PLAN DE RECUPERACIÓN DE SERVICIOS INFORMÁTICOS DEL PROGRAMA INTEGRAL NACIONAL PARA EL BIENESTAR FAMILIAR - INABIF

Firmado digitalmente por CHURA GOMEZ Cesar FAU 20507920722 soft
Motivo: Doy V° B°
Fecha: 21.08.2024 16:02:43 -05:00

Firmado digitalmente por SAIRE LLANA Freddy Oscar FAU 20507920722 soft
Motivo: Doy V° B°
Fecha: 21.08.2024 16:46:56 -05:00

Firmado digitalmente por TORRES BENAVIDES Rosario Ana Maria FAU 20507920722 soft
Motivo: Doy V° B°
Fecha: 21.08.2024 16:52:44 -05:00

CONTENIDO

I. ANTECEDENTES

Mediante la Resolución Ministerial N° 320-2021-PCM, emitida el 30 de diciembre de 2021, se aprueban 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"; esto con la finalidad de fortalecer la implementación de la Gestión de la Continuidad Operativa en las entidades públicas ante la ocurrencia de un desastre o cualquier evento que interrumpa prolongadamente sus operaciones.

De esta forma, se fortalece la capacidad de respuesta ante cualquier tipo de crisis, garantizando la operatividad básica y minimizando los tiempos de recuperación de la operatividad en caso de interrupción de los servicios.

En ese sentido, el Programa Integral Nacional para el Bienestar Familiar - INABIF, viene realizando las acciones necesarias, con la finalidad de verificar y dar seguimiento al enfoque de continuidad operativa que permita a los órganos y/o unidades funcionales enfrentar cualquier evento de gran magnitud; así como, fortalecer la capacidad de respuesta y garantizando la operatividad básica en un menor tiempo.

II. FINALIDAD

El Plan de Recuperación de Servicios Informáticos del INABIF, en adelante EL PLAN, es un instrumento que permite recuperar los servicios informáticos ante un evento ocasionado de manera natural o antrópico, a fin de garantizar la continuidad operativa del INABIF; y a su vez, se determine las medidas y acciones que permitan el cumplimiento de sus objetivos de manera eficiente y eficaz.

III. BASE LEGAL

- Ley N° 29664 Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD), y modificatorias.
- Decreto Supremo N° 038-2021-PCM, aprueba la Política Nacional de Gestión del Riesgo de Desastre al 2050.
- Decreto Supremo N° 048-2011-PCM, aprueba el Reglamento de la Ley N° 29664, que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).

- Decreto Supremo N° 115-2022-PCM, aprueba el Plan Nacional de Gestión del Riesgo de Desastres – PLANAGERD 2022-2030.
- Resolución Ministerial N° 188-2015-PCM, aprueba los Lineamientos para la Formulación y Aprobación de Planes de Contingencia.
- Resolución Ministerial N° 004-2016-PCM y modificatorias, 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 Ministerial N° 320-2021-PCM, aprueba los "Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Públicas de los tres niveles de gobierno".
- Resolución Ministerial N° 213-2024-MIMP, aprueba el Manual de Operaciones del Programa Integral Nacional para el Bienestar Familiar – INABIF.
- Resolución de Dirección Ejecutiva N° 000016-2024-INABIF/DE, conforma el "Equipo de Respuestas ante Incidentes de Seguridad Digital del INABIF".

IV. GLOSARIO DE TÉRMINOS

- **Actividades críticas:** Están constituidas por las actividades que la entidad ha identificado como indispensables y que no pueden dejar de realizarse, conforme a sus competencias y atribuciones señaladas en las normas sobre la materia.
- **Activo:** En relación con la seguridad de la información se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas) que tenga valor para la entidad.
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la entidad.
- **Análisis de riesgo:** Es entender las características de la amenaza y su naturaleza, lo que requiere considerar la probabilidad de ocurrencia del evento, el escenario, el posible impacto y los escenarios en los que se puede dar.
- **Evento:** Un suceso o serie de sucesos que pueden ser internos o externos a la entidad, originados por la misma causa, que ocurren durante el mismo periodo de tiempo.
- **Información:** Cualquier forma de registro electrónico, óptico, magnético o en otros medios, susceptible de ser procesada, distribuida y almacenada.

- **Interrupción:** Evento que detiene las funciones, operaciones o procedimientos habituales de la entidad, sea éste previsto (por ejemplo, huracanes, disturbios políticos) o imprevisto (por ejemplo, un apagón, un ataque terrorista o una falla de la tecnología).
- **Plan de Continuidad Operativa**: Documento que debe formar parte de las operaciones habituales diarias de la Unidad de Tecnología de la Información, incluye la identificación de las actividades y servicios críticos que requieren ser ejecutados y prestados de manera ininterrumpida, la determinación de las medidas y acciones que permitan que la entidad siga de manera eficaz y continua con el cumplimiento de sus operaciones y objetivos. Así como, brindar los procedimientos documentados que guían a las entidades para responder, recuperar, reanudar y restaurar a un nivel predefinido de operación debido a la interrupción.
- **Plan de recuperación de servicios informáticos:** Plan que forma parte del Plan de Continuidad Operativa, el cual busca inicialmente restaurar los servicios de tecnología de información, permitiendo una posterior recuperación de las condiciones previas a su ocurrencia. Para su desarrollo se toma en cuenta la Norma Técnica Peruana NTP ISO/IEC 27001:2014.
- **Proceso:** Conjunto de actividades, tareas y procedimientos organizados y repetibles que producen un resultado esperado.
- **Proceso crítico:** Conjunto de actividades indispensables para la continuidad de las operaciones y servicios que brinda la Institución, cuya falta o ejecución deficiente puede producir no cumplir con los objetivos del proceso, ni con los objetivos estratégicos de la Institución y/o generar pérdidas financieras.
- **Riesgo:** Es el efecto que genera la incertidumbre en los objetivos. Los objetos pueden tener un efecto si no los desviamos de lo esperado. Puede ser positivo, negativo o ambos y puede abordar, crear o dar lugar a oportunidades y amenazas. Los objetivos pueden tener distintos aspectos y categorías, y se pueden aplicar a distintos niveles. El riesgo se suele expresar en términos de fuentes de riesgo, eventos potenciales, sus consecuencias y su probabilidad.
- **Servicios:** La actividad o labor que realiza una persona natural o jurídica para atender una necesidad de la entidad, pudiendo estar sujeta a resultados para considerar terminadas sus prestaciones.
- **Servicios críticos:** Son aquellos servicios que, en caso de falla o suspensión del mismo, puede poner en riesgo importante a la entidad, al afectar sus ingresos, solvencia o continuidad operativa.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

V. JUSTIFICACIÓN

Existen innumerables situaciones que pueden afectar los procesos críticos de la entidad, algunas son fáciles de identificar y se pueden implementar ciertos controles preventivos o sistemas de contingencia para mitigarlas.

Para tener una prevención real ante cualquier imprevisto, se debe realizar un estudio metódico de los riesgos a los cuales está expuesta la entidad, la probabilidad de ocurrencia de estos posibles eventos, el impacto que tendrían sobre la operación y sobre todo cómo se debe reaccionar ante su ocurrencia.

Esta no es una tarea que se deba tomar a la ligera, todo lo contrario, está en juego el prestigio de la entidad, el reconocimiento que tiene en el país e incluso su supervivencia, desde este punto de vista se requiere elaborar un estudio que permita entender a qué riesgos está expuesta, qué hacer para minimizarlo y cuál sería el costo de recuperación.

Dentro de los procesos críticos, se encuentran involucrados los servicios asociados a los Sistemas y las Tecnologías de la Información; pues, el contar con los sistemas administrativos como: Servicio de acceso a Sistema Integrado de Gestión Administrativa - SIGA, Servicio de acceso al Sistema Integrado de Administración Financiera - SIAF y Servicio de acceso al Sistema de Gestión Documental - SGD; correo electrónico y acceso a Internet, permiten asegurar la continuidad operativa.

