seguridad de sistemas operativos en servidores.
- Seguridad perimetral gestionada.
- Uso de conexiones remotas seguras con VPN.

INSTITUTO NACIONAL DE OFTALMOLOGÍA · Oficina de Estadística e Informática ·

11. ESCENARIOS DE RIESGO

Considerando los servicios de TI, y luego de realizar el análisis de riesgos, se han determinado lossiguientes escenarios de riesgo:

Ítem	Escenario	Descripción
a	Destrucción e indisponibilidad del Centro de Datos	En este escenario se considera que los recursos informáticos alojados en el Centro de Datos se encuentran indisponibles a causa de la destrucción originada por un sismo, inundación, incendio, ataque terrorista o intento de denegación de servicios.
b	Indisponibilidad de servidores críticos por falla de hardware o software	En este escenario se considera la indisponibilidad de los servicios críticos causados por una falla física o lógica de los servidores.
c	Indisponibilidad en los servicios críticos por la ocurrencia de un ciberataque	En este escenario se considera la indisponibilidad de los sistemas de información como resultado de un ciberataque.
d	Indisponibilidad en los servicios críticos por falla en la energía eléctrica en el Centro de Datos	En este escenario se considera que el suministro de energía eléctrica del Centro de Datos se encuentre indisponible ocasionando la indisponibilidad de los servicios de tecnologías de la información y pérdida de comunicación en los equipos que conforman la infraestructura tecnológica.
	Indisponibilidad de los servicios críticos por ausencia o	En este escenario se considera que no se encuentra disponible el personal necesario para la administración y gestión de la infraestructura tecnológica y servicios de

INSTITUTO NACIONAL DE OFTALMOLOGÍA · Oficina de Estadística e Informática ·

	indisponibilidad del personal crítico	tecnología, lo cual puede traer como consecuencia la indisponibilidad de los mismos.
f	Indisponibilidad de los servicios críticos por falla en los equipos de comunicaciones	En este escenario se considera que los equipos de redes y comunicaciones se encuentren indisponibles como resultado de una falla física o lógica, lo cual trae como consecuencia la caída de servicios informáticos y pérdida de comunicación en los equipos que conforman la infraestructura tecnológica.

12. ESTRATEGIAS DE RECUPERACIÓN

Se proponen las posibles soluciones de recuperación de los escenarios de riesgos, incluyendo estrategias preventivas y correctivas.

Se han seleccionado alternativas para los escenarios de amenaza identificados que cumplen con los tiempos de recuperación identificados en el Análisis de Impacto Estratégico.

A continuación, se indican las posibles estrategias de recuperación:

a) Destrucción de los recursos informáticos alojados en el centro de datos como resultado de un sismo, inundación o incendio.

- Implementar un Centro de Datos de contingencia en las instalaciones de un proveedor de hosting, además que en caso se presente un escenario de sismo, el proveedor también pueda proporcionar servicios de comunicaciones para el restablecimiento de los servicios críticos.
- Virtualizar los servidores físicos para mejorar los tiempos de recuperación en caso de falla de hardware.
- Realizar copias de respaldo de instaladores de las aplicaciones, de software base, sistema operativo, utilitarios, etc.

INSTITUTO NACIONAL DE OFTALMOLOGÍA · Oficina de Estadística e Informática ·

- Almacenar las copias de respaldo diarias en un ambiente separado del Centro de Datos.
- Asegurarse de contar con enlaces redundantes con el Centro de Datos alterno.
- Contar con switches de respaldo que como mínimo sean de capa 2, para uso de Core y Distribución.
- Implementar sistema de extinción de incendio en el Centro de Datos.
- Eliminar todo material inflamable del ambiente de Centro de Datos.
- Contratar un servicio de mantenimiento preventivo y correctivo para el UPS y banco de baterías.

b) Indisponibilidad de servidores críticos por falla de hardware o software.

- Implementar alta disponibilidad en los servidores virtualizados.
- Virtualizar los servidores físicos para mejorar los tiempos de recuperación en caso de falla de hardware.
- Contar con Acuerdos de Niveles de Servicio (SLA) con los proveedores para que en caso sea necesario, puedan sustituir de manera inmediata los servidores físicos
- Programación de revisiones anuales de obsolescencia tecnológica de las partes internas de los servidores informáticos, para realizar la renovación de las mismas, en caso se requiera.

c) Indisponibilidad en los servicios críticos por la ocurrencia de un ciberataque.

- Mantener actualizado los parches de seguridad en servidores y estaciones de trabajo.
- Mantener actualizado el software de protección anti-malware en cada servidor y estación de trabajo.
- Mantener controles de seguridad perimetral como Firewall, AntiDDoS, UTM gestionado.
- Contratar el servicio de seguridad de aplicaciones Web como WAF.

