PLAN DE CONTINGENCIA INFORMÁTICO Y RECUPERACIÓN DE SERVICIOS DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES DEL SEGURO INTEGRAL DE SALUD v.01

OFICINA GENERAL DE TECNOLOGÍA DE LA INFORMACIÓN

Firmado digitalmente por ORTEGA ROJAS Juan Fredy FAU 20505208626 hard
Motivo: Doy V° B°
Fecha: 06.10.2023 15:32:34 -05:00

OCTUBRE, 2023

Firmado digitalmente por AMBROCIO DOROTEO Teofilo FAU 20505208626 hard
Motivo: Doy V° B°
Fecha: 06.10.2023 15:11:03 -05:00

Firmado digitalmente por REINOSO ZEGARRA Jose Hugo Martin FAU 20505208626 hard
Motivo: Doy V° B°
Fecha: 06.10.2023 15:02:25 -05:00

INDICE

INTRODUCCIÓN

El Plan de Contingencia Informático y Recuperación de Servicios de Tecnología de la Información y Comunicaciones, en adelante el Plan; es un instrumento de gestión para el buen gobierno de las tecnologías de la información y las comunicaciones, que tiene como finalidad garantizar la continuidad operativa de los servicios de tecnología de la información y comunicaciones (TIC).

Este instrumento de gestión se construye a partir de un proceso continuo de planeación, desarrollo, prueba e implantación de procesos y procedimientos de recuperación de información, en caso de que una posible contingencia pueda presentarse en el Seguro Integral de Salud (SIS). Estas acciones buscan asegurar la reanudación eficiente y efectiva de los servicios y operaciones de tecnologías de la información y comunicaciones en el menor tiempo y generando el menor impacto posible.

Asimismo, a través del presente Plan se busca definir y/o establecer lo siguiente:

- Las situaciones y escenarios que pudieran preverse con la finalidad de permitir la operatividad de los sistemas de la entidad a través de las medidas de contingencia.
- La formación del equipo humano y sus roles en casos de contingencia y el procedimiento de activación del Plan de Contingencia.
- El procedimiento general necesario para la restauración y el normal funcionamiento de los sistemas y servicios de la entidad.

El presente Plan se constituye en un instrumento que da el marco de actuación para garantizar la continuidad de los servicios que brinda la entidad, por lo que deberá ser incluido como parte de la documentación para la continuidad operativa del SIS.

1. FINALIDAD

Garantizar la continuidad de los servicios de la tecnología de la información y comunicaciones del Seguro Integral de Salud (SIS), a fin de que se restablezcan en el menor tiempo posible, en caso de la ocurrencia de alguna eventualidad que interrumpa su funcionamiento.

2. OBJETIVOS

2.1 General

Definir el conjunto de actividades, roles y responsabilidades que permitan el restablecimiento de la operatividad de la plataforma tecnológica de la entidad, en caso de la ocurrencia de un evento o la materialización de un riesgo de TIC, que pueda alterar el normal funcionamiento de los sistemas de información críticos de la entidad.

2.2 Específicos

2.2.1 Restablecer con la mayor brevedad posible el funcionamiento de la infraestructura tecnológica por ocurrencia de un evento, en aras de minimizar el impacto y garantizar la correcta recuperación de los sistemas y procesos de la entidad que involucren la Infraestructura de TIC que se encuentren identificadas en el análisis de impacto del negocio.

2.2.2 Optimizar los esfuerzos y recursos necesarios para atender cualquier contingencia de TIC, de manera oportuna y eficiente, definiendo las personas responsables de las actividades a desarrollar antes, durante y después de la emergencia.

2.2.3 Definir actividades y procedimientos a ejecutar en caso de una interrupción de las operaciones de los sistemas y/o procesos que involucren la infraestructura de TIC del SIS, a fin de garantizar la continuidad en la ejecución de las funciones y objetivos estratégicos de la entidad en el menor tiempo posible.

3. ALCANCE

El Plan de Contingencia descrito en este documento busca definir los roles y responsabilidades del personal, así como las actividades para tomar el control frente a situaciones que puedan afectar la continuidad de las operaciones que involucren infraestructura tecnológica, identificadas en el análisis de impacto del negocio, delimitado en la protección y funcionalidad de los sistemas que soportan los procesos de la entidad.

4. BASE LEGAL

- Ley N°28551, Ley que establece la obligación de elaborar y presentar planes de contingencia.
- Ley N°28716, Ley de Control Interno de las Entidades del Estado.
- Ley Nº29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).

- Decreto Supremo Nº 011-2011-SA, Decreto Supremo que aprueba el Reglamento de Organización y Funciones (ROF) del Seguro Integral de Salud, modificado mediante Decreto Supremo N°002-2016-SA, Decreto Supremo que modifica el Reglamento de Organización y Funciones del Seguro Integral de Salud – SIS.
- Decreto Supremo Nº 048-2011-PCM, Decreto Supremo que aprueba el Reglamento de la Ley Nº 29664, que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
- Decreto Supremo N° 034-2014-PCM, Decreto Supremo que aprueba el Plan Nacional de Gestión del Riesgos de Desastres - PLANAGERD 2014-2021.
- Decreto Supremo N° 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.
- Resolución de Contraloría N°320-2006-CG, Resolución de Contraloría que aprueba las Normas de Control Interno.
- Resolución Ministerial N° 028-2015-PCM, Resolución Ministerial que aprueba Lineamientos para la gestión de la Continuidad Operativa de entidades públicas en los tres niveles de gobierno.
- Resolución Ministerial N° 004-2016-PCM, Resolución Ministerial que aprueba el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición”, en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD, Resolución de Secretaría de Gobierno y Transformación Digital que aprueba la Directiva N°001-2023-PCM/SGTD, Directiva que establece el Perfil y Responsabilidades del Oficial de Seguridad y Confianza Digital.
- Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, Resolución de Secretaría de Gobierno y Transformación Digital que establece la implementación y mantenimiento del Sistema de gestión de Seguridad de la Información en las Entidades Públicas.

5. COMUNICACIÓN Y DISTRIBUCIÓN

A continuación, se presentan algunas pautas para la comunicación y distribución del Plan y sus componentes.

5.1. Boletines internos de comunicación.

La publicidad mediante correo electrónico o mensajes al personal, los cuales debe mencionar aspectos relevantes del Plan de Contingencias de la entidad, para así crear consciencia sobre la importancia del tema.

5.2. Charlas y talleres.

Incluir el tema del manejo de contingencias de TIC dentro de la estrategia de sensibilización del Sistema de Gestión de Seguridad de la Información (SGSI), diseñando charlas y talleres que brinden información al respecto.

5.3. Comunicación de la Alta Dirección.

Como líderes de la entidad y del proceso de contingencia de TIC, la alta dirección debe, al menos una vez al año, comunicar a los funcionarios su compromiso de

salvaguardar la información y el plan de contingencia de la entidad, para lo cual utilizará cualquier medio de los mencionados anteriormente.

5.4. Publicación de información de manera continua y accesible.

La intranet del SIS deberá ser utilizada para difundir el Plan de Contingencia. Por otro lado, junto con el Sistema de Gestión de Seguridad de la Información, el Plan deberá de estar publicado de manera controlada.

5.5. Publicación General del Plan.

En la página Web de la entidad se publicará una versión general del documento, teniendo en cuenta que la información que contiene el documento es de índole confidencial, por lo tanto, es solo de uso del personal encargado y/o involucrado en los procesos de contingencia.

Es importante contar con el Plan de Contingencias y los procedimientos que hacen parte de este, debiendo tenerlos disponibles en un lugar seguro, fuera de las instalaciones de la sede principal, con el objeto de que en una interrupción total se pueda garantizar el acceso a estos documentos y su distribución efectiva a los diferentes equipos que participan en la recuperación de los servicios de TIC.

6. MARCO TEORICO

6.1. Plan de Contingencia Informático

El Plan de Contingencia Informático es una herramienta que mitiga el riesgo ante una situación en la que no se pueda continuar con las operaciones por períodos que se prolongan más allá de lo soportado por los procesos del negocio.

Este Plan permite minimizar las consecuencias, en caso de incidentes, con el fin de reanudar las operaciones en el menor tiempo posible, en forma eficiente y oportuna, mediante acciones en diferentes etapas, antes, durante y después del incidente:

- **Antes,** con planes de mantenimiento y ejercicios de simulación como medios de prevención para mitigar los incidentes.
- **Durante**, con la ejecución/activación de los procedimientos establecidos, en el momento de producirse un incidente.
- **Después**, como medio de recuperación de la información, una vez superado el incidente, se regresa al estado previo de la contingencia.

6.2. Definiciones:

a) **Activo de información:** Elemento que contiene o administra información, el cual la entidad debe valorar y proteger, ya que es de gran importancia para el logro de sus objetivos estratégicos.

b) **Amenaza:** Situación o causa potencial que desencadena un incidente que puede resultar en un daño al sistema o a la entidad.

c) **Análisis de riesgos:** Proceso que permite comprender la naturaleza del riesgo y determinar el nivel de riesgo.

d) **Base de datos:** Conjunto de datos organizados y correlacionados, almacenados en un sistema por quien lo utiliza.

e) **Clasificación de los activos de información:** Proceso que consiste en agrupar los activos de información, de acuerdo a atributos o propiedades comunes entre ellos, estableciendo su importancia.

f) **Control:** Medidas para asegurar el cumplimiento de normativas, directivas y estándares vigentes a fin de obtener los resultados esperados**.**

g) **Comité de Gobierno y Transformación Digital**. Es el grupo responsable de la dirección, mantenimiento y supervisión estratégica de los planes, resultados y recursos del SGSI.

h) **Confidencialidad:** Propiedad que garantiza que la información no esté disponible, ni sea divulgada a personas o procesos no autorizados.

i) **Contingencia:** Evento adverso que es posible que suceda en base a la información y modelos predictivos con los que se dispone.

j) **Criterio de aceptación del riesgo:** Condición, establecida formalmente, que ayuda a determinar el nivel de riesgos con los que puede convivir la entidad.

k) **Custodio del activo:** Persona encargada del resguardo de la información. La responsabilidad del custodio es aplicar las políticas, procedimientos y protocolos asociados al acceso a la información que se establezcan por parte de la entidad y del propietario de la información (propietario de los activos), así como los relacionados con su trámite y conservación.).

l) **Desastre:** Cualquier evento que cuando ocurre tiene la capacidad de interrumpir las operaciones de manera parcial o completa.

m) **Disponibilidad:** Propiedad que asegura que los usuarios autorizados tengan acceso a la información cuando la requieran**.**

n) **Equipo de Gestión y Respuesta de Riesgos:** Es el conjunto de especialistas en los activos de información del proceso.

o) **Equipo de Respuestas ante Incidentes de Seguridad Digital:** Conjunto de especialistas responsable de la gestión de incidentes de seguridad digital que afectan los activos de la entidad.

p) **Estimación del riesgo:** Es el proceso mediante el cual se establecen las consecuencias negativas potenciales de un desastre, en base a la identificación del peligro y al análisis de la vulnerabilidad. Asigna valores a la probabilidad y el impacto de un riesgo.

q) **Evaluación de riesgos:** Proceso en el cual una organización debe identificar los riesgos de seguridad en su información, y determinar la probabilidad de ocurrencia de una incidencia y su impacto, esto también determina si el riesgo y/o su magnitud son aceptables o tolerables, para así decidir si corresponde o no tratarlo.

r) **Gestión de riesgos:** Actividades coordinadas para dirigir y controlar el riesgo
en una entidad.

s) **Impacto:** Es el efecto producido en el estado de seguridad del activo.

t) **Incidente:** Acción propia de una amenaza voluntaria o involuntaria que implica la paralización parcial o completa de las actividades.

u) **Incidente de seguridad de la información:** Es cualquier interrupción en los servicios de TIC de una organización, que afecta cualquier aspecto, desde un solo usuario hasta toda la organización. En pocas palabras, un incidente es cualquier incidencia que interrumpe la continuidad del negocio.

v) **Información:** Datos que representan un activo para la entidad, pues posee valor para la misma, independientemente de la forma (impresa, oral, escrita, etc.) o de su origen.

w) **Integridad:** Propiedad de salvaguardar la exactitud y totalidad de los activos de información.

x) **Inventario de activos:** Elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de la entidad. En su sentido más amplio, éstos hacen referencia a la información que se recibe, transforma y produce en la entidad en el cumplimiento de sus funciones.

y) **Mesa de ayuda:** Servicio de atención y soporte que centraliza las solicitudes de los usuarios en una plataforma digital, a fin de resolver consultas técnicas, fallas y problemas, lo que puede conllevar a requerir del apoyo del equipo de soporte técnico.

z) **Nivel de exposición al riesgo:** Graduación de la posibilidad de que un riesgo se materialice y cause un impacto negativo en la entidad.

aa) **Oficial de Seguridad y Confianza Digital:** Es el rol responsable de coordinar la implementación, operación, mantenimiento y mejora continua del SGSI en la entidad pública.

bb) **Plan de Contingencia.** Es un documento que reúne un conjunto de procedimientos alternativos para viabilizar el normal funcionamiento de las tecnologías de la información y comunicaciones (TIC). Cuando alguno de sus servicios se ha afectado negativamente por causa de algún incidente interno o externo a la organización.

cc) **Probabilidad de ocurrencia del riesgo:** Probabilidad de que una amenaza explote una vulnerabilidad.

dd) **Propietario del activo:** Identifica a la persona o la entidad que gestiona el activo, gestiona la transferencia, almacenamiento o destrucción del activo.

ee) **Propietario del riesgo:** Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

ff) **Resiliencia.** La capacidad de un sistema para recuperarse de un fallo y conservar la confiabilidad del servicio cuando este las presenta. Su objetivo es asegurar que todas las operaciones estén protegidas, para que así una amenaza o incumplimiento no afecte todo el negocio.

gg) **Responsable de la unidad de organización de planeamiento y presupuesto:** Debe orientar al Oficial de Seguridad y Confianza Digital para asegurar una adecuada articulación con los instrumentos de gestión institucional, comprendidos en los sistemas administrativos de presupuesto público, planeamiento estratégico, programación multianual y gestión de inversiones.

hh) **Responsable de la unidad de organización de tecnologías de la información** Es responsable de informar al Oficial de Seguridad y Confianza Digital todo incidente de seguridad digital crítico que afecte los procesos misionales y servicios que brinda la entidad.

ii) **Respuesta al riesgo:** Decisión o estrategia para tratar el riesgo, pudiendo ser: aceptar, evitar, transferir o reducir el riesgo.

jj) **Riesgo en la seguridad de la información:** Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

kk) **Riesgo efectivo:** Riesgo que se posee actualmente.

ll) **Riesgo residual:** Riesgo remanente o minimizado después de ser tratado.

mm) **Tratamiento de riesgos:** Proceso de selección e implementación de controles para minimizar el riesgo.

nn) **Usuarios de los activos de información:** Personas que usan los activos de información de la entidad en sus actividades diarias.
oo) **Vulnerabilidad:** Debilidad o ausencia de control en un activo que puede ser explotado por una o más amenazas.

