PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN DE LA SUNASS

ROL	NOMBRE	PUESTO
Elaborado por:	Edgar Rodríguez Romero	Especialista en Infraestructura
	Fernando Ramón Bueno Talavera	Analista en Redes, Comunicaciones y Seguridad Informática
Revisado por:	Luis Victor Méndez Montoya	Especialista en Sistemas e Informática (Oficial de Seguridad y Confianza Digital)
	Zico Alexis Yacila Espinoza	Jefe de la Oficina de Tecnologías de Información
	Kelly Elizabeth Paz Orellana	Jefa (e) de la Unidad de Modernización
Aprobado por:	Manuel Fernando Muñoz Quiroz	Gerente General

ÍNDICE

1. INTRODUCCIÓN

1.1. OBJETIVOS DEL PLAN

1.1.1. Objetivo General

Establecer los principios básicos y el marco necesario para garantizar la continuidad de los servicios y/o procesos frente a situaciones imprevistas, minimizando los riesgos, protegiendo los recursos y activos y facilitando una pronta recuperación.

1.1.2. Objetivos Específicos

- Identificar las aplicaciones y las plataformas consideradas críticas para la operación de la SUNASS.
- Identificar al personal clave interno y externo requerido para la operación de las actividades críticas.
- Definir la funcionalidad mínima que se requiere en caso de contingencia.
- Desarrollar procedimientos específicos y guías de operación en caso de desastre para cada uno de los servicios críticos vitales especificados en el alcance del Plan de Contingencia de Sistemas de Información.
- Desarrollar e impartir la capacitación inicial para el correcto funcionamiento del Plan de Contingencia de Sistemas de Información.
- Establecer un plan de prueba, gestión y mantenimiento necesarias para garantizar los objetivos del Plan de Contingencia de Sistemas de Información.

1.2. ALCANCE DEL PLAN

El alcance del Plan de Contingencia de Sistemas de Información comprende la restauración de los servicios críticos de tecnología de Información que dan soporte a los servicios de la SUNASS.

1.3. REFERENCIAS NORMATIVAS Y LEGALES

- Ley Nº 27332 Ley Marco de los Organismos Reguladores de la Inversión Privada en los Servicios Públicos
- Ley Nº 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
- Decreto Ley N° 25965 Crean la Superintendencia Nacional de Servicios de Saneamiento.
- Decreto Legislativo Nº 1031, Decreto Legislativo que promueve la eficiencia de la actividad empresarial del Estado, su reglamento y modificatorias.
- Decreto Legislativo Nº 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
- Decreto Supremo Nº 048-2011-PCM, Decreto Supremo que aprueba el Reglamento de la Ley Nº 29664, que crea al 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 Nº 115-2022-PCM, “Decreto Supremo que aprueba el Plan Nacional de Gestión del Riesgo de Desastres - PLANAGERD 2022-2030”
- 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 Directoral N°019–2013–JUS/DGPDP, que aprueba la “Directiva de Seguridad de la Información Administrada por lo Bancos de Datos Personales”.
- Mediante Resolución de Consejo Directivo N° 013-2021-SUNASS-CD se aprueba el Plan Estratégico Institucional de la SUNASS correspondiente al periodo 2020-2024.

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

1.4. SIGLAS

CGD : Comité de Gobierno Digital de la SUNASS
DAP : Dirección de Ámbito de la Prestación.
DF : Dirección de Fiscalización.
DPN : Dirección de Políticas y Normas
DRT : Dirección de Regulación Tarifaria.
DS : Dirección de Sanciones.
DU : Dirección de Usuarios.
EPS : Empresa Prestadora de Servicios de Saneamiento.
NTP : Norma Técnica Peruana.
OAF : Oficina de Administración y Finanzas.
ODS : Oficinas Desconcentradas de Servicios.
OTI : Oficina de Tecnologías de Información.
PCSI : Plan de Contingencia de Sistemas de Información.
SISTRAM : Sistema de Trámite Documentario de la SUNASS
SUNASS : Superintendencia Nacional de Servicios de Saneamiento
SGSI : Sistema de Gestión de la Seguridad de la Información
TI : Tecnologías de la Información
TRASS : Tribunal Administrativo de Soluciones de Reclamos de los Usuarios de los Servicios de Saneamiento.
UA : Unidad de Abastecimiento
URH : Unidad de Recursos Humanos

1.5. DEFINICIONES

1.5.1. Activos de Información: Es el bien o servicio tangible o intangible, que genera, procesa o almacena información, en el cual se le atribuye un grado de valor según su criticidad o asociación con los procesos misionales.

1.5.2. Aplicación: Es aquel programa informático que permite a un usuario utilizar una computadora con un fin específico. Las aplicaciones son parte del software de una computadora y suelen ejecutarse sobre el sistema operativo. Una aplicación de software suele tener un objetivo único: navegar en la web, revisar correo, explorar el disco duro, etc.

1.5.3. Amenaza: Es cualquier factor que tiene el potencial para explotar una debilidad y dar lugar a algún tipo de daño a la información o a la institución.

1.5.4. Base de Datos: Es una colección de información organizada de forma que un programa o aplicación pueda seleccionar rápidamente los fragmentos de datos que necesite.

1.5.5. Centro de datos: Es un centro de procesamiento para obtener información, en el cual se albergan los sistemas de información, hardware, componentes asociados, como telecomunicaciones y sistemas de almacenamiento.

1.5.6. Confidencialidad: Propiedad de la información que hace que será protegida para que no sea divulgada sin consentimiento de la persona. Dicha garantía se lleva a cabo por medio de un grupo de reglas que limitan el acceso a esta información.

1.5.7. Control: Medio para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la entidad que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

1.5.8. Cortafuego (Firewall): Dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios y pueden ser implementados en hardware o software, o en una combinación de ambos.

1.5.9. Datos: Son todos aquellos elementos por medio de los cuales es posible la generación de información. Tales elementos pueden ser estructurados (base de datos) o no estructurados (correos electrónicos) y se presentan en forma de imágenes, sonidos o colección de bits.

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

1.5.11. Incidente: Circunstancia o suceso que acontece de manera inesperada y que puede afectar al desarrollo de una actividad, aunque no forme parte de él. En nuestro contexto, es una interrupción de las condiciones normales de operación en cualquier proceso informático en la SUNASS.

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

1.5.13. Método de análisis de riesgos: Es el conjunto de técnicas empleadas para evaluar los riesgos de un proyecto o un proceso. Estos métodos ayudan a tomar decisiones que permiten implementar medidas de prevención ante riesgos potenciales y mitigar su impacto.

1.5.14. 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 PCSI, porque permite aminorar y atenuar la probabilidad de ocurrencia de un estado de contingencia.

1.5.15. 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.

1.5.16. 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.

1.5.17. Plan de Continuidad Operativa: Es el plan definido y documentado que guían a la organización a responder, recuperar, reanudar los servicios de TI después de una interrupción.

1.5.18. Probabilidad: Posibilidad que un evento determinado ocurra en un período de tiempo dado.

1.5.19. Riesgo: Es la posibilidad que ocurra un evento adverso que afecte el logro de los objetivos de la entidad/dependencia.

1.5.20. Sistema de Información: Es el conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su posterior uso. Este involucra a personas, registro de datos, actividades que los procesan y los manuales de procesos o procesos automatizados.

1.5.21. Sistema de Comunicación: Es un conjunto de dispositivos interconectados entre sí que permiten la transmisión de datos e información de un punto a otro. La característica principal de esta transmisión es la de ser bidireccional. El concepto cubre todas las formas de comunicación a distancia, incluyendo radio, telegrafía, televisión, telefonía, transmisión de datos e interconexión de computadoras a nivel de enlace.

1.5.22. RTO *(Recovery Time Objective)*: Se refiere al período de tiempo máximo permitido para la recuperación de los servicios, sistemas o procesos críticos de una organización después de un incidente o interrupción.

2. PLANIFICACIÓN

2.1. IDENTIFICACIÓN DE SISTEMAS DE INFORMACIÓN Y ACTIVOS CRÍTICOS

2.1.1. Inventario de sistemas de información y activos digitales.

La SUNASS comprende la importancia de realizar el inventario de los aplicativos y sistemas de información asi como de los equipos que forman parte del Centro de Datos, lo que le permite tener la trazabilidad de estos, así como tener en el radar aquellos que son de uso recurrente para las actividades diarias y aplicarles los controles que reduzcan el riesgo de impacto sobre los procesos a los que están directamente asociados, manteniendo así el control sobre dichos activos.

En el Anexo N° 02 y Anexo N° 03 se encuentra el listado de aplicativos y sistemas de información asi como de los equipos que forman parte del Centro de Datos inventariado en la SUNASS en los que se señala el nivel de riesgo por cada ítem, el cálculo se realiza de acuerdo con el anexo N° 01.
Para determinar el valor del impacto, en cada uno de ítems, se realizó consultas a las áreas usuarias sobre la afectación en sus procesos si ocurriera algún corte en el servicio brindado. El valor de probabilidad usado para todos los ítems es el mismo debido a que están ubicados en el mismo ambiente.

2.1.2. Clasificación de sistemas y activos según su criticidad e importancia para la continuidad del negocio.

Como parte de su plan de prevención, la SUNASS ha realizado la identificación de los procesos, aplicaciones críticas y los recursos de TI con los que cuenta. Se ha considerado todos los elementos susceptibles a incidentes que activen alguna contingencia. Los procesos y recursos identificados son los siguientes:

Tabla N° 1 –Procesos y Recursos críticos de TI

Proceso Critico	Recursos
Gestión de redes e infraestructura de TI	Equipo de Grupo Electrógeno
	Gabinete Autocontenido del centro de datos
	Equipos de comunicaciones (Switch core, Switch de brode, AccessPoint)
	Enlaces de fibra óptica para Internet
	Equipo de seguridad perimetral (Firewall)
	Cableado de red de datos
	Sistema de almacenamiento (storage)
	Equipo de librería robótica (Drive de cinta)
	Equipo de backup a disco Acserve
	Equipo servidor Blade
	Servidores virtuales
	Central Telefónica
	Servidores físicos
Gestión de sistemas de información y bases de datos	Sistemas de información y portales core
	Correo electrónico y aplicativos colaborativos
	Sistemas de información administrativos
	Base de datos y repositorios utilizados por los sistemas y aplicativos.
Soporte Técnico	Estaciones de trabajo del personal crítico (computadoras de escritorio y portátiles)
Operación y mantenimiento de TIC	Personal crítico responsable de los procesos de TIC.