INSTITUTO NACIONAL DE OFTALMOLOGÍA · Oficina de Estadística e Informática ·

- Desarrollar planes de sensibilización en materia de seguridad de la información y buenas prácticas en el uso de los sistemas informáticos.
- Mantener el monitoreo del rendimiento y consumo de los recursos en los servidores.
- Realizar pruebas anuales de Hacking Ético de terceros especializados.

d) Indisponibilidad en los servicios críticos por falla en la energía eléctrica en el Centro de Datos

- Contratar un servicio de mantenimiento preventivo y correctivo para el UPS, pozo a tierra y banco de baterías.
- Implementar un tablero de transferencia automático (Bypass) en el Centro de Datos para asegurar la continuidad eléctrica ante fallas del sistema de UPS.
- Implementar un sistema de UPS redundante con circuitos independientes que alimenten a los servidores y quipos críticos del Centro de Datos.
- Configurar el monitoreo remoto del UPS con alertas en caso de detectarse falla en el suministro eléctrico y/o banco de baterías.
- Realizar el apagado de los equipos, mientras se cuente con energía del UPS.
- Evaluar contar con un tablero de transferencia (Bypass) en el suministro eléctrico, para asegurar una mínima interrupción de energía ante trabajos de mantenimiento.
- Evaluar el implementar un generador eléctrico para proveer energía al Centro de Datos en casos de falla de la red eléctrica pública.

e) Indisponibilidad de los servicios críticos por ausencia o indisponibilidad del personal crítico

- Eliminar la dependencia funcional de los puestos críticos, capacitando a un reemplazo para cada rol, de tal manera que pueda asumir las funciones en caso el personal principal se encuentre indispuesto.
- Entrenar al personal de la OEI en el proceso de recuperación de los servicios de TI. La capacitación debe ser planificada, estructurada y acorde con las exigencias de recuperación. El entrenamiento se debe evaluar para verificar que se ha logrado sus objetivos.
- Elaborar un programa de vacaciones que garantice la presencia permanente del personal crítico de las diferentes áreas y procesos de OEI, tales como soporte técnico, redes y comunicaciones, sistemas de información y bases de datos, así como seguridad de la información.
- Elaborar una base de datos de conocimiento, en caso el personal encargado de ciertos procedimientos, tanto principal, como de reemplazo se encuentren indispuestos.

f) Indisponibilidad de los servicios críticos por falla en los equipos de comunicaciones

- Contar con switches de respaldo que como mínimo sean de capa 3 de modelo OSI, almacenados en un ambiente separado del Centro de Datos.
- Realizar copias de respaldo periódicas de la configuración de los equipos de comunicaciones.
- Mantener los Acuerdos de Niveles de Servicio (SLA) con los proveedores para que en caso sea necesario, puedan sustituir de manera inmediata los equipos de comunicaciones del Centro de Datos.

INSTITUTO NACIONAL DE OFTALMOLOGÍA - Oficina de Estadística e Informática - REPÚBLICA DEL PERÚ

13. PLAN DE RECUPERACIÓN

Una vez identificados los escenarios de riesgos, se desarrollan los Planes de Recuperación.

No	Escenario	Detecta Situación	Estrategia	Ejecuta el plan	Autorizado para activar el plan
1	Destrucción del Centro de Datos como resultado de un sismo, inundación o incendio	Personal del OEI	Activación del Plan de Recuperación de los servicios Informáticos	Equipo Técnico de la OEI	Jefe de OEI
2	Indisponibilidad de servidores críticos físicos por falla de hardware o software	Personal del OEI	Activación del Plan de Recuperación de los servicios Informáticos	Equipo Técnico de la OEI	Jefe de OEI
3	Indisponibilidad en los servicios críticos por la ocurrencia de un ciberataque	Personal del OEI	Activación del Plan de Recuperación de los servicios Informáticos	Equipo Técnico de la OEI	Jefe de OEI
4	Indisponibilidad en los servicios críticos por falla en la energía eléctrica en el Centro de Datos	Personal del OEI	Activación del Plan de Recuperación de los servicios Informáticos	Equipo Técnico de la OEI	Jefe de OEI.
5	Indisponibilidad de los servicios críticos por ausencia o	Personal del OEI	Activación del Plan de Recuperación	Equipo Técnico de la OEI	Jefe de OEI

	indisponibilidad del personal crítico		de los servicios Informáticos		
6	Indisponibilidad de los servicios críticos por falla en los equipos de comunicaciones	Personal del OEI	Activación del Plan de Recuperación de los servicios Informáticos	Equipo Técnico de la OEI	Jefe de OEI

Notificación de Activación del Plan

La notificación es responsabilidad del Jefe de la Oficina de Estadística e Informática, quien está autorizado para activar el Plan e informar al personal de Operaciones de TI y Desarrollo de Software quienes encabezarán los grupos de recuperación que a su vez informarán a losmiembros del Grupo de Trabajo para la Gestión de Riesgos de Desastres acerca del incidente y de las acciones a ser adoptadas.