6.3. Abreviaciones:

a) **APP:** Aplicativo móvil
b) **ARFSIS**: Aplicativo de Registro de Formatos del SIS.
c) **AST:** Prueba de seguridad de aplicaciones
d) **ATS:** Sistema de Transferencia Automática
e) **BIA:** Análisis de Impacto al Negocio (Bussiness Impact Analysis).
f) **DAST:** Prueba de Seguridad de Aplicaciones Dinámicas.
g) **DIRESA:** Dirección Regional de Salud.
h) **EESS:** Establecimiento de Salud
i) **ESSALUD:** Seguro Social de Salud.
j) **FARMASIS:** Sistema de Gestión para Farmacias del SIS.
k) **FUA:** Formato Único de Atención
l) **GA:** Gestión del Asegurado
m) **GMR:** Gerencia Macro Regional.
n) **GNF:** Gerencia de Negocios y Financiamiento
o) **GREP:** Gerencia de Riesgos y Evaluaciones de las Prestaciones.
p) **IPRESS:** Instituciones Prestadores de Servicios de Salud
q) **MAC:** Mejor Atención al Ciudadano.
r) **MTD:** tiempo de inactividad máximo tolerable (Maximum Tolerable Downtime).
s) **NTP:** Norma Técnica Peruana.
t) **OGTI:** Oficina General de Tecnología de la Información.
u) **PCPP:** Proceso de Control Prestacional
v) **PEAS:** Plan Esencial de Aseguramiento en Salud
w) **PGH:** Padrón General de Hogares
x) **PLANAGERD:** Plan Nacional de Gestión del Riesgos de Desastres.
y) **RENIEC:** Registro Nacional de Identificación y Estado Civil.
z) **ROF:** Reglamento de Organización y Funciones.
aa) **RPO:** Objetivo de Punto de Recuperación.
bb) **RTO:** Tiempo de Recuperación Objetivo
cc) **SAST:** Prueba de Seguridad de Aplicaciones Estáticas.
dd) **SGD:** Sistema de Gestión Documental.
ee) **SGSI:** Sistema de Gestión de Seguridad de la Información.
ff) **SGTD:** Resolución de Secretaría de Gobierno y Transformación Digital.
gg) **SIAF:** Sistema Administrativo Financiero
hh) **SIASIS:** Sistema Integrado de Aseguramiento del SIS.
ii) **SIGA:** Sistema de Gestión Administrativa
jj) **SIGEPS:** Sistema de Información de Gestión de Prestaciones de Salud
kk) **SINAGERD:** Sistema Nacional de Gestión del Riesgo de Desastres.
ll) **SIS:** Seguro Integral de Salud.
mm) **SISFOH:** Sistema de Focalización de Hogares
nn) **SISPAD:** Sistema de Procedimiento Administrativo Disciplinario
oo) **SITEDS**: Sistema de Acreditación de Asegurados de SUSALUD.
pp) **SME:** Supervisión Médica Electrónica
qq) **SOASIS:**
rr) **SUSALUD:** Superintendencia Nacional de Salud.

ss) **TIC:** Tecnología de la Información y Comunicaciones.
tt) **UDR:** Unidades Desconcentradas Regionales.
uu) **UPS:** Fuente de Poder Ininterrumpible **(**Uninterruptible Power Supply)
vv) **VPN:** Red privada virtual
ww) **WRT:** Periodo Máximo Tiempo de Inactividad que puede tolerar la Entidad sin entrar en colapso

7. METODOLOGIA

El desarrollo del presente Plan se ha dado en base a una metodología de matriz de riesgos y la planificación estratégica, que se estructura en 7 fases, las cuales han sido adecuadas al presente plan de la siguiente manera:

Fase 1: Planificación
Fase 2: Determinación de vulnerabilidades y escenarios de contingencia
Fase 3: Determinación de las Estrategias
Fase 4: Elaboración del Plan de Contingencia Informático
Fase 5: Definición y Ejecución del Plan de Pruebas
Fase 6: Implementación del Plan de Contingencia
Fase 7: Monitoreo

7.1 Fase 1: Planificación

7.1.1 Organización

La Oficina General de Tecnología de la Información tiene dentro de sus funciones administrar la confidencialidad e integridad de los sistemas que están a su cargo, así como el establecimiento de mecanismos de registros históricos de modificaciones, autenticación de usuarios, auditoría y control de accesos; además de diseñar, mantener e implantar los sistemas informáticos y la infraestructura necesaria para el cumplimiento de sus funciones y los objetivos de la entidad.

7.1.2 Roles y Responsabilidades dentro del Plan de Contingencias

Para el manejo de la activación del Plan de Contingencia en alguno de sus escenarios, es importante destacar que la Oficina General de Administración de Recursos junto a la Oficina General de Tecnología de la Información (OGTI) son quienes deberán establecer los protocolos de comunicación primarios con la empresa de seguridad y vigilancia, con el fin de establecer los canales de comunicación al interior de la entidad, en caso de presentarse alguna contingencia, como la caída del fluido eléctrico, inundación, sismo, o en el evento de la programación o ejecución de actividades de mantenimiento que afecten el fluido eléctrico de la entidad, en días laborales y no laborales y/o cuando se encuentren o no servidores en las sedes de la entidad.

De igual manera, se deberá priorizar la comunicación con las demás oficinas administrativas de la entidad y la OGTI, para la coordinación logística del lugar y para que la OGTI proceda con el apagado seguro de los elementos del centro de datos. Se debe cumplir con el procedimiento de apagado y encendido del centro de datos, este procedimiento deberá estar desarrollado, administrado, medido y controlado por el responsable de la sala de servidores, y aprobado por la dirección de la OGTI.

El compromiso de los servidores públicos de la entidad, especialmente de la Alta Dirección y de la OGTI, es fundamental debido a que son ellos quienes tienen la responsabilidad de responder de forma adecuada ante un incidente tecnológico inesperado en la operación de la entidad y el desarrollo del trabajo, desde el momento que se declare la interrupción hasta la vuelta a la normalidad, (prevención, mitigación, preparación, alertas, respuestas, rehabilitación y reconstrucción) de forma que se reduzca al mínimo el impacto sobre la prestación del servicio.

A continuación, se definen tres niveles de gestión (estratégico, táctico y operativo) y sus responsabilidades durante una situación de contingencia de TIC, organización que permite segregar funciones y roles para que las tareas y áreas de responsabilidad no presenten conflicto alguno. En cada nivel se debe establecer un plan de sucesión para que en caso de no estar disponible el servidor público principal, su reemplazo pueda actuar con la misma autoridad y responsabilidad, de esta manera cada nivel cumple con una serie de tareas que se complementan para garantizar el logro de las metas establecidas:

A. Nivel Estratégico:

Este nivel corresponde básicamente a la planeación del logro de los objetivos del Plan, se basa en decidir y asignar las políticas, directrices y los recursos para lograr su efectividad en caso de presentarse una interrupción tecnológica no planeada en la entidad.

B. Nivel Táctico:

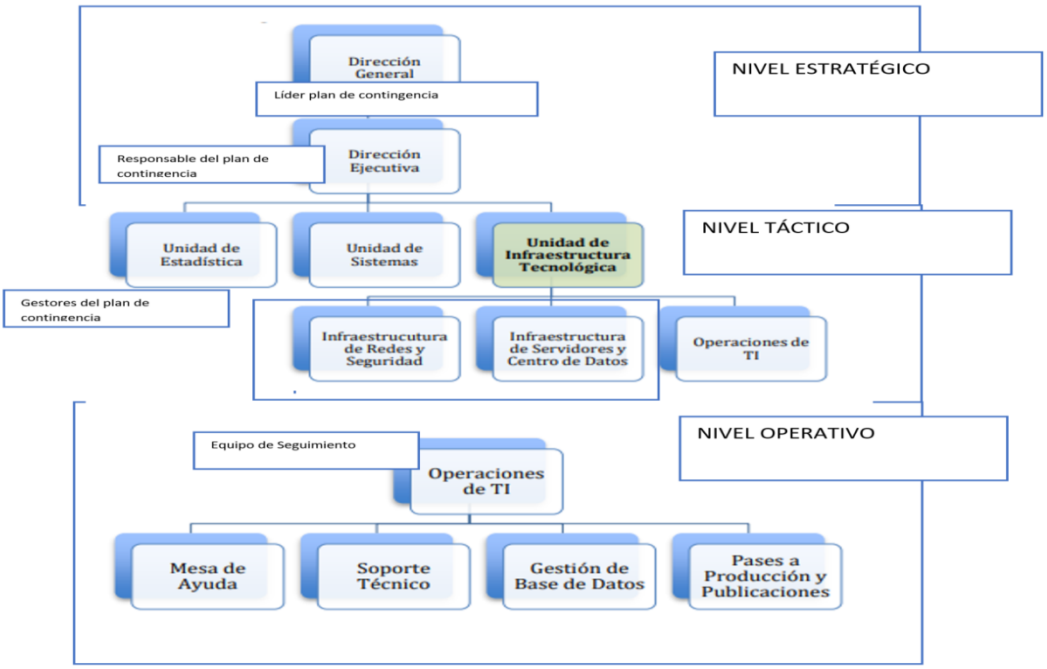
Llevará a cabo la coordinación de las actividades que se deriven del Plan, así como la evaluación de las situaciones de interrupción y dará lineamientos para la operación de mismos, a su vez es el encargado de escalar al nivel estratégico en un lenguaje claro las necesidades de la operación de TI y brindará los insumos para la evaluación.

C. Nivel Operativo:

Este nivel realiza las tareas puntuales en el momento de presentarse un incidente o evento inesperado que activa el Plan de Contingencias de la entidad. Se ejecuta a partir de los lineamientos proporcionados por los niveles estratégico y táctico.

(Ver gráfico en la siguiente página)

Gráfico 1: Organización y Jerarquía del Plan



Fuente: Elaboración propia OGTI

7.1.3 Descripción de roles y responsabilidades dentro del plan

Se describe los roles, responsabilidades y funciones que deben de desempeñar los distintos equipos de la OGTI, del Plan de Contingencia del SIS. En la descripción de sus funciones se establecer las responsabilidades, según el grado de actividad, como prevención (mantenimiento), emergencia (incidencia) y restauración (contingencia).

A. Nivel Estratégico:

Representado por el/la directora General y el Director Ejecutivo de la OGTI, quienes tienen las siguientes funciones:

i. Director General

- Aprueba el plan de Contingencia Informático.
- Guía y supervisa los equipos operativos de contingencia informática en el desarrollo de sus actividades.
- Notifica y mantiene informados a la alta dirección cuando se requiera según el nivel de criticidad.
- Declara el evento de termino de ejecución de operaciones del Plan de Contingencia informático, cuando las operaciones hayan sido restablecidas.

ii. Director Ejecutivo

- Tomar la decisión de activar el Plan de Contingencia Informático.

- Coordinar, dirigir y decidir respecto a acciones o estrategias a seguir en un escenario de contingencia dado.
- 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, al director general acerca del evento de desastre, el progreso de la recuperación y posibles problemas ocurridos durante la ejecución del plan.
- Monitorear, supervisar y vigilar la recuperación de infraestructura de Tecnologías de la Información en el Centro de Datos.
- Contactar a los proveedores para el reemplazo de hardware, software y/o activación de servicios para los sistemas afectados.
- Establecer y supervisar los procedimientos de seguridad de los servicios de TI.
- Coordinar la realización de las pruebas de restauración de hardware y software.
- Participar en las pruebas y simulacros de contingencia.
- Verificar la realización del mantenimiento preventivo a los equipos componentes del Centro de Dato y equipos de cómputo de los profesionales del área.
- Verificar las tareas de copias de respaldo (backup).

B. Nivel Táctico:

Es el equipo encargado de ejecutar las acciones preventivas, de mantenimiento y simulaciones, para prevenir un evento o un desastre. Su finalidad es evitar que se materialice el evento y en caso ocurra un incidente, tienen los medios requeridos y el ejercicio necesario para la contención del incidente, restauración o recuperación de los servicios tecnológicos en el menor tiempo posible.

Es representado por la Unidad de sistemas y la Unidad de Infraestructura tecnológica, infraestructura de redes y seguridad, infraestructura de servidores y centro de datos y Operaciones TI.
Los responsables del equipo de nivel táctico son los líderes de equipo de la **Unidad de Sistemas y Unidad de Infraestructura**.

Para una mejor identificación de las funciones en el nivel táctico, se han agrupado en unidades por especialidad:

i. Unidad 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 las fuentes de los sistemas de información y portales de la entidad.

- Coordinar y verificar que se realicen las copias de respaldo de las fuentes 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.
- Realizar periódicamente las pruebas de restauración de las fuentes de los sistemas de información en producción de la entidad.
- 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 incidencia.
- Solicitar los logs de los aplicativos informáticos afectados durante la incidencia.
- Verificar el estado de las aplicaciones alojados en los servidores de aplicaciones del SIS.
- En caso se quiera desplegar y/o reinstalar los aplicativos informáticos y sistemas de información, de lo contrario verificar que se encuentren funcionando correctamente.
- Elaborar un informe técnico que incluya la evaluación de condiciones de los aplicativos informáticos y sistemas de información del SIS.

ii. Unidad de Infraestructura

Infraestructura de Redes y Seguridad

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

- Realizar las pruebas previas de recuperación.
- Monitorear el funcionamiento de la Central Telefónica.
- Verificar que la central telefónica cuenta con las garantías requeridas.
- Mantener actualizada la lista de anexos y teléfonos.
- Actualizar el software que utiliza la central telefónica.
- Ejecutar las acciones de emergencia en la central telefónica instalada en el Centro de Datos.
- Realizar la evaluación de condiciones de los equipos de telecomunicaciones durante la incidencia.
- Comunicar al Coordinador de área o director las acciones de ejecutadas.
- Debe iniciar el proceso de recuperación de los servicios de comunicaciones, realizando las pruebas de funcionamiento en los equipos afectados de la infraestructura informática y los equipos componentes de comunicaciones del Centro de Datos.
- Restaurar la información de los equipos afectados de la infraestructura informática que afecten los servicios de TI los equipos componentes de comunicaciones del Centro de Datos.
- Notificar al Coordinador, las acciones de recuperación ejecutadas.
- Elaborar un informe técnico, que incluya las acciones de recuperación de los equipos de comunicaciones y los equipos componentes de comunicaciones del Centro de Datos.
- Iniciar el proceso de recuperación de los servicios relacionados a la central telefónica instalada en el Centro de Datos.
- Realizar la evaluación de condiciones de los equipos de telecomunicaciones, durante la incidencia.
- Elaborar un informe técnico, que incluya las acciones de recuperación de la central telefónica ubicada del Centro de Datos.

Infraestructura servidores y centro de datos

- Mantener actualizado el inventario hardware y software utilizado en el Centro de Datos.
- Programar y/o realizar el mantenimiento preventivo de los equipos del Centro de Datos, considerando el tiempo de vida útil y garantía de los mismos.
- Llevar un control detallado del mantenimiento realizado a cada equipo y componentes del Centro de Datos.
- Elaborar informes técnicos de conformidad, luego de cada mantenimiento efectuado, así como elaborar informes periódicos del funcionamiento de los equipos del Centro de Datos.
- Verificar que se mantiene actualizado los diagramas de servidores, la documentación de las configuraciones de

equipos físicos y virtuales, el inventario de software de gestión y otros.
- Realizar las pruebas previas de recuperación.
- Notificar el desastre o incidencia al Coordinador de equipo.
- Ejecutar las acciones de emergencia en los equipos informáticos y componentes instalados Centro de Datos.
- Realizar la evaluación de condiciones de los equipos componentes del Centro de Datos, durante la incidencia.
- Comunicar al Coordinador o director de área las acciones ejecutadas.

C. Nivel operativo:

En este equipo se encuentra el equipo de respuestas ante incidentes, son los que lideran las contingencias, ya que la responsabilidad de la continuidad está a cargo de los profesionales responsables.

7.1.4 Operaciones TI: Definiciones

A. Mesa de ayuda

Servicio de atención y soporte que centraliza las solicitudes de los usuarios en una plataforma digital, a fin de resolver consultas técnicas, fallas y problemas, lo que puede conllevar a requerir del apoyo del equipo de soporte técnico.
- Registrar todos los eventos y monitorear el cumplimiento según la clasificación de impacto que se le asigne.
- Realizar un informe con las evidencias de actividades realizadas según los tickets asignados.
- Publicar y/o comunicar a los usuarios el inicio y fin de la actividad de contingencia o incidentes.

B. Soporte técnico

Personal técnico dedicado a resolver las incidencias reportadas a la Mesa de Ayuda a fin de ser solucionadas.
- Realizar la evaluación de la afectación a los equipos informáticos y periféricos.
- 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.
- Verificar el funcionamiento de los equipos de cómputo de escritorio o portátiles en las sedes afectadas del SIS donde tengan alcance de soporte, deben de distribuir las actividades según una organización inmediata propuesta por el líder de equipo o el director de la OGTI y darles solución a los incidentes priorizando desde la jerarquía y luego por nivel de afectación o nivel de daño.
- Registrar el avance de las soluciones mediante los tickets de atención.
- Elaborar un informe técnico que incluya la evaluación de condiciones de los equipos de cómputo de escritorio y portátil del personal del SIS, luego de efectuado el proceso de recuperación.

