PLAN DE CONTINGENCIA DE TECNOLOGÍAS DE INFORMACIÓN INSTITUTO SUPERIOR TECNOLÓGICO REPÚBLICA FEDERAL DE ALEMANIA

INTEGRANTES

Collantes Portilla Candy

Montalván Pintado Edilsa

Nanfuñay Carrión Javier

Neyra Quesquen Renzo

Chiclayo, Julio del 2023

CONTENIDO

1. INTRODUCCIÓN

Una Organización es susceptible a encontrarse frente a una situación de emergencia que puede originar efectos adversos ocasionando pérdidas de vidas humanas, ambientales, materiales, entre otros. El tiempo y la capacidad de respuesta con que cuenta la empresa son piezas claves para enfrentar, controlar cualquier situación de emergencia que se presente tanto externo como internamente.

En tal sentido, y como buena práctica de TI se ha elaborado el Plan de Contingencia de tecnologías de la información del ISTRFA, dado que la Institución es vulnerable a diferentes hechos que pueden interrumpir los servicios informáticos y afectar el normal funcionamiento de las actividades en la Institución, lo que no sólo afecta a usuarios internos sino también a usuarios externos asimismo el Plan se encuentra alineado al Objetivo estratégico Institucional "Fortalecer la capacidad operativa del ISTRFA".

Así, el presente plan establece los objetivos, el alcance y metodología del plan, a fin de lograr minimizar el impacto negativo de la interrupción de los servicios informáticos, contribuyendo a que la Institución esté preparada ante cualquier eventualidad de contingencia a nivel de tecnología de información, toda vez que se está considerando acciones del antes, durante y después de los incidentes.

2. MARCO TEORICO

2.1 PLAN DE CONTINGENCIA

Es un documento que reúne un conjunto de procedimientos alternativos para facilitar el normal funcionamiento de las Tecnologías de Información y de Comunicaciones (TIC), cuando alguno de sus servicios se ha afectado negativamente por causa de algún incidente interno o externo a la organización.

Este plan permite minimizar las consecuencias en caso de incidente con el fin de reanudar las operaciones en el menor tiempo posible en forma eficiente y oportuna. Asimismo, establece las acciones a realizarse en las siguientes etapas:

- **Antes** de la eventualidad, se contemplará la evaluación de la situación actual de las tecnologías de información en la Institución, a fin de mitigar el nivel de riesgo de las eventualidades. Su importancia radica en que las acciones permitirán disminuir la probabilidad de ocurrencia de una eventualidad que afecte los servicios informáticos.

- **Durante** la eventualidad, se contemplan estrategias frente a las emergencias. Las acciones descritas en estas estrategias permitirán recuperar la actividad normal frente a la emergencia.

- **Después** de la eventualidad, se contempla estrategias para la restauración o recuperación**.** Incluye las acciones a realizarse para regresar al estado normal de los servicios informáticos.

3. OBJETIVOS

3.1 Objetivo General

Establecer disposiciones para garantizar la continuidad de los servicios informático del ISTRFA, en caso de la ocurrencia de alguna eventualidad que interrumpa su funcionamiento, a fin que su restablecimiento sea en el menor tiempo posible.

3.2 Objetivo Específicos

- Identificar, analizar y proteger los servicios informáticos del ISTRFA ante riesgos posibles que pueden afectarlos y, por ende, afectar las operacionesde la Institución.
- Establecer actividades de preparación y acciones que permitan una restauración adecuada de los servicios informáticos en caso de interrupciones, de forma que no se tenga pérdida o afectación a la información.
- Contar con personal debidamente capacitado y organizado para afrontar adecuadamente las contingencias que puedan presentarse con respecto a los servicios informáticos del ISTRFA.
- Establecer actividades que permitan evaluar los resultados obtenidos de la ejecución del plan de contingencia, permitiendo a su vez una mejora continua a dicho plan.

4. BASE LEGAL

- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
- Ley Nº 28551, Ley que establece la obligación de elaborar y presentar planes de contingencia
- Ley N° 28613, Ley del Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica.
- Ley Nº 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
- 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° 026-2014-PCM, que aprueba el Reglamento de Organización y Funciones del Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica.
- Decreto Supremo N° 032·2007-ED que aprueba el Texto Único Ordenado de la Ley N° 28303, Ley Marco de Ciencia, Tecnología e Innovación Tecnológica y reglamento.
- Decreto Supremo N° 034-2014-PCM, Decreto Supremo que aprueba el Plan Nacional de Gestión del Riesgos de Desastres - PLANAGERD 2014-2021.
- Decreto Supremo Nº 048-2011-PCM, Decreto Supremo que aprueba el Reglamento de la Ley Nº 29664, que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
- Resolución Ministerial N° 028-2015-PCM, aprobación de los Lineamientos para la Gestión de la Continuidad Operativa de las entidades públicas en los tres niveles de Gobierno.
- 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.
- Resolución Contraloría General Nº 320-2006-GC que aprueba las Normas de Control Interno para el Sector Público.
- Resolución de Presidencia N° 079-2021-ISTRFA-P, Que aprueba el Plan de Gobierno Digital del Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica 2021-2023
- Directiva N° 005-2021-ISTRFA-SG – "Directiva que regula el uso de los recursos informáticos en el Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica – ISTRFA.

5. ALCANCE

Las disposiciones contenidas en el presente Plan de Contingencia son de cumplimiento obligatorio para las Unidades Ejecutoras que conforman el del ISTRFA y sus respectivas unidades de organización.

6. DEFINICIONES

6.1 Amenaza

Causa potencial de un incidente de seguridad de la información no deseado, que puede resultar en un daño para la organización o el sistema**.**

6.2 I+D+i

Investigación científica, desarrollo tecnológico e innovación tecnológica

6.3 Plan de Contingencia

Plan que contiene las acciones a ejecutar en caso de la materialización del riesgo, con el fin de garantizar la continuidad de los servicios y parque informático del ISTRFA, en caso de la ocurrencia de alguna eventualidad que interrumpa sufuncionamiento.

6.4 Probabilidad

Posibilidad de que un evento determinado ocurra en un periodo de tiempo dado.

6.5 Riesgo

Posibilidad de que suceda algún evento adverso que tendrá un impacto sobre el cumplimiento de los objetivos institucionales o de los procesos para la presentación de servicios al ciudadano. Se expresa en términos de probabilidad y consecuencias.

6.6 Sistema de Información

Es un conjunto de elementos organizados a fin de administrar datos e información necesarios para lograr un objetivo. Dichos sistemas están formados por personas, equipos y procedimientos.

6.7 Vulnerabilidad

Debilidad de un activo o grupo de activos o controles, que pueden ser explotadas por una o varias amenazas. Una vulnerabilidad en sí misma no causa daños.

7. METODOLOGÍA DE TRABAJO

Si bien los planes de contingencia de tecnologías de la información se realizan a fin de prevenir fallas o accidentes en las operaciones de una entidad, para la elaboración de los mismos es importante tener en cuenta el estado de la infraestructura informática y de los servicios informáticos de la Institución, por lo que los planes de cada Institución son muy propios.

En ese sentido, el desarrollo del Plan se basa en las siguientes seis (6) fases:

- ✓ Fase 1: Planificación
- ✓ Fase 2: Determinación de Vulnerabilidades
- ✓ Fase 3: Estrategias del Plan de Contingencia
- ✓ F ase 4: Elaboración del Plan de Contingencia
- ✓ Fase 5: Implementación del Plan de Contingencia
- ✓ Fase 6: Monitoreo

A continuación, se detallan cada uno de las fases:

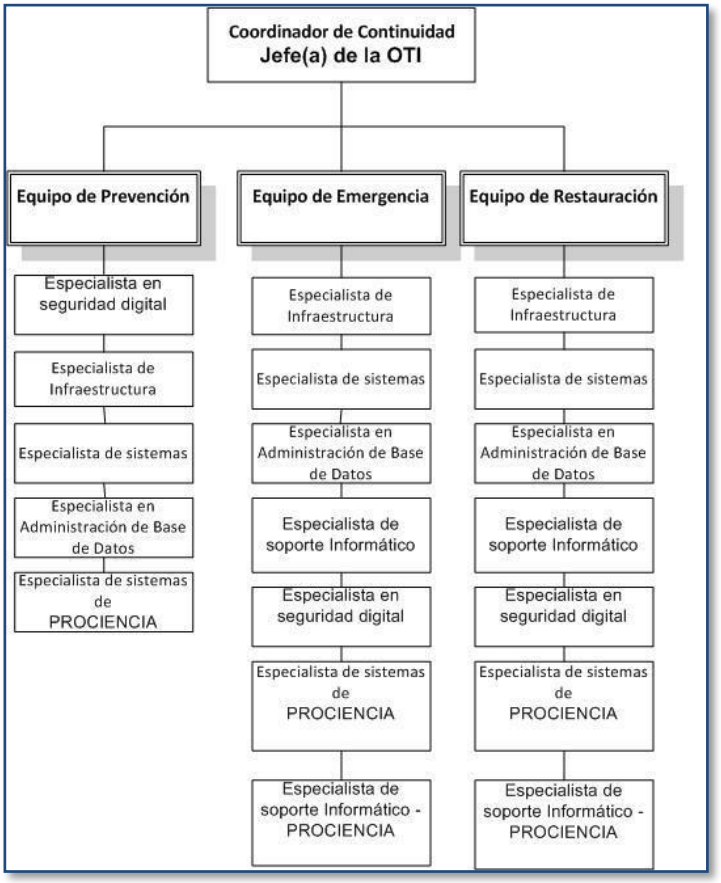
7.1 Fase 1: Planificación

7.1.1 Organización

La Oficina de Tecnologías de la Información (OTI), depende directamente de la Oficina General de Administración (OGA), y es responsable de administrar y brindar soluciones informáticas y soporte técnico en materia de tecnologías de la Información (TIC) a los órganos del ISTRFA, para la mejor ejecución de sus funciones, así como, desarrollar el soporte tecnológico y soluciones informáticas para la operatividad de la red nacional de información científica e interconexión telemática.

Tiene dentro de sus funciones, elaborar y proponer lineamientos, directivas y la homologación de tecnologías informáticas y de comunicaciones para el ISTRFA, sus órganos, proyectos y programas. Para el funcionamiento del Plan de Contingencias de Tecnologías de la información se ha establecido, el siguiente organigrama describiendo los roles y los equipos que conforman el plan de contingencias de TI y está conformado por el personal de la Oficina de Tecnologías de la información (OTI) del ISTRFA y el personal de la Unidad de Tecnologías de Información (UTI) de PROCIENCIA. Los cuáles serán designados a través de memorando.