2.2. ANÁLISIS DE RIESGOS

2.2.1. Metodología de análisis de riesgos

Para determinar el nivel de riesgo de un recurso de TI crítico de la SUNASS, se consideraron los controles existentes que mitigan la afectación de la amenaza, de acuerdo con la aplicación de la metodología de riesgos descrita en el Anexo N° 01 del presente plan.

2.2.2. Identificación de amenazas

Se identifican aquellas amenazas que pueden vulnerar los servicios TIC de la SUNASS, considerando la ubicación geográfica, el contexto actual del Centro de Datos, así como, la percepción del juicio experto. Las amenazas identificadas se describen en la siguiente tabla:

Tabla N° 2 – Amenazas a los servicios de TI

N°	Amenaza (Evento)	Tipo
1	Sismo	Incidentes Naturales
2	Inundación y aniego en el Centro de Datos	
3	Incendio en el Centro de Datos.	
4	Falla en telecomunicaciones.	Tecnológicos
5	Delito informático.	
6	Falla de hardware y software.	
7	Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación.	Físico y ambiental
8	Ausencia o no disponibilidad del personal crítico de TI.	Humanos
9	Pandemia y/o Epidemia	Ambiental

2.2.3. Evaluación de la probabilidad e impacto de los riesgos

a) Nivel de criticidad cualitativo

Una vez determinadas las principales amenazas que pueden afectar los servicios de TI, se calcula el nivel de criticidad estimada, para identificar qué amenazas serán consideradas en la evaluación de riesgos.

Los valores de ocurrencia y percepción se determinan según lo indicado en el Anexo N° 01 del presente plan. El resultado obtenido es:

Tabla N° 3 – Criticidad cualitativa estimada de las amenazas a los servicios de TI

Ítem	Amenaza	Percepción (P)	NivelP.	Ocurrencia (O)	Nivel O	Nivel Criticidad (P x O)	Nivel de Criticidad Cualitativo
1	Sismo	Posible	4	Frecuente	4	16	Moderado
2	Inundación y aniego en el Centro de Datos	Mediana	3	No Frecuente	2	6	Insignificante
3	Incendio en el Centro de Datos	Muy Difícil	1	Rara Vez	1	1	Insignificante
4	Falla en telecomunicaciones.	Mediana	3	Frecuente	4	12	Menor
5	Delitos informáticos.	Posible	4	Frecuente	4	16	Moderado
6	Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación.	Posible	4	Frecuente	4	16	Moderado
7	Falla del hardware y software.	Posible	4	Frecuente	4	16	Moderado
8	Ausencia o no disponibilidad del personal crítico de TI.	Mediana	3	No Frecuente	2	6	Insignificante
9	Pandemia y/o Epidemia	Mediana	3	No Frecuente	2	6	Insignificante

b) Determinación del impacto

La SUNASS ha establecido una escala de 4 valores para determinar el impacto que un incidente tiene sobre los servicios de TI donde se establece el nivel de afectación que puede generar un incidente sobre dichos activos según lo señalado en la Tabla N° 4:

Tabla N° 4 –Niveles de impacto de la indisponibilidad del proceso

Escala	Valor	Afectación
Muy Bajo	**1**	Compromete la ejecución de una actividad, pero el resto del proceso puede continuar.
Bajo	**2**	Compromete la ejecución de un proceso no importante o genera pequeños impactos en su ejecución.
Medio	**3**	Compromete la ejecución de un proceso importante o genera pequeños impactos en su ejecución.
Alto	**4**	Compromete la ejecución de varios procesos o un proceso crítico

2.3. IDENTIFICACIÓN DE CONTROLES PREVENTIVOS

Los impactos de cortes de los servicios de la TIC que han sido identificados en el presente plan pueden mitigarse o eliminarse mediante controles preventivos efectuados sobre la base de la implementación de la NTP ISO 27001 y el ISO 9001. Estos controles son:

- Fuentes de alimentación ininterrumpida (UPS) de tamaño adecuado para proporcionar energía de respaldo a corto plazo a todos los componentes del Centro de Datos.
- Generadores para proporcionar energía de respaldo a largo plazo.
- Sistema de aire acondicionado de precisión para el Centro de Datos.
- Detectores de humo.
- Almacenamiento externo de medios de copia de seguridad.
- Copias de seguridad programadas frecuentes de los sistemas críticos, almacenadas externamente.
- Contrato con acuerdos de niveles de servicio con proveedor de Internet.
- Redundancia en los enlaces de internet, con el mismo proveedor.
- Cámaras de vigilancia al exterior del Centro de Datos.
- Mantenimiento de Tableros eléctricos.
- Contrato de servicio de soporte y mantenimiento de la Base de Datos.
- Sistema de control de acceso al Centro de Datos.
- Solución antivirus instalada en los servidores de red y computadoras.
- Software de ciberseguridad para el seguimiento de logs y capacidades.
- Contrato de mantenimiento para equipos de aire acondicionado del Centro de Datos.
- Contrato de mantenimiento y soporte de la herramienta para realizar las copias de respaldo.
- Contrato de mantenimiento y soporte para la plataforma de servidores.
- Contrato de Soporte y mantenimiento de Central telefónica.
- Contrato de soporte y mantenimiento de Soluciones críticas (Dialapplet y Contactek).
- Contrato de mantenimiento y soporte de equipos de seguridad perimetral.
- Contrato de mantenimiento y soporte de equipos de comunicación (Switches).
- Contrato de mantenimiento de UPS.
- Contrato de mantenimiento de grupo electrógeno.
- Contrato de mantenimiento de gabinetes autocontenidos.
- Controles técnicos de seguridad como los de accesos con privilegios mínimos.
- Sensores de aniegos.
- Uso de conexiones remotas seguras con VPN.
- Prueba anual de los puestos de emergencia.

- Prueba anual de ethical hacking.
- Prueba anual de restauración de datos.

2.4. REQUISITOS MÍNIMOS PARA LA EJECUCIÓN DEL PLAN

- Se debe mantener los controles de acceso a la infraestructura, según lo señalado en el numeral 7.6 de la Directiva "Lineamientos Específicos de la Seguridad de la Información", asi como mantener actualizada la Bitácora de Acceso.
- Se debe contar con respaldos de la información y realizar pruebas, para ello, se debe realizar periódicamente backups de la información, del software y de imágenes del sistema de acuerdo con lo establecido en la caracterización del proceso "Respaldo y Restauración de la Información (GTI-RRI-CR-N2)" y lo señalado en el instructivo "Ejecución de Respaldo y Restauración de la Información (GTI-OTI-IN002)".
- Se debe realizar el mantenimiento de equipos de cómputo, servidores y equipos de comunicaciones en cumplimiento del control A.11.2.4 de la NTP ISO/IEC 27001:2014.
- Se debe cumplir con el control A.17.2 de la NTP ISO/IEC 27001:2014 sobre redundancias en servicios claves.
- Se debe revisar y actualizar de ser el caso los lineamientos de seguridad de forma anual en cumplimiento del control A.5.1.2

2.5. SOBRE LOS LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

La SUNASS ha establecido lineamientos de seguridad de la información a fin de proteger la confidencialidad, la disponibilidad e integridad de la información, recursos, servicios e instalaciones de la entidad en la Directiva "Lineamientos Específicos de Seguridad de la Información".

2.6. ESTRATEGIAS DE PROTECCIÓN Y RECUPERACIÓN

2.6.1. Estrategias de prevención de tecnologías de la información.

a) Almacenamiento y respaldo de la información (BACKUPS)

- Gestionar las copias de respaldo (Backup) de la información almacenada y procesada en el Centro de Datos.
- Verificar la ejecución periódica de las tareas programadas de respaldo de información y comprobación de los medios de respaldo.

b) Replicación de servidores críticos

- El plan incluye una estrategia para la replicación de servidores críticos en el Centro de Datos de SUNASS.

c) Evaluación y gestión de proveedores

- Mantener actualizado el listado de proveedores claves de servicios y recursos de TI, con sus datos de contacto.
- Mantener listas detalladas de necesidades de equipos y sus especificaciones técnicas.

d) Entrenamiento y personal de reemplazo

- Entrenar a todo el personal de la OTI 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.

- Elaborar un programa de vacaciones que garantice la presencia permanente del personal crítico de OTI, tales como soporte técnico, redes y comunicaciones, sistemas de información y bases de datos, así como del administrador de la infraestructura TI.
- Elaborar una base de datos de conocimiento de TI, en caso el personal encargado de ciertos procedimientos, tanto principal, como de reemplazo se encuentren indispuestos.

e) Renovación tecnológica

- Programar dos revisiones anuales de obsolescencia tecnológica de las partes internas de los servidores informáticos, para realizar la renovación de estas, 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

- Verificar y validar de acceso seguro, en remoto, a los sistemas y servicios TI.
- Activar las 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 SUNASS, para entregársela en su domicilio a fin de que cuente con las herramientas necesarias, siguiendo los protocolos dados por la OTI.
- Verificar los accesos seguros de los proveedores a cualquier elemento de la plataforma e infraestructura de servicios TI, a cargo de la OTI en el Centro de Datos.

2.6.2. 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 de la SUNASS 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 ocurrida la contingencia:

a) Acciones durante la contingencia

- Estudiar y evaluar el alcance del desastre en cada área u oficina.
- Notificar y reunir a los demás integrantes del equipo de Emergencia y Restauración de TIC.
- Informar a la Alta Dirección sobre la situación presentada, para decidir la realización de la Declaración de Contingencia.
- 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, así como, 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.

b) Acciones para ejecutar luego de la contingencia

- Evaluar el trabajo de los equipos durante el proceso de recuperación.
- Evaluar la efectividad del Plan de Contingencia.