C. Base de Datos

Conjunto de datos organizados y correlacionados, almacenados en un sistema quien lo utiliza.

- Realizar copias de respaldo de las bases de datos de los aplicativos y sistemas de la entidad.
- Acopiar las copias de respaldo y clasificarlas por tipo de motor de base de datos, aplicativos y sistemas.
- Realizar las pruebas de restauración de bases de datos en coordinación con el Oficial de Seguridad de la Información, director de OGTI y coordinador de área según calendario del plan de mantenimiento desarrollado.
- Realizar la evaluación de las condiciones de los datos y la información almacenada en las diferentes bases de datos, durante la incidencia.
- Verificar el funcionamiento de las bases de datos institucionales.
- Realizar la creación de bases de datos en servidores alternos, en caso sea requerido.
- Restaurar las copias de respaldo correspondientes respetando la prioridad establecida para cada escenario.
- Realizar las pruebas de funcionamiento.
- Elaborar un informe técnico que incluya la evaluación de condiciones de los datos e información del SIS luego de efectuado el proceso de recuperación.

D. Pases a producción y publicaciones.

Etapa de desarrollo de un software consistente en la publicación del mismo para su uso.

- Monitorear los restablecimientos de los sistemas afectados por los incidentes.
- Verificar la integridad de los datos de datos restaurados
- Servir de apoyo en las simulaciones de práctica y prueba de contingencia.
- Reportar cualquier evento que resulte en una posible amenaza o riesgo para los sistemas.

7.2 Fase 2: Determinación de vulnerabilidades y escenarios de contingencia

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

7.2.1 Inventario de Servicios e Infraestructura de TI

Conforme a lo descrito en el Plan de Gobierno Digital de la entidad, a continuación, se presenta la Infraestructura, los servicios de TI y Sistemas de Información que se tienen identificados en la Dirección General de Tecnología de la Información para su gestión y mantenimiento.

A. Sistemas de Información

Actualmente, los procesos se apoyan en sistemas de información diseñados a la medida, así como en sistemas de información cedidos por medio de convenios de transferencia tecnológica por otras entidades y a los cuales el SIS realiza las adecuaciones que considera para ajustarlo a su dinámica funcional.

Así mismo, la entidad cuenta con sistemas de información adquiridos a terceros y otros desarrollados internamente de acuerdo con las necesidades de las áreas usuarias. Se cuenta con contratos de soporte y mantenimiento especialmente para los sistemas misionales y para los demás sistemas de información el soporte es brindado directamente por los profesionales contratados de la OGTI.

A continuación, se presenta la descripción de cada uno de los sistemas de información con que cuenta la entidad:

Tabla 1: Inventario de sistemas

ID	SISTEMA	MODULOS	DESCRIPCIÓN
1	ARFSIS	ARFSIS Atención ARFSIS Procesos Administración de Base de Datos ARFSIS Procesos ARFSIS Procesos Configuración ARFSIS ARFSIS Reportes ARFSIS Programa salud escolar SIASIS ARFSIS Consolidación ARFSIS	Registro de Prestaciones desde un Punto de digitación.
2	PORTAL WEB	Consulta en línea	Permite validar si una persona está afiliada al SIS y corroborar el estado de su afiliación de ser el caso.
3	PORTAL WEB	Mundo IPRESS CONVOCATORIAS CAS PUBLICACION DE CONVENIOS Y CONTRATOS OTROS ESPORADICOS	Información diversa para las IPRESS y público en general
4	SIASIS	IPRESS Privadas - Mixtas: - Ambulatoria	Permite la remisión de prestaciones registradas por parte de las IPRESS PRIVADAS: SISOL y IOL, y las diversas contrataciones especiales como Cirugías Electivas, Consultas Odontológicas, Consultas externas, etc. Cuenta con las opciones de evaluación prestacional y actualización de pagos.
5	SIASIS	Atención: - Referencias EsSalud	El sistema permite registrar referencias de asegurados SIS a ESSALUD mediante tramas para que sean leída por el aplicativo de acreditación ESSALUD y registrar solicitud de referencias de asegurados SIS a ESSALUD.

ID	SISTEMA	MODULOS	DESCRIPCIÓN
6	SIASIS	Intercambio Prestacional: - Reconsideración -> Solicitud	A finales del 2015, se puso a disposición de la DIRESA Callao y EsSalud, el piloto del aplicativo. A inicios del 2016, en coordinación con la GREP, se le dio el visto bueno al módulo, el cual se encuentra actualmente disponible para su uso a nivel nacional. Sin embargo a la fecha no se encuentra en uso (SIN USO).
7	SIASIS	Evaluación Prestacional: - PCPP	El Proceso de Control Prestacional es realizado por las UDRs y GMRs a nivel nacional, mediante el módulo se permite el registro del resultado de las evaluaciones; así como la programación de visitas, monitoreo y seguimiento.
8	SIASIS	Evaluación Prestacional: - RECONSIDERACIONES	Permite el registro de subsanación de observaciones realizadas en el SME, además permite a los Médicos Supervisores la evaluación de las Prestaciones Reconsideradas.
9	SIASIS	Subsidiado: - Anulación de Fichas	Dar de baja afiliaciones subsidiado del antiguo Régimen.
10	SIASIS	Afiliación Subsidiado	Permite Afiliación y Consulta de Afiliación con DNI y Carnet de Extranjería Régimen Subsidiado, validaciones con RENIEC, SUSALUD y SISFOH-MIDIS. Además se puede consultar todos los tipos de Afiliación. Permite afiliar a personas en situación de pobreza y pobreza extrema calificados de acuerdo al Sistema de Focalización de Hogares (SISFOH) y el padrón general de hogares (PGH) (Afiliación PEAS) y afiliar a las personas pertenecientes a grupos poblacionales determinado por norma (Afiliación directa, directa temporal). Y realizar modificaciones de datos y consultar los afiliados de subsidiados regímenes antiguos (sin SISFOH)
11	SIASIS	Independiente - Afiliación Independiente - Consultas y Reportes	Permite afiliar a personas que califican al SIS INDEPENDIENTE de acuerdo al Sistema de Focalización de Hogares (SISFOH). Visualizar los pagos pendientes y por realizar de los afiliados, Así también, permite visualizar el estado de cuenta. Resolución Jefatural N° 111-2015-SIS, orientado a usuarios de GA, MAC, UDR, GMR Y EESS.
12	SIASIS	Subsidiado - Afiliación Temporal	Registro de Afiliaciones temporales, personas que pertenecen a grupos determinados por norma y que son indocumentados. (Código E).

ID	SISTEMA	MODULOS	DESCRIPCIÓN
13	SIASIS	Atención: - Procedimientos Especiales - Sepelio - Traslado - Asignación por Alimentación	- El sistema permite registrar prestaciones preventivas, recuperativas y de rehabilitación otorgadas a asegurados del SIS mediante el FUA, aplicando reglas de consistencias como control de la información. - El sistema permite registrar FUA de Sepelio, el cual está orientado a usuarios de UDR 's y GMR 's a nivel nacional. Inició con la RJ N° 148-2009. - El sistema cuenta con las siguientes funcionalidades: Registrar prestaciones preventivas, recuperativas y de rehabilitación otorgadas a asegurados del SIS mediante el FUA, aplicando reglas de consistencias como control de la información. Registrar prestaciones de exámenes de procedimientos especiales otorgadas a asegurados del SIS Registrar prestaciones por traslado otorgadas a asegurados del SIS mediante el FUA, aplicando reglas de consistencias como control de la información Registrar prestaciones por asignación de alimentación otorgadas a aseguradas gestantes del SIS mediante el FUA, aplicando reglas de consistencias como control de la información.
14	SIASIS	Atención: - Salud Colectiva	El sistema permite registrar actividades colectivas otorgadas a asegurados del SIS y beneficiarios mediante el FAC, aplicando reglas de consistencias como control de la información. Inició con RJ 061-2016/SIS (JUNIO 2016).
15	SIASIS	Catálogos: - Personal de Salud - Registro de Funerarias	- Gestionar la información de los profesionales de salud que otorgan prestaciones, empresas funerarias que son consignadas en las prestaciones por sepelio, medicamentos por unidad ejecutora, insumos.
16	SIASIS	Consulta de Atenciones: - Consultas Supervisor No Tarifado: - Seguimiento de solicitudes - Sepelios	Sistema que permite realizar la consulta de seguimiento de prestaciones tarifadas y no tarifadas.
17	SIASIS	SIASIS: + Farmacia: (Pública) - Registro de Receta - Reimpresión de Receta/Entrega - Consulta de Receta - Reporte FarmaSIS pública + Supervisor Farmasis: - Reporte FarmaSIS GREP - Reporte FarmaSIS GNF FarmaSIS:	Sistema que cuenta con las funcionalidades para el control de la entrega de medicamentos a los asegurados del SIS desde las Oficinas Farmacéuticas Privadas.

ID	SISTEMA	MODULOS	DESCRIPCIÓN
		+ Farmacia: (Privada)	
18	SIASIS	Semisubsidiado: - Modificación de Datos - Reportes y Consultas	Actualización y Consultas SEMI-SUBSIDIADO Y SIS MICROEMPRESAS: Permite realizar modificaciones en las afiliaciones SIS MICROEMPRESAS, afiliaciones del componente semisubsidiado, SIS Independiente y consultas de los pagos realizados por los afiliados.
19	SIASIS	Afiliación NRUS: - Afiliación Presencial - Inscripción Recién Nacido - Actualización de Datos	Permite afiliar a las personas contribuyentes acogidos al NRUS y que realicen sus pagos correspondientes ante SUNAT. Esta a su vez remite al SIS la información de los pagos realizados para poder afiliarlos masivamente o por aplicativo (Afiliación presencial). Así también, inscribir a los recién nacidos cuyo titular cuente con un contrato Semi contributivo NRUS, actualizar los datos del régimen semi contributivo y visualizar los pagos realizados por el contribuyente. Consultar la información del afiliado. Resolución Jefatural N° 159-2013-SIS orientado a usuarios de GA, MAC, UDR, GMR Y EESS.
20	SIASIS	Supervisor No Tarifado: - Administrar No Tarifado - Administrar Sepelios - Administrar Casos Especiales Sepelios - Sub Componente Prestacional -> Evaluar Prestación	- El sistema permite gestionar la supervisión de los expedientes de prestaciones de asignación por alimentación, Traslados, procedimientos especiales. '- Registrar Solicitud de Actualización de datos de acreditado - Registrar Solicitud de Cambio de acreditado con Carta Poder - Visualizar solicitudes pendientes de Cambio de acreditado con Carta Poder de su GMR - Evaluar Solicitud de Cambio de acreditado con Carta Poder - Trazabilidad de los expedientes de Sepelio - Aprobar, observar y generar reportes de FUA de Sepelio, Traslado, Procedimientos Especiales. - Orientado a usuarios de GNF, CONTABILIDAD Y TESORERÍA. Permite programar fechas de cierre automático, cierre final y envío al banco. Permite programar, certificar y transferir pagos.
21	SIASIS	Supervisor No Tarifado: - Administrar Prestaciones 111 Catálogos: - Casas Maternas	- Gestionar la información de Casas Maternas de asignación por alimentación.
22	SIASIS	Intercambio Prestacional: - SME IP	La Supervisión Médica Electrónica del IP, se realiza siguiendo un cronograma dispuesto por EsSalud, en coordinación con la GREP. Una vez concluida el SME, los prestadores firman con EsSalud, el Acta de Conformidad de la evaluación.

ID	SISTEMA	MODULOS	DESCRIPCIÓN
23	SIASIS	Atención: - Cobertura Extraordinaria	Permite el registro y evaluación de las Solicitudes de Cobertura Extraordinaria que realizan los prestadores; adicionalmente permite a GNF la asignación de presupuesto a nivel referencial.
24	SIASIS	IPRESS Privadas - Mixtas: - Emergencia -> Atenciones	Sistema que permite carga de atenciones de IPRESS Privadas de emergencia.
25	SIASIS	Sala Situacional	Permite visualizar los resultados de la producción de atenciones en graficas estadísticas.
26	SIASIS	Catálogos: - Registro de Usuarios V2	Realizar Alta, actualización y Baja de Usuarios, también la asignación/retiro de roles de acceso.
27	SIASIS	CONSULTA MASIVA	Sistema para realizar consultas masivas de datos al web service de RENIEC y SUSALUD.
28	SIGEPS	Módulo de seguridad	Módulo de creación y mantenimiento de módulos, sub módulos y roles del SIGEPS
29	SIGEPS	wsAcreditacion	Web services del SITEDS para generar acreditaciones desde las IPRESS
30	SIGEPS	Retro ARFSIS	Retroalimentación referente al ARFSIS
31	SIGEPS	Registro de Atenciones	REGISTRO DE FUAS PRESTACIONALES
32	SIGEPS	Carga de paquetes ARFSIS	GESTIÓN DE PAQUETES ARFSIS - SOASIS
33	SIGEPS	Consulta de atenciones	CONSULTA DE ATENCIONES
34	SIGEPS	Reporte de atenciones	REPORTES DE ATENCIONES
35	SIGEPS	Nuevo SME	SUPERVISION MEDICA ELECTRÓNICA
36	SIGEPS	PES COVID	Registro de prestaciones económicas de sepelios por COVID-19
37	SIGEPS	LIBRO DE RECLAMACIONES	Gestión del libro de reclamaciones virtual
38	SIGEPS	IPRESS PRIVADAS	Esta opción permite el registro de FUAs prestacionales de las IPRESS privadas en el marco del COVID
39	SOASIS	Recepción de tramas	Recepción de tramas de registro de FUAs
40	SOASIS	Consulta de afiliados	Consulta de afiliados por web services
41	TRAMITE	Gestión de Tramite	Sistema de trámite documentario.
42	APP	Consulta de afiliados Consulta de planes de seguro Afiliaciones virtuales	Aplicativo móvil de afiliaciones virtuales
43	Mesa de partes digital	- Registro de documentos externos - Administración	Gestionar los documentos externos que remiten los ciudadanos, empresas o instituciones
44	SGD	Gestión de Tramite Documentario	Sistema de Gestión de Trámite Documentario

ID	SISTEMA	MODULOS	DESCRIPCIÓN
45	SISPAD	Registrar Expediente Actualizar Expediente Asignación de Expediente Etapa de Investigación Preliminar Etapa de Procedimiento Administrativo Disciplinario Recurso Impugnatorio Segunda Instancia Reportes	SISTEMA DE PROCEDIMIENTO ADMINISTRATIVO DISCIPLINARIO
46	SITEDS	Generación de acreditaciones desde las IPRESS Consulta de histórico Reimpresión de acreditaciones	Generación y gestión de acreditaciones desde las IPRESS
47	Zimbra	Correo electrónico	Envío y recepción de correos electrónicos de la entidad con dominio SIS.GOB.PE Y SISEXT.GOB.PE
48	Mesa de ayuda	Sistemas de mesa de ayuda	Sistema adquirido para la gestión de servicios de soporte y mesa de ayuda.

Fuente: Elaboración propia OGTI

B. Servicios Tecnológicos

Los servicios tecnológicos que brinda la OGTI, están diseñados para mantener un correcto funcionamiento de la plataforma tecnológica de la entidad. Así mismo, permiten brindar una respuesta oportuna a las diferentes eventualidades que en materia de tecnologías de la información puedan afectar el funcionamiento apropiado de la red de datos, equipos tecnológicos, red comunicaciones, entre otros servicios asociados.

Tabla 2: Servicios tecnológicos

SERVICIO	DESCRIPCIÓN	ALCANCE Y FUNCIONALIDAD	IMPORTANCIA PARA EL SIS
EQUIPOS DE CÓMPUTO	Comprende el Mantenimiento Preventivo y correctivo de los Equipos de Cómputo según su plan.	Este servicio de soporte va dirigido a todos los Equipos de Cómputo de propiedad del SIS.	Funcionalidad del Sistema Operativo y demás aplicaciones instaladas en los
SERVIDORES	Hace referencia a la Administración, configuración y disponibilidad de los servidores físicos de la entidad.	Este servicio de soporte va dirigido los servidores que están en el Data center, que está ubicado en la sede central del SIS.	Dirigido para la continuidad y administración de las aplicaciones que están instaladas en estos Servidores del SIS.