Organigrama de la organización del plan de contingencias de Tecnologías de la Información



Fuente: Elaboración propia

7.1.2 Roles, funciones y responsabilidades dentro del Plan

A continuación, se describe los roles, responsabilidades y funciones que deben desarrollar los distintos equipos del Plan de Contingencia de Tecnologías de la Información:

a) Coordinador de Continuidad.

Sera representado por el/la jefe(a) de la OTI y tiene las siguientes funciones:

- Coordinar, dirigir y decidir respecto a acciones o estrategias a seguir en caso de una continencia dado.
- Monitorear, supervisar y vigilar la recuperación de infraestructura de TI en los laboratorios.
- Tomar decisión de activar el Plan de Contingencia de Tecnologías de la Información.
- Declarar el evento de término de la ejecución de las operaciones del Plan de Contingencia de Tecnologías de la Información, cuando las operaciones de los laboratorios hayan sido restablecidas.

b) Equipo de Prevención

Es el equipo encargado de ejecutar las acciones preventivas, antes que ocurra un siniestro o desastre, con el fin de evitar se concrete el siniestro o desastre y en caso ocurriese, tener todas las herramientas o medios necesario para realizar la recuperación de los servicios de tecnologías de la información, en el menor tiempo posible.

El responsable del Equipo de Prevención es el Especialista en seguridad digital y es designado mediante Memorando por el Coordinador de Continuidad. A continuación, se detalla las funciones por cada miembro del equipo de prevención:

Especialista en seguridad digital:

- Establecer y supervisar los procedimientos de seguridad de los servicios de TI.
- Coordinar la realización de pruebas de restauración de hardware y Software.
- Participar en las pruebas de simulacro.
- Verificar las pruebas de copias de respaldo (backup).

Especialista de Infraestructura:

- Contactar a los proveedores para el reemplazo de hardware, software y/o activación de servicios para los sistemas afectados.
- Verificar la realización del mantenimiento preventivo de los equipos de los laboratorios.
- Mantener actualizado el inventario de hardware, software de los laboratorios del ISTRFA.
- Ejecutar y verificar las copias de respaldo (backup)
- Programar el mantenimiento preventivo de los equipos de comunicaciones y de los equipos de Centro de Datos, considerando el tiempo de vida útil y garantía de los mismos.
- Elaborar informes técnicos de conformidad, luego de los

mantenimientos efectuados.
- Elaborar informes periódicos del funcionamiento de los laboratorios.
- Mantener actualizado el diagrama de red, servidores y la documentación de configuración de los equipos de comunicaciones.
- Monitorear la red y definir medidas preventivas para minimizar las contingencias.
- Realizar pruebas previas de recuperación.
- Monitorear el funcionamiento de la central telefónica.
- Mantener actualizado el software que utiliza la central telefónica.
- Mantener actualizado la lista de teléfonos y anexos.

Especialista de sistemas de ISTRFA:
- Coordinar el manteamiento de los sistemas de información existentes.
- Mantener un control actualizado de las versiones de las fuentes de los sistemas de información y de los portales de la entidad.
- Mantener un control de la documentación y validación de los manuales de los sistemas en producción.
- Coordinar periódicamente las pruebas de restauración de las fuentes de los sistemas informáticos de la entidad.

Especialista en Administración de Base de Datos:
- Realizar copias de respaldo de las Bases de Datos de los aplicativos de la entidad.
- Realizar las pruebas de restauración de base de datos en coordinación con la especialista de seguridad de la Información.

Especialista de sistemas de PROCIENCIA
- Coordinar el manteamiento de los sistemas de información existentes.
- Mantener un control actualizado de las versiones de las fuentes de los sistemas de información y de los portales de la entidad.
- Mantener un control de la documentación y validación de los manuales de los sistemas en producción.
- Coordinar periódicamente las pruebas de restauración de las fuentes de los sistemas informáticos de la entidad.

c) Equipo de Emergencia

Es el equipo encargado de ejecutar las acciones requeridas durante la materialización del siniestro o desastre. Con el fin de mitigar el impacto que pueda tener en los equipos de TI del ISTRFA, y procurando salvaguardar su pérdida o deterioro.

El responsable del Equipo de emergencia es el responsable de infraestructura y es designado mediante Memorando por el Coordinador de Continuidad

A continuación, se detalla las funciones por cada miembro del equipo de emergencia:

Especialista de Infraestructura:

- Informar sobre el desastre o incidencia al coordinador de Continuidad
- Ejecutar las acciones de emergencia en los equipos informáticos y los componentes instalados en los laboratorios del ISTRFA.
- Realizar la evaluación de condiciones de los equipos informáticos y comunicaciones de los laboratorios durante la emergencia.
- Ejecutar las acciones de emergencia en los equipos celulares del ISTRFA.
- Informar al coordinador de Continuidad de OTI las acciones de emergencias ejecutadas.

Especialista de sistemas-ISTRFA

- Coordinar acciones para la verificación del estado de los sistemas informáticos, alojados en los servidores de aplicaciones.
- Coordinar acciones para verificar el estado de la base de datos de los sistemas informáticos del ISTRFA.
- Coordinar acciones para verificar los logs de los sistemas informáticos afectados durante la emergencia.

Especialista en Administración de Base de Datos:

- Realizar la evaluación de la información almacenada en las diferentes bases de datos, durante la emergencia.

Especialista de soporte informático

- Realizar la evaluación de la afectación de los equipos informáticos utilizado por los usuarios finales (Computadoras, estabilizadores, impresoras, teléfonos fijos, entre otros).
- Informa al coordinador de continuidad, sobre casos críticos encontrados en los equipos de los usuarios finales que afecta la continuidad de operaciones o pérdida de información.

Especialista en seguridad Digital:

- Apoyar en labores de verificación y validación de operación de los servicios de TI.

Especialista de sistemas-PROCIENCIA

- Coordinar acciones para la verificación del estado de los sistemas informáticos, alojados en los servidores de aplicaciones.
- Coordinar acciones para verificar el estado de la base de datos de los sistemas informáticos de la entidad.
- Coordinar acciones para verificar los logs de los sistemas informáticos afectados durante la emergencia.

Especialista de soporte informático-PROCIENCIA

- Realizar la evaluación de la afectación de los equipos informáticos utilizado por los usuarios finales (Computadoras, estabilizadores, impresoras, teléfonos fijos, entre otros).
- Informa al coordinador de continuidad, sobre casos críticos encontrados en los equipos de los usuarios finales que afecta la continuidad de operaciones o pérdida de información.

d) Equipo de Restauración.

Es el equipo encargado de ejecutar todas las acciones después de haber sido controlado el desastre o siniestro, con el fin de restituir en el menor tiempo posible la operatividad de los equipos tecnológico y recuperar el servicio informático del ISTRFA, de manera conjunta con el coordinador de Continuidad y los especialistas.

El responsable del Equipo de restauración es el Especialista de infraestructura y es designado mediante Memorando por el Coordinador de Continuidad.

A continuación, se detalla las funciones por cada miembro del equipo de restauración:

Especialista de Infraestructura:

- Iniciar el proceso de recuperación de los servicios de TI, realizando pruebas de funcionamiento en los equipos afectados de infraestructura de los laboratorios del ISTRFA.
- Restaurar la información de los equipos afectados de la infraestructura informática que afecten los servicios de los laboratorios del ISTRFA.
- Informar al coordinador de Continuidad de TI las acciones de recuperación ejecutadas.
- Elaborar un informe técnico, que incluya las acciones de recuperación de los equipos de comunicación, central telefónica y de los equipos de los laboratorios.
- Iniciar el proceso de recuperación de los servicios relacionado a la Central telefónica del ISTRFA y de los equipos móviles.
- Realizar la evaluación de las condiciones de los equipos de telecomunicaciones, durante la emergencia.

Especialista de sistemas-ISTRFA

- Coordinar y verificar el estado de los sistemas alojados en los servidores de aplicaciones
- Coordinar el estado de la base de datos de los sistemas de información.
- Coordinar y monitorear la restauración de los sistemas de información y ejecución de pruebas para la verificación de su funcionalidad.
- Verificar que los sistemas de información estén funcionando correctamente.
- Elaborar un informe técnico que incluya la evaluación de condiciones de los sistemas de información del ISTRFA.

Especialista en Administración de Base de Datos:

- Verificar el funcionamiento de las bases de datos del ISTRFA
- En caso sea requerido, realizar la creación de base de datos en servidores alternos.
- Restaurar las copias de respaldo correspondientes.
- Realizar las pruebas de funcionamiento.
- Elaborar un informe técnico que incluya la evaluación de condiciones de los datos del ISTRFA, luego de afectado el proceso de

recuperación.

Especialista de soporte informático-ISTRFA

- Verificar el funcionamiento de los equipos de cómputo del ISTRFA afectada, distribuyendo el trabajo entre los técnicos de soporte.
- Solucionar problemas de conexión de los equipos informáticos, impresoras, escáner, entre otros.
- Elaborar un informe técnico que incluya la evaluación de condiciones de equipos informáticos del ISTRFA, luego de afectado el proceso de recuperación.

Especialista en seguridad en seguridad Digital:

- Supervisar la restauración de los servicios de TI.
- Validar la información documentada de los procedimientos de restauración utilizada.

Especialista de sistemas-PROCIENCIA

- Coordinar y verificar el estado de los sistemas alojados en los servidores de aplicaciones
- Coordinar el estado de la base de datos de los sistemas de información.
- Coordinar y monitorear la restauración de los sistemas de información y ejecución de pruebas para la verificación de su funcionalidad.
- Verificar que los sistemas de información estén funcionando correctamente.
- Elaborar un informe técnico que incluya la evaluación de condiciones de los sistemas de información de la Entidad.

Especialista de soporte informático - PROCIENCIA

- Verificar el funcionamiento de los equipos de cómputo del ISTRFA afectada, distribuyendo el trabajo entre los técnicos de soporte.
- Solucionar problemas de conexión de los equipos informáticos, impresoras, escáner, entre otros.
- Elaborar un informe técnico que incluya la evaluación de condiciones de equipos informáticos de la entidad, luego de afectado el proceso de recuperación.

