GOBIERNO REGIONAL DE ANCASH

"GERENCIA SUB REGIONAL SUBREGIÓN PACIFICO"

Ancash
Gobierno Regional

"PLAN DE CONTIGENCIAS INFORMATICO"

NUEVO CHIMBOTE – PERÚ

TABLA DE CONTENIDO

GOBIERNO REGIONAL ANCASH Sub Gerencia de Planif. Presup. Vº Bº Sub Región Pacífico

GOBIERNO REGIONAL ANCASH Sub Gerencia de Administración Vº Bº Sub Región Pacífico

GOBIERNO REGIONAL ANCASH Sub Gerencia de Planif. Presup. Vº Bº Sub Región Pacífico

REGION ANCASH Informática y Sistemas Sub Región Pacífico

INTRODUCCIÓN

El presente documento define el Plan de Contingencia Informático y Recuperación de Servicios de Tecnología de la Información y Comunicaciones como un proceso continuo de planeación, desarrollo, prueba e implantación de procesos y procedimientos de recuperación en caso de una posible contingencia que pueda presentarse en la Gerencia Sub Regional Subregión El Pacifico. Estas acciones buscan asegurar la reanudación eficiente y efectiva de los servicios y operaciones de Tecnologías de la Información y Comunicaciones en el menor tiempo e impacto posible. El Plan de Contingencia Informático y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones cuenta con documentos que en conjunto permiten la gestión, ejecución, pruebas y mantenimiento, esta disgregación de documentos permiten una fácil y ágil operación por los responsables autorizados, ante situaciones de desastres.

Cualquier Sistema de Redes de Computadoras (ordenadores, periféricos y accesorios) están expuestos a riesgo y puede ser fuente de problemas. El Hardware, el Software están expuestos a diversos Factores de Riesgo Humano y Físicos. Estos problemas menores y mayores sirven para retroalimentar nuestros procedimientos y planes de seguridad en la información. Pueden originarse pérdidas catastróficas a partir de fallos de componentes críticos (el disco duro), bien por grandes desastres (incendios, terremotos, sabotaje, etc.) o por fallas técnicas (errores humanos, virus informático, etc.) que producen daño físico irreparable.

La coordinación de las Tecnologías de la Información y Comunicaciones (TICs) tiene el propósito de proteger la información y así asegurar su procesamiento y desarrollo de funciones institucionales. En base a eso es importante contar con un Plan de contingencia adecuado de forma que ayude a la Gerencia Sub Regional Subregión El Pacifico a recobrar rápidamente el control y capacidades para procesar la información y restablecer la marcha normal de la entidad.

Los responsables del servicio informático están obligados a hacer de conocimiento y explicar con lenguaje entendible a los líderes de los procesos, las posibles consecuencias que la inseguridad insuficiente o inexistente pueda acarrear; de esa manera proponer y poner a consideración las medidas de seguridad inmediatas y a mediano plazo, que han de tomarse para prevenir los desastres que pueda provocar el colapso de los sistemas.

Para realizar el Plan de contingencia informático en la Gerencia Sub Regional Subregión El Pacifico, se tiene en cuenta la información como uno de los activos más importantes de la Institución, además que la infraestructura informática está conformada por el hardware, software y elementos complementarios que soportan la información o datos críticos para la función de la entidad. Este Plan implica realizar un análisis de los posibles riesgos a los cuales pueden estar expuestos nuestros equipos de cómputo y sistemas de información, de forma que se puedan aplicar medidas de seguridad oportunas y así afrontar contingencias y desastres de diversos tipos.

Los procedimientos relevantes a la infraestructura informática, son aquellas tareas que el personal realiza frecuentemente al interactuar con la plataforma informática (entrada de datos, generación de reportes, consultas, etc.). El Plan de Contingencias Informático está orientado a establecer un adecuado sistema de seguridad física y lógica en previsión de desastres, de tal manera de establecer medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o por el hombre.

Es necesario prever cómo actuar y qué recursos necesitamos ante una situación de contingencia con el objeto de que su impacto en las actividades sea lo menor posible

1. GENERALIDADES

1.1. DIAGNOSTICO

Efectuada nuestra revisión de la administración de riesgos de Tecnologías de Información de la Gerencia Sub Regional Subregión El Pacifico consideramos que debe desarrollarse un Plan de Contingencias Informático. Si bien hemos observado la existencia de normas, procedimientos y controles que cubren algunos aspectos de la seguridad de la información, que carece en general de una metodología, guía o marco de trabajo que ayude a la identificación de riesgos y determinación de controles para mitigar los mismos.

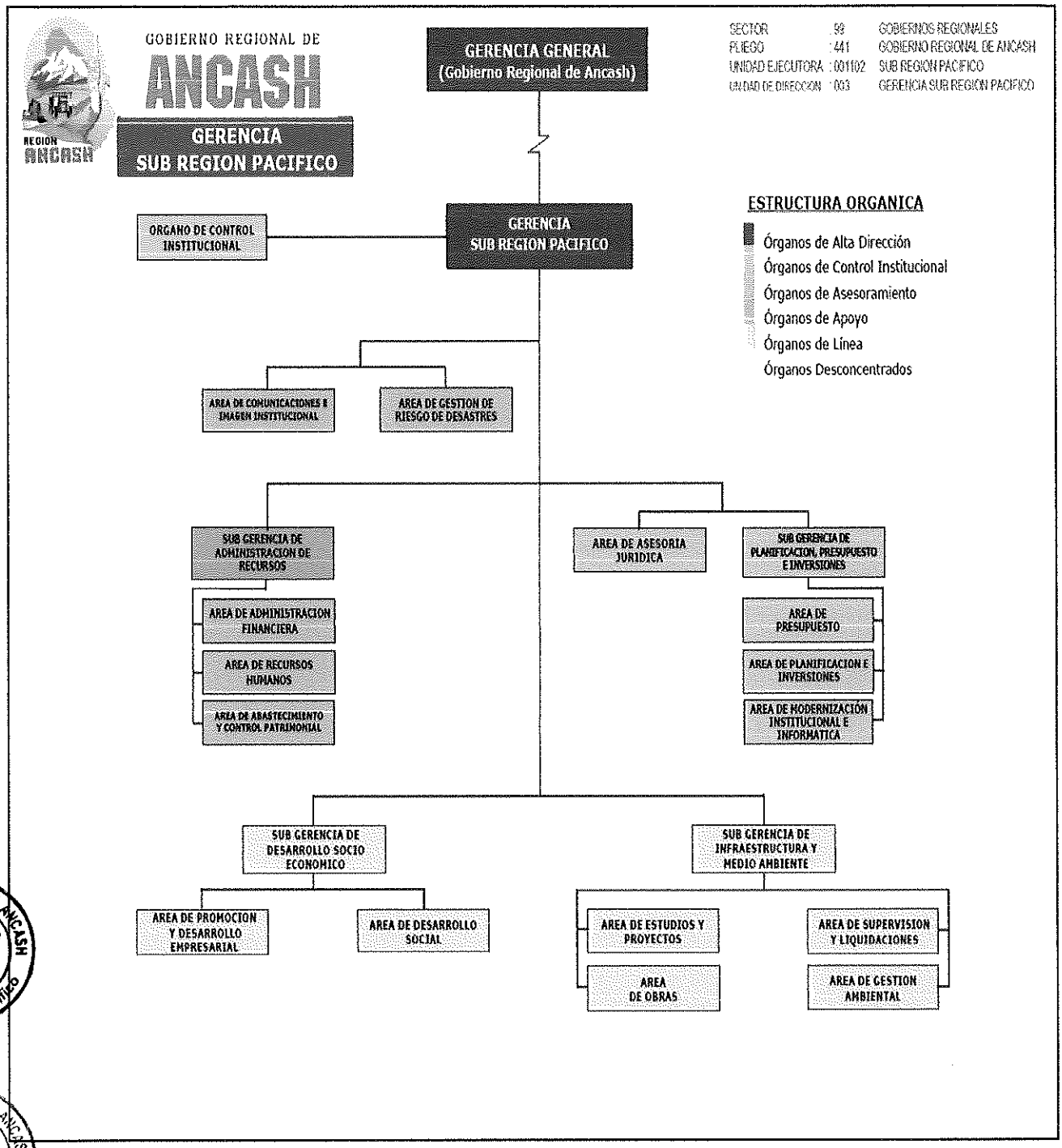
Dentro de los distintos aspectos a considerar en la seguridad, es necesario elaborar Políticas de Seguridad de la Información y una Clasificación de Seguridad de los Activos de Información de la entidad. Cabe mencionar que se ha verificado la existencia de controles, en el caso de la seguridad lógica, sobre los accesos a los sistemas de información, así como procedimientos técnicos establecidos para el otorgamiento de dichos accesos.

Sin embargo, estos controles no obedecen a una definición previa de una Política de Seguridad ni de una evaluación de riesgos de seguridad de la información a nivel de toda la entidad.

Asimismo, podemos mencionar la situación actual de los componentes informáticos como:

- Software:
    - No se cuenta con licencia de software para aplicaciones como antivirus, sistemas operativos, gestor de base de datos, office, entre otros de uso diario para los usuarios de la institución.
- Hardware:
    - Equipos informáticos como computadoras de escritorio que superan los 4 años de vida útil cuyo rendimiento es de gama baja, equipos de red que superan los 5 años de vida útil y son de mala calidad.
    - Servidores Informáticos que superan los 4 años de vida útil, no cuentan con mecanismos de respaldo como UPS y Storage.

1.2. ORGANIGRAMA



GOBIERNO REGIONAL ANCASH Sub Gerencia de Planif. y Presup. V° B° Sub Región Pacífico

GOBIERNO REGIONAL ANCASH Sub Gerencia de Administración V° B° Sub Región Pacífico

GOBIERNO REGIONAL ANCASH Contabilidad V° B° Sub Región Pacífico

REGIÓN ANCASH Informática y Sistemas Sub Región Pacífico

1.3. ESTRUCTURA Y FUNCIONES

- **Gerencia general:**

  Es responsable de coordinar con los sectores, gobiernos locales, organizaciones de base, instituciones públicas y privadas sobre proyectos que cubran necesidades de la población, así mismo, establecer políticas de desarrollo subregional.

- **Área de comunicaciones e imagen institucional:**

  Encargado de elaboración, redacción en medios de comunicación y redes sociales y difusión de notas de prensa, comunicados, reportajes, spots y/o informes especiales de carácter institucional en beneficio de la población.