Es por ello que, el presente instrumento se convierte en parte fundamental del Plan de Continuidad Operativa, el cual permitirá dar un diagnóstico del estado actual del INABIF, frente a un posible incidente o evento fortuito que le impida operar de forma normal y de qué manera podrá responder para asegurar la recuperación de los servicios y/o actividades identificadas como críticas.

VI. OBJETIVO

6.1 Objetivo General

Es objetivo del PLAN, mitigar los factores que limiten la continuidad de su operatividad, basado en la disponibilidad de los servicios informáticos que brinda la Unidad de Tecnología de la Información - UTI, y que se encuentran ubicados en el Centro de Datos del INABIF, ante la ocurrencia de un desastre o cualquier evento que interrumpa sus procesos, ejecutando las funciones críticas identificadas, hasta lograr su recuperación en el menor plazo posible.

6.2 Objetivos específicos

- Identificar los riesgos de continuidad que podrían afectar los servicios críticos que brinda la UTI.
- Desarrollar el análisis del impacto en la operatividad de los servicios críticos ante un desastre.
- Establecer estrategias de recuperación y restauración de los servicios críticos de los Sistemas y Tecnologías de la Información.
- Determinar periodos de recuperación requeridos, ante la caída de los servicios críticos que permitan la continuidad operativa.

VII. ALCANCE

EL PLAN, está orientado a garantizar la continuidad operativa de los servicios informáticos e infraestructura tecnológica, considerados como críticos, que se encuentran ubicados en el Centro de Datos del INABIF; sito en Av. San Martín N° 685 - distrito de Pueblo Libre, provincia y región de Lima.

En el siguiente cuadro se muestran las actividades necesarias para cumplir con los objetivos específicos del PLAN.

Cuadro N° 01
Resumen de objetivos específicos y actividades

Objetivo específico	Actividades
Identificar los riesgos de continuidad que podrían afectar los servicios críticos que brinda la UTI.	Realizar el análisis de riesgo de todos los servicios brindados por la UTI.
	Realizar el análisis de las amenazas que puedan afectar los servicios asociados a los Sistemas y Tecnologías de la Información, con dimensiones de valoración ante diversos tipos de amenazas.
	Realizar el análisis de vulnerabilidades existentes en el entorno y que podrían llegar a concretar amenazas que afectarían a los servicios informáticos.
	Evaluar los riesgos.
Desarrollar el análisis del impacto en la operatividad de los servicios críticos ante un desastre.	Desarrollar el análisis del impacto operacional para determinar la criticidad en el caso de una paralización de los servicios.
	Determinar criticidad de los servicios.
	Establecer las prioridades de recuperación de servicios informáticos.
	Identificar los recursos necesarios para EL PLAN.

Objetivo específico	Actividades
Establecer estrategias de recuperación y restauración de los servicios críticos de los Sistemas y Tecnologías de la Información.	Identificar los diferentes escenarios de paralización de servicios críticos junto con sus diversas alternativas de solución para poder definir estrategias de continuidad. Las alternativas de continuidad deben ser flexibles para actuar sobre diferentes escenarios de paralización.
Determinar periodos de recuperación requeridos, ante la caída de los servicios críticos que permitan la continuidad operativa.	Se debe mostrar las actividades a desarrollar en el antes, durante y después de la interrupción de los servicios críticos. Mostrar el detalle de estrategias de continuidad y alternativas de solución en diversos escenarios. Realizar los lineamientos generales de procedimientos y plantillas de continuidad.

VIII. IDENTIFICACIÓN DE RIESGOS

Para la aplicación del PLAN, se ha considerado los peligros ante los cuales la entidad es vulnerable, teniendo como base las capacidades y funciones que debe cumplir.

Las amenazas a las que la entidad está expuesta se pueden clasificar de la siguiente manera:

- Ataques intencionados.
- Desastres industriales.
- Desastres naturales.
- Errores y fallos no intencionados.

Para efectos de planeamiento, se considera como peor escenario aquellos riesgos que tiene un impacto "Muy Alto" en la continuidad operativa como: La ocurrencia de un ataque informático, incendio o sismo de gran magnitud, el fallo de un componente parte de los servicios críticos, el corte del servicio del fluido de energía eléctrica, el corte del servicio de Internet, entre otros.

A partir de la vigencia del PLAN, todas las unidades funcionales del INABIF, deben establecer sus acciones de continuidad operativa, las mismas que deben guardar relación con el mismo, teniendo en cuenta sus funciones, ámbito de influencia, y responsabilidades.

8.1 Evaluación del riesgo

Para poder realizar la evaluación de los riesgos, se ha utilizado la "Matriz de probabilidad e impacto" referido a las amenazas y su probabilidad de ocurrencia, obteniendo como resultado la "Matriz de evaluación de riesgos".

Los resultados que muestra la "Matriz de evaluación de riesgos" son fundamentales; ya que, en los que se muestran un nivel de riesgo "Muy Alto", son los escenarios donde se deben desarrollar las alternativas de solución a efectos que se evite, mitigue, transfiera; o como también, se acepten determinados riesgos.

Para determinar la valorización del riesgo, se usa~~rá~~ dos criterios, la probabilidad de que ocurra un riesgo, y el impacto sobre la operatividad de los servicios.

Cuadro N° 02
Escala de valoración de la probabilidad de ocurrencia de riesgos

Probabilidad	Descripción
Muy Alta	Es muy probable que ocurra un evento de esta naturaleza en un periodo menor a tres (3) meses.
Alta	Es probable que ocurra un evento de esta naturaleza en un periodo de tres (3) a seis (6) meses.
Media	El evento ocurre en algún momento en un periodo mayor a seis (6) meses a un año.
Baja	Es poco probable que el evento suceda, pero puede ocurrir en algún momento de un periodo de un (1) año a dos (2) años.
Muy Baja	Es muy poco probable que el evento ocurra en un periodo mayor a dos (2) años o no se detectaron vulnerabilidades que aumenten su probabilidad de ocurrencia.

Cuadro N° 03

Matriz para la escala de valoración del riesgo

(Probabilidad de ocurrencia del riesgo / Impacto en la operatividad del servicio)

		PROBABILIDAD				
		Muy Baja	Baja	Media	Alta	Muy Alta
IMPACTO	Muy Bajo	Bajo	Bajo	Bajo	Medio	Medio
	Bajo	Bajo	Bajo	Medio	Medio	Medio
	Medio	Medio	Medio	Medio	Alto	Alto
	Alto	Medio	Medio	Alto	Alto	Muy Alto
	Muy Alto	Medio	Alto	Alto	Muy Alto	Muy Alto

A partir de los Cuadros N°s 02 y 03; se ha construido el siguiente cuadro, denominado "Matriz de evaluación de riesgos", en el cual se identifica la valorización de cada tipo de riesgo.

Cuadro N° 04

Matriz de evaluación de riesgos

Tipo de amenaza	Amenaza	Probabilidad de ocurrencia	Impacto	Valoración del riesgo
Ataques intencionados	Abuso de privilegios de acceso	Alta	Muy Alto	**Muy Alto**
	Ataques de ingeniería social	Muy Alta	Alto	**Muy Alto**
	Ciberataques	Muy Alta	Muy Alto	**Muy Alto**
	Difusión de software dañino	Muy Alta	Muy Alto	**Muy Alto**
	Divulgación de información	Media	Bajo	**Medio**
	Modificación deliberada de la información	Alta	Muy Alto	**Muy Alto**
Desastres industriales	Avería del sistema de climatización	Media	Alto	**Alto**