7.2 Fase 2: Determinación de Vulnerabilidades

En esta fase se realiza la identificación de las aplicaciones críticas, los recursos y el periodo máximo de recuperación de los servicios de TI del ISTRFA, considerando todos los elementos susceptibles de provocar eventos que conlleven a activar la contingencia.

7.2.1 Procesos y recursos críticos

En este proceso se detallan los procesos, aplicaciones y recursos críticos con su expectativa del tiempo de recuperación:

Tabla N° 1 – Procesos y recursos críticos de TI

Proceso	Aplicaciones y/o recursos	Tiempo de Recuperación (RTO)
Gestión de infraestructura Tecnológica	Equipos de comunicaciones	6 h
	Cableado de red de datos	6 h
	Enlaces de cobre y fibra óptica para interconexión entre la sede central y el proveedor de servicios	4 h
	Sistema de almacenamiento	12 h
	Medios de respaldo (backup)	12 h
	Servidores de red críticos: Directorio Activo, File Server, Base de Datos,	24 h
Desarrollo y Mantenimiento de soluciones tecnológica	Sistemas de información administrativos	24 h
	Base de datos y repositorios utilizados por los sistemas y aplicativos.	12 h
Soporte Técnico de las Soluciones y Recursos Tecnológicos	Estaciones de trabajo del personal crítico (computadoras personales y portátiles)	24 h
Gestión de Gobierno Ti	Personal crítico responsable de los procesos de TIC	4 h

RTO: Tempe de recuperación objetivo, es determinado mediante Juicio de expertos.

7.2.2 Identificación de amenazas

Permite identificar aquellas amenazas que pudieran vulnerar los servicios de TI del ISTRFA, considerando la ubicación geográfica, el contexto actual de la sede central y centro de datos, así como del juicio de experto.

Tabla N° 2 – Tipos de Amenazas a los servicios de TI

N°	Amenaza (Evento)	Tipo
01	Terremoto/Sismo	Siniestros Naturales
02	Inundación y aniego en los laboratorios.	
03	Incendio en los laboratorios.	
04	Falla en telecomunicaciones.	Tecnológicos
05	Incidente de Seguridad informática.	
06	Falla de hardware y software.	
07	Falla del suministro eléctrico en los laboratorios y gabinetes de comunicación.	Físico y ambiental
08	Ausencia o no disponibilidad del personal crítico de TI.	Humanos

Una vez determinadas las amenazas que pueden afectar los recursos críticos de TI, se calcula el nivel de probabilidad de ocurrencia, para lo cual se utilizó los valores definidos en la metodología de Gestión de riesgos que se encuentra en la siguiente Tabla:

Tabla N° 3 – Determinación de la Probabilidad

Valor	Clasificación	Definición
1	Muy Bajo	**Puede que no se haya presentado u ocurrir en situaciones excepcionales** (Por Ejemplo: Nunca ha ocurrido)
2	Bajo	**Puede ocurrir en pocas situaciones** (Por Ejemplo: Ha sucedido en la historia de la institución)
3	Medio	**Puede ocurrir a largo plaz**o (Por Ejemplo: Ocurre una vez al año)
4	Alto	**Se produce por tendencia o constantemente** (Por Ejemplo: Ocurre una vez al mes)
5	Muy Alto	**Se produce a corto plazo y sin interrupciones** (Por Ejemplo: Ocurre una o más veces a la semana

A continuación, se detalla el resultado obtenido, en base a la metodología de gestión de riesgos, mediante la cual se ha determinado el valor de probabilidad por cada amenaza**:**

Tabla N°4 – Probabilidad estimada de las amenazas a los servicios de TI

N°	Amenaza (Evento)	Nivel de Probabilidad de ocurrencia (valor)	Nivel de Probabilidad Estimada
1	Sismo.	1	Muy Bajo
2	Inundación y aniego en los laboratorios.	1	Muy Bajo
3	Incendio.	1	Muy Bajo
4	Falla en telecomunicaciones.	3	Medio
5	Incidente de Seguridad informática.	2	Bajo
6	Falla del suministro eléctrico.	2	Bajo
7	Falla del hardware y software.	3	Medio
8	Ausencia o no disponibilidad del personal crítico de TI.	2	Bajo

7.2.3 Identificación de controles existentes

La identificación de controles existentes, permiten conocer que tan protegidos están los recursos de TI del ISTRFA frente a cada amenaza. Los controles existentes son los siguientes:

- Cámaras de vigilancia para la seguridad física de los bienes informáticos.
- Grupo electrógeno para los laboratorios operativo.
- Redundancia en los enlaces de comunicaciones (fibra óptica) y de internet, pero con el mismo proveedor.
- Sistema contra incendios en los laboratorios.
- Respaldo de información y custodia externa de medios de respaldo.

- Solución antivirus instalada en los servidores de red y computadoras.

7.2.4 Evaluación del Nivel de Riesgo

Para determinar el Nivel de Riesgo de un recurso de TI crítico del ISTRFA, se consideraron los controles existentes que mitigan la afectación de la amenaza descritos en el numeral 7.2.2, así como el valor del Nivel de Probabilidad de ocurrencia Identificado en la tabla N° 3 – Probabilidad estimadade las amenazas a los servicios de TI, y los valores definidos de acuerdo a la aplicación de la metodología de gestión de riesgos descrita tabla de impacto (Tabla N°5) y cálculo del nivel de riesgo (Tabla N° 7).

Para calcular el resultado del impacto, se considera el valor del nivel del impacto, definido en la aplicación de la metodología de Gestión de riesgos, de acuerdo a la siguiente tabla:

Tabla N°5 Determinación del Impacto:

Nivel	Descripción	Impacto
5	**Grave**	Si el evento llegara a presentarse, tendría un trágico impacto, comprometiendo la confidencialidad o integridad de información crítica de la entidad o la continuidad de las operaciones por paralización de los servicios críticos más allá de los tiempos tolerables por el negocio.
4	**Mayor**	Si el evento llegara a presentarse, tendría un alto impacto comprometiendo la confidencialidad o integridad de información crítica de la entidad o la continuidad de las operaciones por paralización de los servicios críticos más allá de los tiempos tolerables por el negocio (se puede llegar a comprometer documentos internos clasificados como confidenciales, paralizar o retrasarprocesos claves de la entidad por un tiempo considerable).
3	**Moderado**	Si el evento llegara a presentarse, tendría un moderado 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.
2	**Menor**	Si el evento llegara a presentarse, tendría un menor impacto (El impacto es leve y se puede prescindir del mismo en un tiempo limitado).
1	**Insignificante**	Si el evento llegara a presentarse, no representa un impacto importante para la entidad.

El valor obtenido ha sido en base a la metodología de Gestión de Riesgos (Tabla N°5) que ha determinado el impacto por cada amenaza, siendo el resultado siguiente:

Tabla N°6 Resultado del impacto de los servicios de TI

Item	Recursos Críticos / Amenazas (Eventos)	Terremoto	Inundación y aniego en los laboratorios	Incendio en los laboratorios	Falla en telecomunicaciones	Incidente de Seguridad informática	Falla del suministro eléctrico en los laboratorios y gabinetes de comunicación	Falla del hardware y software	Ausencia o no disponibilidad del personal crítico de TI	Pandemia y/o Epidemia
1	Equipos de comunicaciones.	4	4	5	5	5	2	3	2	1
2	Equipos de protección eléctrica del centro de datos (UPS) y grupo electrógeno	4	4	5	2	1	2	4	3	1
3	Aire acondicionado de los laboratorios.	4	4	5	1	1	2	4	3	1
4	Infraestructura de los laboratorios.	4	4	5	1	1	3	5	4	3
5	Cableado de red de datos.	4	4	5	3	1	1	3	2	1
7	Sistema de almacenamiento (storage).	4	4	5	3	4	2	4	3	1
8	Servidores de red	4	4	5	3	5	2	5	4	1
9	Medios de respaldo	4	4	5	3	2	2	3	3	1
10	Sistemas de información y portales web	4	4	5	3	5	2	5	4	1
11	Base de datos utilizados por los sistemas y aplicativos.	4	4	5	3	5	2	5	4	1
12	Estaciones de trabajo del personal crítico (computadoras personales y portátiles)	4	4	5	3	5	2	3	3	2

Cálculo del Nivel de Riesgo: Se desarrolla considerando el mayor Nivel de Riesgo del recurso afectado por la amenaza que se está analizando. Para la identificación del Nivel de Riesgo se considera la siguiente matriz:

Tabla N° 7 Matriz del Nivel de Riesgo

PROBABILIDAD						
	Muy Alto (5)	5	10	15	20	25
	Alto (4)	4	8	12	16	20
	Medio (3)	3	6	9	12	15
	Bajo (2)	2	4	6	8	10
	Muy Bajo (1)	1	2	3	4	5
		Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Grave (5)
		IMPACTO				

A continuación, se obtiene el resultado de la evaluación del riesgo de los servicios de TI:

Tabla N° 8 – Resultado de la evaluación de riesgos de los servicios de TI

Item	Recursos Críticos / Amenazas (Eventos)	Terremoto	Inundación y aniego en los laboratorios	Incendio en los laboratorios	Falla en telecomunicaciones	Incidente de Seguridad informática	Falla del suministro eléctrico en los laboratorios y gabinetes de comunicación	Falla del hardware y software	Ausencia o no disponibilidad del personal crítico de TI	Pandemia y/o Epidemia
1	Equipos de comunicaciones.	8	8	5	15	5	6	9	4	1
2	Equipos de protección eléctrica de los laboratorios (UPS) y grupo electrógeno	8	8	5	6	2	6	12	9	1
3	Aire acondicionado de los laboratorios.	8	8	5	3	2	6	12	6	1
4	Infraestructura de los laboratorios.	8	8	5	3	1	9	15	8	3
5	Cableado de red de datos.	8	8	5	9	2	3	9	4	1
7	Sistema de almacenamiento (storage).	8	8	5	9	8	6	12	6	1
8	Servidores de red	8	8	5	9	10	6	15	8	1
9	Medios de respaldo	8	8	5	6	4	6	9	6	1
10	Sistemas de información y portales web	8	8	5	9	10	6	15	8	1
11	Base de datos utilizados por los sistemas y aplicativos.	8	8	5	9	10	6	15	8	1
12	Estaciones de trabajo del personal crítico (computadoras personales y portátiles)	8	8	5	9	10	6	9	6	2

7.2.5 Escenarios de riesgo

Se han establecido los siguientes escenarios que corresponden a amenazas con probabilidad de nivel medio o superior:

a) Destrucción e indisponibilidad de los laboratorios por terremoto.
b) Falla en el funcionamiento de los sistemas de información y portales web por delito informático (ataque cibernético, virus, etc.).
c) Indisponibilidad de los servidores de red por falla de hardware y software.
d) Interrupción de comunicaciones por fallas en el suministro eléctrico de los laboratorios y/o en los gabinetes de comunicación de la sede central.
e) Falla en los equipos de telecomunicaciones del ISTRFA.