SERVICIO	DESCRIPCIÓN	ALCANCE Y FUNCIONALIDAD	IMPORTANCIA PARA EL SIS
BASES DE DATOS	Servicio para la creación, respaldo, restauración de a las Bases que interactúan con las Aplicaciones del SIS	Este servicio de soporte va dirigido a las Bases de Datos, la cual están en los servidores que están en el centro de datos del SIS.	Servicio de las Bases de Datos es la que da la continuidad y el funcionamiento de las Aplicaciones del SIS
ALMACENAMIENTO	Este servicio incluye tecnologías que permiten configurar y administrar uno o más servidores de archivos, que son servidores que proporcionan ubicaciones centrales en la red para almacenar archivos y compartirlos con los usuarios finales.	Dirigido a los Backups que soliciten los usuarios sobre archivos o aplicaciones que se necesiten como respaldo para los diferentes procesos que manejan en las diferentes oficinas del SIS	Permite el almacenamiento de archivos o aplicaciones para tener duplicidad de la información según sea solicitada por seguridad de la información.
CENTRO DE COMPUTO	Este servicio incluye servicios de apoyo logístico, instalación de componentes, monitoreo, backups, mantenimientos.	El centro de Cómputo es donde están los Servidores de las aplicaciones que maneja la Entidad, también está la central telefónica, la infraestructura de red Core, el aire acondicionado y UPS	El Centro de Cómputo debe estar en óptimas condiciones en cuanto al sistema eléctrico y aire acondicionado, ya que si estos dos factores no están funcionando se verán afectados los servidores y la central telefónica.
SEGURIDAD INFORMÁTICA	Actividades orientadas a garantizar la confidencialidad, integridad y disponibilidad de la información y la plataforma tecnológica de la Entidad y sus servicios asociados.	La seguridad Informática de la entidad se basa en el Subsistema de Gestión de Seguridad de la Información, la administración del equipo de seguridad perimetral firewall y Políticas del Directorio activo. Se complementa con protección de equipos con software antivirus y en el caso requerido la encriptación de información.	Por medio de este servicio se controla y garantiza el servicio de Internet, y el óptimo funcionamiento de las aplicaciones WEB que tiene la entidad. Se protegen los equipos de cómputo contra la presencia de software malicioso que pretenda daño o robo de información.
PORTALES WEB	Servicios asociados con los sitios WEB desarrollados y mantenidos por el SIS con el propósito de divulgar información y ofrecer servicios de interés general para los colaboradores de la entidad o para los públicos	Está constituido por la Pagina Web e intranet donde se ofrecen los diferentes servicios para usuarios internos y externos de la entidad.	Por medio de este servicio se realizan publicaciones de las diferentes actividades que se realizan en el SIS

SERVICIO	DESCRIPCIÓN	ALCANCE Y FUNCIONALIDAD	IMPORTANCIA PARA EL SIS
	externos.		
INTERNET	Administración de la disponibilidad de los servicios de Internet.	El servicio es utilizado por la Sede Principal y por las Sedes remotas. Cada sede tiene su propio servicio.	Este servicio es importante para la funcionalidad de las aplicaciones Web, correo electrónico y demás actividades que realiza el SIS con otras entidades.
GESTIÓN DE USUARIOS	Servicio para la creación, modificación, eliminación de usuarios y licencias.	El servicio hace referencia a las solicitudes que realizan los funcionarios para la asignación de usuarios o accesos a las aplicaciones que tiene la Entidad.	Es importante para que los funcionarios puedan ingresar a las aplicaciones y realizar las diferentes actividades que se realizan en la Entidad.
COPIAS DE RESPALDO	La OGTI realiza copia a bases de datos de los sistemas de información y de archivos ubicados en el centro de datos.	El servicio busca respaldar la información que se considera crítica y mantener su disponibilidad en el momento requerido. Se respalda la información contenida en el sitio de almacenamiento el centro de datos y el proveedor de almacenamiento y resguardo de cintas.	Mantener respaldo de la información considerada como crítica en la entidad y que se encuentra almacenada en las bases de datos de los sistemas de información misionales y de los archivos alojadas en los servidores del centro de datos.
OFIMÁTICA	Conjunto de aplicaciones y herramientas informáticas que se utilizan en el SIS para el desempeño de sus actividades de oficina.	Este servicio de soporte va dirigido a todos los Equipos de Cómputo del SIS.	Funcionalidad Herramientas informáticas y demás aplicaciones instaladas en los Equipos de cómputo del SIS.
CORREO ELECTRÓNICO	Se refiere a los servicios asociados a la cuenta de correo electrónico, tales como creación y configuración de cuentas de correo, restauración de buzones y sincronización, creación de PST, creación, modificación y eliminación de listas de distribución, compartir contactos y calendario.	Este servicio de soporte va dirigido a la creación y configuración de usuarios que estén previamente aprobados por OGTI.	El Servicio de Correo electrónico se brinda para los funcionarios de Carrera, Provisionales y para algunos Contratistas que trabajan en el SIS.

SERVICIO	DESCRIPCIÓN	ALCANCE Y FUNCIONALIDAD	IMPORTANCIA PARA EL SIS
TELEFONÍA Y CABLEADO ESTRUCTURADO	Los equipos comprenden un mantenimiento preventivo según plan de mantenimiento.	Este servicio va dirigido a todos los usuarios del SIS	Funcionalidad de las comunicaciones en voz y datos en las instalaciones del SIS.
CONECTIVIDAD WI-FI	Brindar Conectividad Inalámbrica a los grupos externos y funcionarios que por su contexto laboral requieren un despliegue constante por las diferentes Direcciones y oficinas del SIS., facilitando el trabajo y el uso de equipos portátiles asignados por la OGTI	Este servicio para la sede principal, es principalmente a los trabajadores, que lo requieran que constantemente se trasladan o no cuenten con un punto físico de conectividad. Se le brinda también al personal de servicios externos o visitas de proveedores.	El servicio de conectividad inalámbrica es una herramienta indispensable en la labor que desarrolla la mayoría de funcionarios que lo requieran dentro de las instalaciones del SIS
IMPRESIÓN Y DIGITALIZACIÓN	Los equipos de cómputo comprenden el mantenimiento preventivo, correctivo según su plan y garantía a las impresoras.	Este servicio va dirigido a todos los usuarios del SIS.	Por la cobertura dentro de la entidad y complejidad que maneja en las áreas se cataloga como importante para la entidad.
RECURSOS AUDIOVISUALES	Servicios de instalación y configuración de equipos de audio y video donde se requiera para las reuniones del SIS.	Este servicio de soporte va dirigido a la configuración de equipos de audio y video.	Funcionalidad Herramientas informáticas y demás aplicaciones del SIS.

Fuente: Elaboración propia OGTI

C. Infraestructura

Para soportar los servicios tecnológicos que se entregan a los Procesos del SIS se tiene establecida una infraestructura tecnológica que está conformada por servicios de conectividad, sistemas de información y elementos físicos. Adicionalmente, el SIS cuenta con un centro de datos propio ubicado en la sede principal, en Av. Paseo de la Republica 1645, La Victoria.

D. Acuerdos de niveles de servicio de tecnología

La Dirección de Tecnologías de la Información ha considerado los Acuerdos de Niveles de Servicio para la prestación de estos servicios, los cuales son definidos teniendo en cuenta el nivel de complejidad y la afectación que cause sobre la infraestructura tecnológica.

(Ver tabla en la siguiente página)

Tabla 3: Niveles de servicio

SERVICIO	CANAL DE ACCESO	DISPONIBILIDAD DE HORARIOS	HORARIOS DE SOPORTE	HORARIO DE USO	REQUISITOS PARA ACCEDER AL SERVICIO
SIASIS	WEB	7 días 24 horas los 365 días del año	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m. y por demanda extra horario de oficina.	7 días 24 horas los 365 días del año	Navegador Mozilla Firefox o Google Chrome Acceso a internet
PORTAL WEB	WEB	7 días 24 horas los 365 días del año	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m.	7 días 24 horas los 365 días del año	Navegador Mozilla Firefox o Google Chrome Acceso a internet
SIGEPS	WEB	7 días 24 horas los 365 días del año	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m. y por demanda extra horario de oficina.	7 días 24 horas los 365 días del año	Navegador Mozilla Firefox o Google Chrome Acceso a internet
SOASIS	WEB	7 días 24 horas los 365 días del año	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m. y por demanda extra horario de oficina.	7 días 24 horas los 365 días del año	Navegador Mozilla Firefox o Google Chrome Acceso a internet
TRAMITE	WEB	7 días 24 horas los 365 días del año	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m. y por demanda extra horario de oficina.	7 días 24 horas los 365 días del año	Navegador Mozilla Firefox o Google Chrome Acceso a internet
APP	WEB	7 días 24 horas los 365 días del año	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m. y por demanda extra horario de oficina.	7 días 24 horas los 365 días del año	Navegador Mozilla Firefox o Google Chrome Acceso a internet

SERVICIO	CANAL DE ACCESO	DISPONIBILIDAD DE HORARIOS	HORARIOS DE SOPORTE	HORARIO DE USO	REQUISITOS PARA ACCEDER AL SERVICIO
Mesa de partes digital	WEB	7 días 24 horas los 365 días del año	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m. y por demanda extra horario de oficina.	7 días 24 horas los 365 días del año	Navegador Mozilla Firefox o Google Chrome Acceso a internet
SGD	WEB	7 días 24 horas los 365 días del año	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m. y por demanda extra horario de oficina.	7 días 24 horas los 365 días del año	Navegador Mozilla Firefox o Google Chrome Acceso a internet
SISPAD	WEB	7 días 24 horas los 365 días del año	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m. y por demanda extra horario de oficina.	7 días 24 horas los 365 días del año	Navegador Mozilla Firefox o Google Chrome Acceso a internet
SITEDS	WEB	7 días 24 horas los 365 días del año	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m. y por demanda extra horario de oficina.	7 días 24 horas los 365 días del año	Navegador Mozilla Firefox o Google Chrome Acceso a internet
CORREO ELECTRONICO	WEB	7 días 24 horas los 365 días del año	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m. y por demanda extra horario de oficina.	7 días 24 horas los 365 días del año	Navegador Mozilla Firefox o Google Chrome Acceso a internet
Mesa de ayuda	WEB	7 días 24 horas los 365 días del año	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m. y por demanda extra horario de oficina.	7 días 24 horas los 365 días del año	Navegador Mozilla Firefox o Google Chrome Acceso a internet
IMPRESIÓN Y DIGITALIZACION	Teléfono Correo Mesa de Servicios	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m.	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m.	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m.	ACCESO A RED

SERVICIO	CANAL DE ACCESO	DISPONIBILIDAD DE HORARIOS	HORARIOS DE SOPORTE	HORARIO DE USO	REQUISITOS PARA ACCEDER AL SERVICIO
CONECTIVIDAD INALAMBRICA	Puntos De Acceso Inalámbrico	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m.	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m.	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m.	Acceso a red interna Equipo de cómputo móvil o teléfono móvil Solicitud de acceso a servicios vía formulario de mesa de ayuda
TELEFONÍA	Acceso por puntos de acceso red	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m.	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m.	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m.	Acceso a red interna Solicitud de acceso a servicios vía formulario de mesa de ayuda
EQUIPO DE COMPUTO	Por solicitud y según necesidad	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m.	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m.	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m.	Solicitud de acceso a servicios vía formulario de mesa de ayuda
OFIMÁTICA	Por solicitud y según necesidad	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m.	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m.	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m.	Solicitud de acceso a servicios vía formulario de mesa de ayuda
SERVIDORES	Acceso según necesidad por los usuarios o población interesada mediante los portales de servicios y accesos a sistemas.	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m.	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m.	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m.	Solicitud de acceso a servicios vía formulario de mesa de ayuda
BASE DE DATOS	Acceso según necesidad por los usuarios o población interesada mediante los portales de servicios y accesos a sistemas.	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m.	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m.	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m.	Solicitud de acceso a servicios vía formulario de mesa de ayuda

SERVICIO	CANAL DE ACCESO	DISPONIBILIDAD DE HORARIOS	HORARIOS DE SOPORTE	HORARIO DE USO	REQUISITOS PARA ACCEDER AL SERVICIO
INTERNET	Solo para el personal del SIS y por solicitud	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m.	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m.	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m.	Solicitud de acceso a servicios vía formulario de mesa de ayuda
COPIAS DE RESPALDO	Solo para el personal del SIS y por solicitud El personal autorizado de la OGTI realiza copias de seguridad según cronograma	Por cronograma definido y por demanda	Por cronograma definido y por demanda	Por cronograma definido y por demanda	Solicitud de acceso a servicios vía formulario de mesa de ayuda Plan de respaldo y resguardo de datos
ALMACENAMIENTO	Solo para el personal del SIS y por solicitud	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m.	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m.	Jornada laboral de lunes a viernes de 8 a.m. a 5 p.m.	Solicitud de acceso a servicios vía formulario de mesa de ayuda

Fuente: Elaboración propia OGTI

E. Inventario de activos

Para este Plan se consideran los activos de información ya clasificados dentro del inventario de activos de información del SGSI. Según la clasificación del activo de información, se presenta el inventario de activos de información, basado en la NTP 27001:2022.

El inicio del análisis de riesgos empieza con el inventario de activos de información del proceso o procesos considerados dentro del alcance del SGSI, la metodología de gestión de riesgos que se usara es basado en la NTP 27001:2022 por lo que se alojará correctamente con el Sistema de Gestión de Seguridad de la Información.

i. Valorización de Activos

El Equipo Especialista de Seguridad de la Información colocará la valoración del activo de información identificado, la cual se define de la siguiente manera:

Tabla 4: Valor del Activo

Activo	Detalle
Alto	Activo importante para SIS. Su disponibilidad es necesaria para los procesos críticos de SIS.
Medio	Constituye un soporte para los activos importantes de SIS. La información puede estar replicada en varias fuentes o existen medios alternos. No compromete los procesos críticos de SIS.
Bajo	Activos secundarios, que constituyen información para la toma de decisiones de un área específica. No compromete ningún proceso crítico de SIS.