- **Área de gestión de riesgos de desastres:**

  Encargada de proporcionar ayuda oportuna y necesaria a la población y a la entidad afectada a fin de superar la situación emergente producida por un desastre de cualquier origen y magnitud.

- **Subgerencia de administración de recursos:**

  Es responsable de dirigir, ejecutar, evaluar y controlar la administración del potencial humano, los recursos económicos - financieros, materiales y de servicio interno de la Gerencia Subregional Subregión Pacifico.

- **Área de recursos humanos:**

  Encargado de utilizar el recurso humano de manera más optima y efectiva a fin de cumplir con las metas institucionales en el menor tiempo posible, con el menor gasto de recursos y con la mayor satisfacción de la población.

- **Área de abastecimiento y control patrimonial:**

  Es el encargado de agilizar los requerimientos de compra, servicios y ejecución de obras en beneficio de la entidad y la población en general.

- **Área de asesoría jurídica:**

  Encargado de dirigir, ejecutar y evaluar los asuntos de carácter legal de la Sub Región Pacifico.

- **Subgerencia de planificación, presupuesto e inversiones:**

  Es responsable de planificar, organizar, dirigir y evaluar las actividades referidas al planeamiento, presupuesto, estudios económicos, estadísticas y racionalización.

- **Área de modernización institucional e informática:**

  Encargado de dirigir las actividades técnicas relacionadas con los recursos de información y de comunicaciones de la entidad.

- **Subgerencia de infraestructura y medio ambiente:**

  Responsable de planificar y ejecutar las obras de infraestructura pública establecidas en el Plan de Acondicionamiento Territorial y el Plan de Desarrollo Urbano así mismo ejecutar y monitorear los planes y políticas locales en materia ambiental; además de ejecutar los mantenimientos de infraestructura pública.

- **Área de obras:**

  Es el área encargada de planificar, dirigir, controlar y evaluar los proyectos desde el momento de su concepción hasta su finalización, todo ello dentro de los plazos y presupuestos establecidos en beneficio de la población.

- **Área de estudios y proyectos:**

  Encargado de evaluar y emitir opinión sobre aspectos técnicos y contenidos mínimos de los estudios de Proyectos de Inversión Pública, a nivel de inversión e inversión, de obras de infraestructura, para su aprobación.

- **Área de supervisión y liquidaciones:**

  Encargada de supervisar y orientar la ejecución de obras o proyectos, y la recepción de las obras concluidas, así como proceder a su liquidación física y financiera.

1.4. RECURSOS INSTITUCIONALES

El presente Plan de Contingencias Informático requiere como respaldo contar con algunos requisitos para la puesta en marcha:

1.4.1. Humanos

Están dados por las personas participantes directa e indirectamente en el desarrollo del Plan, las cuales en un primer momento será el personal de la Área de Modernización Institucional e Informática con que cuenta la Gerencia Subregional Subregión el Pacifico, quienes definirán los procedimientos para poner en operación el Plan de Contingencias Informático.

Tenemos luego a los Gerentes que al comprender la importancia y urgencia de la aplicación de este plan habrán de apoyar las propuestas que dan base a la ejecución del plan de contingencias informático, y han de hacer denominador común para su aplicación. Por último, las personas de diferentes áreas y oficinas de la Gerencia Subregional Subregión el Pacifico

que servirán de nexo para la captura de información y definición de tareas del plan.

El perfil **profesional/técnico** con que debe contar el área de Informática para brindar soporte y asistencia en la ejecución del Plan de Contingencia Informático es el siguiente:

A. Especialista en Desarrollo de Software o afines.
B. Especialista en Servidores, redes y Telecomunicaciones o afines.
C. Especialista en Soporte Técnico o afines.

1.4.2. Materiales

Todas las herramientas de soporte, material de escritorio, computadores, equipos, insumos informáticos, útiles de escritorio, necesario para llevar a cabo el plan deberán ser proporcionados por la Subgerencia de Administración y Recursos en base a los requerimientos formulados por cada necesidad en merito a la incidencia que se presente.

1.4.3. Financieros

Los recursos financieros con que se requiere contar para la aplicación del presente Plan de Contingencia serán financiados por la Entidad, de acuerdo a la incidencia que se presente.

1.4.4. Entrenamiento

El personal participante será entrenado para la aplicación correcta del Plan y para obtener el máximo provecho de acuerdo a la función que han de cumplir como parte conformante del plan, cabe precisar que el financiamiento para el entrenamiento y capacitación deberá ser financiado por la Entidad.

1.4.5. Responsabilidad

La alta dirección habrá de ejercer la función de control y asegurará que las tareas desarrolladas, sean cumplidas de acuerdo a los planteamientos y objetivos del plan.

Los Planes de Contingencia se organizan para que las instituciones puedan prevenir fallas o accidentes en sus operaciones diarias y les permitan seguir activas, en la provisión de servicios o productos, en el caso de que algún componente sufra algún tipo de problema, que condicione el correcto funcionamiento de sus equipos tecnoiógicos, apiicaciones informáticas y otros sistemas críticos.

1.5. INVENTARIO DE RECURSOS INFORMATICOS

1.5.1. Computadoras.

El Inventario actual se muestra en el siguiente cuadro:

EQUIPOS	TOTAL
Computadoras Escritorio	41
Laptops	2
TOTAL	**43**

1.6. APLICATIVOS INFORMATICOS

SISTEMA	DESCRIPCIÓN
Sistema Integrado de Administración y Finanzas (SIAF)	El SIAF es un sistema que automatiza los procedimientos financieros necesarios para registrar los recursos públicos recaudados y aplicarlos a la concreción de los objetivos del sector público. Los módulos con los que cuenta el SIAF son: ▪ Módulo Administrativo. ▪ Módulo de Conciliación de Cuentas. ▪ Módulo de Conciliación de Operaciones del SIAF. ▪ Módulo Contable. ▪ Módulo de Control de Pago de Planillas (MCPP) ▪ Módulo de Ejecución de Proyectos (MEP) ▪ Módulo de Deuda Pública. ▪
Sistema de Gestión Documentaria (SISGEDO)	El Sistema Tramite Documentario es el que se encarga monitoreo, seguimiento de documentos internos entre las distintas áreas e ingresos de documentos externos. El Sistema viene funcionando de manera correcta y se tiene un programador asignado a darle mantenimiento y resolver incidentes que surgieran en el mismo.
	El Sistema Integrado de Gestión Administrativa- SIGA es una herramienta informática que simplifica y automatiza los procesos administrativos en una entidad del Estado y que sigue las

GOBIERNO REGIONAL ANCASH Sub Gerencia de Planificación V° B° Sub Región Pacífico

GOBIERNO REGIONAL ANCASH Sub Gerencia de Administración V° B° Sub Región Pacífico

GOBIERNO REGIONAL ANCASH V° B° Sub Región Pacífico

REGION ANCASH Informática y Sistemas Sub Región Pacífico

Sistema Integrado de Gestión Administrativa (SIGA)	normas establecidas por los Órganos Rectores de los Sistemas Administrativos del Estado. ▪ Logística. ▪ Patrimonio. ▪ Presupuesto por resultados. ▪ Bienes Corrientes. ▪ Tesorería.
(PEGASUS) módulo de planilla	El módulo de planilla del sistema PEGASUS es una herramienta para manejar, almacenar y automatizar procesos de gestión de nómina como el pago de planilla, registro de asistencia y control de vacaciones.

1.7. OBJETIVOS

1.7.1. Objetivo General

Formular un adecuado Plan de Contingencias Informático, que permita la continuidad en los procedimientos informáticos de la Gerencia Subregional Subregión El Pacifico, así como enfrentarnos a fallas y eventos inesperados; con el propósito de asegurar y restaurar los equipos e información con las menores pérdidas posibles en forma rápida, eficiente y oportuna; buscando la mejora de la calidad en los servicios que brinda la entidad.

1.7.2. Objetivos Específicos

- Evaluar, analizar y prevenir los riesgos informáticos en la Gerencia Subregional Subregión El Pacifico que pueda ser suspendida completa o parcialmente la prestación del servicio.
- Establecer los niveles de complejidad de las fallas del sistema y los posibles tiempos de no disponibilidad de las diferentes aplicaciones.

2. Marco Teórico

2.1. Definiciones:

Amenaza: probabilidad de ocurrencia, durante un período específico y dentro de un área determinada, de un fenómeno que puede potencialmente causar daños en los elementos en riesgo.

Contingencia: Evento o suceso que ocurre, en la mayoría de los casos, en forma inesperada y que causa alteraciones en los patrones normales de funcionamiento de una organización.

Elementos en Riesgo: Se refiere a la población, las construcciones, la infraestructura, las edificaciones de las actividades económicas y otros espacios donde éstas se desarrollan, los servicios públicos y el medio ambiente natural que son susceptibles de daños como consecuencia de la ocurrencia de un fenómeno natural o producido por el hombre (artificial).

Vulnerabilidad: La vulnerabilidad se refiere al grado de pérdidas relacionadas con un elemento en riesgo (o un conjunto de elementos en riesgo), que resulta como consecuencia de un fenómeno natural o artificial con una determinada magnitud. Se expresa de una escala de "0" (no hay daños) a "1" (daño total).

Riesgo: Se refiere a la cuantificación de los posibles daños ocasionados a los elementos en riesgo como consecuencia de un fenómeno natural o artificial en términos de vidas perdidas, personas heridas, daños materiales y ambientales e interrupciones de la actividad económica.

Gravedad: Se refiere a la magnitud resultante de los daños provocados por un siniestro. Esta es subdividida en ninguna, insignificante, marginal, crítica y catastrófica y se definen según el factor de evaluación (víctimas, pérdidas económicas, suspensión de operación, daño ambiental).

Seguridad: Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que, en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

Datos: Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos.

Incidente: Es una violación con éxito de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, etc.

Activo: Son todo aquellos recursos o componentes de la institución, tanto físico (tangibles), como lógicos (intangibles) que constituyen su infraestructura, patrimonio, conocimiento y reputación en el mercado.

Plan de Contingencia Informático: 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, como un plan de prevención para mitigar los incidentes.
- Durante, como un plan de emergencia y/o ejecución en el momento de presentarse el incidente.
- Después, como un plan de recuperación una vez superado el incidente para regresar al estado previo a la contingencia.