A continuación, se detallan los escenarios de riesgo y su impacto, para activar el Plan de Contingencia de Tecnologías de la Información conforme a la aplicación de la clasificación de gestión de riesgos que se describe en el Anexo N° 1

Tabla N° 9 – Escenario de Riesgos

Escenario de Riesgo	Descripción	Impacto
a) Destrucción e indisponibilidad de los laboratorios	Este escenario consiste en que los laboratorios deje de funcionar o se destruya, como resultado de un terremoto o incendio, lo cual podría ocasionar caídas de servicios y destrucción de los equipos informáticos alojados en el centro datos, como también los componentes del mismo.	Extremo
b) Falla en el funcionamiento de los sistemas de información y portales web	Se refiere a la falla lógica o caída de los sistemas de información, aplicativos y portales web, lo cual produce que la información o servicios brindados por ellos no estén disponibles.	Extremo
c) Indisponibilidad de los servidores de red por falla de hardware y software.	Se refiere al fallo físico o lógico de los servidores físicos y virtuales, lo cual produce que la información o servicios brindados por ellos no estén disponibles.	Extremo
d) Interrupción de comunicaciones por fallas en el suministro eléctrico de los laboratorios y/o en el gabinete de comunicación del ISTRFA	Este escenario consiste en el corte o interrupción de las comunicaciones entre la sede central y los laboratorios, así como los servicios publicados en internet, como resultado de fallas del sistema eléctrico o equipos de suministro eléctrico, así como el corte de energía eléctrica, lo cual ocasionar caídas de servicios informáticos y pérdidas de comunicación en los equipos de infraestructura tecnológica.	Alto
e) Falla en los equipos de telecomunicaciones del ISTRFA	Se refiere al fallo físico o lógico de los equipos de comunicaciones (Switches, Firewall, Controlador etc.) lo cual produce que la información o servicios brindados por ellos no estén disponibles.	Extremo

7.3 Fase 3: Estrategias del Plan de Contingencias

A continuación, se presentan estrategias para la contingencia operativa en caso de un desastre:

7.3.1 Estrategias de prevención de tecnologías de la información

a) Almacenamiento y respaldo

1. Realización de copias de respaldo de la información almacenada y procesada en los laboratorios.

2. Realización de copias de instaladores de las aplicaciones, de software base, sistema operativo, utilitarios, etc.

3. Verificar la ejecución periódica de las tareas programadas de respaldo de información y comprobación de los medios de respaldo.

   Periodicidad: Trimestral
   Responsables: Especialista de infraestructura y el especialista de seguridad digital.

b) Entorno de réplica

El plan incluye una estrategia para recuperar y ejecutar operaciones de sistemas en instalaciones alternativas por un periodo extendido, propios de la entidad. Y el especialista de Infraestructura, identifica un ambiente adecuado para la recuperación de equipos y servicios de tecnologías de la información de los laboratorios.

Periodicidad: anual.
Responsables: especialista de Infraestructura

c) Evaluación y gestión de proveedores.

Actualizar el listado de proveedores claves de servicios y recursos de TI y mantener listas detalladas de necesidades de equipos y sus especificaciones técnicas.

Periodicidad: Semestral.
Responsables: Especialista de Infraestructura

d) Entrenamiento y personal de reemplazo

El personal de la OTI y UTI, debe entrenarse en el proceso de recuperación de los servicios de TI. El entrenamiento se evalúa para verificar que ha logrado sus objetivos.

Al inicio de cada año se debe realizar un programa de vacaciones que garantice la presencia permanente del personal crítico de las diferentes áreas y procesos de OTI, tales como soporte técnico, redes y comunicaciones, sistemas de información y bases de datos, así como seguridad de la información.

Periodicidad: Semestral.
Responsables: Especialista de seguridad digital

e) Renovación tecnológica.

Se desarrolla la programación en el plan operativo Institucional que incluye acciones de renovación tecnológica.

Periodicidad: Anual.
Responsables: Especialista de Infraestructura

7.3.2 Estrategia frente a emergencias en tecnologías de la información

El alcance de las estrategias frente a emergencias involucra las acciones que deben realizarse durante una emergencia o desastre, a fin de salvaguardar la información del ISTRFA y garantizar la continuidad de los servicios informáticos para lo cual se definen las acciones para mitigar las pérdidas que

puedan producirse en una emergencia o desastre.

A continuación, se citan las acciones que se realizarán durante una contingencia:

Acciones durante la emergencia

1. Notificar y reunir a los demás integrantes del equipo de Emergencia y Restauración.
2. Informar al coordinador de continuidad sobre la situación presentada, para decidir la realización de la Declaración de Contingencia.
3. Determinar si el área afectada es segura para el personal (en caso de catástrofe).
4. Estudiar y evaluar la dimensión de los daños a los equipos, y elaborar un informe de los daños producidos.
5. Proveer facilidades al personal encargado de la recuperación, con la finalidad de asegurar que se realicen las tareas asignadas en los procedimientos que forman parte de este plan.

7.3.3 Estrategia para la restauración de tecnologías de la información

El alcance de las estrategias para la restauración o recuperación involucra las acciones que deben realizarse luego de suscitada una emergencia o desastre, a fin de recuperar la información y los servicios informáticos del ISTRFA para estabilizar la infraestructura tecnológica luego del evento suscitado.

El ciclo considerado para la estrategia de recuperación de tecnologías de la información es el siguiente:

Tabla N° 6 – Prioridad de atención durante la restauración de TI

Prioridad de Atención	Descripción
1	Atención prioritaria: Sistemas de información y equipos que requieran alta disponibilidad de atención a los usuarios y manejen alto volumen de información. Ejemplo: Trámite documentario, Sistema Administrativo Financiero (SIAF), Sistema de gestión administrativa (SIGA), Portal Web institucional, servidores de bases de datos, entre otros.
2	Atención normal: Sistemas de información y equipos no relacionados con la atención a los usuarios y manejen bajo volumen de información. Ejemplo: Sistemas que no requirieran conectividad y/o que cuenten con mayor plazo para la consulta y disponibilidad de información, etc
3	Atención baja: Sistemas de información de uso interno, uso poco frecuente y/o que manejan bajo volumen de información. Asimismo equipos de apoyo. Ejemplo: Intranet entre otros

Los sistemas de información y equipos informáticos, con la respectiva prioridad de atención, en caso de activarse la contingencia informática, se describen en el Anexo N° 2 y Anexo N° 3.

7.4 Fase 4: Elaboración del Plan de Contingencia

Una vez identificados los eventos de contingencia y los escenarios de riesgo, se procede con el desarrollo de los procedimientos del Plan de Contingencia, agrupados por las categorías indicadas previamente, lo cual comprenderá los eventos de mayor impacto, identificado en la matriz e riesgos de contingencia y serán abordados tal como se indica en la siguiente tabla, asimismo en el anexo N°4 se detalla cada formato del procedimiento del plan de contingencia.

Tabla N° 7 – Eventos de mayor impacto para el Plan de Contingencia de información

N°	Evento	Exposición al Riesgo	Formato del Procedimiento Plan de Contingencia - FPPC
1	Incendio en los laboratorios	Extremo	01
2	Terremoto /Sismo	Extremo	02
3	Incidente de Seguridad informática (ataque)	Extremo	03
4	Falla de hardware y software	Extremo	04
5	Falla del suministro eléctrico en los laboratorios y gabinetes de comunicación.	Alto	05

7.5 Fase 5: Implementación del Plan de Contingencia

La implementación del presente plan iniciará en un plazo no mayor de treinta (30) días calendarios después de su aprobación.
Para tal efecto, el/la Oficial de Seguridad de la Información, en coordinación con el Especialista de infraestructura, realizaran las siguientes funciones:

a) Supervisar las actividades de copias de respaldo y restauración.
b) Establecer procedimientos de seguridad en los sitios de recuperación.
c) Organizar las pruebas de restauración de hardware, software y servicios de Tecnologías de Información (TI).
d) Participar en las pruebas y simulacros de desastres.

7.6 Fase 6: Monitoreo

Dado que las condiciones del inmueble del ISTRFA pueden variar con el tiempo, lo mismo que los bienes informáticos, incluidos los equipos informáticos de los laboratorios, es importante que se realice una verificación
del Plan de Contingencia.

Las acciones de verificación se deben realizar de manera trimestral y bajo un ambiente controlado, donde se comprueben que con las acciones definidas los bienes y servicios informáticos respondan de acuerdo a lo esperado, considerando que los procesos pueden variar y afectar la disponibilidad de los sistemas. Por lo que, es importante la ejecución de simulacros de interrupción de servicios informáticos, los cuales deben estar definidos, de forma que se pueda determinar el nivel de éxito de los mismos. Para dichos simulacros se debe considerar lo siguiente:

- Definir a los responsables del simulacro por las diferentes áreas interesadas.
- Evaluar los riesgos, validar el inventario de recursos
- Elaborar un plan de atención de los laboratorios, y según corresponda un plan de atención que abarque todos los bienes informáticos de la Institución

- Se debe comunicar a todo el personal de la Institución sobre los simulacros.
- Se debe realizar una evaluación conjunta con todos los responsables definidos para el simulacro, y plasmar en un documento las mejoras que se requieren plantear.
- Comunicar a todos los interesados el resultado de la evaluación del simulacro.

En base a los resultados obtenidos se realiza la modificación y mantenimiento del presente plan, para lo cual se establecen controles formales para dichas modificaciones. Asimismo, todos los responsables mencionados en el presente plan deberán tener conocimiento de los cambios.

Como parte del mantenimiento del plan de contingencia, se debe contemplar el entrenamiento al personal de la OTI y UTI, a través de capacitaciones virtuales o presenciales de acuerdo a lo planificado por el coordinador de continuidad, y será de manera anual, a fin de que puedan dar una respuesta adecuada a las eventualidades que puedan afectar los servicios informáticos.