Tipo de amenaza	Amenaza	Probabilidad de ocurrencia	Impacto	Valoración del riesgo
	Corte de fluido eléctrico	Alta	Muy Alto	**Muy Alto**
	Fallo de un equipo parte de los servicios críticos	Alta	Muy Alto	**Muy Alto**
	Fallo del servicio de comunicaciones	Alta	Muy Alto	**Muy Alto**
	Incendio por corto circuito	Alta	Muy Alto	**Muy Alto**
	Inundación por rotura de matriz	Muy Baja	Muy Alto	**Medio**
	Problemas con el sistema de UPS	Alta	Medio	**Alto**
Desastres naturales	Inundación por precipitaciones	Baja	Medio	**Medio**
	Sismo de gran magnitud	Alta	Muy Alto	**Muy Alto**
	Tsunami	Baja	Muy Alto	**Medio**
Errores y fallos no intencionados	Alteración accidental de la información	Media	Muy Alto	**Alto**
	Caída del sistema por agotamiento de recursos	Baja	Alto	**Medio**
	Carencia de Alta Disponibilidad (HA)	Media	Alto	**Alto**
	Destrucción de la información	Baja	Muy Alto	**Alto**
	Errores de los administradores de servicios informáticos	Baja	Alto	**Medio**
	Errores de los usuarios	Muy Alta	Medio	**Medio**
	Fallo en las copias de seguridad	Alta	Muy Alto	**Muy Alto**

La Matriz de evaluación de riesgos, evidencia que, los eventos que ponen en riesgo la operatividad de entidad son aquellos que tiene la valoración de **Muy Alto**; por lo que, la entidad tendría que estar preparada para hacer frente a estos riesgos:

- Abuso de privilegios de acceso.
- Ataques de ingeniería social.
- Ciberataques.
- Corte de fluido eléctrico.
- Difusión de software dañino.
- Fallo de un equipo parte de los servicios críticos.
- Fallo del servicio de comunicaciones.
- Fallo en las copias de seguridad.
- Incendio por corto circuito.
- Modificación deliberada de la información.
- Sismo de gran magnitud.

8.2 Análisis del impacto operacional

Para realizar el análisis del impacto de la continuidad operativa del INABIF, se identifican los servicios informáticos necesarios para el desarrollo de sus actividades.

8.2.1 Identificación de los servicios críticos

Para identificar los niveles de criticidad de los servicios que brinda la UTI del INABIF, se debe establecer si un servicio es crítico o no; para ello se utiliza la siguiente tabla:

Cuadro N° 05
Tabla de criticidad de servicio

Valor	Interpretación del proceso crítico
Crítico	Crítico para la operatividad de la entidad.
No Crítico	No crítico para la operatividad de la entidad.

8.2.2 Evaluación de impactos operacionales

Para la evaluación de impactos operacionales se utiliza la matriz siguiente, en la que se identifican las categorías por servicio y si estos servicios son críticos o no.

Cuadro N° 06

Identificación del nivel de criticidad de los servicios brindados por la UTI

Categoría del servicio	Servicio	Nivel	Descripción
Aplicaciones Cliente/Servidor	Servicio de acceso al Sistema Integrado de Administración Financiera – SIAF	**Crítico**	Software Implantado por MEF para realizar la ejecución y el control Presupuestal y Financiero de las Entidades del Estado. Necesario para operar a nivel institucional.
	Servicio de acceso al Sistema de Personal	**No Crítico**	Software cedido por el MEF a fin de elaborar las planillas de pago. Necesario para el pago de planillas.
	Servicio de acceso a Sistema Integrado de Gestión Administrativa - SIGA	**Crítico**	Software que gestiona los actos administrativos (Abastecimiento, Tesorería y Patrimonio). Necesario para operar a nivel institucional.
	Servicio de consulta a Sistema de Trámite Documentario – STD	**No Crítico**	Sistema legado, en el cual se almacenan los trámites realizados entre el 2004 al 2019. Sistema utilizado actualmente para consultas.
	Servicio de consulta al sistema de Marcaciones - Tempus	**No Crítico**	Sistema que administra las marcaciones almacenadas en los terminales de mercado.
	Servicio de consulta al Sistema Integrado Administrativo – Integrix 2000	**No Crítico**	Sistema legado, módulos de Abastecimiento, Patrimonio, Tesorería, Personal, registros realizados entre el 2000 al 2019. Sistema utilizado

Categoría del servicio	Servicio	Nivel	Descripción
			actualmente para consultas.
Aplicaciones Web	Servicio de correo electrónico	**Crítico**	Servidor Zimbra para Correo Electrónico. Necesario para operar a nivel institucional.
	Servicio de acceso al Sistema de Gestión Documental – SGD	**Crítico**	Software de Gestión Documental. Necesario para operar a nivel institucional.
	Servicio de acceso a la Intranet Institucional	**Crítico**	Portal interno de INABIF, utilizado por los servidores de INABIF para acceder a sistemas administrativos y misionales. Necesario para operar a nivel institucional.
	Servicio de acceso a Mesa de Partes Digital	**No Crítico**	Aplicativo que permite recibir los trámites por parte de los ciudadanos de manera virtual. Parte de GOB.PE, el cual es gestionado por la PCM.
	Servicio de acceso a Postulaciones electrónicas	**No Crítico**	Aplicativo que permite gestionar las convocatorias del personal. Parte de GOB.PE, el cual es gestionado por la PCM.
	Servicio de acceso al Portal Institucional	**No Crítico**	Servidor que contiene la información institucional. Parte de GOB.PE, el cual es gestionado por la PCM.
	Servicio de acceso al Portal Estadístico – INABIF en Cifras	**No Crítico**	Servidor que contiene la información institucional mostrada al exterior.

Categoría del servicio	Servicio	Nivel	Descripción
	Servicio de acceso al Aula Virtual	**No Crítico**	Servidor que contiene información de los cursos brindados por la entidad a sus trabajadores.
Base de Datos	Servicio de Base de Datos Oracle	**Crítico**	Base de Datos utilizado por el SGD, Intranet, SIGA.
	Servicio de Base de Datos SQL Server	**No Crítico**	Base de Datos utilizado por los sistemas legados INTEGRIX, TEMPUS, STD
	Servicio de Base de Datos MySQL	**No Crítico**	Base de Datos utilizada para los servicios expuestos a la Web. Mesa de Partes Digital, Postulaciones electrónicas, entre otros.
Seguridad la Información	Servicio de seguridad perimetral – Firewall.	**Crítico**	Servicio de seguridad perimetral.
	Servicio de antispam	**Crítico**	Servicio de seguridad para el servidor de correo electrónico para el filtrado del correo no deseado (SPAM)
	Servicio de Conexión a VPN	**Crítico**	Servicio de Conexión Segura a la Red Local. Necesario para que los usuarios se conecten a los servicios de INABIF.
	Antivirus	**No Crítico**	Servicio de Protección de los equipos de los trabajadores (computadoras).
Sistema de Almacenamiento	Servicio de archivos compartidos	**Crítico**	Servidores para guardar / compartir información. Necesario para acceder a la información compartida.

Categoría del servicio	Servicio	Nivel	Descripción
	Servicio de FTP	**No Crítico**	Servidor para compartir información.
Comunicaciones	Servicio de acceso a Internet	**Crítico**	Servicio para navegar por Internet / Brindar servicio a usuarios externos. Necesario para acceder al SGD, SIAF, Intranet, Correo, exponer servicios y navegar en la Web.
	Servicio de Telefonía Fija	**No Crítico**	Servicio utilizado para la comunicación interna (entre oficinas) y externa (ciudadanos). No indispensable para operar.
	Servicio de Telefonía Móvil	**No Crítico**	Servicio utilizado para la comunicación institucional. No indispensable para operar.
	Servicio de Videoconferencia	**No Crítico**	Servicio de comunicación a través de salas de trabajo. No indispensable para operar.

Los servicios identificados como "Críticos", son necesarios para operar mínimamente ante cualquier desastre, y son los siguientes:

- Servicio de acceso a Internet.
- Servicio de acceso a la Intranet Institucional.
- Servicio de acceso al Sistema de Gestión Documental – SGD.
- Servicio de acceso al Sistema Integrado de Administración Financiera – SIAF.
- Servicio de acceso al Sistema Integrado de Gestión Administrativa – SIGA.
- Servicio de antispam.
- Servicio de archivos compartidos.
- Servicio de Base de Datos Oracle.
- Servicio de conexión a VPN.
- Servicio de correo electrónico.
- Servicio de seguridad perimetral – Firewall.