Método de análisis de riesgos: Los métodos de análisis de riesgos son técnicas que se emplean para evaluar los riesgos de un proyecto o un proceso. Estos métodos ayudan a tomar decisiones que permiten implementar medidas de prevención para evitar peligros potenciales o reducir su impacto.

En el Anexo 1, se detalla la metodología utilizada en el presente Plan.

Plan de prevención: Es el conjunto de acciones, decisiones y comprobaciones orientadas a prevenir la presencia de un evento no deseado, con el propósito de disminuir y mitigar la probabilidad de ocurrencia del mismo en las categorías identificadas en el presente plan. El plan de prevención es la parte principal del Plan de Contingencia porque permite aminorar y atenuar la probabilidad de ocurrencia de un estado de contingencia

Plan de Ejecución: Es el conjunto detallado de acciones a realizar en el momento que se presenta el incidente y activa la contingencia como un mecanismo alterno que permitirá reemplazar a la actividad normal cuando este no se encuentra disponible. Las acciones descritas dentro del plan de ejecución deben ser completamente claras y definidas de forma tal que sean de conocimiento y entendimiento inequívoco del personal involucrado en atender la contingencia.

Plan de recuperación: Es el conjunto de acciones que tienen por objetivo restablecer oportunamente la capacidad de las operaciones, procesos y recursos del servicio que fueron afectados por un evento de contingencia.

Plan de pruebas: Está constituido por un conjunto de pruebas. Cada prueba debe dejar claro qué tipo de propiedades se quieren probar, cómo se mide el resultado, especificar en qué consiste la prueba y definir cuál es el resultado que se espera.

3. Alcance:

El Plan de Contingencia Informático, incluye los elementos referidos a los sistemas de información, aplicativos informáticos, bases de datos, equipos e instalaciones tecnológicas, personal, servicios y otros administrados por el Area de Modernización Institucional e Informática, direccionado a minimizar eventuales riesgos ante situaciones adversas que atentan contra el normal funcionamiento de los servicios informáticos de la entidad.

4. Base Legal:

- Ley N° 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° 034-2014-PCM, Decreto Supremo que aprueba el Plan Nacional de Gestión del Riesgos de Desastres - PLANAGERD 2014-2021.

- Decreto Supremo N° 048-2011-PCM, Decreto Supremo que aprueba el Reglamento de la Ley N° 29664, que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).

- Resolución Ministerial N° 004-2016-PCM - Aprueban 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° 028-2015-PCM, Aprueban Lineamientos para la gestión de la Continuidad Operativa de entidades públicas en los tres niveles de gobierno.

5. Metodología:

El desarrollo del presente Plan seguirá la siguiente metodología basa en siete (07) fases:

- Fase 01: Planificación
- Fase 02: Determinación de vulnerabilidades y escenarios de contingencia.
- Fase 03: Estrategias
- Fase 04: Elaboración de Plan de Contingencia Informático
- Fase 05: Definición y ejecución del plan de pruebas
- Fase 06: Implementación del Plan de Contingencia
- Fase 07: Monitoreo

A continuación, se detalla cada fase:

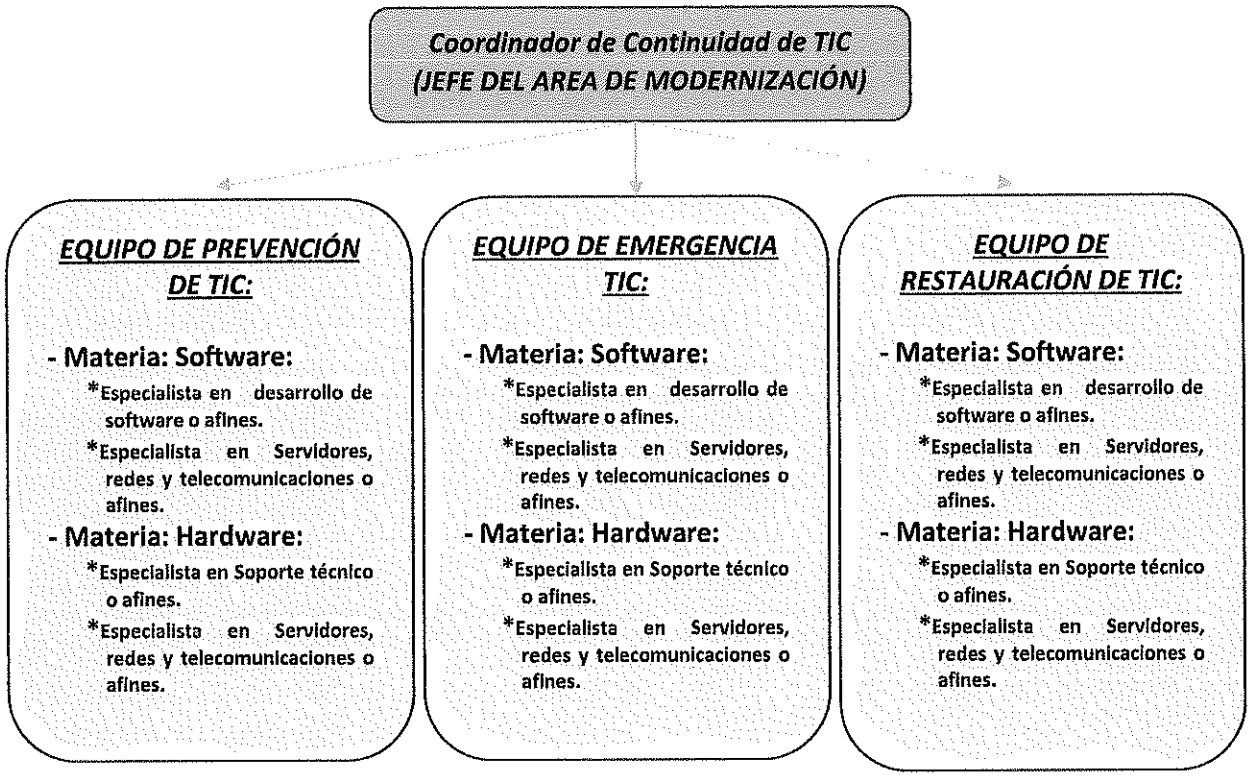
5.1. Fase 01: Planificación

5.1.1. Organización

El Área de Modernización Institucional e Informática depende directamente de la Subgerencia de Planificación, Presupuesto e Inversiones, y tiene dentro de sus funciones administra la integridad, confiabilidad, y seguridad en el acceso de la base de datos institucional, así como establece mecanismos de registro histórico de modificaciones, autenticación de los usuarios, auditoría y control de accesos a la base de datos; además de diseñar, construir, implantar, mantener los sistemas informáticos e infraestructura tecnológica necesaria para el cumplimiento de los objetivos del Ministerio, así como asegurar la disponibilidad y brindar soporte a los mismos.

Para el funcionamiento del Plan de Contingencia Informático y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones, se ha establecido la siguiente organización operativa, conformado exclusivamente por personal del Área de Modernización institucional e Informática:

Figura N° 1 – Organización Operativa del Plan de Contingencia Informático



El jefe del Área de Modernización Institucional e Informática (AMII) debe nombrar un miembro titular y un alterno, por cada integrante de los tres (3) equipos mencionados previamente, detallados en la Figura N° 1. Para tal efecto, se debe contar con la relación del personal de la AMII que forman estos equipos, quienes serán requeridos en el momento de la contingencia.

Asimismo, los responsables de cada Equipo previamente señalados, deben tener operativo su dispositivo móvil para las comunicaciones pertinentes, siendo necesario que el responsable del Equipo de Restauración de TIC cuente con línea abierta disponible, en caso deba comunicarse con proveedores especializados. De igual manera, los correos electrónicos registrados deben estar alojados en plataforma nube, que garantice la disponibilidad de este servicio.

Las actividades planificadas como parte del presente plan podrán ejecutarse en forma presencial, semipresencial o en remoto, conforme a los escenarios de prueba que pudieran desprenderse ante los diversos eventos de mayor impacto considerados para el presente Plan de Contingencia Informático; así como, conforme a las disposiciones vigentes

GOBIERNO REGIONAL ANCASH Sub Gerencia de Planif. y Presup. V° B° Sub Región Pacífico

GOBIERNO REGIONAL ANCASH Sub Gerencia de Administración V° B° Sub Región Pacífico

GOBIERNO REGIONAL ANCASH Contabilidad V° B° Sub Región Pacífico

REGIÓN ANCASH Informática y Sistemas Sub Región Pacífico

5.1.2. Roles, funciones y responsabilidades dentro del Plan

a. Coordinador de Continuidad de TIC:

Esta representado por el jefe del Área de Modernización Institucional e Informática y tiene las siguientes funciones:

- Coordinar, dirigir y decidir respecto a acciones o estrategias a seguir en un escenario de contingencia dado.
- Tomar la decisión de activar el Plan de Contingencia Informático y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones.
- Guiar y supervisar a los equipos operativos de contingencia informática, en el desarrollo de sus actividades.
- Evaluar la extensión de la contingencia y sus consecuencias potenciales sobre la infraestructura tecnológica.
- Notificar y mantener informados, a los miembros del Grupo de Comando de Continuidad Operativa acerca del evento de desastre, el progreso de la recuperación y posibles problemas ocurridos durante la ejecución del plan.
- Monitorear, supervisar y vigilar la recuperación de infraestructura de Tecnologías de la Información (TI) en el Centro de Datos.
- Contactar a los proveedores para el reemplazo de hardware, software y/o activación de servicios para los sistemas afectados.
- Declarar el evento de término de la ejecución de las operaciones del Plan de Contingencia Informático y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones, cuando las operaciones del Centro de Datos hayan sido restablecidas.

b. Equipo de Prevención de TIC:

Es el equipo encargado de ejecutar las acciones preventivas, antes que ocurra un siniestro o desastre. Su finalidad es evitar la materialización y en caso ocurriese, tener todos los medios requeridos para realizar la recuperación de los servicios de tecnologías de la información y comunicaciones, en el menor tiempo posible.

El responsable del Equipo de Prevención de TIC es el/la Especialista en desarrollo de software.