Plan de Contingencia y Recuperación de Servicios de TIC

El Plan de Recuperación de los Servicios de Tecnología de la Información está alineadoa los escenarios de mayor nivel de riesgo, identificados en la Matriz de Riesgos, los cuales serán abordados en planes independientes, tal como se indica en el siguiente cuadro:

N°	Escenario	Nivel de Riesgo	Plan de Recuperación
1	Destrucción del Centro de Datos como resultado de	Alto	PR-01

	un sismo, inundación o incendio		
2	Indisponibilidad de servidores críticos por falla de hardware o software	Alto	PR-02
3	Indisponibilidad en los servicios críticos por la ocurrencia de un ciberataque	Alto	PR-03
4	Indisponibilidad en los servicios críticos por falla en la energía eléctrica en el Centro de Datos	Alto	PR-04
5	Indisponibilidad de los servicios críticos por ausencia o indisponibilidad del personal crítico	Medio	PR-05
6	Indisponibilidad de los servicios críticos por falla en los equipos de comunicaciones	Alto	PR-06

Los Planes de recuperación se encuentran en el **Anexo 01**

INSTITUTO NACIONAL DE OFTALMOLOGÍA · REPÚBLICA DEL PERÚ · Oficina de Estadística e Informática

14. PLAN DE PRUEBAS

14.1 Propósito y alcance

El propósito del Plan de Pruebas es validar las actividades del Plan de Recuperación de los servicios Informáticos, las capacidades del personal de TI en la ejecución del plan y verificar que el desarrollo de las actividades sea correcto.

El alcance de las pruebas del Plan de Recuperación de los servicios Informáticos es probar el restablecimiento de la operatividad de los recursos que forman parte de los escenarios de riesgo.

14.2 Escenarios y estrategias

Los escenarios de pruebas deben simular la inhabilitación de las operaciones en el Centro de Datos con el fin de realizar una prueba que contemple la ejecución de los planes de acción descritos en Plan de Recuperación de los servicios Informáticos, es importante que estas pruebas se coordinen con las áreas usuarias.

En la etapa de planificación de las pruebas se especifica los aspectos que debe cubrir cada escenario

INSTITUTO NACIONAL DE OFTALMOLOGÍA · REPÚBLICA DEL PERÚ · Oficina de Estadística e Informática

Prueba:	**Prueba de Conocimiento del Plan de Continuidad Informático**
Responsable:	Responsable de la unidad Informática
Periodicidad:	Anual
Descripción de la Prueba	

Este escenario consiste en evaluar mediante un test escrito el nivel de conocimiento del equipo del Plan de Recuperación de los servicios Informáticos, así como sus responsabilidades. **Anexo 02**.

Después de la prueba

El responsable debe elaborar un informe de los resultados obtenidos que contenga los siguientes puntos:

- Tipo de prueba:
- Día:
- Duración:
- Participantes:
- Resultados:
- Acciones Correctivas:

De ser necesario se deben actualizar el Plan de Recuperación de los servicios Informáticos con las lecciones aprendidas de esta prueba.

INSTITUTO NACIONAL DE OFTALMOLOGIA · Oficina de Estadística e Informática ·

Prueba:	**Prueba de Contingencia de los servicios Informáticos**
Responsable:	Responsable de la unidad Informatica
Periodicidad:	Anual

Descripción de la Prueba

Este escenario consiste en simular la caída de los servidores poniendo en marcha la activación de servidores de contingencia (máquinas virtuales o hosting alterno).

Antes de la Prueba

- Informar a las áreas usuarias la fecha y ventanas horarias de indisponibilidad de los servicios de TI relacionados con los servidores involucrados.
- Solicitar la participación de usuarios de las áreas de negocio para realizar pruebas en el escenario de contingencia.
- Coordinar con proveedores de servidores o hosting, la fecha de realización de la prueba.
- Realizar copias de respaldo de las máquinas virtuales alojadas en el Storage principal.

El día de la prueba

- Confirmar la asistencia del personal de TI.
- Bajar los sistemas informáticos de la plataforma virtualizada.
- Apagar/desconectar el servidor SQL.
- Apagar los servidores involucrados.
- Realizar la actividad descrita en el Plan de Contingencia Informático.
- Realizar pruebas de conectividad de los sistemas, así como al servidor de archivos, acceso a internet y correo electrónico.
- Documentar todos los problemas identificados. Usar el **Anexo 03**.