8.2.3 Establecimiento de tiempos de recuperación

Los tiempos de recuperación, recomendados por la Norma ISO/IEC 27031:2011 (Directrices para la adecuación de Tecnologías de la Información y Comunicación para la continuidad del negocio) y otras guías para la elaboración del diseño del plan de continuidad de servicios críticos; se detallan en el siguiente cuadro:

Cuadro N° 07
Descripción de tiempos de recuperación

Tiempo de recuperación	Denominación	Descripción
RPO	Objetivo de Punto de Recuperación (Recovery Point Objective)	Punto en el tiempo que puede tolerar un proceso de negocio referente a la pérdida de datos.
RTO	Objetivo de Tiempo de Recuperación (Recovery Time Objective)	Periodo de tiempo para poder recuperar los niveles de servicio mínimos y/o recursos que han sufrido una interrupción.
MTD	Tiempo Máximo de Inactividad Tolerable (Maximum Tolerable Downtime)	Periodo máximo de tiempo de inactividad que puede tolerar la entidad sin entrar en colapso.

Fuente: NTP-ISO/IEC 27031:2012 (revisada el 2022)

El tiempo de tolerancia a fallas, es el tiempo máximo que se estima puede estar inoperativo un servicio, sin que esto impacte drásticamente en la operatividad de la entidad; por lo que, se deben establecer mecanismos que permitan la recuperación dentro de estos tiempos para evitar su paralización.

Por ello, los servicios identificados como "Críticos" en el Cuadro N° 06, son prioridad 1 para su restauración; y los servicios considerados como "No Críticos" son prioridad 2; el siguiente cuadro muestra los niveles de recuperación.

Cuadro N° 08
Prioridad y tiempo de recuperación de los servicios críticos

Nivel de Servicio	Prioridad	RPO (Horas)	RTO (Horas)	MTD (Horas)
Crítico	1	3	4	4
No Crítico	2	10	12	12

En esta tabla, se define el punto y tiempo de recuperación, siendo importante señalar la diferencia entre ambos, ya que punto de recuperación se refiere al tiempo soportado por la entidad en relación a la pérdida de datos, mientras que tiempo de recuperación se refiere al periodo en el que se restablecen los servicios mínimos para seguir operando. El punto de restauración para los servicios críticos es de tres (3) horas y el tiempo de recuperación es de cuatro (4) horas.

8.3 Recursos necesarios para atender los incidentes

De las actividades de detalladas en el numeral 9.4.3, se desprenden los recursos y/o servicios que se requieren para dar respuesta a cada uno de los incidentes indicados:

Recursos humanos:

Los recursos humanos que intervienen ante la interrupción de un servicio crítico, son en primera instancia las personas involucradas en el tipo de incidente generado; sin embargo, para obtener un mejor seguimiento del incidente, es necesario la intervención del "Equipo de Respuestas ante Incidentes de Seguridad Digital del INABIF", conformado mediante la Resolución de Dirección Ejecutiva N° 000016-2024-INABIF/DE, en adelante EL EQUIPO.

Infraestructura tecnológica:

Se requiere contar con Centro de Datos, nivel 3, con las siguientes características:

- Sistema eléctrico estabilizado independiente.
- Sistema de puesta a tierra y estática.
- Sistema de energía suplementaria (UPS).
- Sistema de respuesta ante corte de energía (grupo electrógeno).
- Sistema contra incendios.
- Sistema de seguridad y control de accesos.
- Sistema de climatización.
- Sistema de monitoreo.

Asimismo, se debe contar con equipamiento que garantice alta disponibilidad; por lo que, se requiere que los equipos de comunicaciones; servidores y conexiones se encuentren configurados en redundancia.

Recursos informáticos:

- Computadoras personales.
- Impresora multifuncional.
- Equipos de comunicaciones.
- Gabinetes.
- Aire Acondicionado.
- Sistema de monitoreo y video seguridad.

Servicios necesarios:

- Servicio de acceso a Internet; principal y redundante.
- Servicio de actualización y soporte del Sistema Oracle.
- Servicio de copias de respaldo.
- Servicio de emisión de Certificados Digitales SSL.
- Servicio de licencia de un sistema antivirus.
- Servicio de mantenimiento del sistema de climatización.
- Servicio de mantenimiento del sistema de puesta a tierra.
- Servicio de mantenimiento y soporte de bases de datos.
- Servicio de plataforma como servicio - contingencia
- Servicio de seguridad perimetral.
- Servicio de suscripción de actualización del sistema operativo de servidores.
- Servicio de telefonía fija.
- Servicio de telefonía móvil.
- Servicio de videoconferencia.

IX. ACCIONES PARA LA RECUPERACIÓN DE SERVICIOS INFORMÁTICOS

Para plantear las estrategias de continuidad, nos basaremos en las amenazas identificadas con un riesgo "**Muy Alto**" para proponer alternativas de solución que se adecuen a posibles escenarios de interrupción.

Se brinda el detalle de cómo se debe actuar ante cada posible escenario de paralización con diferentes causas. Si bien es cierto, se plantean diversos escenarios, pero en la "Matriz de evaluación de riesgos" se hace énfasis en los

servicios críticos principales considerados por la entidad según la categorización del "Cuadro N° 08 Prioridad y tiempo de recuperación de los servicios críticos".

Las estrategias para el plan de continuidad de servicios críticos de Tecnologías de la Información se muestran en el Anexo N° 01: Estrategias de acción para mitigar las amenazas a los servicios informáticos.

9.1. Actividades del equipo de respuesta ante un incidente

EL EQUIPO ante la interrupción de un servicio crítico está conformado, entre otros, por los servidores de la UTI que han sido designados con la Resolución de Dirección Ejecutiva N° 000016-2024-INABIF/DE, que se señalan a continuación:

- El/La Coordinador/a de la UTI o quien haga sus veces, actúa como Coordinador/a del Equipo.
- El representante de la UTI quien desempeñe el rol de Gestor/a de Infraestructuras Digitales.
- El representante de la UTI quien desempeña el rol de Gestor/a de Redes y Comunicaciones.

Las actividades mínimas que desarrolla EL EQUIPO; frente a la interrupción de un servicio crítico; antes, durante y después de la interrupción son las siguientes:

a) Actividades del PLAN que se deben realizar *"antes"* de una interrupción de un servicio crítico:

Antes de que se presente alguna interrupción de servicio por determinada causa, EL EQUIPO debe asegurarse que todos los registros se encuentran completos y disponibles, tanto dentro de la entidad como fuera de ésta; es decir, que se debe tener evidencia de los siguientes puntos:

- Elaborar el Plan de Pruebas, a partir del PLAN, que se aplica en cada emergencia para restablecer el servicio afectado; el procedimiento, para cada caso, debe contemplar todas las actividades hasta que se restablezca el servicio. El Plan de Pruebas debe incluir una lista de cotejo.
- Probar cada procedimiento del Plan de Pruebas. Esto incluye las simulaciones, capacitaciones, entrenamientos, seguimientos,

evaluaciones y acciones necesarias. El Plan de Pruebas y el resultado de las pruebas realizadas debe ser informado a la Unidad de Administración y formular los requerimientos identificados, de ser necesario.

- Elaborar la lista del personal interno y externo a quien se reportará determinado incidente, principalmente nombres, apellidos, correo electrónico, número de celular y/o procedimiento para reportar un incidente.
- Disponibilidad necesaria frente a una emergencia (interrupción), hasta lograr restablecer el servicio.
- Verificar que se encuentren disponibles cada uno de los recursos que sean indispensables para mantener la continuidad de las operaciones de la entidad.
- Guardar los registros, incluidos las guías de instalación, configuraciones, usuarios, roles, accesos, niveles de privilegios, etc., y que sean almacenados tanto dentro como fuera de la entidad con fácil acceso a los encargados de los incidentes.
- Actualizar y aprobar EL PLAN, incluyendo las soluciones brindadas en las últimas emergencias superadas.