A continuación, se detallan las funciones por cada integrante del equipo de prevención:

Especialista en Servidores, redes y telecomunicaciones:

- Establecer y supervisar los procedimientos de seguridad de los servicios de TIC.
- Coordinar la realización de las pruebas de restauración de hardware y software.
- Participar en las pruebas y simulacros de desastres.
- Verificar la realización del mantenimiento preventivo a los equipos componentes del Centro de Datos.
- Verificar las tareas de copias de respaldo (backup)

Especialista en desarrollo de software:

- Soporte y mantenimiento de los sistemas y aplicativos instalados en la entidad.
- Documentación, consolidación y validación de los manuales de los sistemas en producción.
- Realizar periódicamente las pruebas de restauración de las fuentes de los sistemas de información en producción de la entidad.
- Realizar copias de respaldo de las bases de datos de los aplicativos y sistemas de la entidad.
- Acopiar las copias de respaldo y clasificarlas por tipo de motor de base de datos, aplicativos y sistemas.
- Realizar las pruebas de restauración de bases de datos en coordinación con el Especialista en Seguridad de la Información.

Especialista en soporte técnico:

- Mantener actualizado el inventario hardware y software utilizado en el Centro de Datos de la entidad.
- Ejecutar y verificar las tareas de copias de respaldo (backup).
- Programar y/o realizar el mantenimiento preventivo de los equipos de comunicaciones y de los equipos componentes del Centro de Datos, considerando el tiempo de vida útil y garantía de los mismos.
- Llevar un control detallado del mantenimiento realizado a cada equipo y componentes del Centro de Datos.
- Elaborar informes técnicos de conformidad, luego de cada mantenimiento efectuado, así como elaborar informes periódicos del funcionamiento del Centro de Datos.
- Verificar que se mantiene actualizado los diagramas de servidores, los diagramas de red, la documentación de las configuraciones de equipos de comunicaciones, l inventario de software de gestión y otros.
- Monitorear la red y definir medidas preventivas para minimizar o evitar las contingencias.
- Realizar las pruebas previas de recuperación

c. Equipo de Emergencia de TIC:

Este equipo es el encargado de ejecutar las acciones requeridas durante la materialización del siniestro o desastre. Su finalidad es mitigar el impacto que puedan tener sobre los equipos tecnológicos y la información de la Gerencia Subregional Subregión El Pacifico, procurando salvaguardar su pérdida o deterioro.

A continuación, se citan las acciones que se realizarán durante la contingencia, según los miembros del equipo:

Especialista en Servidores, redes y telecomunicaciones:

- Notificar el desastre o incidencia al Coordinador de Continuidad de TIC.
- Ejecutar las acciones de emergencia en los equipos informáticos y componentes instalados en el Centro de Datos de la Gerencia Subregional Subregión El Pacifico.
- Realizar la evaluación de condiciones de los equipos de comunicaciones y los componentes del Centro de Datos del Gerencia Subregional Subregión El Pacifico, durante la emergencia.
- Comunicar al Coordinador de Continuidad de TIC las acciones de emergencia ejecutadas

Especialista en desarrollo de software:

- Realizar la evaluación de las condiciones de los aplicativos informáticos y sistemas de información durante la emergencia.
- Solicitar los logs de los aplicativos informáticos afectados durante la emergencia.

Especialista en soporte técnico:

- Realizar la evaluación de la afectación a los equipos informáticos de usuario final (computadoras, teléfonos, impresoras, entre otros).
- Notificar los casos críticos en cuanto a equipos de usuario final, que afecte la continuidad de operaciones y/o la pérdida de información de los usuarios de la Gerencia Subregional Subregión El Pacifico.
- Elaborar informes técnicos de conformidad, luego de cada mantenimiento efectuado, así como elaborar informes periódicos del funcionamiento del Centro de Datos.
- Verificar que se mantiene actualizado los diagramas de servidores, los diagramas de red, la documentación de las configuraciones de equipos de comunicaciones, l inventario de software de gestión y otros.
- Monitorear la red y definir medidas preventivas para minimizar o evitar las contingencias.
- Realizar las pruebas previas de recuperación

d. Equipo de Restauración de TIC:

Este equipo es el encargado de ejecutar las acciones necesarias luego de que el siniestro o desastre esté controlado. Su finalidad es restituir en el menor tiempo posible el funcionamiento de los equipos tecnológicos y recuperar el estado de los servicios informáticos del SUB REGIÓN PACIFICO de manera conjunta con los miembros titulares y suplentes del Grupo de Comando de la Continuidad Operativa y especialistas designados por cada órgano de la Gerencia Subregional Subregión El Pacifico.

Especialista en Servidores, redes y telecomunicaciones:

- Coordinar acciones para la verificación de estado de los sistemas de información alojados en los servidores de aplicaciones.
- Coordinar el estado de las bases de datos de los sistemas de información.
- Coordinar y monitorear la restauración de aplicativos y ejecución de pruebas para verificación de funcionalidad.
- Realizar la evaluación de condiciones de los equipos de telecomunicaciones, durante la emergencia.
- Elaborar un informe técnico, que incluya las acciones de recuperación de los equipos móviles y la central telefónica ubicada del Centro de Datos.

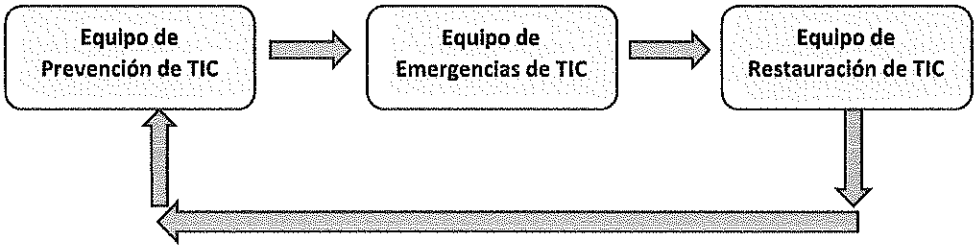
Especialista en desarrollo de software:

- Verificar el funcionamiento de las bases de datos institucionales.
- Realizar la creación de bases de datos en servidores alternos, en caso sea requerido.
- Restaurar las copias de respaldo correspondientes respetando la prioridad establecida para cada escenario.
- Realizar las pruebas de funcionamiento.
- Elaborar un informe técnico que incluya la evaluación de condiciones de los datos e información de la Gerencia Subregional Subregión Pacifico luego de efectuado el proceso de recuperación.

Especialista en soporte técnico:

- Verificar el funcionamiento de los equipos personales en las sedes de la Gerencia Subregional Subregión El Pacifico afectadas, distribuyendo el trabajo entre los técnicos de soporte.
- Solucionar los problemas de conexión y funcionamiento de los equipos personales, impresoras, escáner entre otros.
- Elaborar un informe técnico que incluya la evaluación de condiciones de los equipos personales e información del personal del Gerencia Subregional Subregión El Pacifico, luego de efectuado el proceso de recuperación.

Figura N° 2 – Flujo del orden de operación de los equipos de TI



5.2. Fase 2: Determinación de vulnerabilidades y escenarios de contingencia

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

5.2.1. Procesos y recursos críticos

A continuación, se detalla los procesos, aplicaciones y recursos críticos, con su respectiva expectativa del tiempo de recuperación:

Tabla N° 1 - Procesos y recursos críticos de TI

Proceso crítico	Aplicaciones y/o recursos críticos	Tiempo de Recuperación (RTO)
Gestión de redes e infraestructura de TI	Equipos de comunicaciones.	12 h
	Equipos de protección eléctrica del centro de datos (UPS)	24 h
	Sistema de aire acondicionado del Centro de Datos	24 h
	Infraestructura del Centro de Datos	24 h
	Cableado de red de datos	24 h
	Enlaces de cobre y fibra óptica para interconexión entre la sede central y el centro de datos	4 h
	Sistema de almacenamiento (storage)	24 h
	Medios de respaldo (cintas de backup)	24 h
	Servidores de red críticos: Directorio Activo, File Server, Base de Datos, Ecodoc.	96h
	Servidores de red en general: Citrix, tomcat, jboss.	96h
	Central Telefónica	24h
Gestión de sistemas de información y bases de datos	Sistemas de información y portales core	48 h
	Sistemas de información administrativos	72 h
	Base de datos y repositorios utilizados por los sistemas y aplicativos.	48 h
Soporte Técnico	Estaciones de trabajo del personal crítico (computadoras personales y portátiles)	48 h
Operación y mantenimiento de TICS	Personal crítico responsable de los procesos de TIC.	4 h

*El RTO: Tiempo de Recuperación Objetivo, es determinado por Juicio de Expertos.

5.2.2. Identificación de amenazas

Este paso, permite identificar aquellas amenazas que pudieran vulnerar los servicios TIC de la Sub Region Pacifico, considerando la ubicación geográfica, el contexto actual de la sede central y centro de datos, así como la percepción del juicio experto.

Tabla N° 2 - Amenazas a los servicios de TI

N°	Amenaza (Evento)	Tipo
01	Terremoto/Sismo	Siniestros Naturales
02	Inundación y aniego en el Centro de Datos.	
03	Incendio en el Centro de Datos.	
04	Falla en telecomunicaciones.	Tecnológicos
05	Delito informático.	
06	Falla de hardware y software.	
07	Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación.	Físico y ambiental
08	Ausencia o no disponibilidad del personal crítico de TI.	Humanos
09	Pandemia y/o Epidemia	Ambiental

Una vez determinadas las amenazas que pueden afectar los recursos críticos de TI, se calcula el nivel de probabilidad estimada, a fin de identificar las amenazas que serán consideradas en la evaluación de los riesgos. A continuación, se detalla el resultado obtenido:

Tabla N° 3 - Probabilidad estimada de las amenazas a los servicios de TI

N°	Amenaza (Evento)	Ocurrencia	Percepción	Nivel Probabilidad estimada
01	Terremoto.	2	4	Moderado
02	Inundación y aniego en el Centro de Datos.	2	2	Menor
03	Incendio en el Centro de Datos.	1	3	Menor
04	Falla en telecomunicaciones.	3	4	Moderado
05	Delitos informáticos.	2	4	Moderado
06	Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación.	3	3	Moderado
07	Falla del hardware y software.	3	3	Moderado
08	Ausencia o no disponibilidad del personal crítico de TI.	2	3	Menor
09	Pandemia y/o Epidemia	1	2	Menor

5.2.3. Identificación de Controles Existentes

- La identificación de controles existentes, permiten conocer que tan protegidos están los recursos de TI del SUB REGIÓN PACIFICO frente a cada amenaza.