INSTITUTO NACIONAL DE OFTALMOLOGIA · Oficina de Estadística e Informática ·

Después de la prueba

Los responsables deben elaborar un informe de los resultados obtenidos en el

Anexo 03 que contenga los siguientes puntos:

- Tipo de prueba:
- Día:
- Duración:
- Participantes:
- Resultados:
- Acciones Correctivas:

De ser necesario se deben actualizar el Plan de Recuperación de los servicios Informáticos con las lecciones aprendidas de esta prueba.

15. PLAN DE COMUNICACIÓN Y CAPACITACIÓN

Las previsiones para las situaciones de contingencia no pueden considerarse fiables hasta que se hayan ejercitado. La comunicación y sensibilización hacia el personal del INO, ayudará a mantener y mejorar las acciones de respuesta ante eventos que generen indisponibilidad de los servicios o aplicaciones tecnológicas de mayor criticidad para la Institución.

Para la comunicación y capacitación se consideran los siguientes aspectos:

PERSONAL:

- El equipo de soporte Informático.
- El equipo de Desarrollo de sistemas.
- El equipo de redes y comunicaciones
- El equipo de administración de servidores y seguridad Informática
- El equipo de administradores de la Web y seguridad perimetral.

INSTITUTO NACIONAL DE OFTALMOLOGÍA · Oficina de Estadística e Informática ·

TEMAS:

- Responsabilidades en el Plan de Recuperación de los servicios Informáticos.
- Procedimientos de recuperación.
- Pruebas de recuperación.
- Mejora continua del Plan de Recuperación de los servicios Informáticos.

Las capacitaciones deberán ser ejecutadas en grupos objetivos diferentes, considerando en uno de ellos al personal de soporte Informático, Desarrollo de sistemas, redes y comunicaciones y el otro grupo a la personal administración de servidores y seguridad Informática y a los administradores de la Web y seguridad perimetral.

El INO ha establecido las siguientes actividades como parte del plan de comunicación y capacitación, las mismas que deben ejecutarse por lo menos una vez al año debiendo difundir las actualizaciones del Plan de Recuperación de los servicios Informáticos y responsabilidades del personal sobre reactivar las operaciones en caso de interrupción:

Actividad	Descripción
Capacitación	Preparar una presentación que resuma el Plan de Recuperación de los servicios Informáticos .
	a) Imprimir copias del plan para ser distribuidas durante la capacitación.
	b) Convocar al personal mencionado en el Plan de Recuperación de los servicios Informáticos .
	c) Desarrollar la capacitación al personal de OEI

INSTITUTO NACIONAL DE OFTALMOLOGÍA · Oficina de Estadística e Informática ·

	d) Con la retroalimentación obtenida, evaluar la modificación del Plan de Recuperación de los servicios Informáticos
Evaluación	a) Preparar una evaluación escrita de conocimiento para cada persona del equipo del plan de Contingencia Informático para verificar las responsabilidades que tienen.
	b) Con la retroalimentación obtenida, evaluar la modificación del Plan de Recuperación de los servicios Informáticos .

16. ANEXO

- Anexo 01: plan de recuperación

ANEXO 01

Plan de Recuperación

Plan de Recuperación:	PR-01
Escenario:	En este escenario se considera que los recursos informáticos alojados en el Centro de Datos se encuentran indisponibles a causa de la destrucción originada por un sismo, inundación o un incendio.
Estrategia	1. Implementar un centro de contingencia en las instalaciones de un proveedor de hosting, además que en caso se presente un escenario de contingencia, el proveedor también pueda proporcionar servicios de comunicaciones para el restablecimiento de los servicios críticos.
	2. Virtualizar los servidores físicos para mejorar los tiempos de recuperación en caso de falla de hardware.
	3. Realización de copias de instaladores de las aplicaciones, de software base, sistema operativo, utilitarios, etc.
	4. Implementar enlaces redundantes con el Centro de Datos alterno
	5. Contar con switches de respaldo que como mínimo sean de capa 3 de modelo OSI.
Servicios TI:	Analizando el escenario de riesgo y considerando la lista de servicios y activos, se determina que los servicios de TI a recuperar se pueden agrupar y recuperar en el siguiente orden de prioridad:
	1. Red de datos (Equipos de comunicaciones)
	2. Internet y Seguridad Perimetral
	3. Servicio de Autenticación de Red

INSTITUTO NACIONAL DE OFTALMOLOGÍA · Oficina de Estadística e Informática ·

	4.	Base de datos.
	5.	Sistema de almacenamiento (Storage)
	6.	Servidores Físicos
	7.	Sistema de Virtualización (Hipervisor)
	8.	Servidores Virtuales