Una vez realizadas las pruebas para comprobar que el Plan de Pruebas ha funcionado tal y como se esperaba; debe ser evaluado para retroalimentar con comentarios, conclusiones y recomendaciones que permitan mejorarlo y ajustarlo a las nuevas necesidades. Las pruebas a realizar son de: seguridad, mantenimiento, soporte, recuperación, disponibilidad, funcionalidad y desempeño.

b) Actividades del PLAN que se deben realizar "durante" una interrupción de un servicio crítico:

Cuando se presente alguna interrupción de servicio por determinada causa, EL EQUIPO deben realizar las siguientes actividades:

- Informar a los responsables (interno o externo) a cargo del servicio crítico a fin de iniciar el proceso de recuperación.
- Utilizar los recursos indispensables para la recuperación, utilizando los recursos previstos como contingencia; copias de respaldo u servicios de contingencia que se disponga.
- Ejecutar el Plan de Pruebas desarrollando las actividades según la lista de cotejo.

- Ejecutar el procedimiento para poner en funcionamiento el equipamiento/servicio de alta disponibilidad que cuente la entidad; en caso sea necesario durante el periodo de emergencia.

c) Actividades del PLAN que se deben realizar "después" de una interrupción de un servicio crítico:

Se debe verificar el cumplimiento de todas las actividades y procedimientos necesarios para superar la emergencia; y documentar las acciones desplegadas; así como todo lo nuevo no contemplado en el procedimiento establecido en el Plan de Pruebas, a fin de ser incorporadas en emergencias similares futuras; las actividades mínimas a realizar son:

- Terminada la emergencia, se remite a la Unidad de Administración, el Informe correspondiente, que contenga como mínimo lo siguiente:

  - El diagnóstico de las causas raíz que ocasionaron la interrupción del servicio crítico.
  - Lo relevante de la recuperación, las estrategias aplicadas, los resultados obtenidos y un breve resumen del trabajo realizado.
  - El retorno a la normalidad con los comentarios conclusiones y recomendaciones que permitan mejorar EL PLAN mediante las lecciones aprendidas en cada emergencia superada.

- Actualizar EL PLAN, y el Plan de Pruebas que incluya las nuevas situaciones presentadas en las últimas emergencias.

9.2. Gestión de los incidentes

Reportado/identificado una falla o interrupción de un servicio, el servidor que tenga el rol de Gestor/a de Incidentes en EL EQUIPO, realiza las siguientes acciones:

- Notificar a los usuarios clave sobre la interrupción del servicio.
- Aperturar y registrar el incidente.
- Confirmar que se haya solucionado el incidente.
- Notificar a los usuarios el restablecimiento de los servicios.
- Cerrar el incidente.

Para el registro del incidente se utiliza el Anexo N° 02: Formato para el registro de incidentes.

9.3. Actividades a desarrollar por tipo de incidente

Las actividades a desarrollar por cada tipo de incidente se encuentran detalladas en el Anexo N° 03: Actividades generales para las alternativas de solución en los diversos escenarios.

Asimismo, debido a que las actividades mencionadas en el párrafo anterior deben ser actualizadas periódicamente, es necesario que EL EQUIPO realice la actualización respetiva, haciendo de conocimiento a la Dirección Ejecutiva de las mismas mediante un Informe.

9.4. Requerimientos

9.4.1. Requerimiento de personal

La entidad debe asegurarse de que todo el personal al que le asignan responsabilidades del PLAN, pueda ejecutarlo; es por ello que, su ejecución está a cargo del EQUIPO, el cual tiene entre otras, la función de "Adoptar medidas para la gestión de riesgos e incidentes de seguridad digital que afecten a los activos de la entidad", y está conformado de la siguiente manera:

- El/La Coordinador/a de la UTI o quien haga sus veces, actúa como Coordinador/a del Equipo.
- Un/Una representante de la UTI o quien haga sus veces, desempeña el rol de Gestor/a de Incidentes.
- Un/Una representante de la UTI o quien haga sus veces, desempeña el rol de Gestor/a de Infraestructuras Digitales.
- Un/Una representante de la UTI o quien haga sus veces, desempeña el rol de Gestor/a de Redes y Comunicaciones.
- Un/Una representante del equipo de atención al usuario de la UTI o quien haga sus veces, quien tiene el rol de miembro.
- El/La Oficial de Seguridad y Confianza Digital, quien tiene el rol de miembro.

El personal debe capacitarse constantemente en materia de seguridad y tecnologías de la información, por lo que deben estar comprendidas en el Plan de Desarrollo de las Personas de la entidad; asimismo, cuando se adquiera infraestructura tecnológica, el rubro de capacitaciones debe ser parte de los términos de referencia.

9.4.2. Requerimiento de infraestructura tecnológica

En el caso de infraestructura tecnológica, si bien es cierto se cuenta con un Centro de Datos, que tiene nivel 1; sin embargo, a fin de enfrentar los riesgos es necesario contar con un Centro de Datos nivel 3, para lo cual se elaborará el proyecto correspondiente.

9.4.3. Requerimiento de recursos de informáticos

Actualmente se cuenta la infraestructura necesaria para brindar los servicios, existiendo brechas a nivel de infraestructura que permitan contar equipos en redundancia que garanticen la alta disponibilidad; sin embargo, con la implementación de un nuevo Centro de Datos, las brechas se reducirán drásticamente.

9.4.4. Requerimiento de servicios necesarios

Para operar bajo condiciones que permitan hacer frente y mitigar las amenazas, el INABIF viene contratando servicios, a fin de que estos sean trasladados a los usuarios finales o en su defecto a fin de mejorar la seguridad; sin embargo, a fin de cubrir al 100% los riesgos identificados en EL PLAN, es necesario adquirir algunos servicios complementarios, los cuales se detallan a continuación:

- Servicio de acceso a Internet; principal y redundante.
- Servicio de actualización y soporte del Sistema Oracle.
- Servicio de copias de respaldo.
- Servicio de emisión de Certificados Digitales SSL.
- Servicio de licencia de un sistema antivirus.
- Servicio de mantenimiento del sistema de climatización.
- Servicio de mantenimiento del sistema de puesta a tierra.
- Servicio de mantenimiento y soporte de bases de datos.
- Servicio de plataforma como servicio - contingencia
- Servicio de seguridad perimetral - Firewall.
- Servicio de suscripción de actualización del sistema operativo de servidores.
- Servicio de telefonía fija.
- Servicio de telefonía móvil.
- Servicio de videoconferencia.

9.4.5. Recursos presupuestales

Cuadro N° 09
Listado de servicios contratados/adquiridos que coadyuvan a la entrega de servicios brindados por la UTI

N°	Servicio necesario	Costo anual	Estado	Presupuestado en el año	Vigencia del servicio
1	Servicio de acceso a Internet; principal y redundante.	160,000.00	Contratado	Si	22/Oct/2024
2	Servicio de actualización y soporte del Sistema Oracle.	36,000.00	Contratado	Si	8/May/2026
3	Servicio de copias de respaldo.	**70,000.00**	**No Contratado**	**No**	
4	Servicio de emisión de Certificados Digitales SSL.	14,000.00	Contratado	Si	31/May/2025
5	Servicio de licencia de un sistema antivirus.	38,000.00	Contratado	Si	28/Dic/2024
6	Servicio de mantenimiento del sistema de climatización.	**5,000.00**	**No Contratado**	**No**	
7	Servicio de mantenimiento del sistema de puesta a tierra.	12,000.00	Contratado	Si	21/May/2025
8	Servicio de mantenimiento y soporte de bases de datos.	30,000.00	Contratado	Si	21/May/2025
9	Servicio de plataforma como servicio - contingencia	**70,000.00**	**No Contratado**	**No**	
10	Servicio de seguridad perimetral - Firewall.	240,000.00	Contratado	Si	22/Oct/2024
11	Servicio de suscripción de actualización del sistema operativo de servidores.	**34,000.00**	**No Contratado**	**No**	
12	Servicio de telefonía fija.	42,000.00	Contratado	Si	24/Nov/2025
13	Servicio de telefonía móvil.	164,000.00	Contratado	Si	29/May/2025
14	Servicio de videoconferencia	12,500.00	Contratado	SI	27/Mar/2025
Costos anuales de servicios necesarios		**927,500.00**			

Los servicios no contratados a la fecha ascienden aproximadamente al monto de S/ 179,000.00 (Ciento setenta y nueve mil con 00/100 soles); los mismos que serán ejecutados, con base a la disponibilidad y/o priorización presupuestal con la que cuenta la UTI.