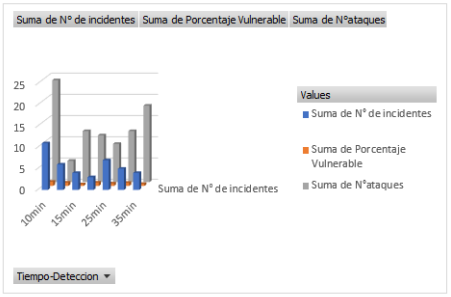
INDICADORES DE CLAVES DE DESEMPEÑO

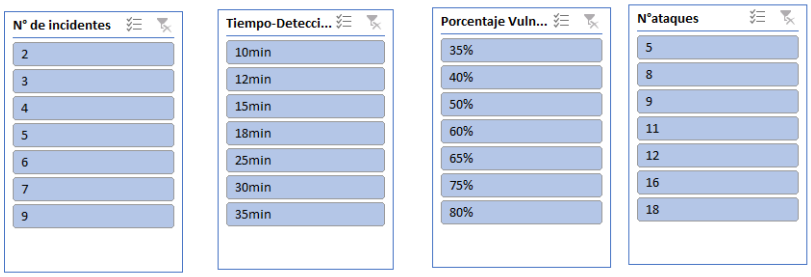
N° de incidentes	Tiempo-Deteccion	Porcentaje Vulnerable	N°ataques	N° Interrucciones	Tiempo_Resolucion	N° Errores
4	15min	40%	12	15	20	6
7	25min	60%	9	19	25	4
9	10min	65%	16	21	14	9
6	12min	80%	5	13	10	5
2	10min	35%	8	17	30	9
5	30min	75%	12	15	20	5
3	18min	80%	11	18	18	8
4	35min	50%	18	11	15	4

Porcentaje_Incidentes	respuesta de la red	carga de App/sitios web	capacidad	copia de seguridad/recuperación	Tiempo fallos	tiempo de actividad
60%	10min	4	4000mb	40min	6min	20min
40%	12min	8	3500mb	50min	12min	40min
35%	10min	6	2500mb	30min	10min	15min
20%	9min	5	500mb	20min	9min	10min
45%	12min	8	4500mb	45min	15min	12min
25%	15min	9	1500mb	35min	10min	30min
20%	10min	5	5000mb	30min	8min	25min
50%	16min	7	4250mb	25min	11min	18min

PKI 1 Seguridad de los sistemas informáticos

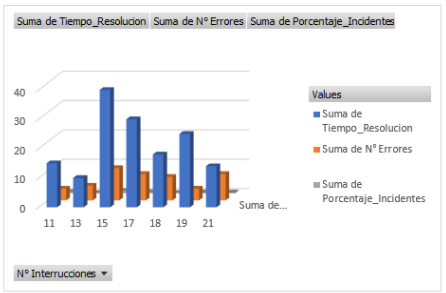
Etiquetas de fila	Suma de N° de incidentes	Suma de Porcentaje Vulnerable	Suma de N°ataques
10min	11	1	24
12min	6	0,8	5
15min	4	0,4	12
18min	3	0,8	11
25min	7	0,6	9
30min	5	0,75	12
35min	4	0,5	18
Total general	**40**	**4,85**	**91**

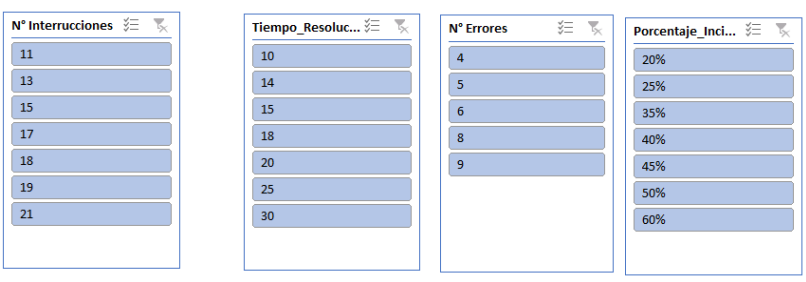




PKI 2 Impactos y problemas de la tecnología de la información

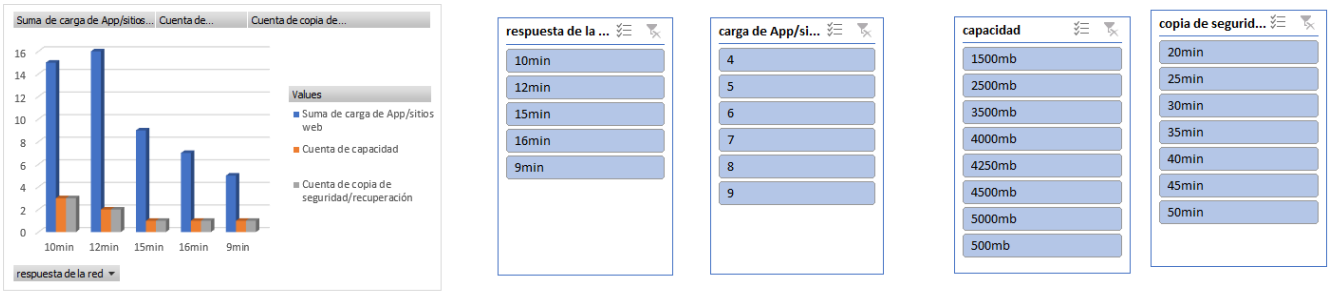
Etiquetas de fila	Suma de Tiempo_Resolucion	Suma de N° Errores	Suma de Porcentaje_Incidentes
11	15	4	0,5
13	10	5	0,2
15	40	11	0,85
17	30	9	0,45
18	18	8	0,2
19	25	4	0,4
21	14	9	0,35
Total general	**152**	**50**	**2,95**





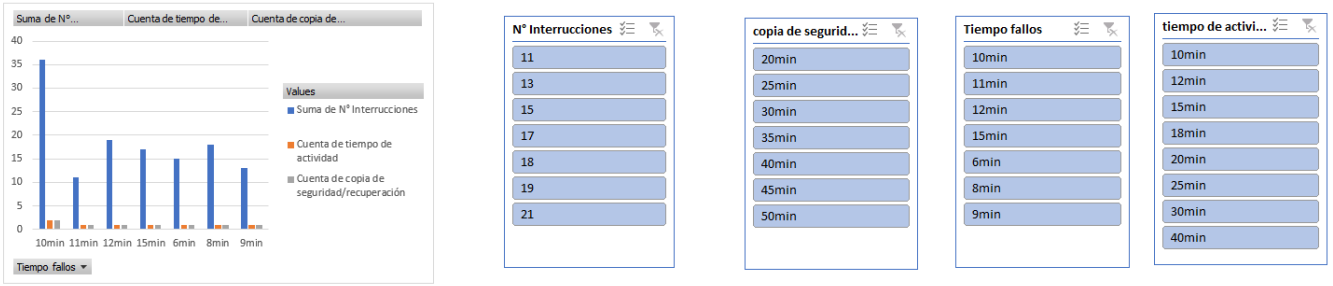
PKI 3 Rendimiento de la infraestructura de TI

Suma de carga de App/sitios web	Cuenta de capacidad	Cuenta de copia de seguridad/recuperación
15	3	3
16	2	2
9	1	1
7	1	1
5	1	1
52	**8**	**8**



PKI 4 Disponibilidad del sistema:

Etiquetas de fila	Suma de N° Interrucciones	Cuenta de tiempo de actividad	Cuenta de copia de seguridad/recuperación
10min	36	2	2
11min	11	1	1
12min	19	1	1
15min	17	1	1
6min	15	1	1
8min	18	1	1
9min	13	1	1
Total general	**129**	**8**	**8**



ANEXO N° 1

Clasificación de Riesgos:

Los riesgos serán clasificados de acuerdo con los niveles definidos por los propietarios de Riesgos, según su grado de exposición, lo cual se muestra en la siguiente tabla:

Nivel	Criterio	Descripción
25-20	**EXTREMO**	Genera un alto impacto a la Institución y es muy probable que ocurran. Aquel riesgo que al presentarse puede causaruna afectación directa a la estrategia, no se debe continuarcon las actividades hasta que se realicen acciones que aporten a la mitigación de este.
16-12	**ALTO**	Genera un impacto a la Institución, y es más probable queocurran. Aquel riesgo que al presentarse puede originar una afectación a los procesos de negocio, se debe realizaracciones correctivas a corto o mediano plazo a fin de mitigar el nivel de riesgo e iniciar acciones preventivas con el fin que el riesgo no se manifieste.
10-5	**MEDIO**	Genera un impacto a la Institución, y es probable que ocurran ocasionalmente. Aquel riesgo que al presentarsepuede originar una afectación a los procesos de soporte, se debe tomar acciones a mediano o largo plazo a fin deque el riesgo no se manifieste.
4-3	**LIGERO**	Genera bajo impacto a la Institución y es poco probableque ocurran. Aquel riesgo que al presentarse no generaafectación en prestación de servicio de la Institución. Se recomienda actividades de retención del riesgo.
2-1	**BAJO**	No generan impacto a la Institución y es improbable queocurra. Aquel riesgo que al presentarse no afecta el funcionar de la Institución. Se pueden continuar con las actividades sin llevar a cabo controles adicionales.