Fuente: Elaboración propia OGTI

Tabla 5: Inventario de activos basado en ISO27001

CODIGO	ACTIVO	CATEGORIA DEL ACTIVO	UBICACIÓN FISICA O LOGICA	UBICACIÓN GEOGRAFICA	CLASIFICACION				FRECUENCIA DE USO					PROPIETARIO	CUSTODIO	VALOR DEL ACTIVO
					PUBLICO	USO INTERNO	CONFIDENCIAL	RESTRINGIDA	DIARIO	SEMANAL	QUINCENAL	ANUAL	EVENTUAL			
AI-1	Sala de Servidores	FISICO	Sede Central SIS	Av. Paseo de la República 1645, La Victoria				X	X					DIRECTOR OGTI	Coordinador de centro de datos	Alto
AI-2	Sistema de almacenamiento de Datos de respaldo del centro de datos	SOFTWARE	Sede Central SIS – centro de datos	Av. Paseo de la República 1645, La Victoria			X		X					DIRECTOR OGTI	Coordinador de centro de datos	Alto
AI-3	Datos de Respaldo (back UP)	INFORMACION	Sede Central SIS – centro de datos	Av. Paseo de la República 1645, La Victoria			X			X				DIRECTOR OGTI	Coordinador de centro de datos	Alto
AI-3	Software de autenticación de directorio activo	SOFTWARE	Sede Central SIS – centro de datos	Av. Paseo de la República 1645, La Victoria			X		X					DIRECTOR OGTI	Coordinador de centro de datos	Alto
AI-4	Información digital de Personal de Operaciones	INFORMACION	Sede Central SIS – centro de datos	Av. Paseo de la República 1645, La Victoria				X	X					DIRECTOR OGTI	Coordinador de centro de datos	Alto
AI-5	Infraestructura de área de Operadores de Centro de datos	FISICO	Sede Central SIS – centro de datos	Av. Paseo de la República 1645, La Victoria			X		X					DIRECTOR OGTI	Coordinador de centro de datos	Medio

CODIGO	ACTIVO	CATEGORIA DEL ACTIVO	UBICACIÓN FISICA O LOGICA	UBICACIÓN GEOGRAFICA	CLASIFICACION				FRECUENCIA DE USO					PROPIETARIO	CUSTODIO	VALOR DEL ACTIVO
					PUBLICO	USO INTERNO	CONFIDENCIAL	RESTRINGIDA	DIARIO	SEMANAL	QUINCENAL	ANUAL	EVENTUAL			
AI-6	Servicio de Energía Eléctrica	SERVICIOS	Sede Central SIS – centro de datos	Av. Paseo de la República 1645, La Victoria		X			X					DIRECTOR OGTI	Operaciones	Alto
AI-7	Grupo Electrógeno	FISICO	Sede Central SIS	Av. Paseo de la República 1645, La Victoria		X							X	DIRECTOR OGTI	coordinador de centro de datos, mantenimiento de operaciones SIS	Medio
AI-8	UPS	FISICO	Sede Central SIS – centro de datos	Av. Paseo de la República 1645, La Victoria		X							X	DIRECTOR OGTI	coordinador de centro de datos	Medio
AI-9	Infraestructura de Red	FISICO	Sede Central SIS – centro de datos	Av. Paseo de la República 1645, La Victoria		X			X					DIRECTOR OGTI	coordinador de centro de datos	Medio
AI-11	Sistema de seguridad de puertas de acceso al centro de operaciones uy sala de servidores	FISICO	Sede Central SIS – centro de datos	Av. Paseo de la República 1645, La Victoria			X		X					DIRECTOR OGTI	coordinador de centro de datos	Medio
AI-12	Personal de operaciones de Centro de Datos	RECURSOS HUMANOS	Sede Central SIS – centro de datos	Av. Paseo de la República 1645, La Victoria		X			X					RRHH-SIS	recursos humanos	Alto

Fuente: Elaboración propia OGTI

7.2.2 Identificación de Riesgos

Para el Plan de Contingencias del SIS se tienen en cuenta los riesgos tecnológicos identificados dentro del análisis de riesgos de seguridad de la información.

A. Análisis de Riesgos

Un SGSI basado en la norma ISO 27001 se fundamenta principalmente en la identificación y análisis de las principales amenazas para, a partir de este punto de partida, poder establecer una evaluación y planificación de dichos riesgos, se usará la metodología de gestión de riesgos del SGSI.

B. Identificar Amenazas

Con la lista de activos de información, se realiza la identificación de las amenazas asociadas a cada uno de ellos. A continuación, se presenta una lista de posibles amenazas genéricas agrupadas por cada tipo de activo que podría ser afectado.

Las amenazas presentadas no representan una totalidad ya que en el ejercicio de las actividades de la entidad se presentarán nuevas amenazas al ciclo de vida de los sistemas informáticos del SIS, por lo que las actualizaciones de este plan actualizarán esta lista presente, con el fin de generar nuevos planes de acción.

Tabla 6: Lista de amenazas

N°	Tipología de Amenaza	Tipo
1	Acceso no autorizado a la información	Amenazas a la Información – Activos Primarios
2	Modificación no autorizada de la información	
3	Eliminación no autorizada de la información	
4	Robo de activos contenedores de información	
5	Inadecuada eliminación de activos contenedores de información	
6	Corrupción de datos por error de procesamiento	
7	Uso extra laboral de la información	
8	Ataques de hacking/cracking sobre la información	
9	Virus informáticos que alteran o eliminan la información	
10	Fuga de Información	
11	Adulteración intencional del software (bombas lógicas, sabotaje)	Amenazas al Software - activos de soporte
12	Cambios no autorizados sobre el software (mantenimientos)	
13	Actualizaciones no controladas del software (parches)	
14	Instalación de software no licenciado o autorizado	
15	Copia no controlada del código fuente del software	
16	Saturación de la operación del software	
17	Hacking/cracking	
18	Virus informáticos	
19	Error humano en los cambios en el software (bugs)	
20	Incompatibilidad en la operación con otros software	
21	Corto circuito	Amenazas a Activos Físicos (hardware físicos). Activos de Soporte
22	Filtraciones de agua	
23	Filtración de polvo	
24	Corrosión de equipos	
25	Congelación de equipos	
26	Desconexión de equipos	
27	Saturación de humedad en ambientes	

N°	Tipología de Amenaza	Tipo
28	Fallas del sistema de aire acondicionado	Amenazas a Activos Físicos (hardware físicos). Activos de Soporte
29	Radiación electromagnética	
30	Robo de equipos o de sus componentes	
31	Incumplimiento del plan de mantenimiento	
32	Uso inadecuado de los equipos	
33	Desconfiguración del equipo	
34	Obsolescencia de los componentes del equipo	
35	Falla de servicios para las telecomunicaciones	Amenazas a Servicios – activo de servicios
36	Degradación de servicios para las telecomunicaciones	
37	Falla de la provisión de energía eléctrica	
38	Incumplimiento de fechas por parte de proveedores	
39	Provisión de servicios defectuosos (personal)	
40	Provisión de recursos defectuosos (materiales)	
41	Falla en servicios de información provistos por clientes	
42	Contaminación del ambiente por gases	Amenazas a Personal – activo de RRHH
43	Uso de credenciales falsificadas	
44	Bloqueo del acceso al centro de trabajo	
45	Dificultad en el desplazamiento hacia el centro de trabajo	
46	Asaltos/secuestros	
47	Enfermedad	
48	Agotamiento Físico y mental	
49	Sismo	Amenazas a Ubicaciones Físicas -activo de soporte
50	Inundación	
51	Hundimiento de suelos	
52	Incendio	
53	Destrucción intencional de los ambientes (protestas)	

Fuente: Elaboración propia OGTI

C. Evaluación del Valor del Riesgo

Impacto

Se determina el impacto de acuerdo a la siguiente tabla:

Tabla 7: Valorización del Impacto del Riesgo

Nivel	Descripción	Impacto
5	Extremo	Impacta en forma severa en SIS al punto de comprometer la confidencialidad o integridad de información crítica y/o la continuidad de las operaciones por paralización de los servicios críticos más allá de los tiempos tolerables por el negocio. El impacto es a toda SIS y su efecto repercute en todo el personal involucrado.
4	Alto	Impacta en forma grave a un área o servicio específico de SIS, se puede llegar a comprometer documentos internos clasificados como confidenciales, paralizar o retrasar procesos claves por un tiempo considerable. Su efecto está limitado dentro de la SIS.
3	Mediano	El impacto sobre la confidencialidad, integridad y disponibilidad de la información es limitado en tiempo y alcance. Su efecto es para un proceso de soporte o actividad específica que puede subsanarse en corto plazo.
2	Bajo	El impacto es leve y se puede prescindir del mismo en un tiempo limitado.
1	No Significativo	No representa un impacto importante para la SIS.

Fuente: Elaboración propia OGTI

D. Estimar la Probabilidad de Ocurrencia del Riesgo

Se determina la probabilidad de ocurrencia de acuerdo a la siguiente tabla:

Tabla 8: Probabilidad de Ocurrencia del Riesgo

Valor	Clasificación	Definición
1	Muy Baja	El evento no ocurre nunca o casi nunca. Ha ocurrido al menos 1 vez al año.
2	Baja	Si bien el evento puede ocurrir el periodo entre uno y otro evento puede ser muy grande. Al menos 2 veces al año.
3	Moderada	Es posible que ocurra el evento con una frecuencia baja. 3 o 4 veces al año.
4	Alta	Existen antecedentes de que el evento ocurrirá, dentro de un plazo de tiempo que implique una acción para enfrentarlo, pero la frecuencia no es alta. 1 vez al mes.
5	Muy Alta	El evento se sabe que ocurre con cierto grado de certeza y que la frecuencia es alta. 1 vez a la semana o más.

Fuente: Elaboración propia OGTI

E. Evaluación del Riesgo

Al culminar el análisis de riesgos, se procede a la evaluación de los riesgos identificados, se tomará la probabilidad de ocurrencia del riesgo como datos de entrada. Los resultados del análisis de riesgos serán comparados con los criterios de riesgos establecidos.

Se determina el inventario de activos presentado en el informe anterior para ser usado en el análisis.

- **Nivel de Riesgo**

  El riesgo efectivo es la medida del daño probable causado por una amenaza, que se materializa en un activo. Con el valor obtenido del producto del Impacto por la Probabilidad el Equipo de Trabajo obtendrá el Nivel de Riesgo de acuerdo a la siguiente tabla:

Tabla 9: Valorización del Riesgo

TABLA DE VALORIZACIÓN DE RIESGOS					
Impacto		Probabilidad		Nivel de Riesgo	
Extremo	5	Muy Alta	5	Extremo	25
Alto	4	Muy Alta	5	Extremo	20
Mediano	3	Muy Alta	5	Extremo	15
Bajo	2	Muy Alta	5	Alto	10
No Significativo	1	Muy Alta	5	Mediano	5
Extremo	5	Alta	4	Extremo	20
Alto	4	Alta	4	Extremo	16
Mediano	3	Alta	4	Alto	12
Bajo	2	Alta	4	Mediano	8
No Significativo	1	Alta	4	Bajo	4
Extremo	5	Moderada	3	Extremo	15
Alto	4	Moderada	3	Alto	12
Mediano	3	Moderada	3	Alto	9

TABLA DE VALORIZACIÓN DE RIESGOS					
Impacto		Probabilidad		Nivel de Riesgo	
Extremo	5	Muy Alta	5	Extremo	25
Alto	4	Muy Alta	5	Extremo	20
Mediano	3	Muy Alta	5	Extremo	15
Bajo	2	Muy Alta	5	Alto	10
No Significativo	1	Muy Alta	5	Mediano	5
Extremo	5	Alta	4	Extremo	20
Alto	4	Alta	4	Extremo	16
Bajo	2	Moderada	3	Mediano	6
No Significativo	1	Moderada	3	Bajo	3
Extremo	5	Baja	2	Alto	10
Alto	4	Baja	2	Mediano	8
Mediano	3	Baja	2	Mediano	6
Bajo	2	Baja	2	Bajo	4
No Significativo	1	Baja	2	No Significativo	2
Extremo	5	Muy Baja	1	Mediano	5
Alto	4	Muy Baja	1	Bajo	4
Mediano	3	Muy Baja	1	Bajo	3
Bajo	2	Muy Baja	1	No significativo	2
No Significativo	1	Muy Baja	1	No significativo	1

Fuente: Elaboración propia OGTI

Los riesgos serán clasificados de acuerdo a niveles, según su grado de exposición, según la siguiente tabla:

Tabla 10: Nivel de Riesgo

Rango de Riesgo	Nivel de Riesgo	Descripción de las Consecuencias
De 15 a 25	**Extremo**	Puede afectar seriamente a SIS, en términos de paralización de las operaciones. Requiere acción correctiva inmediata más allá del tiempo tolerable, pérdidas considerables o demandas legales y daño considerable.
De 9 a 12	**Alto**	Puede afectar los niveles de operación y servicio de SIS, incumplimiento de metas, y divulgación no autorizada de información fuera de SIS. Requiere una acción correctiva sujeta a la discreción de los Propietarios del Riesgo en términos de plazos y compromisos.
De 5 a 8	**Mediano**	Afecta a los activos de información de soporte a los activos principales, puede afectar la disponibilidad en áreas específicas de SIS. La divulgación no autorizada no representa perjuicio importante para la SIS. Su aceptación está sujeta a la revisión de los Propietarios del Riesgo.
De 3 a 4	**Bajo**	No causa un efecto considerable en SIS. Usualmente son aceptados sin revisión.
De 1 a 2	No Significativo	El efecto para SIS es insignificante. Usualmente no se les considera para la gestión de riesgos.

Fuente: Elaboración propia OGTI

- **Nombre del Riesgo (interpretación)**
  Se asignará un nombre al riesgo que sirva para diferenciarlo respecto de otros.
  Se muestra un ejemplo de cómo se construye la narración del riesgo o escenario de riesgo, esto es usado solo para efectos de exposición de resultados iniciales por el especialista o el oficial de seguridad de la información.

Tabla 11: Ejemplo de Narración

Elemento	Ejemplo de narración
Activo de Información	Archivos de configuración lógica de switches y router
Amenaza	Acceso no autorizado a los archivos de configuración lógica de switches y router, por parte de atacantes internos y/o atacantes externos.
Vulnerabilidad	No se guardan los archivos de configuración lógica de switches y router con algún de software de encriptación en los discos duros de los administradores.
Nombre del Riesgo	Perdida de datos de configuración de equipos de comunicación
Impacto	Impacto en las operaciones dado que la información puede ser aprovechada por un hacker para futuros ataques.
Escenario de Riesgo	Si ocurre un acceso no autorizado a los archivos de configuración lógica de switches y router, entonces puede causar un impacto en las operaciones dado que la información puede ser aprovechada por un hacker para futuros ataques debido a que no se guardan los archivos de configuración lógica de switches y router con algún de software de encriptación en los discos duros de los administradores.

Fuente: Elaboración propia OGTI

- **Matriz de riesgos**
  La matriz de riesgos analiza los riesgos del proyecto en función de su probabilidad y gravedad. Una vez que se identifiquen los riesgos, se podrá calcular el impacto general y otorgarle a cada riesgo la prioridad que le corresponda.
  La Matriz de riesgos esta presentada con los riesgos más comunes y a su vez los que representan a las actividades del SIS.

7.2.3 Clasificación de Interrupciones y Nivel de Afectación a los Servicios de TI.

La activación o no del Plan de Contingencias, dependerá del resultado de la ejecución del procedimiento de Gestión de Incidentes de Seguridad y/o las decisiones tomadas por los niveles Estratégico y Táctico descritos en este Plan, frente a la situación que genere la interrupción del servicio tecnológico, así como los eventos descritos en el Análisis de Impacto al Negocio (BIA).

Los incidentes que pasan a ser tratados dentro del Plan de Contingencia son evaluados de acuerdo con el impacto que tienen sobre la prestación del servicio tecnológico del SIS., de acuerdo con la siguiente clasificación:

Tabla 12: Clasificación por tipo de interrupción de la continuidad

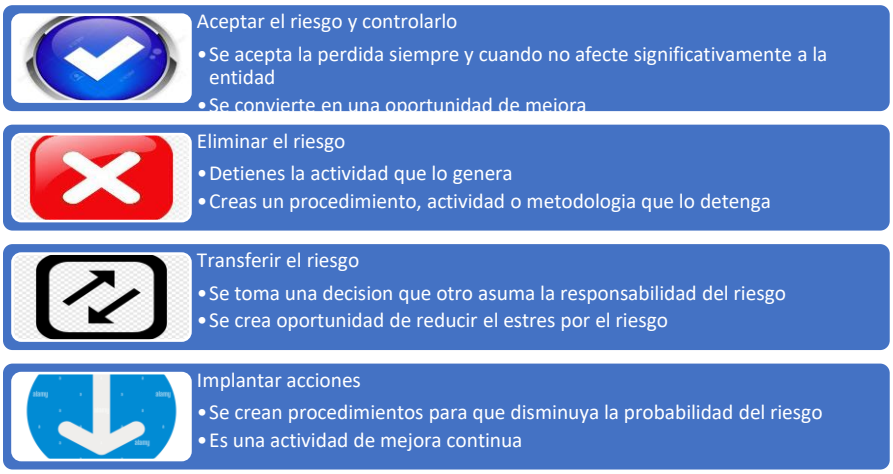
TIPO DE INTERRUPCIÓN	CARACTERÍSTICAS	EJEMPLOS	Prioridad
TOTAL	Evento que inhabilita el centro de datos para prestar sus servicios. No permite que el equipo de tecnología siga laborando en las instalaciones principales de la empresa.	Terremotos. Incendio. Orden Público. Fallo eléctrico en el sector.	1
PARCIAL	Evento que afecta a más de un recurso informático de manera drástica ocasionando la suspensión parcial del funcionamiento del hardware o software considerados como críticos.	Fallas técnicas en equipos servidores que alojan más de un aplicativo, bases de datos.	2
ESPECIFICA	Evento que afecta puntualmente un recurso necesario para la prestación de los servicios de Informática.	Fallas técnicas de un equipo que aloja un sistema o servicio. Ausencia de personal clave.	3

Fuente: Elaboración propia OGTI

A. Tratamiento del Riesgo

Una vez establecidos los principales riesgos, es decir aquellos con mayor impacto, debemos tratarlos de manera adecuada mediante una de las siguientes estrategias:

Gráfico 2: Estrategias para el Tratamiento de Riesgo



Fuente: Elaboración propia OGTI

B. Escenarios de Riesgos

De las actividades generales a ejecutar en una contingencia, las responsabilidades y tareas de los roles que intervienen en el Plan de Contingencias y los riesgos identificados para el proceso de Gestión de Tecnologías de la Información, surgen de escenarios que la OGTI identificó para la atención y tratamiento; escenarios en los cuales los recursos tecnológicos, personas, proveedores e infraestructura se pueden ver afectados por una situación que causa interrupción total o parcial y que afectan el normal funcionamiento de los servicios de TI que soportan los procesos de la entidad.