- Mantenimiento de generadores eléctricos y UPS. El mantenimiento de generadores (grupo electrógeno está a cargo de Servicios Generales de la Oficina de Abastecimiento) y el mantenimiento de UPS está a cargo de la AMII).
- Mantenimiento para equipos de aire acondicionado del Centro de Datos.
- Respaldo de información y custodia externa de medios de respaldo.
- Solución antivirus instalada en los servidores de red y computadoras.
- Solución de protección de portales y aplicaciones web publicadas en internet a través de solución en la nube.
- Póliza de seguro contra todo riesgo.

5.2.4. Evaluación del Nivel de Riesgo

Para determinar el Nivel de Riesgo de un recurso de TI crítico de la Sub Región Pacifico, se consideraron los controles existentes que mitigan la afectación de la amenaza descritos en el punto 6.2.2 y de acuerdo a la aplicación de la metodología de riesgos descrita en el Anexo 1, se obtuvo el siguiente resultado:

Tabla N° 4 - Resultado de la evaluación de riesgos de os servicios de TI

	Recursos Críticos / Amenazas (Eventos)	Terremoto	Inundación y aniego en el Centro de Datos	Incendio en el Centro de Datos	Falla en telecomunicaciones	Delitos informáticos	Falla del suministro eléctrico en el Centro de Datos 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.									
2	Equipos de protección eléctrica del centro de datos (UPS).									
3	Aire acondicionado de precisión del Centro de Datos.									
4	Infraestructura del Centro de Datos.									
5	Cableado de red de datos.									
8	Servidores de red									
9	Sistemas de información y portales web									
10	Base de datos utilizados por los sistemas y aplicativos.									
11	Estaciones de trabajo del personal crítico (computadoras personales y portátiles)									
12	Personal crítico responsable de los procesos de TIC.									

5.2.5. Escenarios de riesgo

- Destrucción e indisponibilidad del centro de datos por terremoto.
- Falla en el funcionamiento de los sistemas de información y portales web por delito informático (ataque cibernético, virus, etc.).
- Indisponibilidad de los servidores de red por falla de hardware y software.
- de comunicaciones por fallas en el suministro eléctrico del Centro de Datos y/o en los gabinetes de comunicación de la sede central.

A continuación, se presenta el consolidado de los escenarios de riesgo y su impacto, para activar el Plan de Contingencia Informático.

Tabla N° 5 - Escenarios de Riesgos

Escenario de Riesgo	Descripción	Impacto
Destrucción e indisponibilidad del centro	Este escenario consiste en que el Centro de Datos 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	Extremo
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
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

5.3. Fase 3: Estrategias del Plan de Contingencia

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

5.3.1. Estrategias de prevención de tecnologías de la información

a) **<u>Almacenamiento y respaldo de la información (BACKUPS)</u>**

- Gestión de copias de respaldo (Backup) de la información almacenada y procesada en el Centro de Datos, de acuerdo a la Directiva N° 009-2018-SUB REGIÓN PACIFICO/SG, en donde se define la frecuencia de los respaldos de información considerando la criticidad de los datos, así como los criterios de identificación de los medios, la frecuencia de rotación y transporte al sitio externo.
- Realización de copias de instaladores de las aplicaciones, de software base, sistema operativo, utilitarios, etc.
- Verificar la ejecución periódica de las tareas programadas de respaldo de información y comprobación de los medios de respaldo.
- Se utiliza lugares alternativos externos para el almacenamiento de las copias de respaldo a cargo de proveedor externo.

b) Sitios Alternos para el Centro de Datos

El plan incluye una estrategia para recuperar y ejecutar operaciones de sistemas en instalaciones alternativas por un periodo extendido; los sitios alternativos podrán ser:

- Propios de la entidad.
- Instalaciones alquiladas.

Para tal efecto, se debe identificar un ambiente adecuado como lugar alterno para la recuperación de equipos y servicios de tecnologías de la información del Centro de Datos.

c) Evaluación y gestión de proveedores

- Listado de proveedores claves de servicios y recursos de TI, con sus datos de contacto actualizados.
- Mantener listas detalladas de necesidades de equipos y sus especificaciones técnicas.
- Si es necesario, adquirir o habilitar hardware y software, así como transportarlos al sitio alterno de ser el caso; las estrategias básicas para disponer de equipo de reemplazo serán:

    - Acuerdos con proveedores: Establecer acuerdos de nivel de servicios con los proveedores de software, hardware y medios de soporte; se debe especificar el tiempo de respuesta requerido.

    - Equipos de respaldo: Los equipos requeridos se compran por adelantado y se almacenan en una instalación segura externa. (*)
    Equipo compatible existente: Equipo existente en sitios alternativos.

(*) Comprar los equipos cuando se necesitan puede ser mejor financieramente, pero puede incrementar de manera significativa el tiempo de recuperación. Asimismo, almacenar un equipo sin ser usado es costoso, pero permite que la recuperación comience más rápidamente.

d) Entrenamiento y personal de reemplazo

- Todo el personal de la AMII, debe entrenarse en el proceso de recuperación de los servicios de TI. La capacitación debe ser planificada, estructurada y acorde con las exigencias de recuperación. El entrenamiento se debe evaluar para verificar que ha logrado sus objetivos.
- Se debe elaborar un programa de vacaciones que garantice la presencia permanente del personal crítico de las diferentes áreas y procesos de AMII,

tales como soporte técnico, redes y comunicaciones, sistemas de información y bases de datos, así como seguridad de la información.
- Elaboración de una base de datos de conocimiento, en caso el personal encargado de ciertos procedimientos, tanto principal, como de reemplazo se encuentren indispuestos.

e) Renovación tecnológica

- Programación de dos revisiones anuales de obsolescencia tecnológica de las partes internas de los servidores informáticos, para realizar la renovación de las mismas, en caso se requiera.
- Registrar las incidencias de deterioro de los equipos de almacenamiento, procesamiento y comunicaciones, para en base a las estadísticas de este registro adquirir equipos de contingencia.

f) Activación de trabajo remoto

- Verificación y validación de acceso seguro, en remoto, a los sistemas y servicios TICs.
- Activación de redes virtuales VPN, siempre y cuando el equipo a conectarse cuente con los mecanismos de seguridad informáticos necesarios.
- En caso el usuario no cuente con un equipo para realizar su trabajo remoto, se le pueda habilitar el equipo asignado, que se encuentra en la sede de la Sub Región Pacifico, para entregársela en su domicilio a fin de que cuente con las herramientas necesarias, siguiendo los protocolos dados por la Oficina de Abastecimiento
- Realizar el Trámite Certificados digitales, para instalarlos en los equipos de los usuarios, fuera de la institución.
- Activación del desvío de las llamadas telefónicas a los usuarios asignados encarados de la atención de la central telefónica.

- Verificación de los accesos seguros de los proveedores a cualquier elemento de la plataforma e infraestructura de servicios TICs, a cargo de la AMII en el Centro de Datos.

5.3.2. 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 SUB REGIÓN PACIFICO 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 y después de una contingencia:

Acciones durante la contingencia

- Estudiar y evaluar el alcance del desastre en cada área de responsabilidad.
- Notificar y reunir a los demás integrantes del equipo de Emergencia y Restauración de TIC.
- Informar al responsable del Grupo de Comando de Continuidad Operativa sobre la situación presentada, para decidir la realización de la Declaración de Contingencia y activación del sitio alterno o de respaldo.
- Determinar si el área afectada es segura para el personal (en caso de catástrofe).
- Estudiar y evaluar la dimensión de los daños a los equipos y sus facilidades, y elaborar un informe de los daños producidos.
- 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.

5.3.3. 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 SUB REGIÓN PACIFICO para estabilizar la infraestructura tecnológica luego del evento suscitado. Para lo cual se definen las pautas que permitan al personal de la AMII garantizar la continuidad de las operaciones en la entidad.

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

Figura N° 3 - Ciclo de la estrategia de recuperación de TI

La priorización de la restauración de los servicios de tecnologías de información De la Sub Region Pacifico se ejecutará de acuerdo a lo indicado en la siguiente Tabla de información:

Tabla N° 6 - Prioridad de atención durante la restauración de TIC

Prioridad de Atención	Descripción
1	Atención prioritaria: Sistemas de información y equipos que requieran alta disponibilidad de atención a los usuarios externos y manejen alto volumen de información. Ejemplo: Trámite documentario, Sistema Administrativo Financiero (SIAF), Sistema de gestión administrativa (SIGFYS), Portal Web institucional, servidores de bases de datos, gestor documental Alfresco, 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, CITES, interclima, COP20, etc.

En el Anexo 2 y Anexo 3 se detallan los sistemas de información y equipos informáticos, con la respectiva prioridad de atención, en caso de activarse la contingencia informática.

Acciones después de la contingencia

- Evaluar el trabajo de los equipos durante el proceso de recuperación.
- Evaluar la efectividad del Plan de Contingencia.
- Evaluar la efectividad del sitio alterno de contingencia y sus facilidades.

5.4. Fase 4: Elaboración del Plan de Contingencia y Recuperación de servicios de TIC.

Una vez identificados los eventos de contingencia y los escenarios de riesgos, se desarrollan los Planes de Contingencia agrupados por las categorías indicadas previamente. El Plan de Contingencia y Recuperación de los Servicios de Tecnología de la Información y Comunicaciones comprenderá los eventos de mayor impacto, identificados en la Matriz de Riesgo de Contingencia, los cuales serán abordados en formatos independientes, tal como se indica en el siguiente cuadro:

Tabla N° 7 - Eventos de mayor impacto para el Plan de Contingencia Informático

N°	Evento	Exposición al Riesgo	Formato Plan de
1	Terremoto /Sismo	Extremo	FPC - 01
2	Delito informático (ataque)	Extremo	FPC - 02
3	Falla de hardware y software	Extremo	FPC - 03
4	Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación.	Alto	FPC - 04

En el Anexo 4 se presenta el desarrollo de cada formato.

5.5. Fase 5: Definición y Ejecución de Plan de Pruebas

El plan de pruebas está enfocado principalmente a simular situaciones de contingencia en caso de incidencias producidas sobre equipos, información y procesos, manejados en situaciones reales y cuyos respaldos si pueden ser empleados y replicados en una hipotética situación de contingencia.

Con el fin de garantizar la ejecución integral de la prueba, se diseñará un conjunto de casos de pruebas funcionales, que serán ejecutados por los equipos operativos de la AMII, los cuales probarán, verificarán y observarán cualquier incidencia que se origine durante dicha prueba, a fin de retroalimentar cualquier acción que pueda corregir el plan.