ANEXO N°3

LISTADO DE APLICACIONES Y SISTEMAS DE INFORMACIÓN CLASIFICADOS POR PRIORIDAD DE ATENCIÓN PARA LA RECUPERACIÓN

Servidores críticos alojados en la Nube				
Nº	**Sistema**	**Descripción**	**Tipo**	**Prioridad**
1	Correo Electrónico, herramientas de colaboración, página Web	El correo electrónico, es una herramienta que permite facilitar una eficiencia comunicación interna y externa entre los servidores del ISTRFA	Web	1
2	CTI Vitae (ex Directorio Nacional de Investigadores)	Es un software en entorno Web; permite que las personas que declaran estar profesionalmente vinculadas a la CTI en el Perú, puedan registrar sus datos personales, proyectos, producciones científicas, entre otros., la cual se pone a disposición de los usuarios de la plataforma.	Web	1
3	Sistema de Beneficios tributarios	Aplicativo WEB, que permite el ingreso en línea de las postulaciones a proyectos de I+D+i, así como el proceso de gestión y seguimiento de las solicitudes presentadas, dentro de los límites de tiempo dispuestos por Ley.	Web	1
4	Sistema de Evaluadores	Permite el registro de los evaluadores que trabajan en las diferentes aplicaciones del ISTRFA y PROCIENCIA	WEB	1
5	Registro Nacional de Investigadores (REGINA)	Aplicativo WEB, que permite atender las solicitudes de calificación de los investigadores según criterios especificados según Reglamento.	Web	1
6	Directorio Nacional de Instituciones V.2015	Es una aplicación que permite el registro detallado de las Instituciones del SINACYT	Web	1
Servidores críticos alojados en los laboratorios				
Nº	**Sistema**	**Descripción**		**Prioridad**
1	Sistema Integrado de Gestión Administrativa (SIGA)	Soporta la gestión de procesos administrativos. El proceso de Selección en sus distintas etapas, seguimiento de ejecución de contratos.	Escritorio	1
2	SIAF	Sistema que permite la gestión de datos relacionado a los procesos de gasto e ingreso a nivel administrativo.	Escritorio	1
3	Trámite Documentario	Aplicativo Web para el intercambio documental entre las Oficinas del ISTRFA	Web	2
4	Sistema de Control de Asistencia	Permite el manejo de papeletas, marcaciones, actividades, compensaciones y vacaciones del trabajador.	Web	3
5	Sistema de Planillas	Sistematiza los procesos de remuneraciones del personal, así mismo emite la planilla de pagos del personal, y genera la información de registro para la SUNAT.	Escritorio	2
6	Sistema de Gestión del Archivo Central	Permite gestionar el flujo de información que se da en los archivos físicos de la Institución, así, cada archivo es clasificado según su importancia, ubicación por área y fecha de emisión.	Escritorio	2
7	Libro de Reclamaciones	Permite registrar en línea los reclamos de los usuarios por la atención de los servicios de la Entidad.	Web	2
8	Sistema de Registro de Visitas	Aplicativo para el control de visitas en la institución.	Web	2
9	Sistema de Mesa de Partes	Usado para la recepción de documentos por mesa de partes del ISTRFA.	Web	1
10	SPIJ	Permite consulta información jurídica del país.	Web	3

11	Sistema Integrado de Gestión	Permite registrar, evaluar y monitorear las postulaciones de las diferentes convocatorias.	Web	1
12	Repositorio de Datos de PROCIENCIA - RDOC	Permite guardar archivos digitalizados	Web	1

* La presente tabla se actualizará conforme se implemente sistemas sin necesidad de modificar el presente plan.

ANEXO N°4

FORMATOS DEL PROCEDIMIENTOS DE CONTINGENCIA INFORMÁTICO Y RESTAURACIÓN DE SERVICIOS DE TI

ISTRFA	Evento: Incendio en los laboratorios	FPC – 01

1. PROCEDIMIENTO DE PREVENCIÓN

a) Situación actual

- Todas las oficinas han designado a un delegado para casos de emergencia, así también cada Oficina cuenta con un extintor, si bien los delegados han sido capacitados inicialmente, no se considera que la periodicidad de dichas capacitaciones es óptima.
- Sobre el caso de incendios, se precisa que el inmueble y cada una de las oficinas cuenta con puertas cortafuego, lo que ayudaría a contener el fuego, por un periodo de tiempo, en la ubicación en que se haya generado.
- Con respecto al mantenimiento de los equipos informáticos, no se tiene un espacio adecuado para realizarlo y reducir el riesgo de incendio al hacer uso de equipos de soldadura, materiales inflamables, como alcohol isopropílico, tiner acrílico o aerosoles. Este riesgo implica un mayor impacto al realizarse trabajos de mantenimiento, por parte de la OTI u otras oficinas, que hacen uso de este tipo de herramientas en horas laborables.
- Sobre los laboratorios, no se tiene un centro de datos alterno; y en caso un incendio logre destruir un 50% de las oficinas antes de ser controlado, el impacto en los laboratorios sería alto, toda vez que los equipos se verían realmente afectado y la información almacenada ahí también se afectaría.
- La información generada por las aplicaciones alojadas en la nube es respaldada constantemente en línea; la información generada por aplicaciones alojadas en equipos de los laboratorios se respalda en discos de almacenamiento local de forma diaria y progresiva, pero son enviados a la nube cada 15 días aprox. Por tanto, de darse el incendio en el lapso previo al envío de los respaldos locales a la nube, se tiene riesgo de pérdida de la información.
- Cabe precisar que no se tiene habilitado un lugar para que la totalidad de empleados trabajen en tanto el inmueble sea restaurado.

Infraestructura:

- Centro de Datos

Recursos Humanos

- Personal de la entidad.

b) Objetivo

Establecer las acciones que se ejecutarán ante un incendio a fin de minimizar el tiempo de interrupción de las operaciones en el ISTRFA, sin exponer la seguridad de las personas.

c) Personal Encargado

El/La coordinador/a de Continuidad, es quien debe dar los lineamientos y dar cumplimiento a las Condiciones de Prevención de Riesgo del presente Plan. Por su parte, el Grupo de Prevención debe realizar las acciones descritas en el punto e).

d) Condiciones de Prevención de Riesgo
- Inspecciones de seguridad realizadas periódicamente al centro de datos.
- Mantenimiento de las salidas libres de obstáculos.
- Funcionamiento de los extintores contra incendio
- Funcionamiento de las luces de emergencia.
- Mantenimiento de detectores de humo contra incendio.

e) Acciones del Equipo de Prevención
- Evaluar en coordinación con el coordinador de Continuidad un ambiente para los laboratorios.
- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo y restauración de información como base de datos, código fuentes y ejecutables.
- Programar, supervisar el mantenimiento preventivo a los equipos de los laboratorios.
- Realizar periódicamente el mantenimiento preventivo y correctivo del UPS.
- Realizar periódicamente el mantenimiento preventivo y correctivo de los servidores alojado en los laboratorios.
- Mantener vigente los extintores contra incendio.

2. PROCEDIMIENTO EJECUCIÓN

a) Eventos que activan la contingencia
La contingencia se activará al ocurrir un incendio. El proceso de contingencia se activará inmediatamente después de ocurrir el evento.

b) Personal que autoriza la contingencia informática
El/La Coordinador/a de Continuidad.

c) Personal Encargado
Equipo de Emergencia.

d) Acciones para ejecutar a corto plazo
- Desconectar el fluido eléctrico y cerrar las llaves de gas u otros líquidos inflamables si corresponde.
- Establecer medidas que permitan garantizar que los respaldos realizados estén totalmente funcionales y que permita recuperar la información exacta a partir de los mismos.
- Realizar de forma más frecuente el backup de la información en la nube.
- Evaluar el alcance del desastre en cada área de responsabilidad y notificar y reunir a los demás integrantes del equipo de Emergencia y Restauración.

e) Duración
La duración total del evento dependerá del grado del incendio y losdaños a la infraestructura.

3. PROCEDIMIENTO DE RECUPERACIÓN

a) Personal Encargado
El personal encargado es el/la Coordinador/a de Continuidad y el Equipo de Restauración, cuyo rol principal es asegurar el normal desarrollo de los servicios de TI del ISTRFA.

b) Descripción de actividades
El plan de recuperación está orientado a recuperar en el menor tiempo posible las actividades afectadas durante la interrupción del servicio.

En caso, el evento haya sido de considerable magnitud, se deberá:
- Verificar la disponibilidad de recursos para la contingencia como: manuales técnicos de instalación del sistema de información, almacenamiento de datos, sistemas comunicación, hardware, y copias de respaldo.
- Movilizar al equipo de restauración al sitio alterno de recuperación.
- Establecer contacto con los proveedores clave y terceros para proporcionar instrucciones

inmediatas y/o notificarles cualquier requisito de ayuda sobre la recuperación de negocio.

c) Mecanismos de Comprobación

El equipo de emergencia, presentará un informe al/el coordinador de Continuidad, explicando qué parte de las actividades u operaciones de tecnologías dela información han sido afectadas y cuáles son las acciones tomadas.

d) Desactivación del Plan de Contingencia

El/La Coordinador/a de Continuidad desactivará el Plan de Contingencia una vez que se haya tomado las acciones descritas en el presente Plan de Recuperación.

ISTRFA	Evento: Terremoto /Sismo	FPC – 02

1. PROCEDIMIENTO DE PREVENCIÓN

a) Situación actual:

- Actualmente la institución cuenta con luces de emergencia en determinados puntos, así como cuenta con señalización de zonas seguras de la institución.
- Se realiza simulacros de prevención ante cualquier posible sismo y/o terremoto que pudiera ocurrir.
- Actualmente no se cuenta con un centro de datos alterno ante un posible terremoto y/o sismo que pudiera ocurrir y consigo perjudicar el equipamiento que se encuentra dentro de los laboratorios del ISTRFA.
- El ISTRFA, cuenta con servicios y servidores alojado en la nube, el mismo que no se vería afectado ante cualquier sismo o terremoto que pudiera ocurrir.

b) Objetivo

Establecer las acciones que se ejecutarán ante un terremoto/sismo a fin de minimizar el tiempo de interrupción de las operaciones del ISTRFA, sin exponer la seguridad de las personas.

c) Personal Encargado

El/la coordinado/ra de Continuidad del ISTRFA, es quien debe dar los lineamientosy dar cumplimiento a las Condiciones de Prevención de Riesgo del presente Plan. El Equipo de Prevención debe realizar las acciones descritas en el punto e).

d) Condiciones de Prevención de Riesgo

- Realización de simulacros de evacuación con la participación de todo el personal del ISTRFA.
- Conformación de las brigadas de emergencia, y capacitarlas anualmente.
- Mantenimiento de las salidas libres de obstáculos.
- Señalización de las zonas seguras y las salidas de emergencia.
- Funcionamiento de las luces de emergencia.
- Definición de los puntos de reunión en caso de evacuación.

e) Acciones del Equipo de Prevención

- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo y restauración de información de base de datos, código fuentes y ejecutables.
- Programar, supervisar el mantenimiento preventivo a los equipos componentes de los laboratorios.
- Mantener actualizado el inventario hardware y software utilizado en los laboratorios del ISTRFA.
- Llevar un control de versiones de las fuentes de los sistemas de información y portales del ISTRFA.