Los escenarios preliminares de riesgos identificados calificados como extremos (según Matriz de Riesgos) para la contingencia de TI se presentan a continuación:

- No disponibilidad del personal de TI
- No disponibilidad de los proveedores de TI o soporte externo
- No disponibilidad de las comunicaciones
- No disponibilidad de los servicios y aplicaciones de TI

Las estrategias consideradas para estos escenarios se mencionan en el presente documento el punto 12 “Estrategias de pruebas del plan de contingencias de TI”, se adjuntarán los escenarios con sus procedimientos y que por contener información (instructivos) de índole confidencial, es solo para uso del personal encargado de cada sistema o infraestructura.

7.2.4 Aspectos Generales para la Atención de una Contingencia

El Plan de Contingencia, se activa frente a una situación de interrupción de un servicio y/o infraestructura de TI o de acuerdo con lo determinado por el procedimiento de Gestión de Incidentes de Seguridad y/o lo que exprese el nivel estratégico o táctico del Plan.

A continuación, se presentan las actividades generales que se deben tener en cuenta por los roles definidos dentro del Plan, para la atención de una situación de contingencia de TIC.

Tabla 13: Actividad, responsable y acción

ACTIVIDAD	RESPONSABLE	ACCIÓN
1	Funcionarios de la OGTI	Reportar la falla en el sistema de mesa de servicios que tenga dispuesta la entidad siguiendo el procedimiento de Atención de requerimientos de soporte a los sistemas de información y equipos informáticos.

ACTIVIDAD	RESPONSABLE	ACCIÓN
2	Responsable del Sistema de Mesa de Servicios	• Analiza la falla. En caso de corresponder a un incidente de seguridad, traslada la acción al procedimiento de Gestión de Incidentes de seguridad. • Si la situación no es un incidente de seguridad, pero afecta la operación de algún servicio de TI, informa a la dirección para la toma de decisiones.
3	Equipo de Respuestas ante Incidentes	Evalúa y determina si el incidente corresponde a una contingencia. En este caso informa al responsable del Plan de contingencia.
4	Director(a) de la Oficina General de Tecnología de la Información	Autoriza la puesta en marcha del Plan de Contingencia de TI, notificando a las áreas afectadas y a los niveles estratégico y táctico del Plan de Contingencias de TI.
5	Gestor del plan de contingencia	Gestiona las actividades del Plan de Contingencia de TI, asignando a los funcionarios que realizaran las labores operativas de recuperación según el tipo de interrupción y los servicios y/o infraestructura afectada.
6	• Líder y equipo de atención del Plan de Contingencia • Administradores de Infraestructura y Aplicaciones • Equipos de apoyo de acuerdo • con la especialidad	• Ejecuta las actividades de recuperación junto con el equipo de atención e informa al Gestor del Plan de Contingencia según lo descrito en el escenario de contingencia a solucionar). • Realiza pruebas de recuperación del servicio y/o infraestructura afectada y reporta al Gestor del Plan de Contingencia la finalización de las actividades implementadas.
7	• Gestor del plan de contingencia • Coordinadores de la OGTI	• Informa al Director de Tecnologías de la Información y las Comunicaciones la finalización de las actividades de recuperación. • Coordina las actividades para el restablecimiento de la operación normal de los servicios de TI.
8	• Líder del Plan de Contingencia • Administradores de Infraestructura y Aplicaciones.	Inicia las acciones pertinentes para el restablecimiento del proceso normal (según lo descrito en el escenario de contingencia a solucionar).
9	Grupo de atención del Plan de Contingencias de TI.	Actualiza Hoja de vida del equipo, servidor o del sistema de información sobre la incidencia presentada.

ACTIVIDAD	RESPONSABLE	ACCIÓN
10	• Director de la OGTI • Gestor del plan de contingencia • Coordinadores de la OGTI • Líder del Plan de Contingencia. • Administradores de Infraestructura y Aplicaciones.	• Realizar análisis de las fallas presentadas y de los indicadores del proceso. • Documenta los resultados y lecciones aprendidas.
11	Director de la OGTI	• Autoriza la finalización del plan. • Informa a las áreas afectadas la normalización en la prestación de los servicios de TI. • Autoriza el cierre de la contingencia e informa al Comité o a la Alta Dirección, el balance de la situación de contingencia atendida.

Fuente: Elaboración propia OGTI

A. Sistemas de Información y Aplicaciones

- Realizar inventario de los sistemas de información y/o aplicativos afectados de acuerdo con las características relacionadas en el documento Plan de Contingencias.
- Preparar y configurar un equipo de cómputo de acuerdo con las características y condiciones de conectividad especificadas relacionadas en el documento Plan de Contingencias del sistema de información y/o aplicación afectado.
- Restaurar copia de seguridad de la base de datos correspondiente, así como la copia de respaldo más reciente del código fuente o del archivo de instalación o ejecutable.
- Revisar permisos de acceso y cuentas de usuario del sistema de información afectado.
- Verificar la conexión entre la base de datos y el sistema y/o aplicativo.
- Realizar pruebas de procesamiento y transaccionalidad de datos entre los sistemas y/o aplicativos en el equipo dispuesto para la atención de la contingencia.
- Paralelo a estas actividades, en el sistema afectado, se debe identificar la causa que generó la contingencia y tomar las acciones pertinentes para superar la situación de acuerdo con lo descrito en el Plan.
- En caso de que la contingencia se presente en un servicio, sistema de información y/o aplicativo que cuente con un soporte técnico y/o garantía, se debe informar al contratista la contingencia presentada, monitorear los acuerdos de niveles de servicio establecidos contractualmente y gestionar la atención y restauración del servicio con el contratista.

B. Recursos Tecnológicos e Infraestructura

- Realizar inventario físico de la infraestructura afectada de acuerdo con las características relacionadas en el documento Plan de Contingencias.

- Determinar las características técnicas de la infraestructura física afectada.
- Con la infraestructura no afectada y dependiendo la situación presentada, realizar las actividades planteadas en los diferentes escenarios para atender la contingencia y restaurar el servicio de TIC afectado.
- Verificar las conexiones entre servicios de TIC y la infraestructura dispuesta para la atención de la contingencia.
- Realizar pruebas de transaccionalidad de datos y/o conexiones en el equipo dispuesto para la atención de la contingencia.
- Paralelo a estas actividades, en la infraestructura afectada se debe identificar la causa que generó la contingencia y tomar las acciones pertinentes para superar la situación de acuerdo con lo descrito en el Plan.
- En caso de que la contingencia se presente en infraestructura que cuente con un soporte técnico y/o garantía, se debe informar al contratista la contingencia presentada, monitorear los acuerdos de niveles de servicio establecidos contractualmente y gestionar la atención y restauración del servicio con el contratista.

C. Recurso Humano

Los funcionarios asignados por parte de la Oficina General de Tecnología de la Información para la atención de una contingencia que afecte un servicio de TI se presentan a continuación:

Tabla 14: Recurso Humano

RESPONSABLE	ROL	CONTACTO
Director General de la OGTI	Responsable del plan de Contingencia	Director General de la OGTI
Director ejecutivo de la OGTI	Gestor del Plan de Contingencia	Director Ejecutivo
Profesional Especializado	Responsable de infraestructura de redes y seguridad	Responsable De Unidad De Infraestructura Tecnológica
Profesional Especializado	Responsable de infraestructura de servidores y centro de datos	Coordinador De Infraestructura De Servidores
Profesional Especializado	Responsable de operaciones TI	Coordinador De Operaciones
Profesional Especializado	Responsable de Unidad de Sistemas	Profesional con responsabilidad en sistemas o quien se designe.
Profesional Especializado	Responsable de Gestión de Base de Datos	Coordinador De Operaciones
Profesional Especializado	Responsable de Pases a Producción y publicaciones	Coordinador De Operaciones

Fuente: Elaboración propia OGTI

D. Aspectos Logísticos

Cuando ocurra una situación inesperada que conlleve a la materialización de un riesgo identificado en este Plan de Contingencia, el funcionario afectado o los funcionarios afectados deberán reportarlo de inmediato a través de la mesa de servicios que tenga dispuesta la entidad o comunicándose directamente a la OGTI con el anexo 0800. y/

o al correo soporte@sis.gob.pe, una vez reportada la contingencia se activará por parte de la OGTI, el respectivo procedimiento para el manejo de la interrupción.

7.2.5 Evaluación de Impactos Operacionales

Teniendo en cuenta los elementos operacionales de la entidad, se requiere evaluar el nivel de impacto de una interrupción dentro de la Entidad. El impacto operacional permite evaluar el nivel negativo de una interrupción en varios aspectos de las operaciones del negocio; el impacto se puede medir utilizando un esquema de valoración, con los siguientes niveles: A, B o C.

Nivel A: La operación es crítica para el negocio. Una operación es crítica cuando al no contar con ésta, la función del negocio no puede realizarse.
Nivel B: La operación es una parte integral del negocio, sin ésta el negocio no podría operar normalmente, pero la función no es crítica.
Nivel C: La operación no es una parte integral del negocio.

La tabla siguiente muestra los niveles de criticidad de la entidad, que contempla un sistema **de tolerancia a fallas por horas**, cuya propiedad permite que un sistema pueda seguir operando normalmente a pesar de que una falla haya ocurrido en alguno de los componentes del sistema; por lo tanto, la tolerancia a fallas es muy importante en aquellos sistemas que deben funcionar todo el tiempo. La generalización de los activos es usada del inventario de aplicaciones V4.0. Este análisis de tolerancia fue extraído del análisis de registro y por consulta a los profesionales responsables de las aplicaciones.

Tabla 15: Nivel de criticidad

Categoría (función del Negocio)	Proceso (servicios)	Nivel	Tolerancia a Fallas (horas)	Descripción-
Aplicaciones	ARFSIS	B	1	Registro de Prestaciones desde un Punto de Digitación
	PORTAL WEB	B	8	Gestionar los documentos e información pública para los ciudadanos a nivel nacional.
	SIASIS	B	1	Afiliación al seguro, control de entrega de medicamentos, supervisión de expedientes, supervisar casas maternas, intercambio de personal, solicitud de cobertura, atención de emergencia, graficas estadísticas de producción, alta y baja de usuarios, consulta masiva a RENIEC y SUSALUD.

Categoría (función del Negocio)	Proceso (servicios)	Nivel	Tolerancia a Fallas (horas)	Descripción-
	SIGEPS	B	1	Creación y mantenimiento de módulos, submódulos y roles SIGEPS. web services Retroalimentación ARFSIS registro de FUAS PRESTACIONALES Consulta y reporte de atenciones Supervisión médica electrónica Registro de prestaciones económicas de sepelios por COVID-19 Gestiona del libro de reclamaciones virtual Registro de FUAs prestaciones de las IPRESS privadas en el marco del COVID.
	SOASIS	B	4	recepción de tramas de registro de FUAs Consulta de afiliados por web services
	TRAMITE	C	8	Sistema de trámite documentario
	APP	C	8	Aplicativo móvil de afiliaciones virtuales
	MESA DE PARTES DIGITAL	B	4	Gestionar los documentos externos que remiten los ciudadanos, empresas o instituciones
	SGD	B	8	Sistema de Gestión de Trámite Documentario
	SISPAD	C	8	Sistema de procedimiento administrativo disciplinario
	SITEDS	B	4	Generación y gestión de acreditaciones desde las IPRESS
	Correo Electrónico	A	4	Correo electrónico alojado en el centro de datos del SIS
Infraestructura	Centro de datos	A	24	Cuarto De máquinas donde se encuentran los servidores y equipos de comunicaciones
	Base de datos	A	4	Servidores de base de datos
	Seguridad perimetral de red	A	8	Equipos como firewall, proxy etc
	Servidor de almacenamiento	B	8	Servidor de almacén de archivos del SIS
	Red local y de internet	A	8	Switch de red y cableado de red de la entidad
Recursos Humanos	Interno/externo	B	8	Recursos humanos que son trabajadores internos sin distinción de tipo de contrato, proveedores de servicios, locadores, etc.

Fuente: Elaboración propia OGTI

7.2.6 Establecimiento de Tiempos de Recuperación

Una vez identificados los procesos críticos del negocio, se deben establecer los tiempos de recuperación que son una serie de componentes correspondientes al tiempo disponible para recuperarse de una alteración o falla de los servicios; el entendimiento de estos componentes es fundamental para comprender el BIA. Los tiempos de recuperación de describen a continuación:

Tabla 16: Definición de tiempos de recuperación

Tiempo de Recuperación	Descripción
RPO	Magnitud de la pérdida de datos medida en términos de un periodo de tiempo que puede tolerar un proceso de negocio.
RTO	Tiempo Disponible para Recuperar Sistemas y/o recursos que han sufrido una alteración.
WRT	Periodo Máximo Tiempo de Inactividad que puede tolerar la Entidad sin entrar en colapso
MTD	Suma de tiempos RTO y WRT, define el tiempo de inactividad máximo tolerable, es la cantidad de tiempo que un proceso (aplicación, infraestructura) puede interrumpirse sin causar consecuencias inaceptables.

Fuente: Elaboración propia OGTI

Una vez identificados los procesos críticos del negocio, función que hace parte del análisis de los impactos operacionales, se procede a identificar el MTD, que corresponde al tiempo máximo de inactividad que puede tolerar una organización antes de colapsar y se hace la clasificación a fin de priorizar la recuperación del proceso (servicio). Esto quiere decir que si por ejemplo un proceso tiene un periodo máximo de tiempo de inactividad (MTD) de un (1) día, este debe tener mayor prioridad para iniciar el evento de recuperación, en razón al poco tiempo de tolerancia de la inactividad, frente a otros que tienen mayor tolerancia. La prioridad se define según el cuadro de **Clasificación por tipo de interrupción de la continuidad.**

Tabla 17: Clasificación por tiempo máximo de inactividad

Categoría (función del Negocio)	Proceso (servicios)	MTD (en horas) RTO+WRT	Prioridad de Recuperación
Aplicaciones (microservicios)	ARFSIS	24	2
	PORTAL WEB	12	3
	SIASIS	24	1
	SIGEPS	24	1
	SOASIS	8	2
	TRAMITE	8	3
	APP	36	3
	MESA DE PARTES DIGITAL	8	3
	SGD	8	2
	SISPAD	16	3
	SITEDS	8	2

Categoría (función del Negocio)	Proceso (servicios)	MTD (en horas) RTO+WRT	Prioridad de Recuperación
Infraestructura .	Centro de datos	9	1
	Base de datos	9	1
	Seguridad perimetral de red	9	1
	Servidor de almacenamiento	9	1
	Red local y de internet	9	1
Recursos Humanos	Interno/externo	9	2

Fuente: Elaboración propia OGTI

A. Disposición de los RTO/RPO (Recovery Time Objective / Recovery Point Objective)

i. **RTO: Tiempo de Recuperación Objetivo**:
Asociado con la restauración de los recursos que han sido alterados de las Tecnologías de la Información; comprende el tiempo disponible o tiempo tolerable para recuperar recursos alterados.

ii. RPO: Objetivo de punto de recuperación.
Se trata de una métrica que determina cuál es la frecuencia con la que una empresa debe realizar sus copias de seguridad. Esto determinará la cantidad de datos que puede permitirse perder en caso de que suceda un ataque o desastre informático.