Asimismo, para la adecuada ejecución del PLAN, es necesario mantener los servicios actualmente contratados para los siguientes años.

X. CRONOGRAMA DEL PLAN RECUPERACIÓN DE SERVICIOS INFORMÁTICOS

Actividades	2024	2025		Responsable
	IV Trimestre	I Trimestre	II Trimestre	
Implementar el Servicio de plataforma como servicio - contingencia	**X**			UTI
Implementar el Servicio de copias de respaldo.	**X**			UTI
Implementar el Servicio de suscripción de actualización del sistema operativo de servidores.	**X**			UTI
Implementar el Servicio de mantenimiento del sistema de climatización.	**X**			UTI
Capacitar al Equipo de Respuesta para recuperación de servicios informáticos		**X**		UTI
Formular el Plan de Prueba		**X**		UTI
Ejecutar el Plan de Pruebas		**X**		UTI
Implementar lecciones aprendidas			**X**	UTI

XI. ANEXOS

Anexo N° 01: Estrategias de acción para mitigar las amenazas a los servicios informáticos.

Anexo N° 02: Formato para el registro de incidentes.

Anexo N° 03: Actividades generales para las alternativas de solución en los diversos escenarios.

Anexo N° 01
Estrategias de acción para mitigar las amenazas a los servicios informáticos

TIPO DE AMENAZA	AMENAZA	POSIBLE ESCENARIO DE FALLA DE LOS SERVICIOS	POSIBLE CAUSA DE FALLA DE LOS SERVICIOS	N° DE ESTRATEGIA	ESTRATEGIA(A) DE CONTINUIDAD
Ataques intencionados	Abuso de privilegios de accesos	Borrado o alteración de datos y/o archivos.	Usuario disconforme con accesos administrativos a los sistemas	1	• Contar con copias de respaldo. • Contar con los sistemas operativos en sus últimas versiones. • Instalar los paquetes de actualización. • Contar con software antivirus actualizado. • Contar con un sistema de seguridad perimetral. • Contar con un sistema antispam. • Realizar patrullaje electrónico. • Contar con procedimiento para contactar al proveedor de seguridad perimetral, software antivirus, software antispam. • Contar con políticas de acceso al Centro de Datos.
	Ataques de ingeniería social	Captura de credenciales para ser utilizadas en delitos informáticos.	Usuarios pocos capacitados para identificar amenazas informáticas		
	Ciberataques	Daño o secuestro de datos o archivos de algún sistema crítico	Delincuentes informáticos que deliberadamente quieren hacer daño a la entidad		
	Difusión de software dañino	Daño o secuestro de datos o archivos de algún sistema crítico	Delincuentes informáticos con acceso a los recursos informáticos		
	Modificación deliberada de la información	Borrado o alteración de datos y/o archivos.	Delincuentes informáticos con credenciales validadas		

TIPO DE AMENAZA	AMENAZA	POSIBLE ESCENARIO DE FALLA DE LOS SERVICIOS	POSIBLE CAUSA DE FALLA DE LOS SERVICIOS	N° DE ESTRATEGIA	ESTRATEGIA(A) DE CONTINUIDAD
Desastres industriales	Corte de fluido eléctrico	Corte de fluido eléctrico en las instalaciones donde se ubica el Centro de Datos.	• Cortes programados. • Cortes no programados. • Corte por falta de pago	2	• Contar con un grupo electrógeno estable en el edificio. • Contar con un sistema óptimo de UPS • Realizar el mantenimiento preventivo de los equipos e instalaciones eléctricas. • Contar con procedimiento para contactar al proveedor de energía eléctrica.
	Fallo de uno de los equipos parte de los servicios críticos	Falla de uno de los componentes computacionales o conectividad parte de la infraestructura Tecnológica en los cuales se soporta los servicios críticos de INABIF	• Término de la vida útil del equipo o componente. • Falta de mantenimiento del equipo o componente. • Falla de fábrica del equipo o componente. • Daño por algún evento externo.	3	• Contar con plan de mantenimiento. • Contar con plan de renovación de equipos por obsolescencia tecnológica. • Contar con sistema de puesta a tierra. • Contar con estabilizadores de energía eléctrica. • Contar con el registro de las garantías de los equipos y componentes. • Contar con el procedimiento de contacto del fabricante o servicio técnico autorizado local.
		Falla de uno de los componentes de seguridad/contingencia como: UPS; Aire Acondicionado; equipo contra incendio; grupo electrógeno parte de la infraestructura Tecnológica en los cuales se soporta los servicios críticos de INABIF			

TIPO DE AMENAZA	AMENAZA	POSIBLE ESCENARIO DE FALLA DE LOS SERVICIOS	POSIBLE CAUSA DE FALLA DE LOS SERVICIOS	N° DE ESTRATEGIA	ESTRATEGIA(A) DE CONTINUIDAD
	Fallo del servicio de comunicaciones.	Corte del servicio de Internet	• Falta de pago del servicio. • Problema con el router ubicado en la oficina principal. • Problema con la red del proveedor	4	• Contar con el procedimiento de contacto del fabricante o servicio técnico autorizado local. • Contar con un proveedor alterno para que entre en funcionamiento inmediatamente luego de una caída
	Incendio por corto circuito.	Problema en los tableros de energía eléctrica parte del circuito eléctrico del Centro de Datos	• Cruce de un componente parte de la infraestructura tecnológica del Centro de Datos. • Falla de alguna de las llaves térmicas. • Recalentamiento de los cables que alimentan los tableros eléctricos	5	• Contar con sistema contra incendios. • Contar con un sistema de puesta a tierra. • Contar con plan de mantenimiento preventivo de las instalaciones eléctricas • Contar con mecanismo de redundancia pasivo o activo.
Desastres naturales	Sismo de gran magnitud	Sismo de gran magnitud que afecte la infraestructura civil donde se encuentre ubicados los equipos en los que soporta los servicios críticos	Corte de fluido eléctrico	2	Actuar conforme según la estrategia definida en el escenario de falla
			Fallo de uno de los equipos parte de los servicios críticos	3	
			Fallo del servicio de comunicaciones.	4	

TIPO DE AMENAZA	AMENAZA	POSIBLE ESCENARIO DE FALLA DE LOS SERVICIOS	POSIBLE CAUSA DE FALLA DE LOS SERVICIOS	N° DE ESTRATEGIA	ESTRATEGIA(A) DE CONTINUIDAD
			Incendio por corto circuito.	5	
Errores y fallos no intencionados	Fallo en las copias de seguridad.	Fallo en la ejecución del software del sistema de copias de seguridad o en el equipo en que se ejecuta.	Mala realización de la copia de seguridad (no se realizó prueba de restauración periódica)	6	• Contar con políticas para realizar las copias de seguridad. • Verificar el estado de las copias de seguridad. • Realizar el mantenimiento y pruebas de los dispositivos/equipos donde se generan/guardan las copias de seguridad
			Mal cálculo de espacio en cinta para backup		
			Dispositivo en el que se almacenan las copias se encuentra dañado.		
			Negligencia por parte de la persona encargada de hacer las copias de seguridad.		