2. PROCEDIMIENTO DE EJECUCIÓN

a) Eventos que activan la contingencia

La contingencia se activará al ocurrir un sismo. El proceso de contingencia se activará inmediatamente después de ocurrir el evento

b) Personal que autoriza la contingencia informática

El/La Coordinador/a de Continuidad.

c) Personal Encargado

Equipo de Emergencia.

d) Acciones para ejecutar a corto plazo

- Desconectar el fluido eléctrico y cerrar las llaves de gas u otros líquidos inflamables.
- Se hará sonar la sirena o alarma para casos de sismo, dando aviso al personal, que posteriormente será evacuado de las instalaciones.
- El personal integrante de la brigada para casos de sismos actuará de inmediato, manteniendo la calma en el lugar y dirigiendo a las demás personas por las rutas de escape establecidas.
- Todo el personal se reunirá en zonas preestablecidas como seguras hasta que el sismo culmine. Se esperará un tiempo prudencial, ante posibles réplicas. En caso de tratarse de un sismo de magnitud leve, los trabajadores retornarán a sus labores; sin embargo, de producirse un sismo de gran magnitud, el personal permanecerá en áreas seguras y se realizarán las evaluaciones respectivas de daños y estructuras antes de reiniciar las labores.
- Se rescatará a los afectados por el sismo, brindándoles inmediatamente los primeros auxilios y, de ser necesario, se les evacuará al hospital o centro de salud más próximo.
- Evaluación de los daños ocasionados por el sismo sobre las instalaciones físicas, ambientes de trabajo, instalaciones eléctricas, documentos, etc.
- Inventario general de documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos.
- Limpieza de las áreas afectadas por el sismo.

e) Duración

La duración del evento dependerá del grado del sismo, la probabilidad de réplicas y los daños a la infraestructura.

3. PROCEDIMIENTO DE RECUPERACIÓN

a) Personal Encargado

El personal encargado es el/la Coordinador/a de Continuidad y el Equipo de Restauración, cuyo rol principal es asegurar el normal desarrollo de los servicios y operaciones de TI del ISTRFA.

b) Descripción de actividades

- Brindar atención inmediata de las personas accidentadas.
- Mantener al personal en las zonas de seguridad previamente establecidas por un tiempo prudencial hasta el cese de las réplicas.
- Retirar todos los escombros que pudieran generarse por el sismo, los mismos que serán colocados en el depósito de residuos sólidos.
- Verificar la disponibilidad de recursos para la contingencia como: manuales técnicos de instalación del sistema de información, almacenamiento de datos, sistemas, comunicación, hardware, y copias de respaldo.
- Supervisar el progreso de las operaciones de recuperación y de servicios de TI.
- El Equipo de restauración de TI restaurarán el espacio de trabajo para permitir que el personal crítico dela oficina pueda operar, para lo cual deberán:
  - Ejecutar los procedimientos de recuperación de la plataforma tecnológica.
  - Verificar que las aplicaciones críticas se hayan recuperado y estén funcionando

correctamente.
- Confirmar los puntos de recuperación de datos de las aplicaciones.
- Verificar que las funcionalidades de comunicación están funcionando correctamente.
- Verificar que equipos básicos como escáner, impresora estén disponibles y operacionales para dar soporte a los requisitos de la entidad.
- Asegurar que el ambiente del área de trabajo, las aplicaciones están funcionando según lo estimado una vez concluida la emergencia o siniestro.

c) Mecanismos de Comprobación
El/La equipo de restauración, presentará un informe al coordinador de Continuidad, explicando qué parte de las actividades u operaciones de tecnologías dela información han sido afectadas y cuáles son las acciones tomadas.

d) Desactivación del Plan de Contingencia
El/La Coordinador/a de Continuidad desactivará el Plan de Contingencia.

ISTRFA	Evento: Incidente de Seguridad informática (ataque)	FPC – 03

1. PROCEDIMEINTO DE PREVENCIÓN

a) Situación actual:
- Si bien la instalación de software, sea propietario o de desarrollo interno, es realizado y/o supervisado por la OTI, existen casos en que el personal instala software en sus equipos sin autorización ni supervisión de la OTI, poniendo en riesgo sus equipos pues puede ser software virulento.
- Se cuenta con un software de antivirus corporativo, el cual se renueva de forma periódica
- El personal no es consciente a plenitud sobre el riesgo e impacto de hacer uso de software sin supervisión de la OTI, así como de abrir correos electrónicos de dudosa procedencia o hacer uso de dispositivos de almacenamiento externos sin los cuidados adecuados. Todo esto podría dañar no sólo al bien informático sino también a la información almacenada.
- Se cuenta con mecanismos de seguridad perimetral, para evitar el acceso no autorizado a la red institucional.
- Es preciso describir que el malware es un software malicioso o software malintencionado, que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario, eliminando datos del equipo. Incluye virus, gusanos, troyanos, keyloggers, botnets, ransomwares o secuestradores, spyware, adware, hijackers, keyloggers, rootkits, bootkits, rogues, etc.

b) Objetivo
Restaurar la operatividad de los equipos y servicios después de eliminar los malware o reinstalar las aplicaciones dañadas.

c) Personal Encargado
El Equipo de Prevención es el responsable del correcto funcionamiento de los servidores,estaciones de trabajo, sistemas de información y servicios de TI de acuerdo a sus perfiles.

d) Condiciones de Prevención de Riesgo
- Instalación de parches de seguridad en los equipos.
- Aplicación de filtros para restricción de correo entrante, y revisión de archivos adjuntos enlos correos y así prevenir la infección de los terminales de trabajo por virus.
- Contar con antivirus instalados en cada estación de trabajo y debe estar actualizado permanentemente.
- Contar con equipos de respaldo ante posibles fallas de las estaciones y servidores, para su reemplazo provisional hasta su desinfección y habilitación.
- Restricción del acceso a Internet a las estaciones de trabajo que por su uso no lo requieran.

- Deshabilitación de los puertos de comunicación USB en las estaciones de trabajo que no los requieran habilitados, para prevenir la conexión de unidades de almacenamiento externo
- Capacitar y concientizar al personal del ISTRFA, sobre la importancia de laseguridad de la información.

e) Acciones del Equipo de Prevención
- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo de información procesada y almacenada en los laboratorios.
- Llevar un control de versiones de las fuentes de los sistemas de información y portales de la entidad.
- Realizar pruebas de restauración de la información almacenada en los repositorios y bases de datos.
- Documentar y validar los manuales de restauración de los sistemas de información en producción.

2. PROCEDIMIENTO DE EJECUCIÓN

a) Eventos que activan la contingencia
- Mensajes de error durante la ejecución de programas.
- Lentitud en el acceso a las aplicaciones
- Falla en el sistema operativo y aplicaciones de los equipos.

b) Personal que autoriza la contingencia informática
El/La Coordinador/a de Continuidad y el/la Oficial de Seguridad de la Información pueden activar la contingencia.

c) Personal Encargado
Equipo de prevención

d) Acciones para ejecutar a corto plazo
- Desconectar de la red de datos del ISTRFA, el servidor o la estación infectada ovulnerada.
- Verificar si el equipo se encuentra infectado, utilizando un detector de malware/virus actualizado. En el caso de aplicaciones, verificar si el código o la información de las bases de datos ha sido alterada.
- Guardar la muestra del virus detectado y remitirlo al proveedor del antivirus. En el caso de hacking a aplicaciones, se debe guardar el archivo modificado, a nivel de software y base de datos.
- En caso no solucionarse el problema, formatear el equipo y restaurar copia de respaldo

e) Duración
En caso se confirme un Incidente de Seguridad informática en estaciones de trabajo la duración del evento no deberá ser mayor de 24 horas y en servidores de centro de datos de 04 horas.

3. PROCEDIMIENTO DE RECUPERACIÓN

a) Personal Encargado
El equipo de restauración, luego de restaurar el correcto funcionamiento del servidor,estación de trabajo (PC, laptop), sistemas de información y portales web, coordinará con el usuario responsable e informará a su jefe inmediato para reanudar las labores de trabajo.

b) Descripción de actividades
- Instalación y configuración de software, drivers y servicios necesarios para el funcionamiento de la información a recuperar en el ISTRFA.
- Instalación del motor de base de datos, con sus respectivas librerías y niveles de seguridad.
- Realización de la restauración de la base de datos con la última copia de seguridad disponible.
- Conectar el servidor o la estación de trabajo a la red del ISTRFA.
- Efectuar las pruebas necesarias con el usuario final de los equipos y/o sistemas de información

afectados.
- Ejecutar análisis de vulnerabilidad
- Comunicar el restablecimiento del servicio.

c) Mecanismos de Comprobación

Se registrara el incidentes Sistema de Gestión de Tickets utilizado por soporte técnico de la OTI y se informará al Comité de Gestión de Seguridad Digital.

El/La Especialista de infraestructura de Redes y/o el personal de soporte técnico, según sea el caso, presentará un informe a el/la jefe/a de OTI, informando que parte del servicio u operaciones se han visto afectadas, y cuáles son las acciones tomadas.

e) Desactivación del Plan de Contingencia

El/La Coordinador/a de Continuidad desactivará el Plan de Contingencia.

ISTRFA	Evento: Falla de hardware y software	FPC – 04

1. PROCEDIMIENTO DE PREVENCIÓN

a) Situación actual

- Los laboratorios se encuentra conectado a una red eléctrica estabilizada y conectado a UPS.
- Los equipos informáticos en general, se ha detectado que en diversas oficinas existen interrupciones del fluido eléctrico, lo que afecta a los bienes informáticos, con apagados imprevistos, lo que daña progresivamente los componentes de las computadoras o genera que un bien quede en desuso o requiera una revisión técnica, consumiendo tiempo o presupuesto.
- Se ha detectado parpadeo en las luminarias, lo que se ha más evidente cuando se hace uso del aire acondicionado, por lo que es importante tener clara la capacidad de carga eléctrica que se debe manejar en el inmueble y así evitar el impacto negativo en los bienes informáticos.
- No existe un circuito eléctrico exclusivo para los equipos informáticos.
- Dependiendo del equipo, las fallas pueden ser atendidas o resueltas por el personal interno de la OTI, pero en otros casos es necesario sea remitido a una empresa especializada. En ambos casos es importante que se proporcione una atención rápida a las fallas que presenten los equipos.
- En los casos en que los sistemas de información están alojados en la nube, su disponibilidad está supeditada a la disponibilidad de la infraestructura de la empresa que brinda dicho servicio, así como de las actualizaciones que dicha empresa pudiese realizar. Esto, dado que dichas actualizaciones pueden generar un funcionamiento inadecuado de los servicios

b) Objetivo

Asegurar la continuidad de las operaciones, con los medios de respaldo adecuados de lasimágenes de los servidores o máquinas virtuales en producción.

c) Personal Encargado

El equipo de Prevención.

d) Condiciones de Prevención de Riesgo

- Revisión periódica de los registros (Logs) de los servidores, para prevenir mal funcionamientode los mismos.
- Contar como mínimo con los backups quincenales de datos de las aplicaciones en desarrollo/producción de la entidad.
- Contar con servicios de soporte y mantenimiento que contemple actividades de prevención, revisión del sistema y mantenimiento general.