La información que se desarrollará como parte del Plan de Pruebas, tiene el siguiente esquema:

- Metodología (descripción de la prueba a efectuarse)
- Alcances (áreas afectadas / personal involucrado)
- Resultados

Las pruebas relacionadas a este plan, se deberán ejecutar semestralmente, en los meses de junio y diciembre, con el fin de evaluar la preparación de la entidad, ante la ocurrencia de un siniestro y realizar los ajustes necesarios y deberán ser registradas en el formato detallado en el Anexo N° 05.

5.6. Fase 6: Implementación del Plan de Contingencia

La implementación del presente plan se realizará a partir del segundo mes de su aprobación. Para tal efecto, el/la Oficial de Seguridad de la Información, realiza las siguientes funciones:

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

5.7. Fase 7: Monitoreo

La fase de Monitoreo permite tener la seguridad de que se podrá reaccionar en el tiempo preciso y con la acción correcta. Esta fase es primordialmente de mantenimiento. Cada vez que se da o realiza un cambio en la infraestructura, debemos de realizar la adaptación respectiva.

A continuación, se enumeran las actividades principales a realizar:

- Realizar mantenimiento de la documentación técnica de operación de los servicios de TI.
- Revisión continua de las aplicaciones, sistemas de información y portales web.
- Revisión continua del sistema de copias de respaldo (backups).
- Revisión y mantenimiento de los sistemas de soporte eléctrico del Centro de Datos.

GOBIERNO REGIONAL ANCASH Sub Gerencia de Planif. y Presup. V° B° Sub Región Pacífico

GOBIERNO REGIONAL ANCASH Sub Gerencia de Administración V° B° Sub Región Pacífico

GOBIERNO REGIONAL ANCASH Contabilidad V° B° Sub Región Pacífico

REGIÓN ANCASH Informática y Sistemas Sub Región Pacífico

Anexos:

- Anexo 1 Metodología aplicada a la gestión de riesgos.
- Anexo 2 Listado de aplicaciones y sistemas de información clasificados por prioridad de atención para la recuperación de TIC
- Anexo 3 Listado de equipos del Centro de Datos y Gabinetes de Comunicación clasificados por prioridad de atención para la recuperación de TIC.
- Anexo 4

  Formatos del Plan de Contingencia Informático y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones por evento de riesgo.
- Anexo 5

  Formato de Control y certificación de las Pruebas del Plan de Contingencia y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones.

ANEXO 1
METODOLOGÍA APLICADA A LA GESTIÓN DE RIESGOS

1. **Cálculo de la Probabilidad de Ocurrencia de la Amenaza**. Para realizar este cálculo, se toman en cuenta dos variables: "Ocurrencia" y "Percepción".

   Se considera "ocurrencia" a la frecuencia en que se presentan los eventos a evaluar, sobre la base de los registros históricos de incidentes que hayan afectado a la Sub Region Pacifico directamente. Se consideró la siguiente tabla de valores para el cálculo:

N°	Ocurrencia	Descripción
1	Rara Vez	Se presentó al menos una vez en los últimos 20 años / Nunca se presentó
2	No Frecuente	Se presentó al menos una vez en los últimos 10 años
3	Moderada	Se presentó más de una vez en los últimos 5 años
4	Frecuente	Se presentó por lo menos una vez al año en los últimos 5 años
5	Muy Frecuente	Se presentó más de una vez al mes en el último año

La "Percepción" está basada netamente en la sensación de los expertos, de que la amenaza en cuestión podría ocurrir, se consideró la siguiente tabla de valores para el cálculo:

#	Percepción	Descripción
1	Muy Difícil	• <= 1% probabilidad, o • El acontecimiento requiere de circunstancias excepcionales, o • La probabilidad es nula, incluso en un futuro a largo plazo
2	Difícil	• >1% ó <=10% de probabilidad, o • Puede ocurrir pero no será anticipada
3	Mediana	• >10% ó <=50% de probabilidad, o • Puede ocurrir en el mediano plazo
4	Posible	• >50% ó <=75% de probabilidad, o • Podría ocurrir anualmente
5	Muy Posible	• >75% ó 100% de probabilidad, o • El impacto está ocurriendo ahora, o • Podría ocurrir dentro de unos meses

Los valores definidos para la Ocurrencia y Percepción son promediados y consolidados a fin de obtener una Probabilidad de Ocurrencia consensuada, asociada a cada amenaza en evaluación.

2. **Identificación de las amenazas que se tomarán en cuenta para la evaluación**. De la combinación de las variables descritas se obtiene la Probabilidad Estimada, que sirve como valor discriminatorio para seleccionar que amenazas se deberían evaluar para el alcance. Aquellas que resultan en un nivel de probabilidad estimada insignificante, según la tabla siguiente, no son tomados en cuenta.

Nivel de Probabilidad Estimada	Interpretación
Extrema	Probabilidad de ocurrencia alta (Evaluación de prioridad alta)
Moderado	Probabilidad de ocurrencia intermedia (Eval. de prioridad baja)
Menor	Probabilidad de ocurrencia muy baja (Eval. sin prioridad)
Insignificante	No se cree que ocurra (Desestimar evaluación)

3. **Cálculo de la Probabilidad de Afectación del Recurso. Se utiliza la siguiente tabla de valores para el cálculo:**

#	Probabilid	Descripción
1	Improbable	Se cuenta con controles razonablemente suficientes que responden a un programa de mantenimiento (evaluados y mejorados), se evidencia que han respondido a acontecimientos ocurridos y ejercicios realizados
2	Baja	Se cuenta con controles razonablemente suficientes que responden a un programa de mantenimiento y responden a los ejercicios y pruebas realizadas.
3	Moderada	Se cuenta con controles que responden a un programa de mantenimiento y responden a los ejercicios y pruebas realizadas, pero no son suficientes.
4	Alta	Algunos controles se prueban esporádicamente, debido a que no cuentan con un programa definido o de existir no se cumple con ei mismo.
5	Muy Alta	Bajo nivel de controles o los controles existentes no son efectivos o eficientes.

GOBIERNO REGIONAL ANCASH Sub Gerencia de Planif. y Presup. V° B° Sub Región Pacífico

GOBIERNO REGIONAL ANCASH Sub Gerencia de Administración V° B° Sub Región Pacífico

GOBIERNO REGIONAL ANCASH Contabilidad V° B° Sub Región Pacífico

REGIÓN ANCASH Informática y Sistemas Sub Región Pacífico

4. **Cálculo del Impacto del Recurso**. Se utiliza la siguiente tabla de valores para el cálculo:

#	Impacto	Descripción
1	No significativo	Tiene un efecto nulo o muy pequeño en las operaciones de la sede evaluada.
2	Menor	Afecta hasta en 6 horas las operaciones de la sede evaluada.
3	Moderado	Afecta hasta en 24 horas las operaciones de la sede evaluada.
4	Mayor	Afecta hasta en 48 horas las operaciones de la sede evaluada.
5	Catastrófico	Afecta por más de una semana las operaciones de la sede evaluada.

5. **Cálculo del Nivel de Riesgo**. Se calcula 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:

Probabilidad de Afectación		Impacto				
		No Significativo (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Muy Alta	(5)	Alto	Alto	Extremo	Extremo	Extremo
Alta	(4)	Moderado	Alto	Alto	Extremo	Extremo
Moderada	(3)	Bajo	Moderado	Alto	Extremo	Extremo
Baja	(2)	Bajo	Bajo	Moderado	Alto	Extremo
Improbable	(1)	Bajo	Bajo	Moderado	Alto	Alto

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

Nivel de riesgo	Interpretación
Extremo	Riesgo no deseable, se requiere acción correctiva
Alto	Riesgo no deseable que requiere de una acción correctiva, pero se permite una discreción de la gerencia sobre los plazos y compromisos.
Moderado	Riesgo aceptable con revisión de la dirección
Bajo	Riesgo aceptable, pero sin revisión.

ANEXO 2

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

N°	Sistema / Aplicativo	Breve descripción	Área Usuaria	Motor de BD	Tipo	Prioridad
1	Sistema Integrado de Administración y Finanzas (SIAF)	El SIAF es un sistema que automatiza los procedimientos financieros necesarios para registrar los recursos públicos recaudados y aplicarlos a la concreción de los objetivos del sector público	Todas las areas.	Fox	Escritorio	1
2	Sistema Integrado de Gestión Administrativa (SIGA)	El Sistema Integrado de Gestión Administrativa- SIGA es una herramienta informática que simplifica y automatiza los procesos administrativos en una entidad del Estado y que sigue las normas establecidas por los Órganos Rectores de los Sistemas Administrativos del Estado.	Todas las areas.	Sqlserver	Escritorio	1
3	(PEGASUS) módulo de planilla	El módulo de planilla del sistema PEGASUS es una herramienta para manejar, almacenar y automatizar procesos de gestión de nómina como el pago de planilla, registro de asistencia y control de vacaciones.	Recursos Humanos	Sqlserver	Escritorio	2
4	Sistema de Gestión Documentaria (SISGEDO)	El Sistema Tramite Documentario es el que se encarga monitoreo, seguimiento de documentos internos entre las distintas áreas e ingresos de documentos externos.	Tramite Documentario	Sqlserver	web	2

GOBIERNO REGIONAL ANCASH Sub Gerencia de Planif. y Presup. V° B° Sub Región Pacífico

GOBIERNO REGIONAL ANCASH Sub Gerencia de Administración V° B° Sub Región Pacífico

GOBIERNO REGIONAL ANCASH Contabilidad V° B° Sub Región Pacífico

REGIÓN ANCASH Informática y Sistemas Sub Región Pacífico

ANEXO 3

LISTADO DE EQUIPOS DEL CENTRO DE DATOS Y GABINETES DE COMUNICACIÓN CLASIFICADOS POR PRIORIDAD DE ATENCIÓN PARA LA RECUPERACIÓN DE TIC

N°	Tipo de Equipo	Rol	Descripción	Prioridad
2	Servidor	Virtualizado Aplicación	SIAF	1
2	Servidor	Virtualizado Aplicación	SIGA	1
3	Servidor	Controlador de Dominio	Servidor de dominio de red. (Directorio Activo, DNS).	1
4	Servidor	Aplicación	Pegasus	2
5	Servidor	Servidor Web	SISGEDO	2
6	UPS	Energía	Equipo de suministro eléctrico para servidores y equipos de comunicaciones	2
7	Aire acondicionado	Acondicionamiento	Aire acondicionado de precisión para el Centro de Datos	2
14	Switchs	Comunicaciones	Switches.	2

ANEXO 4

FORMATOS DEL PLAN DE CONTINGENCIA INFORMÁTICO Y RESTAURACIÓN DE SERVICIOS DE TIC

SUB REGION PACIFICO	Evento: Terremoto /Sismo	FPC - 01

1. PLAN DE PREVENCIÓN

a) Descripción del evento

Los sismos son movimientos en el interior de la tierra, que generan una liberación repentina de energía, que propaga en forma de ondas provocando el movimiento del terreno.