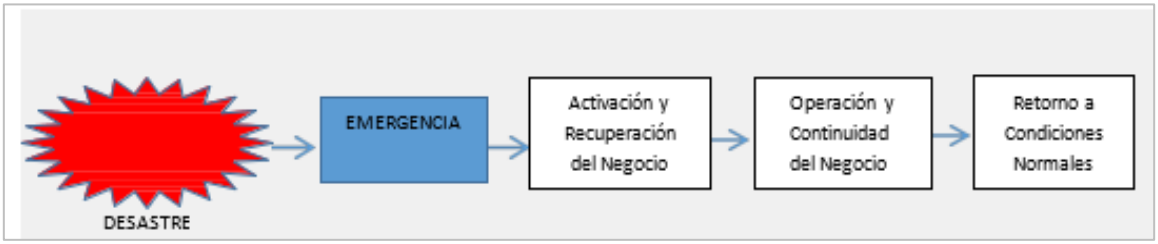
2.6.3. Estrategia para la restauración de tecnologías de la información

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 de la SUNASS para estabilizar la infraestructura tecnológica luego del evento suscitado.

Para ello, se definen las pautas que permitan al personal de la OTI garantizar la continuidad de las operaciones en la entidad.

El ciclo considerado para la estrategia de recuperación de las TI es el siguiente:

Figura N° 1 – Ciclo de la estrategia de recuperación de TI



La priorización para la restauración de los servicios de las TI de la SUNASS se ejecutará de acuerdo con lo indicado en la siguiente tabla:

Tabla N° 5 – Prioridad de atención durante la restauración de las TIC

Prioridad de Atención	Descripción
1	**Atención prioritaria:** Servicio de Internet, servicio de telefonía, correo electrónico, 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 Integrado de Gestión Administrativa (SIGA), Portal Web institucional, servidores de bases de datos, Sistema DialApplet, Sistema ContacTEK, 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: Melissa, etc.

En el Anexo 02 y Anexo 03 se detallan los sistemas de información y equipos informáticos, con la respectiva prioridad de atención, en caso de activarse la contingencia.

2.7. PLANES DE RECUPERACION PARA SISTEMAS DE INFORMACIÓN Y ACTIVOS CRÍTICOS

Una vez identificados los eventos de mayor impacto y los escenarios de mitigación de riesgos, se desarrolla el Plan de Contingencia atendiendo las categorías indicadas previamente.

El PCSI de la SUNASS comprende los eventos de mayor impacto, identificados en la Criticidad estimada en la tabla 3, los cuales serán abordados en formatos independientes, tal como se indica en la siguiente tabla:

Tabla N° 6 – Eventos de mayor impacto para el PCSI de la SUNASS

N°	Evento	Exposición al Riesgo	Formato Plan de Contingencia
1	Sismo	Moderado	Formato FPC 01 (ver anexo N° 5)
2	Delito informático (ataque)	Moderado	Formato FPC 02 (ver anexo N° 5)
3	Falla de hardware y software	Moderado	Formato FPC 03 (ver anexo N° 5)
4	Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación.	Moderado	Formato FPC 04 (ver anexo N° 5)

En el Anexo 05 se presenta el desarrollo de cada formato.

2.8. CÁLCULO DEL RTO

El RTO expresa el tiempo en el cual la SUNASS puede tolerar la falta de funcionamiento de sus aplicaciones y la caída del nivel de servicio asociada sin afectar la continuidad del negocio. Este tiempo se calcula en la siguiente tabla:

Tabla N° 7 – Calculo del RTO

		Impacto Operacional en el Tiempo				
Proceso Critico	**Componentes**	**0-3 hora**	**3 - 6 horas**	**6 -12 horas**	**12- 24 horas**	**24 - a más horas**
Gestión de redes e infraestructura de TI	Equipo de Grupo Electrógeno	Muy Bajo	Bajo	Medio	Alto	Alto
	Gabinete Autocontenido del Centro de Datos	Muy Bajo	Bajo	Medio	Alto	Alto
	Equipos de comunicaciones (Switch core, Switch de brode, AccessPoint)	Muy Bajo	Muy Bajo	Bajo	Medio	Alto
	Enlaces de fibra óptica para Internet	Muy Bajo	Bajo	Medio	Alto	Alto
	Equipo de seguridad perimetral (Firewall)	Bajo	Medio	Medio	Alto	Alto
	Cableado de red de datos	Muy Bajo	Muy Bajo	Bajo	Medio	Medio
	Sistema de almacenamiento (storage)	Muy Bajo	Bajo	Medio	Alto	Alto
	Equipo de librería robótica (Drive de cinta)	Muy Bajo	Muy Bajo	Bajo	Medio	Alto
	Equipo de backup a disco Acserve	Muy Bajo	Bajo	Medio	Alto	Alto
	Equipo servidor Blade	Muy Bajo	Bajo	Medio	Alto	Alto
	Servidores virtuales	Muy Bajo	Bajo	Medio	Alto	Alto
	Central Telefónica	Muy Bajo	Bajo	Medio	Alto	Alto
	Servidores físicos	Muy Bajo	Bajo	Medio	Alto	Alto
Gestión de sistemas de información y bases de datos	Sistemas de información y portales core	Muy Bajo	Bajo	Medio	Alto	Alto
	Correo electrónico y aplicativos colaborativos	Muy Bajo	Bajo	Medio	Alto	Alto
	Sistemas de información administrativos	Muy Bajo	Bajo	Medio	Alto	Alto
	Base de datos y repositorios utilizados por los sistemas y aplicativos.	Muy Bajo	Bajo	Medio	Alto	Alto
Soporte Técnico	Estaciones de trabajo del personal crítico (computadoras de escritorio y portátiles)	Muy Bajo	Bajo	Bajo	Medio	Alto
Operación y mantenimiento de TIC	Personal crítico responsable de los procesos de TIC.	Muy Bajo	Bajo	Bajo	Medio	Medio
Nota: Cómo impacta en las operaciones no tener disponible el componente en el tiempo						
El RTO se establece considerando el tiempo en que un impacto comienza a ser Alto.						

3. ROLES Y RESPONSABILIDADES:

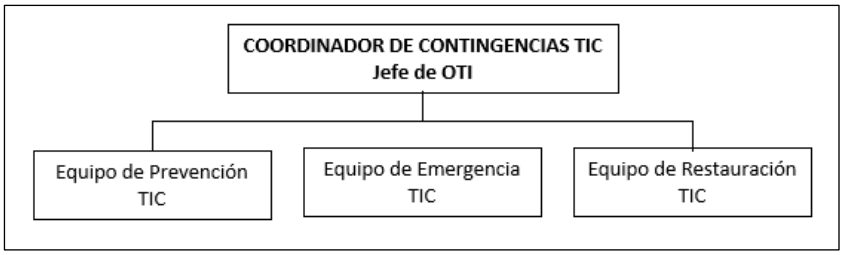
La OTI tiene dentro de sus funciones desarrollar e implementar la políticas de seguridad promoviendo la privacidad y control de datos en el acceso de la base de datos institucional, así como, establecer mecanismos de registro histórico de modificaciones, autenticación de los usuarios, auditoría y control 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 de la SUNASS, así como, asegurar la disponibilidad y brindar soporte a los mismos.

Para el funcionamiento del PSCI, se ha establecido la siguiente organización operativa estructurada por roles, los cuales son asumidos exclusivamente por personal de la OTI.

3.1. ESTRUCTURA DE GOBERNANZA Y RESPONSABILIDADES EN LA GESTIÓN DE CONTINGENCIAS

El/La jefe/a de la OTI debe nombrar un miembro titular y un alterno para cada uno de los tres (3) equipos conformados: Equipo de prevención, Equipo de Emergencia y Equipo de restauración (Detallado en la figura N° 2). Para tal efecto, se debe contar con la relación del personal de la OTI que conforma cada equipo, quienes serán requeridos en el momento de la contingencia.

Figura N° 2 . Organización Operativa del PSCI



Los responsables de cada equipo deben tener operativo el dispositivo móvil, para las comunicaciones pertinentes, de igual manera, los correos electrónicos registrados deben estar alojados en plataforma nube, que garantice la disponibilidad de este servicio.
La relación del personal de la OTI que asume cada rol dentro del PCSI debe ser actualizada de manera permanente y socializada a todo el personal de la SUNASS.

Las actividades planificadas como parte del presente plan podrán ejecutarse en forma presencial, semipresencial o en forma remota, conforme a los escenarios de prueba que pudieran desprenderse ante los diversos eventos de mayor impacto considerados para el presente PSCI; así como, conforme a las disposiciones vigentes.
Los roles, responsabilidades y funciones que deben desarrollar los equipos del PCSI son:

a. Coordinador de Continuidad de TIC

Este rol es asumido por el/la jefe/a de la OTI y tiene las siguientes responsabilidades:

- Coordinar, dirigir y decidir respecto a acciones o estrategias a seguir en un escenario de contingencia dado.
- Tomar la decisión de activar el PSCI.
- 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 la Alta Dirección 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 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 PCSI, cuando las operaciones del Centro de Datos hayan sido restablecidas.

b. Equipo de Prevención de TIC

Es el encargado de ejecutar acciones preventivas, antes que ocurra un incidente. La finalidad de estas actividades del equipo es evitar la materialización y proveer todos los medios requeridos para, en caso ocurriese, realizar la recuperación de los servicios de tecnologías de la información y comunicación, en el menor tiempo posible.

El liderazgo del equipo de Prevención de TIC será asumido por el personal de redes y comunicaciones. Las responsabilidades de cada rol dentro del equipo de prevención son:

- **Infraestructura Tecnológica**
  - 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.
  - 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 estos.
  - Llevar un control detallado del mantenimiento realizado a cada equipo y componentes del Centro de Datos
  - Verificar que se encuentren actualizados los diagramas de servidores.
  - Mantener actualizado el inventario hardware y software utilizado en el Centro de Datos de la SUNASS.
  - Ejecutar y verificar las tareas de copias de respaldo (backup).
  - Elaborar informes técnicos de conformidad, luego de cada mantenimiento efectuado, así como elaborar informes periódicos (semestrales) del funcionamiento del Centro de Datos.
  - Realizar las pruebas previas de recuperación.
  - Realizar copias de respaldo de las bases de datos de los aplicativos y sistemas de la entidad.