- Disponer de servidores de bases de datos de contingencia, con la instalación del motor de base de datos.

e) Acciones del Equipo de Prevención.
- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo y restauración de información.
- Programar y supervisar el mantenimiento preventivo y correctivo a los equipos componentes del Centrode Datos.
- Mantener actualizado el inventario hardware y software de los laboratorios del ISTRFA.
- Realizar monitoreo del funcionamiento de los servidores instalados en los laboratoriospara su correcto funcionamiento.
- Establecer con la empresa que brinda servicios de nube, mecanismos para una comunicación anticipada de las actualizaciones (u otras acciones) que vayan a realizar y que pudiese impactar en los servicios del ISTRFA.
- Determinar la necesidad de adquisición de nuevos equipos considerando el tiempo de vida, y el impacto de un funcionamiento inadecuado de los mismos.

2. PROCEDIMIENTO DE EJECUCIÓN

a. Eventos que activan la contingencia
- Fallas en la conexión. Indisponibilidad del sistema de información y/o aplicativo.
- Identificación de falla en la pantalla de las estaciones de trabajo y/o servidores de aplicaciones.

b. Personal que autoriza la contingencia informática
El/La Coordinador/a de Continuidad.

c. Personal Encargado
Equipo de Emergencia.

d. Acciones para ejecutar a corto plazo
- Contar con la disponibilidad del personal para la reparación rápida de los equipos.
- Establecer con la empresa que brinda servicios de nube, mecanismos para una comunicación anticipada de las actualizaciones (u otras acciones) que vayan a realizar y que pudiese impactar en los servicios del ISTRFA, de forma tal que se puedan ejecutar simulacros y evaluar su impacto, previniendo una interrupción de los servicios.
- Acceder a las copias de respaldo para la restauración de la información en el servidor averiado
- Verificar que el equipo se encuentre en garantía, de lo contrario de implementará un nuevo servidor virtual.

e. Duración
El tiempo máximo de la contingencia no debe sobrepasar las seis (6) horas

3. PROCEDIMIENTO DE RECUPERACIÓN

a) Personal Encargado
El Equipo de Restauración, después de validar la corrección del problema de acceso a los servidores, y el/la Coordinador/a de Continuidad informará a los Jefes de las áreas para la reanudación de las operaciones de los servicios afectados en el servidor averiado.

b) Descripción de actividades
- Instalación y configuración del sistema operativo, drivers y servicios necesarios para el funcionamiento del sistema de información a recuperar.
- Instalación y configuración del sistema de información y el motor de la base de datos, consus respectivas librerías y niveles de seguridad.
- Proceder a la restauración de las copias de respaldo, de la información de los servidores afectados.

- Verificar que la data y los aplicativos se hayan restaurado correctamente.
- Ejecutar pruebas de acceso a los sistemas y aplicaciones.
- Comunicar mediante correo electrónico a los usuarios la reanudación de los servicios.

c) Mecanismos de Comprobación

Se registrará el incidente en el Sistema de Gestión de Tickets utilizado por la Mesa de Ayuda y Soporte Técnico de la OTI, precisando las acciones realizadas.

El/La Especialista de infraestructura y Redes, presentará un informe a el/la jefe/a de OTI, informando que parte del servicio u operaciones se han visto afectadas, y cuáles son las acciones tomadas.

d) Desactivación del Plan de Contingencia

El/La Coordinador/a de Continuidad desactivará el Plan de Contingencia.

ISTRFA	Evento: Falla del suministro eléctrico en los laboratorios	FPC – 05

1. PROCEDIMIENTO DE PREVENCIÓN

a) Situación actual:

- El inmueble cuenta con luces de emergencia en determinados puntos, pero se ha verificado que algunos no encendieron correctamente en la OTI, por lo que es importante su validación.
- La continuidad del fluido eléctrico de los laboratorios está soportada en 3 UPS que dan un promedio de 2 horas para el apagado progresivo de los equipos, dichos UPS emiten correos de advertencia al ponerse en funcionamiento, lo que alerta a los especialistas de la OTI, para que ejecuten las acciones correspondientes para un apagado adecuado.
- Es importante que el personal se concientice sobre la importancia de usar adecuadamente el tiempo que brindan los UPS para el apagado de los servicios alojados en los servidores de los laboratorios, a fin de realizar adecuadamente el apagado de los equipos y evitar que queden defectuosos y/o dañar información.
- No se realizan simulacros de interrupciones de fluido eléctrico en los laboratorios, y no existen procedimientos formales de apago y encendido del mismo

b) Objetivo

Restaurar las funciones consideradas como críticas para el servicio.

c) Personal Encargado

- El/la Coordinador/a de Continuidad, es el responsable de atender y supervisar las respuestas ante el incidente.
- El/La Jefe/a de la Oficina de Logística de la OGA es el responsable de realizar las coordinaciones para restablecer el suministro de energía eléctrica con los proveedores de energía.
- El Equipo de Prevención debe realizar las acciones descritas en el punto e).

d) Condiciones de Prevención de Riesgo

- Para los servicio diarios que realiza el ISTRFA se cuenta con grupo electrógeno y con equipos UPS necesario para asegurar el suministro eléctrico en los equipos consideradas como críticos
- El grupo electrógeno, puede proporcionar suficiente energía eléctrica para soportar una operación continua de 4 horas como mínimo. El tiempo variará de acuerdo a la función que cumplan
- El Equipo UPS cuentan con mantenimiento preventivo y con suficiente energía para soportar una operación continua de 30 minutos como mínimo. El tiempo variará de acuerdo a la función que cumplan.
- Realización de pruebas periódicas del equipo UPS para asegurar su correcto funcionamiento.
- Capacidad del UPS para proteger los servidores de archivos, base de datos y aplicaciones, previniendo la pérdida de datos durante las labores. La autonomía del equipo UPS no deberá

ser menor a 30 minutos.

e) Acciones del Equipo de Prevención.
- Revisar periódicamente y de forma conjunta con Servicios Generales de la Oficina de Logística las instalaciones eléctricas de los laboratorios y programar y supervisar el mantenimiento preventivo y correctivo a los equipos componentes del Centrode Datos.
- Coordinar y supervisar el mantenimiento preventivo de pozos a tierra, aire acondicionado de los laboratorios, UPS, grupo electrógeno, transformador y del gabinete de baterías trimestralmente.
- Verificar que la red eléctrica utilizada en los laboratorios sea estabilizada. En caso no existanse debe gestionar la implementación de lo requerido con el área respectiva.
- Revisar la presencia de exceso de humedad en la sala de energía de los laboratorios del ISTRFA.

2. PROCEDIMIENTO DE EJECUCIÓN

a. Eventos que activan la contingencia
- Fallas en la conexión. Indisponibilidad del sistema de información y/o aplicativo.
- Identificación de falla en la pantalla de las estaciones de trabajo y/o servidores de aplicaciones.

b. Personal que autoriza la contingencia informática
El/La Coordinador/a de Continuidad.

c. Personal Encargado
Equipo de Emergencia.

d. Acciones para ejecutar a corto plazo
- Contar con la disponibilidad del personal para la reparación rápida de los equipos.
- Establecer con la empresa que brinda servicios de nube, mecanismos para una comunicación anticipada de las actualizaciones (u otras acciones) que vayan a realizar y que pudiese impactar en los servicios del ISTRFA, de forma tal que se puedan ejecutar simulacros y evaluar su impacto, previniendo una interrupción de los servicios.
- Acceder a las cintas de respaldo para la restauración de la información en el servidor averiado
- Verificar que el equipo se encuentre en garantía, de lo contrario de implementará un nuevo servidor virtual.

e. Duración
El tiempo máximo de la contingencia no debe sobrepasar las seis (6) horas

3. PROCEDIMIENTO DE RECUPERACIÓN

a) Personal Encargado
El Equipo de Restauración, quienes se encargarán de realizar las acciones de recuperación necesarias.

b) Descripción de actividades
- Al retorno de la energía comercial se verificará por el lapso de media hora que no haya interrupciones o fluctuaciones de energía
- Proceder a encender la plataforma tecnológica ordenadamente de acuerdo al siguientedetalle:
  - Equipos de Comunicaciones (router, switches core, switches de acceso)
  - Equipos de almacenamiento (storage)
  - Servidores físicos por orden de prioridad
  - Servidores virtuales por orden de prioridad
- La contingencia finaliza cuando retorna la energía eléctrica y todos los equipos se encuentran operativos brindando servicio.

c) Mecanismos de Comprobación

El/La Especialista de infraestructura y Redes, presentará un informe a el/la jefe/a de OTI, informando que parte del servicio y equipos han fallado, y cuáles son las acciones correctivas a realizar.

d) Desactivación del Plan de Contingencia

El/La Coordinador/a de Continuidad desactivará el Plan de Contingencia una vez que se recupere la funcionalidad del suministro eléctrico y la operatividad de los sistemas y servicios de tecnología de la información.

CRONOGRAMA

Grupo: 3		Organización de Recursos TI - ATI -III-NOCHE											2023
N°	Actividades	Mayo				Junio				Julio			
	Meses - Semanas	1	2	3	4	1	2	3	4	1	2	3	4
1	Fase 1: Planificación	x	x	x	x	x	x	x					
2	Fase 2: Determinación de Vulnerabilidades					x	x	x	x				
3	Fase 3: Estrategias del Plan de Contingencia					x	x	x	x				
4	F ase 4: Elaboración del Plan de Contingencia								x	x	x	x	
5	Fase 5: Implementación del Plan de Contingencia										x	x	x
6	Fase 6: Monitoreo												x