Este evento incluye los siguientes elementos mínimos identificados por la Sub Region Pacifico, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Infraestructura:
- Oficinas y/o Centro de Datos Principal

Recursos Humanos
- Personal de la entidad.

b) Objetivo

Establecer las acciones que se ejecutarán ante un sismo a fin de minimizar el tiempo de interrupción de las operaciones de la Sub Región Pacifico, sin exponer la seguridad de las personas.

c) Entorno

Este evento puede afectar las instalaciones de la Sede Central y el Centro de Datos, al ubicarse en la misma ciudad y distritos colindantes.

d) Personal Encargado

El Grupo de Comando de Continuidad Operativa de la Sub Región Pacifico, es quien debe dar los lineamientos y dar cumplimiento a las Condiciones de Prevención de Riesgo del presente Plan. Por su parte, el Equipo de Prevención de TIC debe realizar las acciones descritas en el punto f).

e) Condiciones de Prevención de Riesgo
- Inspecciones de seguridad realizadas periódicamente.
- Contar con un plan de evacuación de las instalaciones de la Sub Región Pacifico, el mismo que debe ser de conocimiento de todo el personal que labora en todas las sedes.
- Realización de simulacros de evacuación con la participación de todo el personal de las distintas sedes.
- Conformación de las brigadas de emergencia, y capacitarlas semestralmente.
- 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.

f) Acciones del Equipo de Prevención de TIC
- Evaluar en coordinación con el Grupo de Comando de Continuidad Operativa el ambiente para el Centro de Datos, en el sitio alterno.
- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo y restauración de información base de datos, código fuentes y ejecutables.
- Programar, supervisar el mantenimiento preventivo a los equipos componentes del Centro de Datos.
- Mantener actualizado el inventario hardware y software utilizado en el Centro de Datos de la entidad.
- Llevar un control de versiones de las fuentes de los sistemas de información y portales de la entidad.

2. PLAN 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) Procesos Relacionados antes del evento
- Tener la lista actualizada de los servidores por Direcciones y/u Oficinas.
- Mantenimiento del orden y limpieza de los ambientes de la sede central y Centro de Datos.
- Inspecciones trimestrales de seguridad externa.
- Realización de simulacros internos en horarios que no afecten las actividades.

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

d) Personal Encargado
Brigada de Emergencia de TIC.

e) Descripción de las actividades después de activar la contingencia
- Desconectar el fluido eléctrico y cerrar las llaves de gas u otros líquidos inflamables si corresponde.
- Evacuar las oficinas de acuerdo a las disposiciones de los Brigadistas de Evacuación, utilizando las rutas establecidas durante los simulacros. Considerar las escaleras de emergencia, señalización de rutas, zonas de agrupamiento del personal, etc. Por ningún motivo utilizar los ascensores.
- Verificar que todo el personal de la Sub Región Pacifico que labora en el área se encuentren bien.
- Alejarse de las lunas (ventanas) para evitar sufrir cortes por roturas y/o desprendimiento de trozos de vidrio.
- Evaluación de los daños ocasionados por el sismo sobre las instalaciones físicas, ambientes de trabajo, estanterías, 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. En todo momento se coordinará con personal de mantenimiento de la Sub Región Pacifico, para las acciones que deban ser efectuadas por ellos.

En caso se requiera la habilitación del ambiente provisional alterno para restablecer la función de los ambientes afectados, el/la jefe /a del área de modernización institucional e informática deberá coordinar con el/la Sub gerente de administración y recursos /a de la OGA.

f) Duración
Los procesos de evacuación del personal del SUB REGIÓN PACIFICO deberán ser calmados y demorar 5 minutos como máximo.
La duración total del evento dependerá del grado del sismo, la probabilidad de réplicas y los daños a la infraestructura.

3. PLAN DE RECUPERACION

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

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 los equipos de respaldo 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.

- Supervisar el progreso de las operaciones de recuperación y de servicios de TI y mantener informado al Grupo de Comando de Continuidad Operativa.

- Restauración de los servicios y operaciones de TI en el sitio alterno. El Equipo de restauración de TIC restaurarán el espacio de trabajo para permitir que el personal crítico de la 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. o 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 y las telecomunicaciones están funcionando según lo estimado tanto en el sitio alterno, como al retornar al sitio original, una vez concluida la emergencia o siniestro.

- Registrar todos los gastos operacionales relacionados con la continuidad del negocio.

c) Mecanismos de Comprobación
El/La Coordinador/a de Continuidad de TIC, presentará un informe al Grupo de Comando de Continuidad Operativa, explicando qué parte de las actividades u operaciones de tecnologías de la información han sido afectadas y cuáles son las acciones tomadas.

d) Desactivación del Plan de Contingencia
El/La Coordinador/a de Continuidad de TIC desactivará el Plan de Contingencia informático una vez que se haya tomado las acciones descritas en el presente Plan de Recuperación, mediante una comunicación electrónica al Grupo de Comando de Continuidad Operativa.

e) Proceso de Actualización
El proceso de actualización será en base al informe presentado por el/la Coordinador/a de Continuidad de TIC, luego del cual se determinará las acciones a tomar.

SUB REGION PACIFICO	Evento: Delito Informatico	FPC-02

1. PLAN DE PREVENCIÓN

a) Descripción del evento

Alteración de datos de los portales y sistemas de información a través de ataque cibernético (hacking) y/o malware.

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.

Este evento incluye los siguientes elementos mínimos identificados por la Sub Región Ancash, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación:

Hardware
- Servidores.
- Estaciones de Trabajo.

Software
- Software Base.
- Sistemas de información, aplicativos y portales de la Sub Región Pacifico.

b) Objetivo

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

c) Entorno

Este evento se puede darse en cualquiera de los servidores y estaciones ubicadas en el Centro de Datos y en la sede principal de la Sub Región Pacifico.

d) Personal Encargado

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

e) Condiciones de Prevención de Riesgo

- Instalación de parches de seguridad en los equipos.
- Establecimiento de políticas de seguridad para prevenir el uso de aplicaciones no autorizadas en las estaciones de trabajo.
- Aplicación de filtros para restricción de correo entrante, y revisión de archivos adjuntos en los correos y así prevenir la infección de los terminales de trabajo por virus.
- Contar con antivirus instalados en cada estación de trabajo, el mismo que 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.

- Eliminación o restricción de lectoras y/o quemadores de CD en estaciones de trabajo que 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.
- Capacitación al personal de AMII, sobre Ethical Hacking a las Bases de Datos, Sistemas Operativos, Servidores y Sistemas Informaticos.
- Ejecución de ataques de Hacking Ético por terceros especializados.

f) Acciones del Equipo de Prevención de TIC

- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo de información de la información procesada y almacenada en el Centro de Datos.
- 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. PLAN DE EJECUCIÓN

a) Eventos que activan la Contingencia
- Mensajes de error durante la ejecución de programas.
- Lentitud en el acceso a las aplicaciones.
- Falla general en el equipo (sistema operativo, aplicaciones).

b) Procesos relacionados antes del evento
Cualquier proceso relacionado con el uso de las aplicaciones en los servidores y en las estaciones de trabajo.

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

Personal encargado
Equipo de Emergencia de TIC.

e) Descripción de las actividades después de activar la contingencia
- Desconectar o retirar de la red de datos de la Sub Región Ancash, el servidor o la estación infectada o vulnerada.
- 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.
- Rastrear de ser necesario el origen de la infección u ataque (archivo infectado, correo electrónico, hacking, etc.)
- Guardar la muestra del virus detectado y remitirlo al proveedor del antivirus utilizado. En el caso de hacking a aplicaciones, se debe guardar el archivo modificado, a nivel de software y base de datos.
- Eliminar el agente causante de la infección, es decir, remover el malware/virus del sistema.
- Probar el sistema.
- En caso no solucionarse el problema, formatear el equipo y restaurar copia de respaldo.

f) Duración
La duración del evento no deberá ser mayor DOS HORAS en caso se conforme la presencia de un virus en estaciones de trabajo y de CUATRO HORAS en servidores de red. Esperar la indicación del personal de soporte técnico para reanudar el trabajo.

3. PLAN DE RECUPERACION

a) Personal Encargado

El equipo de restauración de TIC, luego de restaurar el correcto funcionamiento del servidor, estación de trabajo (PC, laptop), sistemas de información y portales web, coordinará con el usuario responsable del mismo y/o director del área para reanudar las labores de trabajo con el equipo o sistema que fue afectado.

b) Descripción de actividades

Se informará a él/la director/a de AMII de la Sub Región Pacifico el tipo de malware/virus, o tipo de ataque encontrado y el procedimiento usado para removerlo.

Estas actividades deben contemplar como mínimo:

- Instalación y puesta a punto de un cómputo compatible y hardware necesarios para la instalación del sistema de información con las características mínimas exigidas.
- 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, con sus respectivas librerías y niveles de seguridad.
- Instalación de aplicaciones adicionales necesarias para el funcionamiento del sistema de información.
- Realización de la restauración de la base de datos con la última copia de seguridad disponible (Restore).
- Reinicio del servicio, prueba y afinamiento del sistema de información.
- Conectar el servidor o la estación a la red de la Sub Region Pacifico.
- Efectuar las pruebas necesarias con el usuario final de los equipos y/o sistemas de información afectados.
- Solicitar la conformidad de la restauración realizada del equipo y o sistema de información afectado.
- Comunicar el restablecimiento del servicio

En función a esto, el/la Oficial de Seguridad de la Información, tomará las medidas preventivas del caso enviando una alerta vía correo al personal de la Sub Región Pacifico.

El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de incidentes de seguridad de la información.

c) Mecanismos de Comprobación

Se llenará el formato de incidentes de seguridad de la información y se informará al Comité de Gestión de Seguridad de la Información.