- **Redes y Comunicaciones**
  - Verificar que se encuentren actualizados los diagramas de red, la documentación de las configuraciones de equipos de comunicaciones y el inventario de equipos.
  - Monitorear el funcionamiento de la Central Telefónica.
  - Verificar que la central telefónica cuente con las garantías requeridas.
  - Actualizar el software que utiliza la central telefónica.

- **Desarrollo de sistemas**
  - Coordinar acciones de mantenimiento de sistemas de información existentes asegurando el cumplimiento del ciclo de vida de software.
  - Llevar un control de versiones de los códigos fuente de los sistemas de información y portales de la entidad.
  - Coordinar y verificar que se realicen las copias de respaldo de los códigos fuente de los aplicativos informáticos existentes en un ambiente adecuado.
  - Soporte y mantenimiento de los sistemas y aplicativos instalados en la entidad.
  - Documentación, consolidación y validación de los manuales de los sistemas en producción.
  - Participar periódicamente de las pruebas de restauración de los códigos fuente de los sistemas de información en producción de la entidad.

- Participar las pruebas de restauración de bases de datos en coordinación con el Especialista en Administración de Infraestructura de Tecnologías de la Información y Comunicación.

- **Soporte Técnico**
  - Mantener actualizado el inventario hardware y software utilizado en las unidades orgánicas.
  - Ejecutar y verificar las tareas del antivirus en los equipos de cómputo de los usuarios.
  - Elaborar informes técnicos de conformidad, luego de cada mantenimiento efectuado, a los equipos de cómputo (ver cronograma en Anexo 07).
  - Monitorear las actualizaciones de los equipos de cómputo de las áreas y oficinas.
  - Mantener actualizada la lista de anexos y teléfonos.

c. Equipo de Emergencia de TIC

Es el encargado de ejecutar las acciones requeridas durante la materialización de un incidente. La finalidad de las acciones realizadas por este equipo es mitigar el impacto que puedan tener sobre los equipos tecnológicos y la información de la SUNASS, procurando salvaguardar su pérdida o deterioro.

El liderazgo del equipo será asumido por el especialista de infraestructura tecnológica. Las responsabilidades de cada rol dentro del equipo durante la contingencia son:

- **Infraestructura Tecnológica**
  - 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 SUNASS.
  - Realizar la evaluación de condiciones de los equipos de comunicaciones y los componentes del Centro de Datos de la SUNASS, durante la emergencia.
  - Comunicar al Coordinador de Continuidad de TIC las acciones de emergencia ejecutadas.
  - Apoyar en las labores de verificación y validación de operación de los servicios de TIC.
  - Soporte y administración de infraestructura

- **Redes y Comunicaciones**
  - Realizar la evaluación de condiciones de los equipos de telecomunicaciones, post emergencia.
  - Soporte y administración de redes.

- **Desarrollo de sistemas**
  - Coordinar acciones para la verificación de estado de los sistemas de información alojados en los servidores de aplicaciones.
  - Coordinar acciones para verificar el estado de las bases de datos de los sistemas de información.
  - Realizar la evaluación de las condiciones de los aplicativos informáticos y sistemas de información durante la emergencia.
  - Solicitar los logs para revisión y verificación de los Sistemas informáticos afectados durante la emergencia.
  - Realizar la evaluación de las condiciones de los datos y la información almacenada en las diferentes bases de datos, durante la emergencia.

- **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 SUNASS.

d. Equipo de Restauración de TIC

Este equipo es el encargado de ejecutar las acciones necesarias luego de que el incidente 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 de la SUNASS.

El liderazgo del equipo será asumido por el coordinador de desarrollo de sistemas. Las responsabilidades de cada rol dentro del equipo son:

- **Infraestructura Tecnológica**
  - Debe iniciar el proceso de recuperación de los servicios de tecnología de la información, realizando las pruebas de funcionamiento en los equipos afectados de la infraestructura informática y los equipos componentes del Centro de Datos de la SUNASS.
  - Restaurar la información de los equipos afectados de la infraestructura informática que afecten los servicios de TI y los equipos componentes del Centro de Datos de la SUNASS.
  - Notificar al Coordinador de Continuidad de TIC, las acciones de recuperación ejecutadas.
  - Elaborar un informe técnico, que incluya las acciones de recuperación de los equipos de comunicaciones y los equipos componentes del Centro de Datos.
  - Supervisar la restauración de los servicios de TI.
  - Validar la información documentada de los procedimientos de restauración utilizados.

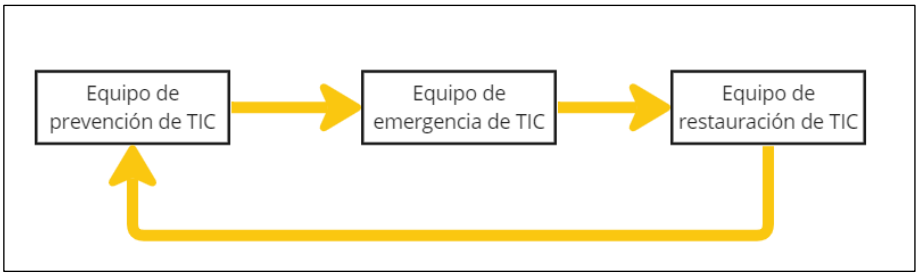
- **Redes y Comunicaciones**
  - Iniciar el proceso de recuperación de los servicios relacionados a la central telefónica instalada en el Centro de Datos de la SUNASS, así como a los equipos móviles, equipos de comunicación.
  - Realizar la evaluación de condiciones de los equipos de telecomunicaciones, durante la emergencia.
  - Elaborar un informe técnico, que incluya las acciones de recuperación de la central telefónica, servidores y equipos de comunicación, ubicada del Centro de Datos.

- **Desarrollo de sistemas**
  - 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.
  - Verificar el estado de las aplicaciones alojados en los servidores de aplicaciones de la SUNASS.
  - En caso se quiera desplegar y/o reinstalar los aplicativos informáticos y sistemas de información se deberá contar con manuales.
  - Elaborar un informe técnico que incluya la evaluación de condiciones de los aplicativos informáticos y sistemas de información de la SUNASS.
  - Verificar el funcionamiento de las bases de datos institucionales.
  - Realizar la creación de bases de datos en servidores alternos, en caso sea requerido.
  - Verificar las copias de respaldo correspondientes respetando la prioridad establecida para cada escenario.

- **Soporte Técnico**
  - Verificar el correcto funcionamiento de los equipos personales de la SUNASS, distribuyendo el trabajo entre el personal 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 de la SUNASS, luego de efectuado el proceso de recuperación.

Cabe precisar que los equipos podrían ejecutar sus responsabilidades de forma paralela, de acuerdo con el siguiente orden de operación:

Figura N° 3. Flujo del orden de operación de los equipos de TI



3.2. COMUNICACIÓN DE ROLES Y RESPONSABILIDADES A LOS/AS SERVIDORES/AS

El/La jefe/a de la OTI, mediante memorándum circular, designa a los miembros titulares y suplentes que conformarán el equipo de gestión operativa del PCSI. Posteriormente, hace extensiva dicha designación mediante comunicación a todas las unidades de organización de la SUNASS.

3.3. COORDINACIÓN CON EL GRUPO DE COMANDO DEL PLAN DE CONTINUIDAD OPERATIVA

El/La jefe/a de la OTI comunica de manera oportuna al Grupo de Comando de Continuidad Operativa la activación del PCSI, así como el nivel de impacto en los servicios y activos de información, a fin de evaluar las acciones a realizar de manera conjunta siguiendo los lineamientos del Plan de Continuidad Operativa.

4. COMUNICACIÓN Y COORDINACIÓN

4.1. PROCEDIMIENTOS DE COMUNICACIÓN INTERNA Y EXTERNA DURANTE UNA CONTINGENCIA

Frente a cualquier incidente el procedimiento de comunicaciones se debe realizar r según el siguiente cuadro:

Tabla N° 9 – Procedimiento de comunicaciones

N°	Incidente	Descripción de medios de comunicación
1	Sismo	La comunicación para las áreas internas será a través de teléfonos celulares de los/as servidores/as: mensajes de texto, llamadas telefónicas, correo electrónico. La comunicación al público será realizada por la OCII a través de los medios digitales
2	Delito informático (ataque)	La comunicación para las áreas internas será a través de teléfonos celulares de los/as servidores/as: mensajes de texto, llamadas telefónicas, correo electrónico.

N°	Incidente	Descripción de medios de comunicación
3	Falla de hardware y software	La comunicación para las áreas internas será a través de teléfonos celulares de los/as servidores/as: mensajes de texto, llamadas telefónicas, correo electrónico.
4	Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación.	La comunicación para las áreas internas será a través de teléfonos celulares de los/as servidores/as: mensajes de texto, llamadas telefónicas, correo electrónico.