Anexo N° 02

Formato para el registro de incidentes

Registro de incidente N° _____ -20___	
Fecha:	
Lugar:	
Servicio/s crítico/s afectado/s:	
1. OBJETIVO	
Contar con el registro de los incidentes de interrupción de los servicios críticos de los sistemas de información y tecnologías de la información y comunicaciones que afecten la continuidad operativa de la entidad.	
2. ALCANCE DE LA INTERRUPCIÓN DEL SERVICIO	
3. ESCENARIO DEL SERVICIO CRÍTICO AFECTADO	
3.1 Antes de la emergencia	
Emergencia	
Diagnóstico	
3.2 Durante la emergencia	
Detalle de la solución	
3.3 Después de la emergencia	
Normalidad	
4. DESCRIPCIÓN DE EVENTOS NUEVOS O NO CONTEMPLADOS EN EL PLAN	

4.1 El responsable del servicio verificó que el servicio crítico fue restablecido
5. RECOMENDACIONES A IMPLEMENTAR ANTE FUTUROS INCIDENTES SIMILARES
6. FIRMA DEL RESPONSABLE GESTOR DEL INCIDENTE

Anexo N° 03

Actividades generales para las alternativas de solución en los diversos escenarios

A continuación, se detalla las acciones y actividades a desarrollar ante un evento que indisponga un servicio crítico de los sistemas de información tecnologías de la información y comunicaciones del Programa Integral Nacional para el Bienestar Familiar - INABIF.

1. CORTE DEL FLUIDO ELÉCTRICO

1.1. Corte del fluido eléctrico por parte del proveedor.

Acciones a seguir previo a cualquier tipo de corte del fluido eléctrico:

- De contar con grupo electrógeno; verificar que se cuente con una dotación de combustible para un periodo no menor de cuatro (4) hora y que las conexiones de "By Pass" se encuentren en buenas condiciones, verificando su funcionamiento; estas revisiones deben hacerse cada seis (6) meses en coordinación con servicios generales de la Sub Unidad Abastecimiento.
- Verificar que las Unidades Suplementarias de Energía (UPS) se encuentren en funcionamiento y que las Baterías se encuentren con Carga; además de verificar el periodo de autonomía sea no menor a 30 minutos, en caso de corte fluido eléctrico; esta verificación se realizará cada (6) seis meses.

Acciones a seguir ante el corte del fluido eléctrico programado:

- Verificar que las Unidades Suplementarias de Energía (UPS) se encuentren en funcionamiento y que las Baterías se encuentren con Carga.
- De contar con grupo electrógeno, verificar que se cuente con la dotación suficiente de combustible para el periodo de corte y que las conexiones de "By Pass" se encuentren en buenas condiciones.
- De no contar con grupo electrógeno, gestionar la contratación del servicio por el periodo que será suspendido.
- Solicitar al personal de servicios generales se encuentre presente en la fecha y hora de la programación del corte, a fin que los equipos operen correctamente durante el corte del corte.

Acciones a seguir ante el corte del fluido eléctrico no programado:

- Comunicar al proveedor de energía eléctrica.
- Verificar que las Unidades Suplementarias de Energía (UPS) se encuentren en funcionamiento.
- Monitorear la carga de las baterías de los UPS.
- Alertar al Equipo de Respuestas ante Incidentes de Seguridad Digital del INABIF.
- De contar con grupo electrógeno, verificar que se haya puesto en operatividad y garantizar la dotación combustible para un funcionamiento de ocho (8) horas.
- Realizar, conjuntamente con la Sub Unidad de Abastecimiento, el seguimiento al proveedor de energía eléctrica a fin que se restituya el servicio.

1.2. Corte del fluido eléctrico por la falla en los tableros de energía eléctrica

Ante la falla de alguna de las llaves eléctricas o la falla de cables que genere el corte de energía se deben tomar las siguientes medidas:

- Comunicar a servicios generales de la Sub Unidad de Abastecimiento, comunicando el incidente.
- Asegurar que las Unidades Suplementarias de Energía (UPS) del Centro de Datos estén en funcionamiento correctamente.
- Alertar al Equipo de Respuestas ante Incidentes de Seguridad Digital del INABIF.
- De contar con grupo electrógeno, verificar que se haya puesto en operatividad y garantizar la dotación combustible para un funcionamiento de ocho (8) horas.

2. FALLA EN LAS UNIDADES SUPLEMENTARIAS DE ENERGÍA (UPS)

2.1. Fallo de UPS que protege a los servidores críticos

Las Unidades Suplementaria de Energía (UPS); son equipos de protección ante cortes del fluido eléctrico; estos están compuestos de baterías internas para que suministre energía durante un periodo de tiempo (autonomía). Si ocurriera algún fallo general o en sus baterías no podrían soportar la carga de

servidores críticos; lo que expondría a los equipos a apagados intempestivos ante un corte fortuito de fluido eléctrico.

Acciones a seguir ante la falla de un UPS en garantía:

- Comunicar inmediatamente al proveedor del UPS.
- Alertar al responsable de servicios generales de la Sub Unidad Abastecimiento, a fin que disponga del personal especialista eléctrico.
- Alertar al Equipo de Respuestas ante Incidentes de Seguridad Digital del INABIF.
- Retirar del circuito eléctrico el equipo que ha presentado falla.
- Realizar seguimiento con el proveedor del UPS para ponerlo operativo nuevamente.

Acciones para el mantenimiento de los UPS en garantía:

Acciones si ocurre algún fallo de la configuración de desviación de energía principal a la energía de reserva almacenada en las baterías del UPS (ByPass) para realizar los mantenimientos preventivos:

- Asegurar que el proveedor de UPS brinde una solución lo más pronto posible.
- Alertar al responsable de servicios generales de la Sub Unidad Abastecimiento, a fin que disponga del personal especialista eléctrico.
- Alertar al Equipo de Respuestas ante Incidentes de Seguridad Digital del INABIF.
- Realizar el seguimiento hasta que el UPS entre en funcionamiento.

3. FALLA DEL SERVICIO DE COMUNICACIONES

Acciones si ocurre una falta de pago del servicio, algún problema con el router ubicado en la oficina principal o algún problema con la red del proveedor:

- Comunicar inmediatamente al proveedor principal de Internet.
- Asegurar que el proveedor alterno entre en funcionamiento inmediatamente.

En paralelo se deben realizar las siguientes actividades:

- Realizar seguimiento urgente al proveedor principal de Internet para restablecer el servicio.
- Validar la conectividad del enlace brindado por el proveedor alterno.

4. CORTE DEL SISTEMA DE GESTIÓN DOCUMENTAL – SGD

Acciones si ocurre alguna caída por error de programación del mismo sistema SGD o algún problema con el router ubicado en la sede del INABIF o del proveedor de internet:

- Comunicar inmediatamente al proveedor para la revisión del servicio.
- Comunicar inmediatamente al personal de la Unidad de Tecnología de la Información para verificar los enlaces de comunicación en la red interna.
- Realizar seguimiento urgente al proveedor de Internet para restablecer el servicio.
- Realizar seguimiento urgente al proveedor ONPE para revisar el servicio SGD.
- Asegurar la conectividad del enlace brindado por el proveedor alterno.

5. PROBLEMA DE INOPERATIVIDAD DE LA BASE DE DATOS INSTITUCIONAL

Acciones si las aplicaciones no se pueden conectar a la Base de Datos Institucional (Oracle).

Antes de la contingencia:

1. Cumplir con el procedimiento de Respaldo de Información (Bases de Datos).
2. Mantener actualizados los parches de seguridad en los servidores.
3. Guardar una copia de respaldo en un servidor local y enviar otra copia al proveedor de custodia.
4. Supervisar el cumplimiento de las actividades 1, 2 y 3 establecidas en esta etapa.

Durante la contingencia

- Evaluar las causas de la inoperatividad del servidor y la posibilidad de restablecerlo.

- Para el caso donde el servidor no pueda restablecerse, deberá de comunicar a un Proveedor del Servicio de base de datos, sobre el suceso para que identifique las causas e intentar restablecerlo.
- Para el caso donde el servidor no pueda restablecerse, deberá reinstalarse
- Levantar la copia de respaldo en el servidor de Base de Datos reinstalado, realizar las configuraciones necesarias para la comunicación entre la base de datos y las aplicaciones informáticas.
- Gestionar las pruebas con los usuarios principales de los sistemas de información.
- Supervisar el cumplimiento de las actividades durante la contingencia.
- Revisar los controles principales de seguridad para la configuración en contingencia.