Adicionalmente, se aplica el **WRT**, es decir el tiempo que es requerido para completar el trabajo que ha estado interrumpido con el propósito de volverlo a la normalidad.

Tabla 18: Clasificación por tiempo máximo de inactividad

Categoría (función del Negocio)	Proceso (servicios)	Identificación de recursos críticos de Sistemas TI	Tiempo de Recuperación objetivo – RTO (en horas)	Tiempo de Recuperación de Trabajo – WRT (en horas)
Aplicaciones (microservicios)	ARFSIS	• ARFSIS Atención • ARFSIS Procesos Administración de Base de Datos • ARFSIS Procesos • ARFSIS Procesos Configuración ARFSIS • ARFSIS Reportes • ARFSIS Programa salud escolar • SIASIS ARFSIS Consolidación ARFSIS	22	2
	PORTAL WEB	• Consulta en línea	10	2

Categoría del (función Negocio)	Proceso (servicios)	Identificación de recursos críticos de Sistemas TI	Tiempo de Recuperación objetivo – RTO (en horas)	Tiempo de Recuperación de Trabajo – WRT (en horas)
		• Mundo IPRESS • CONVOCATORIAS CAS • PUBLICACION DE CONVENIOS Y CONTRATOS • OTROS ESPORADICOS		
	SIASIS	• IPRESS Privadas - Mixtas: Ambulatoria • Atención: Referencias EsSalud • Evaluación Prestacional: PCPP Subsidiado: • Evaluación Prestacional: RECONSIDERACIONES • Subsidiado: Anulación de Fichas • Afiliación Subsidiado • Independiente - Afiliación • Independiente - Consultas y Reportes • Subsidiado - Afiliación Temporal • Atención: Procedimientos Especiales Sepelio Traslado Asignación por Alimentación • Atención: Salud Colectiva • Catálogos: Personal de Salud Registro de Funerarias • Consulta de Atenciones: Consultas • Supervisor No Tarifado: Seguimiento de solicitudes – Sepelios • Semi subsidiado: Modificación de Datos Reportes y Consultas	22	2

Categoría del (función Negocio)	Proceso (servicios)	Identificación de recursos críticos de Sistemas TI	Tiempo de Recuperación objetivo – RTO (en horas)	Tiempo de Recuperación de Trabajo – WRT (en horas)
		• Afiliación NRUS: Afiliación Presencial Inscripción Recién Nacido Actualización de Datos • Supervisor No Tarifado: Administrar No Tarifado Administrar Sepelios Administrar Casos Especiales Sepelios Sub Componente Prestacional -> Evaluar Prestación" • Supervisor No Tarifado: Administrar Prestaciones 111 • Catálogos: Casas Maternas • Intercambio Prestacional: SME IP • Atención: Cobertura Extraordinaria • IPRESS Privadas - Mixtas: Emergencia -> Atenciones • Catálogos: Registro de Usuarios V2 • Consulta Masiva		
	SIGEPS	• Módulo de seguridad • wsAcreditacion • Retro ARFSIS • Registro de Atenciones • Carga de paquetes ARFSIS • Consulta de atenciones • Reporte de atenciones • Nuevo SME • PES COVID • LIBRO DE RECLAMACIONES • IPRESS PRIVADAS	22	2
	SOASIS	• Recepción de tramas • Consulta de afiliados	7	1
	TRAMITE	Gestión de Tramite	7	1
	APP	• Consulta de afiliados	34	2

Categoría del (función Negocio)	Proceso (servicios)	Identificación de recursos críticos de Sistemas TI	Tiempo de Recuperación objetivo – RTO (en horas)	Tiempo de Recuperación de Trabajo – WRT (en horas)
		• Consulta de planes de seguro • Afiliaciones virtuales		
	MESA DE PARTES DIGITAL	• Registro de documentos externos • Administración	7	1
	SGD	Gestión de Tramite Documentario	7	1
	SISPAD	• Registrar Expediente • Actualizar Expediente • Asignación de Expediente • Etapa de Investigación Preliminar • Etapa de Procedimiento Administrativo Disciplinario • Recurso Impugnatorio • Segunda Instancia • Reportes	14	2
	SITEDS	• Generación de acreditaciones desde las IPRESS • Consulta de histórico • Reimpresión de acreditaciones	7	1
	Correo Electrónico 1	Sistema de correo electrónico en nube	8	1
	Correo Electrónico 2	Sistema de correo electrónico Zimbra en centro de datos	8	1
Infraestructura .	Centro de datos	Servidores donde se alojan todos los sistemas, distintas marcas	8	1
	Base de datos	Sistemas de almacenamiento y administración	8	1
	Seguridad perimetral de red	Firewall /proxy	8	1
	Servidor de almacenamiento	Sistema back up Almacén de cintas Servidor de archivos	8	1
	Red local y de internet	Servicio internet Telefonía IP local Equipo de distribución de red local física e inalámbrica	8	1
Recursos Humanos	Interno/externo	Personal profesional y técnico	8	1

Fuente: Elaboración propia OGTI

7.3 Fase 3: Determinación de las Estrategias

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

7.3.1 Estrategias de prevención de tecnologías de la información

A. Almacenamiento y respaldo de la información (BACKUPS)

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

B. Sitios Alternos para el Centro de Datos

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

- Propios de la entidad.
- Instalaciones alquiladas.

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

C. Evaluación y gestión de proveedores

Listado de proveedores claves de servicios y recursos de TI, con sus datos de contacto actualizados.

Mantener listas detalladas de necesidades de equipos y sus especificaciones técnicas.

Si es necesario, adquirir o habilitar hardware y software, así como transportarlos al sitio alterno de ser el caso; las estrategias básicas para disponer de equipo de reemplazo serán:

- Acuerdos con proveedores: Establecer acuerdos de nivel de servicios con los proveedores de software, hardware y medios de soporte; se debe especificar el tiempo de respuesta requerido.
- Equipos de respaldo: Los equipos requeridos se compran por adelantado y se almacenan en una instalación segura externa[1].
- Equipo compatible existente: Equipo existente en sitios alternativos.

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

D. Entrenamiento y personal de reemplazo

Todo el personal de la OGTI, debe entrenarse en el proceso de recuperación de los servicios de TI. La capacitación debe ser planificada, estructurada y acorde con las exigencias de recuperación. El entrenamiento se debe evaluar para verificar que ha logrado sus objetivos.

Se debe elaborar un programa de vacaciones que garantice la presencia permanente del personal crítico de las diferentes áreas y procesos de OGTI, tales como soporte técnico, redes y comunicaciones, sistemas de información y bases de datos, así como seguridad de la información.

Elaboración de una base de datos de conocimiento, en caso el personal encargado de ciertos procedimientos, tanto principal, como de reemplazo se encuentren indispuestos.

E. Renovación tecnológica

Programación de dos revisiones anuales de obsolescencia tecnológica de las partes internas de los servidores informáticos, para realizar la renovación de las mismas, en caso se requiera.

Registrar las incidencias de deterioro de los equipos de almacenamiento, procesamiento y comunicaciones, para en base a las estadísticas de este registro adquirir equipos de contingencia.

F. Activación de trabajo remoto

Verificación y validación de acceso seguro, en remoto, a los sistemas y servicios por la OGTI.

Activación de redes virtuales VPN, siempre y cuando el equipo a conectarse cuente con los mecanismos de seguridad informáticos necesarios.

En caso el usuario no cuente con un equipo para realizar su trabajo remoto, se le pueda habilitar el equipo asignado, que se encuentra en la Sede Central del SIS, para entregársela en su domicilio a fin de que cuente con las herramientas necesarias, siguiendo los protocolos dados por la Oficina de Abastecimiento.

Realizar el Trámite Certificados digitales, para instalarlos en los equipos de los usuarios, fuera de la entidad.

Activación del desvío de las llamadas telefónicas a los usuarios asignados encarados de la atención de la central telefónica.

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

7.3.2 Estrategia frente a emergencias en tecnologías de la información

El alcance de las estrategias frente a emergencias involucra las acciones que deben realizarse durante una emergencia o desastre, a fin de salvaguardar la información del SIS y garantizar la continuidad de los servicios informáticos para lo cual se definen las acciones para mitigar las pérdidas que puedan producirse en una emergencia o desastre. A continuación, se citan las acciones que se realizarán durante y después de una contingencia:

A. Acciones durante la contingencia

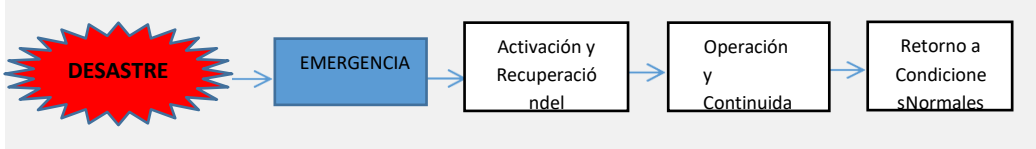
- Estudiar y evaluar el alcance del desastre en cada área de responsabilidad.
- Notificar y reunir a los demás integrantes del equipo de Emergencia y Restauración de TIC o la que haga sus veces.
- Informar al responsable del Grupo de Comando de Continuidad Operativa o la que haga sus veces, sobre la situación presentada, para decidir la realización de la Declaración de Contingencia y activación del sitio alterno o de respaldo.
- Determinar si el área afectada es segura para el personal (en caso de catástrofe).
- Estudiar y evaluar la dimensión de los daños a los equipos y sus facilidades, y elaborar un informe de los daños producidos.
- Proveer facilidades al personal encargado de la recuperación, con la finalidad de asegurar que se realicen las tareas asignadas en los procedimientos que forman parte de este plan.

7.3.3 Estrategia para la restauración de tecnologías de la información

El alcance de las estrategias para la restauración o recuperación involucra las acciones que deben realizarse luego de suscitada una emergencia o desastre, a fin de recuperar la información y los servicios informáticos del SIS para estabilizar la infraestructura tecnológica luego del evento suscitado. Para lo cual se definen las pautas que permitan al personal de la OGTI garantizar la continuidad de las operaciones en la entidad.

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

Gráfico 3: Ciclo de la estrategia de recuperación de TI



Fuente: Elaboración propia OGTI

La priorización de la restauración de los servicios de tecnologías de información del SIS se ejecutará de acuerdo a lo indicado en la siguiente Tabla de información:

(Ver tabla en la siguiente página)

Tabla N° 19 Prioridad de atención durante la restauración de TIC

Prioridad de Atención	Descripción
1	Atención prioritaria: Sistemas de información y equipos que requieran alta disponibilidad de atención a los usuarios externos y manejen alto volumen de información. Ejemplo: El Sistema de Gestión Documental (SGD), Sistema Administrativo Financiero (SIAF), Sistema de gestión administrativa (SIGA), Portal Web institucional, servidores de bases de datos, dominio de red (Directorio Activo), servidor de archivos compartidos, correo electrónico institucional (@ipsresspublicas, @sisext.pe y @sisservicios.gob.pe), campus virtual, sistema de administrativo de personal, sistema de planillas del personal, sistema de control de asistencias, ARFSIS, SIASIS, SIGEPS, SOASIS, consulta de afiliados, mesa de partes digital, SISPAD, SITEDS, plataforma de interoperabilidad, Sistema de Inteligencia de Negocios, sistemas estadísticos 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.

Fuente: Elaboración propia OGTI

En la Tabla N° 1, 4 y 5; se detallan los sistemas de información y equipos informáticos, con la respectiva prioridad de atención, en caso de activarse la contingencia informática.

7.3.4 Acciones después de la contingencia

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

7.4 Fase 4: Elaboración del Plan de Contingencia y Recuperación de Servicios de TIC

Una vez identificados los eventos de contingencia y los escenarios de riesgos, se desarrollan los Planes de Contingencia agrupados por las categorías indicadas previamente.

El Plan de Contingencia y Recuperación de los Servicios de Tecnología de la Información y Comunicaciones comprenderá los eventos de mayor impacto, identificados en la Matriz de Riesgo de Contingencia, los cuales serán abordados en formatos independientes, tal como se indica en el siguiente cuadro:

Tabla 20: Eventos de mayor impacto para el Plan de Contingencia Informático

N°	Evento	Exposición al Riesgo
1	Terremoto /Sismo	Extremo
2	Delito informático (ataque)	Extremo
3	Falla de hardware y software	Extremo
4	Falla del suministro eléctrico en elCentro de Datos y gabinetes de comunicación.	Alto

Fuente: Elaboración propia OGTI

7.5 Fase 5: Definición y Ejecución del Plan de Pruebas

Esta estrategia define los aspectos básicos que requieren ser probados periódicamente, a fin de medir el comportamiento integral e individual de los recursos asignados y/o los procedimientos definidos para la atención de una interrupción de un servicio de TIC.

7.5.1 Tipos y Frecuencia de pruebas

La programación de las pruebas obedece a varios factores entre los cuales se pueden mencionar:

- Programación periódica establecida con los equipos de administración de sistemas de información y plataforma tecnológica como mecanismo de control de calidad de la función de contingencia. (por ejemplo, después de la terminación de un proyecto, a los tres (3) meses y posteriormente cada 6 meses).
- Cuando se realicen modificaciones de hardware, software operativo, de infraestructura y/o aplicativos; o cuando existan cambios significativos en la plataforma tecnológica cubierta por el Plan.
- También pueden realizarse cuando se prevea el riesgo de que suceda un evento que afecte la entidad, como problemas laborales o de orden público.

Desde el punto de vista del cubrimiento o alcance, los tipos de pruebas pueden ser:

A. Pruebas de escritorio (Detallada y documental)

Se trata de un tipo de prueba programada y controlada que consiste en una revisión detallada del Plan de Contingencias de TIC y los procedimientos implicados. Para su ejecución se verifica la existencia del plan y sus procedimientos, y se convoca a los diferentes funcionarios de la OGTI responsables del proceso o sistema de información a participar en un taller en donde se da lectura al plan en forma ordenada, bajo la moderación del responsable del Plan con el fin de determinar fallas y omisiones con el criterio experto de quienes participan. En este ejercicio se tienen en cuenta las dependencias de las diferentes actividades.

Es recomendable ejecutar este tipo de prueba antes de ejecutar una prueba real y una vez sea publicada alguna actualización del presente

Plan. Es obligatorio usar la documentación propuesta para las simulaciones y registro de ejercicios.

B. Pruebas reales (Tecnológicas)

Este tipo de prueba puede ser parcial o total, donde se prueban secciones o elementos individuales del Plan, como puede ser, un aplicativo o una plataforma o se prueban todos los componentes. Las pruebas reales son cinco, de las cuales la selección de las que se vayan a realizar lo determina el director del Plan o en su defecto el líder del Plan.

C. Prueba General

Consiste en probar el desempeño de la plataforma tecnológica designada para las contingencias en un ambiente de interrupción total, la cual consiste en realizar un simulacro donde se compruebe de manera integral la ejecución de las siguientes actividades:

- Pruebas de suministro de energía eléctrica (Corte del servicio de energía y verificación de la entrada de las UPS en funcionamiento, luego a paso de grupo electrógeno).
- Prueba del canal de respaldo del servicio de Internet.
- Desconexión del canal principal de Internet y verificación que el canal secundario sigue en conexión.
- Puesta en producción de los equipos de respaldo y sistemas de información del SIS ubicados en la sede alterna y que se encuentran en calidad de contingencia. (se debe de crear un plan que contemple un centro de datos alterno ya sea físico o en nube y un grupo de equipos de cómputo que esté disponible fuera de las instalaciones de la sede central, estos equipos que por su naturaleza deben de tener las mismas características técnicas que los equipos de los operadores, tendrán su propio plan de mantenimiento y ejercicio como simulacro de activación y desactivación.
- Recuperación de la información de las copias de respaldo de información, para verificar su correcto proceso de restauración (de acuerdo con lo descrito en el Procedimiento para la Realización y Control de Copias de Respaldo).