4.2. MECANISMOS DE COORDINACIÓN CON TERCEROS

Los mecanismos de coordinación con terceros como proveedores, clientes, autoridades, entre otros, se encuentran determinadas en el siguiente listado:

Tabla N° 10 – Listado de Proveedores

Equipo	Nivel de atención	Empresa	Teléfono	Contacto	Correo	Dirección
Firewall Switches Servidores Blade	1	PMS	01 640-8098	Soporte PMS	soporte@pms.com.pe	Calle Ricardo Angulo Nº 726 - Oficina 201 - Edificio Corpac 2 - San Isidro, Lima – Perú
	2		913359484	Angel Mittani	angel.mittani@pms.com.pe	
	3		988188624	Jorge Zapata	jorge.zapata@pms.com.pe	
	4		996911576	Fernando Espinoza	ventas@pms.com.pe	
UPS Grupo electrógeno AIRE Acondicionado Data center	1	Elise	997 588 845	Carlos Castro	ccastro@elise.com.pe	Calle Camino Real 1801, Interior B-15 Santiago de Surco 15063
	2		997 588 767	Jose Pérez	jlperez@elise.com.pe	
	3		997 588 968	Daniella Diaz	planner.cre@elise.com.pe	
	4		997 582 889	Carlos Carrera	ccarrera@elise.com.pe	
VMware	1	Open Nova It Consulting S.A.C.	950 464 907	Andy Reyes	andy.reyes@opennova.pe	Av. General Garzón Nº 1413 Dpto. L- Lima-Jesus Maria
Internet	1	Optical Technologies S.A.C	01 500-7575	Operadores TAC	operadores@optical.pe	Av. Jose Gálvez Barrenechea Nro 545- Urb.Corpac-San Borja
	2		970 357 963 936 959 744 955 479 866 947 292 291	Cesar Chuqui Frank Sojo Alejandro Gonzalez Luis Bacilio	cchuqui@optical.pe fsojo@optical.pe agonzalez@optical.pe lbacilio@optical.pe	
	3		981 116 382	Susana Quiroz	squiroz@optical.pe	
	4		950 959 295	Giuliana Garayar	ggarayar@optical.pe	
telefonía Fija	1	Claro	01 610-2273	Operador de Soporte	atencioncorporativa@claro.com.pe	Torre Corporativa Av. Nicolás Arriola 480
	2		992 092 649	Karla Rojas	karla.rojas@claro.com.pe	

5. CAPACITACIONES Y CONCIENCIACIÓN EN SEGURIDAD DE LA INFORMACIÓN

El propósito que se cumple en este punto es brindar un conjunto de actividades que le permitan a la SUNASS realizar la capacitación y entrenamiento de su personal frente a diversos eventos que afecten la continuidad de los procesos y servicios de las TI.

Para la efectividad del entrenamiento y capacitación del personal se definen los siguientes roles:

a) Responsable de capacitación:

El/la jefe/a de la OTI en coordinación con la URH es el encargado de gestionar las actividades a realizar para la capacitación. Entre ellas están:

- Establecer un programa de capacitación
- Definir los tipos de público a los que ira dirigida
- Elegir el instructor que brindara la capacitación

Al final de la capacitación se debe contar con evaluaciones, test o encuestas para medir su efectividad.

b) Instructor de capacitación:

Es la persona encargada de llevar a cabo las capacitaciones. Sus principales actividades son:

- Contar con material para su exposición
- Brindar capacitación al personal

Las competencias del instructor deberán estar relacionadas al conocimiento del caso y su desenvolvimiento, entre las principales están:

- Capacidad de hablar y transmitir las ideas frente al público
- Tener dominio y conocimiento del tema a capacitar
- Experiencia como instructor, creatividad e innovación

c) Personal por instruir:

Se considera a todo el personal de la SUNASS, sin embargo, el tipo de capacitación variará dependiendo de los grupos o unidades de organización a capacitar.

6. PLAN DE PRUEBAS

Para el desarrollo de las pruebas se utilizará el tipo de prueba de escritorio, el cual consiste en la simulación en un ambiente amigable libre de estrés, a fin de que los equipos conformados en dicho plan de contingencia obtengan los primeros contactos de este.

6.1. CRONOGRAMA DE PRUEBAS

6.1.1. Horarios

Todas las pruebas se realizarán en un horario establecido días previos de la fecha de la prueba. Para establecer este horario se consideran los siguientes criterios:

- **Horario no laboral**: Se ha determinado que es preferible realizar las pruebas fuera de las horas de trabajo normales para minimizar el impacto en las operaciones diarias del negocio y reducir la interrupción para los empleados. Por lo tanto, se programarán las pruebas durante los fines de semana, feriados o períodos de menor actividad, siempre que sea factible.

- **Horario de menor impacto**: En caso de que no sea posible llevar a cabo las pruebas fuera del horario laboral, se tomará **en** consideración el momento del día en el que haya menos actividad o menor impacto en las operaciones críticas. Se evitarán las horas pico de trabajo y se buscarán momentos en los que los sistemas o servicios sean menos utilizados.

- **Requisitos del sistema**: Se consultará con los equipos de TI para conocer las ventanas de mantenimiento o actualización programadas de los sistemas. Se evitará programar las pruebas durante estas ventanas y se coordinará con los equipos de TI para evitar conflictos con otras actividades planificadas.

- **Participación del personal clave**: Se identificará y coordinará la participación del personal clave que debe estar presente durante las pruebas. Se tendrán en cuenta sus horarios y disponibilidad al planificar las pruebas, asegurándose de que estén disponibles durante los horarios seleccionados.

6.1.2. Cronograma de pruebas

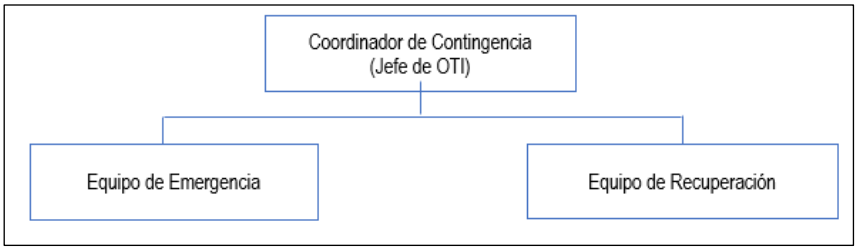
Se ha considerado realizar una prueba de cada escenario en el transcurso de un año. Según los señalado el siguiente cuadro:

Evento	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic
Sismo			M				F					
Delito informático				M			F					
Falla de hardware y/o software					M		F					
Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación			M			F						

M: Ejercicio de Mesa
F: Ejercicio funcional

6.2. ESTRUCTURA ORGANIZACIONAL Y FUNCIONAL

La estructura de los equipos de recuperación, los suplentes, las funciones y responsabilidades que darán soporte a las pruebas ante un evento se organizan de la siguiente forma:



6.2.1. Coordinador de Contingencia de TIC

La OTI funge como órgano técnico, responsable de orientar, promover, generar la transferencia y adaptación de las TIC de la SUNASS.

El rol del/de la jefe/a de la OTI, ante una situación de crisis de los servicios de TI de la SUNASS es dar la autorización para la declaratoria de continuidad del servicio.

Nombre	Acciones a realizar	UO	Teléfono	Correo electrónico	Suplente	Teléfono y correo del suplente
Zico Alexis Yacila Espinoza	Autorizar el inicio a la ejecución del plan de la continuidad y la Declaratoria de continuidad del servicio de TI Comunicar a autoridades superiores de la decisión técnica de activación de la continuidad de los servicios de TI (declaración de situación en crisis) y a las dependencias afectadas Dar la orden de inicio a la ejecución del plan de la continuidad	OTI	961580775	zyacila@sunass.gob.pe	Ronald Francisco Quispe Moran	99192867 rquispe@sunass.gob.pe

UO: Unidad de Organización

6.2.2. Equipo de emergencia - continuidad de pruebas

Cumple las siguientes responsabilidades para administrar el PCSI:

- Participar activamente en todo el proceso de prueba del PCSI
- Apoyar para que los recursos técnicos, materiales y otros, estén disponibles en todo el proceso de continuidad de la SUNASS.
- Facilitar plantillas para documentar y recopilar las actividades de la gestión de la continuidad de TI.
- Coordinar con las jefaturas de las unidades de la SUNASS para que cuenten con la documentación de las pruebas de continuidad.
- Capacitar al recurso humano sobre la gestión de continuidad de los servicios.
- Resguardar la documentación de los planes de mejoras de los procesos críticos y dar seguimiento.
- Coordinar la evaluación del proceso de pruebas de continuidad del servicio una vez finalizado y registro de las propuestas de mejoras del plan.

Nombre	Acciones a realizar	UO	Teléfono	Correo electrónico	Suplente	Teléfono y correo del suplente
Joh Albert Olivárez Olano	Coordinar la ejecución de las pruebas. Coordinar que se elabore la documentación de las pruebas.	OTI	961580775	jolivarezo@sunass.gob.pe	Ricardo Javier Vásquez Rodríguez	Cel:99167941 rvasquez@sunass.gob.pe

UO: Unidad de Organización

6.2.3. Equipo de recuperación – continuidad de pruebas

Este equipo está conformado por los funcionarios que representan a la(s) unidades de organización de la SUNASS que utilizan los servicios críticos de TIC y que son los encargados de realizar las pruebas a partir de una declaratoria de continuidad de los servicios de TI. Entre las responsabilidades que deben realizar, tenemos:

- Participar activamente y documentar las pruebas del PCSI.
- Evaluar el resultado del proceso de pruebas de continuidad del servicio una vez finalizado y apoyar con propuestas para mejora el plan.
- Desarrollar y actualizar los procedimientos de recuperación de los sistemas de información y activos críticos a partir de los resultados de las pruebas de contingencia.
- Evaluar el proceso de pruebas y proponer mejoras al PCSI

UO	Nombre del equipo	Servicios	Rol/ Puesto	Nombre del Miembro	Líder	Acciones a realizar	Tel.	Correo electrónico	Participa en la Prueba
OTI	Equipo de Soporte	Instalación y configuración de sistemas informáticos en arrendamiento (HW, SW) Servicio de instalación de firma digital Servicio de instalación de correo electrónico. Instalación de servicio de impresión	Soporte Técnico	John Albert Olivarez Olano	Zico Alexis Yacila Espinoza	- 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 los usuarios de la Sunass - Continuidad de operaciones y/o la pérdida de información de los usuarios de la Sunass.	994753005	jolivarezo@sunass.gob.pe	Sí

UO: Unidad de Organización

UO	Nombre del equipo	Servicios	Rol/ Puesto	Nombre del Miembro	Líder	Acciones a realizar	Tel.	Correo electrónico	Participa en la Prueba
OTI	Equipo de Infraestructura	Infraestructura servicio (IaaS) Directorio Activo, correo institucional. MEP compartido Infraestructura Servicio Internet	Especia-lista de Infraes-tructura	Edgar Rodriguez	Zico Alexis Yacila Espinoza	- 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 Sunass. - Realizar la evaluación de condiciones de los equipos de comunicaciones y los componentes del Centro de Datos de la Sunass, durante la emergencia. - Comunicar al Coordinador de Continuidad de TIC las acciones de emergencia ejecutadas. - Apoyar en las labores de verificación y validación de operación de los servicios de TIC. - Soporte y administración de infraestructura	961580775	zyacila@sunass.gob.pe	Sí