Después de la contingencia

1. Revisar el funcionamiento, para identificar si existen cambios que no han sido recuperados porque no se encontraban configurados en la copia de respaldo y solicitar el pase a producción de base de datos en caso corresponda.
2. Ejecutar el pase a producción con los cambios solicitados.
3. Validar que la información puede ser consultada en el servidor configurado.
4. Gestionar las pruebas con los usuarios principales de los sistemas de información.
5. Supervisar el cumplimiento de las actividades 2, 3 y 4 establecidas en esta etapa.
6. Revisar el restablecimiento de los controles de seguridad y copias de seguridad.

6. PROBLEMA DE INOPERATIVIDAD DE LAS APLICACIONES INSTITUCIONALES

Antes de la contingencia

1. Mantener el registro de cambios y versiones del código fuente de las aplicaciones.
2. Cumplir con el Respaldo de Información (servidores de aplicaciones, códigos fuente de las aplicaciones).
3. Revisar que el antivirus instalado en los servidores se encuentre actualizado.

4. Mantener actualizados los parches de seguridad en los servidores.
5. Supervisar el cumplimiento de las actividades 1, 2, 3 y 4 establecidas en esta etapa.

Durante la contingencia.

- Evaluar las causas de la inoperatividad del servidor y la posibilidad de restablecerlo.
- Para el caso donde el servicio o equipo comprometido no pueda restablecerse, se deberán levantar las copias de respaldo de los servidores más recientes.
- Realizar las configuraciones necesarias para la comunicación con el servidor de la base de datos.
- Gestionar las pruebas con los usuarios principales de los sistemas de información.
- Revisar los controles principales de seguridad para la configuración de contingencia.

Después de la contingencia

1. Coordinar con el dueño del proceso soportado por el sistema de información, para identificar si existen cambios que no han sido recuperados porque no se encontraban configurados en la copia de respaldo.
2. En caso lo soliciten, ejecutar el pase a producción para actualización de información.
3. Realizar pruebas sobre la aplicación.
4. Supervisar el cumplimiento de las actividades 1, 2 y 3 establecidas en esta etapa.

7. PROBLEMA DE HARDWARE / SOFTWARE DEL SISTEMA DE COPIAS DE SEGURIDAD

Acciones si ocurre una mala realización de la copia de seguridad; problema del servidor a copiar, un mal cálculo de espacio para la copia de respaldo:

- Buscar y restaurar una copia de información con más anterioridad que la esperada a la fecha de pérdida.
- Buscar información perdida en el Centro de Datos alterno.

- Solicitar al proveedor el custodio de las copias de respaldo para buscar la información más cercana a la fecha de pérdida.
- Asegurar nuevamente la ejecución de otra copia de seguridad.
- Validar continuamente las copias de seguridad realizadas mediante pruebas de restauración.

8. BORRADO DE INFORMACIÓN EN ALGÚN SERVICIO UTILIZADO POR EL USUARIO FINAL

Acciones si ocurre mal tratamiento de los archivos o por no bloquear las sesiones utilizadas para los diversos servicios por parte de los usuarios:

- Validar inmediatamente que la información borrada se encuentre replicada en el Servidor de Copias de Respaldo para proceder a recuperarla.
- Buscar y restaurar la copia de información más cercana a la fecha de pérdida.
- Buscar información perdida en el Servidor de Copias de Respaldo.
- Solicitar al proveedor el custodio de las copias de respaldo para buscar la información más cercana a la fecha de pérdida.
- Restaurar información a una fecha anterior aceptable.
- Brindar charlas constantes de concientización a los usuarios para el tratamiento de sus archivos de trabajo.

9. INCIDENTE OCURRIDO AL PROVEEDOR CUSTODIO EN EL TRASLADO DE COPIAS DE SEGURIDAD

Acciones en caso se de poca seguridad utilizada para trasladar las copias de la información:

- Validar inmediatamente que la información borrada se encuentre replicada en el Centro de Datos para proceder a recuperarla.
- Buscar y restaurar una copia de información con más anterioridad que la esperada a la fecha de pérdida.
- Buscar información perdida en el Servidor de Copias de Respaldo.
- Solicitar al proveedor el custodio de las copias de respaldo para buscar la información más cercana a la fecha de pérdida.
- Restaurar información a una fecha anterior aceptable.

- Brindar charlas constantes de concientización a los usuarios para el tratamiento de sus archivos de trabajo.

10. SATURACIÓN DE PROCESAMIENTO, MEMORIA Y ESPACIO EN SERVIDORES

Acciones si ocurre una mala configuración de balanceo de carga entre servidores, no hay configuración de alertas en los equipos de monitoreo o por falta de monitoreo por parte del administrador de red:

- Buscar y restaurar la copia de información más cercana a la fecha de pérdida.
- Pasar servicios al servidor de contingencia para disminuir la saturación de recursos.
- Asegurar el monitoreo de recursos por parte del Administrador de Red.
- Mejorar configuración de alertas para monitorear el uso general de recursos de servidores.
- Verificar funcionamiento de Calidad de Servicio (QoS) y Ancho de Banda (BW) en el Centro de Datos.
- Verificar funcionamiento de servicios de replicación.

11. PROBLEMA DE RÉPLICAS ENTRE SERVIDORES DE ARCHIVOS

Acciones si ocurre una mala configuración de las réplicas del servicio DFS:

- Buscar y restaurar la copia de información más cercana a la fecha de la última replicación.
- Revisar funcionamiento del Servicio de Replicación de los Sistemas de Archivos Distribuidos (DFS) para la distribución de información entre Servidores de Archivos.
- Solicitar al proveedor el custodio de las copias de respaldo para buscar la información más cercana a la fecha de pérdida.
- Documentar tamaños de replicación para llevar un control de información y copias de seguridad.

12. PROBLEMA DE RÉPLICAS DEL SERVIDOR DE CORREOS – ZIMBRA

Acciones si ocurre una mala configuración del servicio Zimbra para replicación de bases de datos:

- Buscar y restaurar la copia de información más cercana a la fecha de la última replicación.
- Revisar funcionamiento del servicio de replicación Zimbra para la distribución de Bases de Datos de MailBox (Herramienta de gestión de correos electrónicos).
- Solicitar al proveedor el custodio de las copias de respaldo para buscar la información más cercana a la fecha de pérdida.
- Documentar tamaños de replicación para llevar un control de información y copias de seguridad.

13. BORRADO DE ARCHIVOS IMPORTANTES DE OTRA ÁREA O USUARIO

Acciones si se presenta un usuario disconforme / molesto / etc.:

- Validar inmediatamente que la información borrada se encuentre replicada en el Centro de Datos para proceder a recuperarla.
- Buscar y restaurar la copia de información más cercana a la fecha de pérdida.
- Buscar información perdida en el Centro de Datos.
- Solicitar al proveedor el custodio de las copias de respaldo para buscar la información más cercana a la fecha de pérdida.
- Restaurar información a una fecha anterior aceptable.
- Revisar continuamente las copias de seguridad realizadas mediante pruebas de restauración.
- Derivar el caso a Gestión Humana para coordinar sanción.

14. DAÑO DE ARCHIVOS DE ALGÚN SISTEMA CRÍTICO

Acciones si se presenta un usuario disconforme / molesto / etc.:

- Recuperar un servidor físico / virtual necesario para levantar el sistema / aplicación que fue dañada.
- Buscar y restaurar la copia de información más cercana a la fecha de pérdida.
- Implementar un mecanismo de control y monitoreo de acceso / permisos a los archivos del sistema.

15. ATAQUES DE DELINCUENTES INFORMÁTICOS

Acciones si se presenta un usuario que brinda credenciales de acceso o información confidencial que le sirve al atacante para ingresar a los servicios:

- Revisar registros (logs) de accesos para identificar y cerrar puertos y conexiones utilizadas por el atacante.
- Cerrar conexiones a los sistemas.
- Realizar copias de seguridad de la información y enviarlas urgente al proveedor custodio.
- Brindar charlas constantes de concientización a los usuarios para poder contrarrestar las técnicas de Ingeniería Social utilizadas por los hackers y atacantes.