El personal de Técnico de Soporte y/o Especialista en Redes y Comunicaciones. según sea el caso, presentará un informe a el/la Director/a de AMII, explicando que parte del servicio u operaciones se han visto afectadas, y cuáles son las acciones tomadas.

d) Desactivación del Plan de Contingencia

Con el aviso de el/la Coordinador/a de Continuidad de TIC del SUB REGIÓN PACIFICO, se desactivará el presente Plan.

e) Proceso de Actualización

El problema de infección o alteración presentado en la estación de trabajo y/o servidor de red, en base al informe que describe los problemas presentados, se determinarán las acciones de prevención a tomar.

SUB REGION PACIFICO	Evento: Falla de hardware y software	FPC-03

1. PLAN DE PREVENCIÓN

a) Descripción del evento

El hardware de servidores es el recurso principal para almacenar, procesar y proteger los datos, permitiendo acceso controlado y procesamiento de transacciones rápido para cumplir con los requisitos de las aplicaciones de la entidad.

El software

En ausencia del mismo, los sistemas de información que dependen del mismo no pueden funcionar, siendo la parte afectada o causa de la contingencia, los cuales se muestran a continuación:

Hardware

- Servidores de Base de Datos, Aplicaciones, Archivos
- Storage

Software

- Aplicativos usados por SUB REGIÓN PACIFICO y de servicio al ciudadano

Información

- Información contenida en base de datos.
- Información contenida en repositorios de información

b) Objetivo

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

c) Entorno

Se puede producir durante el servicio, afectando a las aplicaciones usadas para dar soporte a las operaciones de la Sub Región Pacifico.

d) Persona Encargado

Equipo de Prevención de TIC.

e) Condiciones de Prevención de Riesgo

- Revisión periódica de los registros (logs) de los servidores, para prevenir mal funcionamiento de los mismos.
- Contar con los backups diarios de datos de las aplicaciones en desarrollo/producción de la entidad, así como de las imágenes de los servidores.
- 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.
- Disponer de servidores de Aplicaciones de contingencia, con software de instalación tomcat, jboss, wildfly.

f) Acciones del Equipo de Prevención de TIC

- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo y restauración de información.
- Programar, supervisar el mantenimiento preventivo a los equipos componentes del Centro de Datos.
- Mantener actualizado el inventario hardware y software utilizado en el Centro de Datos de la entidad.
- Realizar monitoreo del funcionamiento de los servidores instalados en el Centro de Datos para su correcto funcionamiento.
- Realizar revisiones de obsolescencia tecnológica de los servidores y componentes internos de forma anual.

2. PLAN DE PREVENCIÓN

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) Procesos Relacionados antes del evento

Disponibilidad de las copias de respaldo.
Disponibilidad de instaladores de sistemas operativos y motor de base de datos.

c) Personal que autoriza la contingencia

El/La Coordinador/a de Continuidad de TIC debe activar la contingencia.

d) Descripción de las actividades después de activar la contingencia

- Realizar la revisión del servidor averiado, buscando un recurso de reemplazo
- verificando que dicho equipo cuente con garantía, de lo contrario se implementará un nuevo servidor virtual configurado de acuerdo a lo requerido.

Solicitar las cintas de respaldo para poder proceder a la restauración de la información almacenada en el servidor averiado.

e) Duración

El tiempo máximo de la contingencia no debe sobrepasar las cuatro (4) horas.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado

El Equipo de Restauración de TIC, luego de validar la corrección del problema de acceso a los servidores, y el/la Coordinador/a de Continuidad de TIC informará a los directores y/o directores de áreas para la reanudación de las operaciones de los servicios afectados en el servidor averiado.

b) Descripción de actividades

El plan de recuperación estará orientado a recuperar en el menor tiempo posible las actividades afectadas durante la interrupción del servicio afectado por falla de los servidores.

Se debe realizar como mínimo las siguientes actividades:

- Instalación y puesta a punto de un cómputo compatible y hardware necesarios para la instalación del sistema de información con las características mínimas exigidas.

- 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, con sus 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.
- Brindar los permisos de acceso a los usuarios finales.
- Remitir un mensaje electrónico a los usuarios del SUB REGIÓN PACIFICO informando la reanudación de los servicios.

En función a esto, se tomarán las medidas preventivas del caso y se revisará el plan de contingencia para actualizarlo en caso sea necesario.

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 AMII, precisando las acciones realizadas.

El/La Especialista en Redes y Comunicaciones, presentará un informe a el/la Director/a de AMII, explicando que parte del servicio u operaciones se han visto afectadas, y cuáles son las acciones tomadas.

d) Desactivación del Plan de Contingencia

Con el aviso de el/la Coordinador/a de Continuidad de TIC, se desactivará el presente Plan.

e) Proceso de Actualización

Con el informe presentado por el/la Especialista en Redes y Comunicaciones, quien identifica las causas de la pérdida o fallas de la base de datos institucional, se determinará las acciones preventivas necesarias que deberían incluirse en el presente plan.

En caso existiese información pendiente de actualización, el/la Especialista en Redes y Comunicaciones deberá iniciar las labores de actualización de los procedimientos o guías de recuperación de servidores.

SUB REGION PACIFICO	**Evento:** **Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación.**	FPC-04

1. PLAN DE PREVENCIÓN

a) Descripción del evento

Falla general del suministro de energía eléctrica en el Centro de Datos o sede principal de la entidad.

Este evento incluye los siguientes elementos mínimos identificados por la Sub Región Pacifico, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Servicios Públicos:

- Suministro de Energía Eléctrica

Hardware

- Servidores y sistema de almacenamiento de información (storage)
- Estaciones de Trabajo
- Equipos de Comunicaciones

Equipos Diversos

- UPS y generador eléctrico
- Aire acondicionado

b) Objetivo

Restaurar las funciones consideradas como críticas para el servicio.

c) Entorno

Este evento puede darse en cualquiera de las instalaciones del SUB REGIÓN PACIFICO, considerando la Sede Central y la sede donde se ubica el Centro de Datos, por tener cada una de ellas los gabinetes de comunicación y equipos que brinda servicios informáticos a los usuarios a nivel interno y externo.

d) Personal Encargado

El/La director/a de la Oficina de Abastecimiento de la OGA y el/la Coordinador/a de Continuidad de TIC son los responsables de realizar las coordinaciones para restablecer el suministro de energía eléctrica. El Equipo de Prevención de TIC debe realizar las acciones descritas en el punto f).

e) Condiciones de Prevención de Riesgo

- Durante las operaciones diarias del servicio u operaciones del SUB REGIÓN PACIFICO se contará con los UPS necesarios para asegurar el suministro eléctrico en los equipos consideradas como críticos.
- Equipos 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 los equipos UPS.
- Realización de pruebas periódicas de los equipos UPS para asegurar su correcto funcionamiento.

- Capacidad de los 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.
- Disponibilidad de UPS para proteger los equipos de vigilancia (cámaras, sistemas de grabación) y de control de acceso a las instalaciones del SUB REGIÓN PACIFICO (puertas, contactos magnéticos, etc.)

- Verificación del cableado eléctrico de todas las sedes del Ministerio del Ambiente, una vez por año.
- Instalación de luces de emergencia con tolerancia de 15 minutos, accionados automáticamente al producirse el corte de fluido eléctrico, los cuales deben estar instalados en los ambientes críticos.

f) Acciones del Equipo de Prevención de TIC
- Revisar periódicamente y de forma conjunta con el área de Servicios Generales las instalaciones eléctricas del Centro de Datos y Sede principal de la entidad.
- Coordinar y supervisar el mantenimiento preventivo de pozos a tierra, aire acondicionado de precisión del Centro de Datos, UPS, transformador y del gabinete de baterías trimestralmente.
- Verificar que la red eléctrica utilizada en el Centro de Datos y la red de cómputo de la sede principal sea estabilizada. En caso no existan se debe gestionar la implementación de lo requerido con el área respectiva.
- Revisar la presencia de exceso de humedad en la sala de energía del centro de datos del Ministerio del Ambiente.

2. PLAN DE EJECUCION

a) Eventos que activan la contingencia
Corte de suministro de energía eléctrica en los ambientes del SUB REGIÓN PACIFICO.

b) Procesos Relacionados antes del evento
Cualquier actividad de servicio dentro de las instalaciones.

c) Personal que autoriza la contingencia
El/La Director/a de OGA y/o Coordinador de Continuidad de TIC pueden activar la contingencia.

d) Descripción de las actividades después de activar la contingencia
- Informar a el/la Director/a de la Oficina de Abastecimiento del problema presentado.
- Comunicar a la empresa prestadora de servicios de energía eléctrica la falta de energía.
- Dar aviso del corte de energía eléctrica en forma oportuna a todas las áreas del SUB REGIÓN PACIFICO y coordinar las acciones necesarias.
- Las actividades afectadas por la falta de uso de aplicaciones, deberán iniciar sus procesos de contingencia a fin de no afectar las operaciones en curso.
- En el caso de los equipos que entren en funcionamiento automático con UPS's, se deberá monitorear el tiempo de autonomía del equipo y no exceder el indicado anteriormente.
- En caso la interrupción de energía en el Centro de Datos sea mayor a dos (02) horas, se deberán apagar los equipos en forma ordenada mientras funcione el UPS y hasta que regrese el fluido eléctrico.

e) Duración
El tiempo máximo de duración de la contingencia dependerá del Proveedor externo de energía eléctrica.

3. PLAN DE RECUPERACION

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

b) Descripción de actividades

El evento será evaluado y registrado de ser necesario en el formato de incidentes de seguridad de la información.
Se debe realizar como mínimo las siguientes 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 siguiente detalle:
- 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 en Redes y Comunicaciones presentará un informe a el/la Director/a de la AMII, explicando que parte del servicio, equipos u operaciones de tecnología de la información han fallado y cuáles son las acciones correctivas y/o preventivas a realizar.

Este informe deberá ser elevado al Grupo de Comando de Continuidad Operativa del SUB REGIÓN PACIFICO.

d) Desactivación del Plan de Contingencia

El/La Coordinador de Continuidad de TIC 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.

e) Proceso de Actualización

En base al informe que describe los problemas presentados, se determinarán las acciones de prevención a tomar.

GOBIERNO REGIONAL ANCASH Sub Gerencia de Planif. y Presup. V° B° Sub Región Pacífico

GOBIERNO REGIONAL ANCASH Sub Gerencia de Administración V° B° Sub Región Pacífico

GOBIERNO REGIONAL ANCASH Contabilidad V° B° Sub Región Pacífico

REGIÓN ANCASH Informática y Sistemas Sub Región Pacífico