UO: Unidad de Organización

6.3. ESCENARIOS CONSIDERADOS

Para el presente plan se ha considerado los siguientes escenarios:

No	Escenario	participantes
1	Sismo	- Servicios generales - OTI - Oficial de Seguridad y Confianza Digital
2	Delito Informático	- OTI - Oficial de Seguridad y Confianza Digital
3	Falla de hardware y Software	- OTI - Oficial de Seguridad y Confianza Digital
4	Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación	- Servicios generales - OTI - Oficial de Seguridad y Confianza Digital

6.4. EJERCICIOS DE MESA

Los ejercicios de mesa son simulaciones diseñadas para probar y evaluar la efectividad del PCSI en un entorno controlado y sin riesgos reales. Estos ejercicios permiten a los equipos de respuesta a emergencias practicar y mejorar sus habilidades de gestión de crisis:

6.4.1. Ejercicios de crisis.

a) **Sismo:** Este ejercicio involucra la simulación de terremoto. El equipo de respuesta a emergencias practica la implementación del plan de contingencia, incluyendo la evaluación de daños, el establecimiento de comunicaciones alternativas, la coordinación con las autoridades locales y la gestión de la recuperación

b) **Delito informático (ataque):** En este ejercicio, se simula un ciberataque que afecta a la organización. El equipo de respuesta a emergencias se reúne y debe seguir el plan de contingencia para identificar la causa del ataque, contener el incidente, mitigar los efectos y restaurar los sistemas afectados

c) **Falla de hardware y software:** En este ejercicio se simula una falla física o lógica en alguno de los equipos de institución. El equipo de respuesta a emergencia debe seguir el plan de contingencia para garantizar la continuidad de las operaciones afectadas por esta incidencia.

d) **Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación:** En este ejercicio, se simula una interrupción prolongada del suministro eléctrico en las instalaciones de la organización. El equipo de respuesta a emergencias debe seguir el plan de contingencia para garantizar la continuidad de las operaciones críticas mediante el uso de generadores de respaldo, sistemas de alimentación ininterrumpida (SAI) y la implementación de medidas de ahorro energético

6.4.2. Etapas del ejercicio de mesa

Las etapas del ejercicio de mesa son las siguientes:

a) **Activación del plan de contingencia:** Se notifica al equipo de respuesta a emergencias sobre la falla en el Centro de Datos y se activa el PCSI. Los miembros del equipo se reúnen para coordinar las acciones.

b) **Evaluación de la situación:** El equipo evalúa la magnitud de la falla, identifica los sistemas y servicios afectados, y determina el impacto en las operaciones de la SUNASS. Se establece una línea de comunicación con el personal de TI y se recopila información adicional sobre la causa de la falla.

c) **Restauración de servicios:** El equipo de respuesta a emergencias trabaja en estrecha colaboración con el personal de TI para restaurar los sistemas y servicios afectados. Se siguen los procedimientos establecidos en el PCSI.

d) **Comunicación interna y externa:** Se establece un proceso de comunicación para mantener informado al personal de la SUNASS sobre la situación y las acciones en curso. Además, se notifica a las partes interesadas relevantes sobre la interrupción de los servicios y las medidas tomadas para resolver el problema.

e) **Evaluación y lecciones aprendidas:** Una vez que se restablecen los sistemas y servicios, el equipo de respuesta a emergencias realiza una evaluación posterior al ejercicio. Se identifican las fortalezas y debilidades del PCSI, se documentan las lecciones aprendidas y se proponen mejoras para futuras situaciones de fallas de hardware y software.

f) **Informes y documentación.** Se establece un informe del planteamiento de pruebas realizadas, así como el registro de las actividades realizadas adjuntando resultados, observaciones y recomendaciones.

6.5. EJERCICIOS FUNCIONALES.

Los ejercicios funcionales son simulaciones prácticas diseñadas para evaluar y mejorar la capacidad de respuesta del equipo, organización o sistema ante situaciones de crisis. A través de la simulación de eventos reales o escenarios adversos, los ejercicios funcionales permiten poner a prueba la coordinación, comunicación, toma de decisiones y habilidades técnicas de los participantes. El objetivo es identificar fortalezas, debilidades y áreas de mejora en la preparación, respuesta y recuperación frente a situaciones críticas.

6.5.1. Objetivos de las pruebas funcionales

Para el presente plan de pruebas funcionales se han establecido objetivos alineados a los objetivos institucionales como son:

- Evaluar la capacidad de recuperación de los sistemas críticos y la infraestructura tecnológica después de una interrupción, a fin de garantizar una restauración rápida y eficiente.
- Verificar la efectividad de los procedimientos de activación del plan de continuidad y la comunicación interna durante una situación de crisis, asegurando una respuesta coordinada y oportuna
- Evaluar la eficacia de los mecanismos de respaldo y recuperación de datos, verificando la integridad y disponibilidad de la información crítica de la institución
- Evaluar la capacidad de los equipos de gestión de incidentes para identificar, analizar y mitigar los riesgos durante una interrupción, minimizando el impacto en las operaciones comerciales.

6.5.2. Procedimientos de pruebas

Para el procedimiento de pruebas se sigue paso a paso lo establecido en el anexo 5 del PCSI a fin de poder evaluar su eficacia y proponer mejoras a sus diferentes componentes.

6.5.3. Informes y documentaciones

Al terminar la prueba programada se debe informar los diferentes sucesos, observaciones y recomendaciones a el/la jefe/a de la OTI y a cada una de las unidades de organización participantes.

6.5.4. Evaluación y seguimiento

Una vez terminado las pruebas se debe realizar una evaluación de los resultados de las pruebas como es tiempo de respuesta y afectación, afectación del incidente en la operatividad de la SUNASS entre otros.

7. MONITOREO Y MEJORA CONTINUA

Es probable que, durante la evaluación y el control del PCSI, se detecte la necesidad de realizar ajustes para adecuar las medidas planificadas a la realidad de la contingencia actual.

Realizando pruebas se descubrirán elementos operacionales que requieren ajustes para asegurar el éxito en la ejecución del plan, de tal forma que dichos ajustes perfeccionen los planes preestablecidos, esto se aprecia en el anexo 4.

8. ANEXOS

- Anexo N° 01 - Metodología aplicada a la gestión de riesgos del PCSI.
- Anexo N° 02 - Aplicaciones y sistemas de información clasificados por prioridad de atención para la recuperación de TIC.
- Anexo N° 03 - Equipos del Centro de Datos y gabinetes de comunicación clasificados por prioridad de atención para la recuperación de TIC.
- Anexo N° 04 - Formatos del PCSI desarrollado por escenario.
- Anexo N° 05 – Reporte de control y certificación de la prueba.

ANEXO N° 1 - METODOLOGÍA APLICADA A LA GESTIÓN DE RIESGOS DEL PCSI

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 SUNASS directamente, según se muestra en la siguiente tabla:

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

Por otro lado, la "percepción" está basada netamente en la sensación de los expertos, de que la amenaza en cuestión podría ocurrir, según se muestra en la siguiente tabla:

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

2. **Identificación de las amenazas que se tomarán en cuenta para la evaluación**.

De la combinación de las variables descritas se obtiene el nivel de criticidad cualitativo, que sirve como valor discriminatorio para seleccionar que amenazas se deberían evaluar para el alcance del presente plan.

Aquellas amenazas que resultan en un nivel de criticidad cualitativo estimado "insignificante" o "menor", según la tabla siguiente, no son tomados en cuenta:

Nivel de Criticidad Cualitativa	Nivel de Criticidad	Interpretación
Extrema	**>=20**	Probabilidad de ocurrencia alta (Evaluación de prioridad alta)
Moderado	**>=15**	Probabilidad de ocurrencia intermedia (Evaluación de prioridad baja)
Menor	**>=10**	Probabilidad de ocurrencia muy baja (Evaluación sin prioridad)
Insignificante	**>=1**	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:

Probabilidad	Valor	Descripción
Improbable	1	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.
Baja	2	Se cuenta con controles razonablemente suficientes que responden a un programa de mantenimiento y responden a los ejercicios y pruebas realizadas.
Moderada	3	Se cuenta con controles que responden a un programa de mantenimiento y responden a los ejercicios y pruebas realizadas, pero no son suficientes.
Alta	4	Algunos controles se prueban esporádicamente, debido a que no cuentan con un programa definido o de existir no se cumple con el mismo.
Muy Alta	5	Bajo nivel de controles o los controles existentes no son efectivos o eficientes.

4. Cálculo del Impacto del Recurso.

Se utiliza la siguiente tabla de valores para el cálculo:

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

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)	Moderado	Alto	Extremo	Extremo	Extremo
Alta	(4)	Moderado	Alto	Alto	Extremo	Extremo
Moderada	(3)	**Bajo**	Moderado	Alto	Alto	Extremo
Baja	(2)	**Bajo**	Moderado	Moderado	Alto	Alto
Improbable	(1)	**Bajo**	**Bajo**	**Bajo**	Moderado	Moderado

La interpretación de cada cuadrante de calor o Nivel de Riesgo de la amenaza en evaluación se muestra en la tabla siguiente:

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

ANEXO N° 2 - APLICACIONES Y SISTEMAS DE INFORMACIÓN CLASIFICADOS POR NIVEL RIESGO DE ATENCIÓN PARA LA RECUPERACIÓN DE TIC

N°	Sistema/Aplicación	Descripción	Probabilidad de afectacion	Impacto	Nivel de Riesgo
1	Registro de diagnóstico de plantas de tratamiento de agua potable – registro	Formulario web de registro para el diagnóstico de plantas de tratamiento de agua potable llenado por las EPS.	3	3	Alto
2	Mesa de ayuda	Sistema que permite el seguimiento a los incidentes y problemas reportados por los usuarios de la SUNASS, su atención y estadísticas de los mismos.	3	3	Alto
3	Sistema de monitoreo rural	sistema web que permite la programación, ejecución, seguimiento y generación de indicadores de la información recogida en el monitoreo rural (monitoreo rural y visita atm) que realizan las ODS.	3	2	Moderado
4	Sistema de notificaciones electrónicas (casilla)	Sistema web para la notificación digital de resoluciones emitidas por la Sunass a las EPS (SEDAPAR) a través de bandejas, así como también la generación de un formato en pdf para la notificación en físico a los accionantes realizada por notificadores de trámite documentario.	3	3	Alto
5	Sistema de registro de información de área técnica municipal	Sistema web que permite el registro, consulta y la generación de indicadores de la información ingresada por los responsables de las áreas técnicas municipales a nivel nacional.	3	2	Moderado
6	Sistema de consulta de los reportes IPM	Sistema de carga y consulta de los reportes IPM (índice de precios al por mayor) para los especialistas de fiscalización (sede central y ODS)	3	2	Moderado
7	Servicio de aporte por regulación v 2.0 (Sar) – web	Sistema en que se registran la información de todos los aportes regulatorios de las EPS que realizan a la SUNASS.	3	3	Alto
8	Sistema de captura de información de las EPS (sicap)	Sistema instalado localmente para el registro periódico (mensual, trimestral, semestral, anual, a solicitud) de las variables de gestión y la generación de un .dat para que el prestador lo remita por ftp a la SUNASS.	3	3	Alto
9	Sistema de información de las EPS (SIEPS)	Sistema que procesa la información generada por la EPS en el SICAP (.dat) y remitida por ftp que sirve de insumo para la generación de indicadores de gestión (equipo de benchmarking) y para la consulta de los especialistas de supervisión. Actualmente se accede a la consulta desde acceso remoto ya que no es compatible con el Windows 10.	3	3	Alto

N°	Sistema/Aplicación	Descripción	Probabilidad de afectacion	Impacto	Nivel de Riesgo
10	Sistema integrado de gestión administrativa (SIGA)	Herramienta informática que simplifica y automatiza los procesos administrativos y que sigue las normas establecidas por los órganos rectores de los sistemas administrativos del estado.	3	4	Alto
11	Sistema de admisión del curso de extensión universitaria (CEU)	Formulario de inscripción y módulo de administración de la información personal de los postulantes al CEU.	3	1	Bajo
12	Sistema de gestión documental del consejo directivo	Sistema de gestión de documentos del consejo directivo.	3	3	Alto
13	Sistema de registro de interrupciones del servicio de agua y alcantarillado	Sistema web para el reporte de las EPS sobre las interrupciones programadas e imprevistas del servicio de agua.	3	3	Alto
14	Sistema de publicación de convocatorias de personal	Sistema que publica las convocatorias de personal (CAP, CAS, prácticas) de la SUNASS.	3	2	Moderado
15	Sistema de registro y seguimiento de sanciones	Sistema web de la dirección de sanciones para el registro, consulta y seguimiento de las sanciones a las EPS. la DF cuenta con accesos de consulta.	3	2	Moderado
16	Sistema del programa educativo	Sistema web para el registro de II.EE en el programa educativo y en el concurso del programa educativo (inscripción y registro de proyecto).	3	1	Bajo
17	Sistema de trámite institucional (SISTRAM)	Sistema de trámite documentario institucional	3	3	Alto
18	Módulo de la mesa de partes virtual	Sistema de trámite documentario institucional	3	3	Alto
19	SISTRAM - módulo de control de registros de DAP	Es un módulo del sistema de tramite documentario de la SUNASS.	3	3	Alto
20	SISTRAM - módulo de control de registros de DF	Módulo del SISTRAM para el control de registros de expedientes y documentos para la supervisión de las EPS por parte de la DF.	3	3	Alto
21	SISTRAM - módulo de atención de reclamos y apelaciones	Módulo del SISTRAM para el control de registros de las apelaciones, quejas, impugnaciones y escritos que maneja el TRASS.	3	3	Alto
22	Contactek (crm)	CRM de la institución donde se almacenan todas las atenciones a los usuarios, tipo de atención, necesidad y otros servicios a fin de mejorar la atención con el ciudadano	3	3	Alto

N°	Sistema/Aplicación	Descripción	Probabilidad de afectacion	Impacto	Nivel de Riesgo
23	Nube SUNASS pública - plataforma	Software libre - owncloud 8.1 - repositorio web público para cargar, compartir y consultar documentación entre las unidades organizacionales de la SUNASS, las ODS y externos. complementa el file server y el SISTRAM.	3	2	Moderado
24	Nube SUNASS Interna	Software libre - owncloud 10.2.1 - repositorio web interno (red SUNASSS) vinculado al ad para cargar, compartir y consultar documentación entre las unidades organizacionales de la SUNASS y las ODS. complementa el file server y el SISTRAM.	3	3	Alto
25	DIALAPPLET.	Sistema de atención al ciudadano, permitiendo la multicanalidad de la atención mediante llamadas telefónicas y Wassap.	3	3	Alto
26	Aplicativo informático de gobierno corporativo de las EPM - v2	Sistema web de registro de las EPM sobre los órganos de gobierno, el cumplimiento del código de buen gobierno corporativo (cbgc), y registro del monitoreo por parte de los especialistas de la DF-piloto.	3	2	Moderado
27	Simulador web de facturación para el ciudadano (Yacumetro)	Es una aplicación web que permite al ciudadano simular el monto de facturación de los servicios de agua y alcantarillado, a partir de un volumen de consumo mensual y otros parámetros (EP, lugar de residencia, categoría y modalidad de facturación).	3	1	Bajo
28	Sistema GRD	El sistema de gestión de riesgos y desastres permite gestionar los incidentes o emergencias que se presentan a nivel nacional. estas emergencias pueden ser registradas en el sistema GRD, el cual utiliza un navegador web para ser accedido	3	3	Alto

ANEXO N° 3 - EQUIPOS DEL CENTRO DE DATOS Y GABINETES DE COMUNICACIÓN CLASIFICADOS POR NIVEL DE RIESGOPARA LA RECUPERACIÓN DE TIC

N°	Tipo de Equipo	Rol	Descripción	Probabilidad	Impacto	Nivel de Riesgo
1	Equipo de Almacenamiento	Almacenamiento	Equipo de almacenamiento de información, donde se configuran las máquinas virtuales.	3	3	Alto
2	Servidor Blade	Virtualización	Servidor que se brinda recursos de procesador y memoria para las máquinas virtuales.	3	3	Alto
3	Servidor	Backup	Servidor donde se encuentra instalado el software de respaldo, para respaldo y restauración de información.	3	3	Alto
4	Librería de Backup	Backup	Equipo donde se realizan las copias de respaldo en medios magnéticos, y es utilizado para la restauración de información.	3	2	Moderado
5	Servidor	Base de Datos	Base de Datos Oracle.	3	3	Alto
6	Servidor	Servidor de replicación	Servidor que replica máquinas virtuales críticas.	3	1	Bajo
7	Servidor	Servidor Dataloger	Servidor que almacena información de los equipos Dataloger	3	3	Alto
8	Switch	Comunicaciones	Switches Core, swicthes de acceso	3	3	Alto
9	UPS	Energía	Equipo de suministro eléctrico para servidores y equipos de comunicaciones	3	2	Moderado
10	Transformador	Energía	Equipo de suministro eléctrico para servidores y equipos de comunicaciones	3	2	Moderado
11	Aire acondicionado	Acondicionamiento	Aire acondicionado de precisión para el Centro de datos	3	3	Alto

N°	Tipo de Equipo	Rol	Descripción	Probabilidad	Impacto	Nivel de Riesgo
12	Central Telefónica	Comunicaciones	Central telefónica institucional, para la recepción de llamadas y derivaciones tanto internas como externas.	3	2	Moderado
13	UTM Firewall	Seguridad	Brindar seguridad perimetral de la red interna y externa de SUNASS	3	3	Alto
14	Servidor	Comunicaciones	Servidor dialapplet, el cual permite la atención y orientación del ciudadano	3	3	Alto

ANEXO N° 4 - FORMATOS DEL PCSI DESARROLLADOS POR ESCENARIO

SUNASS	Evento: Sismo	FPC – 01

1. PLAN DE PREVENCIÓN

a) Descripción del evento

Un sismo es un movimiento brusco y violento de la Tierra causado por la liberación de energía acumulada en las placas tectónicas. En el marco del PCSI, la SUNASS, ha identificado los siguientes elementos mínimos para la recuperación de los servicios afectados:

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 SUNASS, 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 en el mismo distrito.

d) Personal Encargado

El Grupo de Comando para la Continuidad Operativa de la SUNASS, 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 literal f) señalado en este formato.

e) Condiciones de Prevención de Riesgo

Las siguientes acciones estarán a cargo del área de servicios generales:
- Realizar inspecciones de seguridad realizadas periódicamente.
- Contar con un plan de evacuación de las instalaciones de la SUNASS, el mismo que debe ser de conocimiento de todo el personal que labora en la sede central.
- Realizar simulacros de evacuación con la participación de todo el personal.
- Conformar las brigadas de emergencia, y capacitarlas semestralmente.
- Realizar mantenimiento de las salidas libres de obstáculos.
- Contar con señalización de las zonas seguras y las salidas de emergencia.
- Verificar el funcionamiento de las luces de emergencia.
- Definir los puntos de reunión en caso de evacuación.

f) Acciones del Equipo de Prevención de TIC
- 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 al ocurrir el evento.

b) Personal que autoriza la activación del plan de contingencia El/La Coordinador/a de Continuidad de TIC.

c) Personal Encargado
Equipo de Emergencia de TIC.

d) Descripción de las actividades después de activar la contingencia
- Desconectar el fluido eléctrico del Centro de Datos.
- Revisar la afectación en los equipos y servicios
- Comunicar con las áreas afectas que se ha iniciado el plan de recuperación.

3. PLAN DE RECUPERACIÓN

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 SUNASS.

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.
- 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.
- El Equipo de restauración de TIC repondrán 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.
    - 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.
- Registrar todos los gastos operacionales relacionados con la continuidad del negocio.

c) Mecanismos de Comprobación
Se deberá coordinar con el área usuaria para que valide el restablecimiento del servicio tras lo cual 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 PCSI 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.

SUNASS	Evento: Delito informático	FPC – 02

1. PLAN DE PREVENCIÓN

a) Descripción del evento

Un delito informático se refiere a actividades ilegales que se realizan utilizando tecnología informática o redes digitales, como la violación de páginas web y sistemas de información. En el caso de la SUNASS, este tipo de evento puede afectar elementos clave de su infraestructura tecnológica. Algunos de los componentes identificados como parte afectada o como causa de la contingencia son:

Hardware

- Servidores: Los servidores de la SUNASS son fundamentales para el funcionamiento de los sistemas y el almacenamiento de datos críticos.
- Estaciones de Trabajo: Las estaciones de trabajo utilizadas por el personal de la SUNASS también pueden verse afectadas por delitos informáticos, comprometiendo la seguridad y la integridad de la información.

Software

- Servidores: Los servidores de la SUNASS son fundamentales para el funcionamiento de los sistemas y el almacenamiento de datos críticos.
- Estaciones de Trabajo: Las estaciones de trabajo utilizadas por el personal de la SUNASS también pueden verse afectadas por delitos informáticos, comprometiendo la seguridad y la integridad de la información.

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/o estaciones ubicadas en el Centro de Datos y en la sede central de la SUNASS.

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

- Instalar parches de seguridad en los equipos.
- Establecer políticas de seguridad para prevenir el uso de aplicaciones no autorizadas en las estaciones de trabajo.
- Aplicar 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.
- Capacitar al personal de la OTI, sobre Ethical Hacking a las Bases de Datos, Sistemas Operativos, Servidores y Sistemas Informáticos.
- Ejecutar ataques de Ethical Hacking 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.
- Información de un repositorio cifrada
- 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 activación del plan de contingencia
El/La Coordinador/a de Continuidad de TIC y/o el/la Oficial de Seguridad y Confianza Digital.

d) 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 SUNASS, 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 cuatro (4) horas en caso se confirme la presencia de un virus en estaciones de trabajo y de ocho (8) horas en servidores de red. Esperar la indicación del personal de soporte técnico para reanudar el trabajo.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado
El equipo de restauración de TIC, luego de restituir 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 jefe/a inmediato del área para reanudar las labores de trabajo con el equipo o sistema que fue afectado.

b) Descripción de actividades
Se informará a el/la jefe/a de OTI de la SUNASS el tipo de malware/virus, o tipo de ataque encontrado y el procedimiento usado para removerlo.

Estas actividades deben contemplar como mínimo:
- Instalar y poner a punto de un equipo de cómputo compatible y hardware necesarios para la instalación del sistema de información con las características mínimas exigidas.
- Instalar y configurar el sistema operativo, drivers y servicios necesarios para el funcionamiento del sistema de información a recuperar.
- Instalar y configurar el sistema de información y el motor de la base de datos, con sus respectivas librerías y niveles de seguridad.
- Instalar aplicaciones adicionales necesarias para el funcionamiento del sistema de información.
- Realizar la restauración de la base de datos con la última copia de seguridad disponible (Restore).
- Reiniciar el servicio, prueba y afinamiento del sistema de información.
- Conectar el servidor o la estación a la red de la SUNASS.
- 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 y Confianza Digital, tomará las medidas preventivas del caso enviando un comunicado cada vez que suceda este tipo de evento vía correo electrónico al personal de la SUNASS.

El evento será evaluado y registrado en la Bitácora de Gestión de Eventos y Debilidades de Seguridad de la Información.

c) Mecanismos de Comprobación
Se deberá coordinar con el área usuaria para que valide el restablecimiento del servicio tras lo cual el personal Técnico de Soporte y/o Especialista en infraestructura, según sea el caso, presentará un informe a el/la jefe/a de OTI con copia al OSCD, 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 de la Sunass, 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.

SUNASS	Evento: Falla de hardware y software	FPC - 03

1. PLAN DE PREVENCIÓN

a) Descripción del evento

En un plan de continuidad de TI, se identifica un evento relacionado con el hardware de servidores y el software utilizado por la entidad. Estos elementos desempeñan un papel crucial en el almacenamiento, procesamiento y protección de datos, así como en el cumplimiento de los requisitos de las aplicaciones de la entidad. A continuación, se detallan los componentes específicos que son considerados como parte afectada o causa de la contingencia:

Hardware

- Servidores de Base de Datos, Aplicaciones, Archivos: Estos servidores son esenciales para alojar y gestionar los datos críticos y las aplicaciones empresariales de la entidad.
- Storage: El almacenamiento de datos, como sistemas de almacenamiento en disco, almacenamiento en red (NAS) o almacenamiento en cinta, juega un papel fundamental en la retención y recuperación de información.

Software

- Aplicativos usados por la SUNASS y de servicio al ciudadano: El software utilizado por la entidad, incluyendo aplicaciones internas y sistemas de servicio al ciudadano, se ve directamente afectado en caso de una contingencia. Su funcionamiento adecuado es esencial para mantener las operaciones comerciales y la atención a los usuarios.

Información

- Información contenida en base de datos: Los datos almacenados en las bases de datos de la entidad, que pueden incluir información crítica sobre clientes, transacciones y registros, son parte integral de la operación y deben protegerse adecuadamente.
- Información contenida en repositorios de información: Los repositorios de información, como sistemas de gestión documental o repositorios de archivos, pueden contener documentos importantes y sensibles que son vitales para el funcionamiento continuo de la entidad.

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 SUNASS.

d) Personal 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 estos.
- 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 EJECUCIÓN

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

b) Personal que autoriza la activación del plan de contingencia
El/La Coordinador/a de Continuidad de TIC.

c) 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.
- Avisar sobre el corte de servicio a los usuarios afectados

d) Duración
El tiempo máximo de la contingencia no debe sobrepasar las seis (6) 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 jefes de las unidades de organización 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 restituir 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:
- Instalar y poner a punto un equipo de cómputo compatible necesarios para la instalación del sistema de información con las características mínimas exigidas.
- Instalar y configurar el 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 de la SUNASS informando la reanudación de los servicios.

En función a esto, se tomarán las medidas preventivas del caso y se revisará el PCSI 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 OTI, precisando las acciones realizadas y solicitando la validación del restablecimiento del servicio al área usuaria afectada.

El/La Especialista en infraestructura, presentará un informe a el/la jefe/a de la OTI con copia al Oficial de Seguridad y Confianza Digital, 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

En base al informe presentado por el/la Especialista en Infraestructura, 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.

SUNASS	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 central de la entidad.
Este evento incluye los siguientes elementos mínimos identificados por la SUNASS, 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 las instalaciones de la SUNASS, considerando la Sede Central, por tener un gabinete de comunicación y equipos que brinda servicios informáticos a los usuarios a nivel interno y externo.

d) Personal Encargado

El/La jefe/a de la UA 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) del presente formato.

e) Condiciones de Prevención de Riesgo
- Contar con un contacto del proveedor de energía.
- Contar con un grupo electrógeno con sistemas de transferencia automático para el Datacenter y/o para el Edificio
- Contar con un sistema óptimo de UPS en el edificio y/o Datacenter
- Contar con mantenimiento preventivo anual de grupos electrógenos
- Contar con mantenimiento preventivo anual de UPS's
- Realizar la inspección anual de los tableros eléctricos
- Realizar la inspección anual de cableado eléctrico
- Mantenimiento anual de pozo de tierra
- Contar con contrato de soporte de UPS
- Contar con contrato de soporte de Grupo Electrógeno
- Inspección que los equipos de los colaboradores estén conectados a la red estabilizada
- Inspeccionar semestralmente la climatización del Datacenter
- Garantizar que los equipos de comunicación estén conectados al UPSdel Datacenter
- Verificación del cableado eléctrico de toda la sede de la SUNASS 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 central de la entidad.
- Coordinar y supervisar el mantenimiento preventivo de pozos a tierra, aire acondicionado de precisión del Centro de Datos, UPS, grupo electrógeno, 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 central sea estabilizada.
- Revisar la presencia de exceso de humedad en la sala de energía del Centro de Datos de la SUNASS.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la contingencia
Corte de suministro de energía eléctrica en los ambientes de la SUNASS.

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

c) Personal que autoriza la activación del plan de contingencia
El/La jefe/a de OAF y/o Coordinador de Continuidad de TIC.

d) Descripción de las actividades después de activar la contingencia
- Informar a el/la jefe/a de la UA 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 de la SUNASS y coordinar las acciones necesarias.
- En el caso de los equipos que entren en funcionamiento automático con UPS´s, y grupo electrógeno se deberá monitorear el tiempo de autonomía del equipo.
- En caso la interrupción de energía en el Centro de Datos sea mayor a cuatro (04) horas, se deberá realizar las gestiones necesarias para suministrar combustible al grupo electrógeno 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 RECUPERACIÓN

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.
- La contingencia finaliza cuando retorna la energía eléctrica y todos los equipos se encuentran operativos brindando servicio.

c) Mecanismos de Comprobación
Se deberá coordinar con el área usuaria para que valide el restablecimiento del servicio tras lo cual el/La Especialista en infraestructura presentará un informe a el/la jefe/a de la OTI con copia al OSCD, 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 de la SUNASS.

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

ANEXO N° 5 – REPORTE DE CONTROL Y CERTIFICACIÓN DE LA PRUEBA

PRUEBA N°	
Fecha de la Prueba	
Escenario de Prueba:	
Área Responsable:	

INFORMACIÓN DEL PROCESO

Metodología:	
Alcance:	

Condiciones de Ejecución

Equipo		Aplicación/Sistema	
Ubicación		Fecha de Backup	

RESULTADO DE LA PRUEBA

Satisfactorio	☐
Satisfactorio con observaciones	☐
Deficiente	☐

Observaciones	
Cambios o Actualizaciones	

Participante	Cargo	Firma