D. Pruebas de suministro de energía eléctrica

Los sistemas de alimentación de energía eléctrica y el sistema de alimentación ininterrumpida que consta de un grupo electrógeno y el UPS (por sus siglas en inglés - Uninterruptible Power Supply), son el sistema que garantiza la energía eléctrica ininterrumpida a la sala de servidores del SIS, cuando haya una suspensión de este servicio.

La prueba consiste en verificar la activación automática de la puesta en marcha de la UPS y grupo electrógeno cuando se suspende la energía eléctrica. Adicionalmente se puede realizar prueba de autonomía, la debe mantener el suministro energía a los equipos conectados a la red eléctrica regulada, medir el tiempo y la carga del pase de energía al grupo electrógeno.

Las pruebas sirven para realizar mediciones y pruebas del sistema de regulación de voltaje que consta del módulo de control (bypass) y del sistema de trasferencia automática (ATS) del sistema de respaldo del centro de datos.

E. Prueba de Canal de Respaldo del Servicio de Internet

Consiste en desconectar el canal activo del servicio de Internet, para que entre en servicio la redundancia de este, la prueba se realiza con servicios activos e inactivos y estos deberán continuar funcionando en tiempo real sin inconvenientes.

F. Prueba de Puesta en Producción de los Equipos de Respaldo

Consiste en instalar y preparar los equipos de contingencia de los sistemas definidos por el equipo de contingencias, los cuales serán ubicados en una sede alterna o en la locación definida para la prueba, con las características técnicas requeridas de acuerdo con los servicios de TI que se requieran con el fin de verificar el funcionamiento y puesta en producción, estos equipos deben de figurar con un nivel de atención muy alto por su importancia de la ejecución del plan.

G. Prueba de Restauración de Información

Consiste en realizar una restauración de las copias de seguridad más reciente que se tienen de los sistemas de información y/o aplicativa que seleccione el responsable del Plan de Contingencias Informático, utilizando los procedimientos existentes de restauración y verificar la comunicación entre los aplicativos y las bases de datos.

H. Prueba de seguridad de aplicaciones (AST)

Este análisis debe de realizarlo un especialista en ciberseguridad calificado y cuya única función es el análisis de seguridad de la OGTI. Estas pruebas garantizan que las aplicaciones estén libres de vulnerabilidades y riesgos, y reduce la superficie de ciber ataques. Según su necesidad se requerirán de 2 tipos.

i. **SAST (Prueba de seguridad de aplicaciones estáticas).**
   Consiste en realizar pruebas en su código fuente en reposo para identificar todas las fuentes de vulnerabilidad (ejemplo: inyección SQL)
   Se ejecuta siempre antes de cada lanzamiento de proyecto o actualización o despliegue, se ejecuta como un ejercicio White box.

ii. **DAST (Prueba de seguridad de aplicaciones dinámicas).**
   Consiste en observar el comportamiento de la aplicación. Se realiza en una aplicación en funcionamiento y requiere que este se ejecute para interactuar con ella y evaluarla. Recopila información y genera escenarios de prueba de ataque.

I. Prueba de reemplazo de personal

Consiste de inhabilitar al profesional responsable de la actividad del plan y verificar los tiempos de respuesta ejemplo (tiempo de llegada a

las instalaciones desde su residencia y/o tiempo de conexión y solución al incidente).

Evaluación de la prueba
Una vez se haya realizado la prueba y como actividad final, es necesario efectuar una evaluación o revisión de su desarrollo en la cual estén analizados los objetivos, los parámetros, los criterios establecidos, las fallas y fortalezas.

7.5.2 Etapas de la Prueba

Se enfoca en simulaciones de contingencia en caso de incidencias producidas sobre los equipos, información y los procesos manejados en situaciones reales, en estas situaciones hipotéticas los respaldos son empleados quedando registro de una copia como punto estable.
Se diseña un consunto de casos de pruebas funcionales, estos casos pueden ser elegidos de la matriz de riesgos, escogiendo claro está el riesgo con el nivel más aceptable y según la complejidad escalar hasta los riesgos que generen más impacto; estos eran ejecutados por los equipos de la OGTI; el resultado de la prueba verificara cualquier incidencia que se origine durante dicha prueba y a fin de tener un registro histórico y retroalimentar cualquier acción que pueda actualizar el plan.

Todo lo desarrollado en los planes de pruebas tendrán el siguiente esquema: Revisar Anexo 3: Documentación de Pruebas del Plan de contingencia Informático.

- Descripción de la prueba (detalle, objetivos previos, etc.).
- Alcance (áreas afectadas/ personal involucrado).
- Resultados (detalle, paso a paso de la actividad simulada y paso a paso real).

A continuación, se presentan las etapas que se deben realizar para el desarrollo de una prueba al Plan.

Tabla 21: Etapa de prueba ejemplo

ETAPA	DESCRIPCION
Planeamiento de la prueba	Definir los equipos participantes, los objetivos específicos de la prueba y confirmar con la localidad alterna la fecha y hora de realización.
Notificación de la prueba a los equipos de trabajo.	Notificar a los equipos participantes la realización de la prueba y verificar que todos ellos estén enterados.
Alistamiento y habilitación de los sitios alternos para la prueba.	Incluye contar con todos los elementos necesarios para iniciar el proceso de prueba.
Puesta en producción de los equipos de cómputo o sistemas de información en la sede alterna que se haya determinado para la prueba.	Actividades de los equipos de recuperación tendientes a restaurar y sincronizar los Aplicaciones.

ETAPA	DESCRIPCION
Operación en los sitios alternos para la prueba.	Actividades de los equipos de recuperación tendientes a probar la operación en los sitios alternos para los equipos de contingencia.
Limpieza de los datos después de la prueba.	Borrar todos los archivos sensibles en la localidad alterna de contingencia.
Evaluación de la prueba	Reunirse con el personal que participó en la prueba para identificar problemas y aciertos del plan de contingencia de TI.

Fuente: Elaboración propia OGTI

Documentación de las Pruebas
Para realizar el registro de la ejecución de las pruebas al Plan de Contingencias, se utilizará el formato descrito en el Anexo 3 – "Formato de Documentación de Pruebas del Plan de Contingencias de TI" de este documento.

7.6 Fase 6: Implementación del Plan de Contingencia

El Plan aplica las actividades necesarias para mantener operantes y/o reestablecer los servicios de TI, sistemas de información, aplicativos y la infraestructura tecnológica que los soporta. Para su implementación es necesario tener en cuenta las estrategias del Plan de Contingencia que hace parte integral de este documento, y que, por contener instructivos, es solo para uso del personal encargado de cada sistema o infraestructura., el formato debe de seguir la línea de eventos de antes, durante y después del incidente.

Antes: Refiere a la prevención, como un conjunto de ejercicios que mitigan la probabilidad de ocurrencia de un incidente u ocurrencia.
Durante: Es el conjunto de acciones a realizar cuando se presenta un incidente y activa la contingencia.
Después: Refiere a la recuperación y pruebas, estas acciones reestablecen oportunamente la continuidad de las operaciones de la OGTI de los recursos afectados por el evento de contingencia.

Para considerar el tiempo que se necesita para el adecuamiento al plan, la implementación de éste se realizará el tercer mes después de su aprobación.
Para efecto de cumplimiento, el Oficial de Seguridad y de Confianza Digital junto a la Dirección Ejecutiva y la dirección de línea deben de supervisar el cumplimiento y exigir que las herramientas diseñadas para este plan sean usadas con el fin de mantener los registros.

Después del análisis de riesgos y de impacto se desarrollan planes agrupados por los eventos más comunes y de mayor impacto que fueron identificados en la Matriz de Riesgos, estos serán abordados de manera independiente según lista:

A. SISMO. – Formato Contingencia Sismo

Para considerar un sismo como un plan de contingencia propio se toma en cuenta el impacto producido y las consecuencias acumuladas por el evento ya que por su valor de riesgo no lo califica como alto o extremo pero si sus consecuencias acumuladas ya que al presentarse un evento sísmicos es probable que todas las amenazas identificadas para el centro de datos y área de operaciones de la OGTI (el total del inventario de activos) en la matriz de

riesgos todas se manifiesten a la vez o por partes, por lo que se considera un plan propio para eventos sísmicos.

B. FALLA DE SUMINISTRO ELÉCTRICO. - Formato Contingencia Falla de Suministro Eléctrico

Se considera este plan por ser un evento que dentro de análisis de riesgos es repetitivo y se considera generar un plan por la relación que implica y la necesidad del ejercicio ante los incidentes.

C. DELITO INFORMÁTICO. - Formato Contingencia Delito Informático

Se considera este punto por necesidad, existe dentro del análisis de las calificaciones considerado como grave de múltiples puntos. Además de que en la actualidad los ejercicios de seguridad informática y de información deben de ser continuos.

D. FALLA DE HARDWARE Y SOFTWARE. – Formato Falla de Hardware y Software

Se considera este punto por ser recurrente en el ejercicio de las actividades de la OGTI, en el análisis de riesgos se de muestran como grave todo lo relacionado con hardware y software de la OGTI.

7.7 Fase 7: Monitoreo

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

A continuación, se enumeran las actividades principales a realizar:

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

8 ANEXOS

Anexo 1 Gestión de Incidentes

Anexo 2 Formatos del Plan de Contingencia Informático y Recuperación de Servicios de Tecnologías de la Información y comunicaciones por evento de riesgo.

Anexo 3 Formato de Control y certificación de las Pruebas del Plan de Contingencia y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones.

Anexo 4 Matriz de Riesgo.

Firmado digitalmente por ORTEGA ROJAS Juan Fredy FAU 20505208626 hard
Motivo: Doy V° B°
Fecha: 06.10.2023 15:33:23 -05:00

Firmado digitalmente por AMBROCIO DOROTEO Teofilo FAU 20505208626 hard
Motivo: Doy V° B°
Fecha: 06.10.2023 15:12:35 -05:00

Firmado digitalmente por REINOSO ZEGARRA Jose Hugo Martin FAU 20505208626 hard
Motivo: Doy V° B°
Fecha: 06.10.2023 15:03:31 -05:00

ANEXO 1

GESTION DE INCIDENTES

	Gestión de incidentes	Versión: 01
	Informe de causas	Fecha: 02/11/2022
		Página 1 de 6

Aplicación	:	**Nombre de la aplicación**
Atención	:	Nombre del usuario
Fecha	:	Fecha de incidente
Asunto	:	Detalle de Incidente
Ticket(s)	:	Numero Tickets relacionados al incidente
Revisado por	:	Nombre del Soporte - Cargo

	Gestión de incidentes	Versión: 01
	Informe de causas	Fecha: 02/11/2022
		Página 2 de 6

1. RESUMEN EJECUTIVO

Resumen general, con fecha, hora y número de ticket, servicio afectado e impacto (del SGSI o análisis del plan de contingencias), si hay afectación adicional, se debe detallar la causa raíz, la solución paso a paso y plan de acción usado (esto es a criterio del profesional, los planes de acción pueden o no ser documentada)
Esto debe ser llenado por el soporte a cargo y revisada por su coordinador, el documento se adjunta formando grupos según criterio profesional.

Para registro de bitácora:

Servicio(s) Afectados:	<<Nombre del servidor o aplicación>>		Impacto:	Alto, medio, bajo
			Estado:	ABIERTO CERRADO
Duración del Incidente:	Inicio desde reporte DD/MM/AA hh:mm:ss	Fin desde reporte DD/MM/AA hh:mm:ss	Tiempo de Indisponibilidad:	XX hrs y xx min

2. ANÁLISIS DE LA CAUSA RAIZ

Este punto detalla las actividades que se realizaron para encontrar la causa raíz (detalle de marca de hora cuando el operador encuentra la falla), tiene como objetivo el registro histórico de incidentes, las evidencias se colocan en anexos.

a. Se recibe reporte que usuario perdió conexión
b. Se revisa registro de su última conexión
c. Se revisa la aplicación
d. etc

(el orden del análisis lo definirá un futuro como buena práctica)

RCA (ACR) – Usando Metodología de los 5 ¿Por qué?
¿Por qué? # 1: Primera causa por que falla ejm: usuario no se conecta
Respuesta # 1:.por qué paso
¿Por qué? # 2: porque paso la falla ejm, se desconectó tarjeta de red
Respuesta # 2: por que sucedió
¿Por qué? # 3: por qué sucedió la falla ejm, usuario movió equipo o limpieza lo hizo
Respuesta # 3: por qué razón
¿Por qué? # 4:
Respuesta # 4:
¿Por qué? # 5:
Respuesta # 5:

Causa Raiz
El usuario XXX reporta que no tiene conexión, se revisa reportes de conexión xxx y al verificar físicamente se encuentra tarjeta desconectada

3. PLANES DE ACCIÓN

Se detalla recomendaciones inmediatas o de corto o mediano plazo, la decisión de aplicación de solución de incidentes debe de ser coordinadas con el usuario siempre presente.
Se cierra el incidente cuando la actividad termine
El seguimiento lo debe de hacer el coordinador de área o un responsable encargado quien revise calidad de servicio.
En caso de una actividad que tome mas tiempo de lo esperado (las métricas se usarán después del registro para las buenas prácticas), el coordinador de área o responsable encargado deberá de monitorear la solución y cierre.

PLAN DE ACCIÓN DURANTE EL INCIDENTE			
Actividad	**Responsable**	**Hora Realizado**	**Estado**
Acción realizada para recuperar el servicio	Especialista	Fecha y Hora	Cerrado
Acción realizada para recuperar el servicio	Especialista	Fecha y Hora	Cerrado
PLAN DE ACCIÓN POST INCIDENTE			
Actividad	**Responsable**	**Fecha de Compromiso**	**Estado**
Revisión de eventos. Encontrando la causa de la indisponibilidad.	Especialista 1	xx/xx	Cerrado
Descripción de la actividad propuesta	Especialista responsable	Fecha	Abierto
PLAN DE ACCIÓN DE MEJORAS			
Actividad	**Responsable**	**Fecha de Compromiso**	**Estado**
Solicitar incluir en la Política de Monitoreo al servidor	Gestión	Fecha	Abierto
Se recomienda instalar licencia de RD porque el periodo de gracia expiro. (Evidencia 4)	Gestión	Fecha	Cerrado

4. CONCLUSIONES

Se detalla el resultado final con un resumen desde la causa.

5. ANEXOS

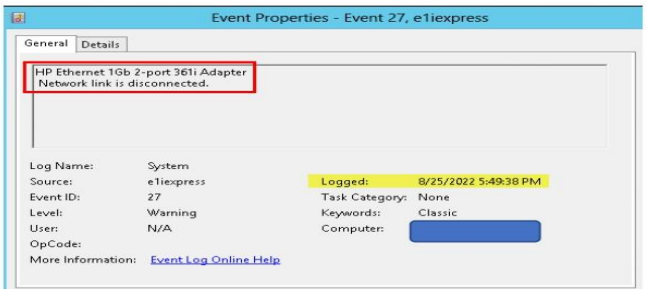
Se deberán colocar las evidencias correctamente codificadas
a) Cronología del incidente

Ejemplo de Cronología:

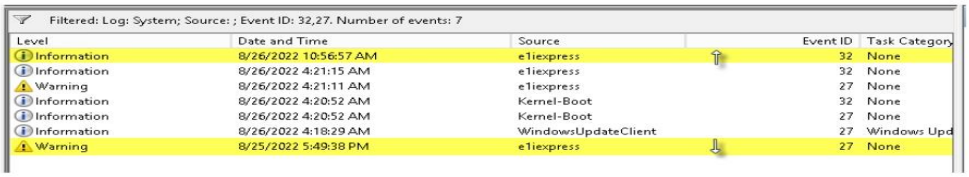
DETECCIÓN DEL EVENTO	
xx/NOV 09:00 am	Se generó el ticket XXXXX a partir de la alerta del evento XXXXXXXXX
xx/NOV 09:110 am	USUARIO notificó que el sistema ABC empezó a mostrar mensajes de error
DURANTE EL EVENTO	
xx/NOV 10:00 am	Se verifica servicios de conexión desde servidor
xx/nov 10:10 am	Se verifica perdida de conexión con el enlace

POST EVENTO	
xx/nov 10:15 am	USARIO informa que se restablece el acceso
xx/nov 10:20 am	Se revisa los eventos. Encontrando tarjeta de red Principal desconectada de forma manual.

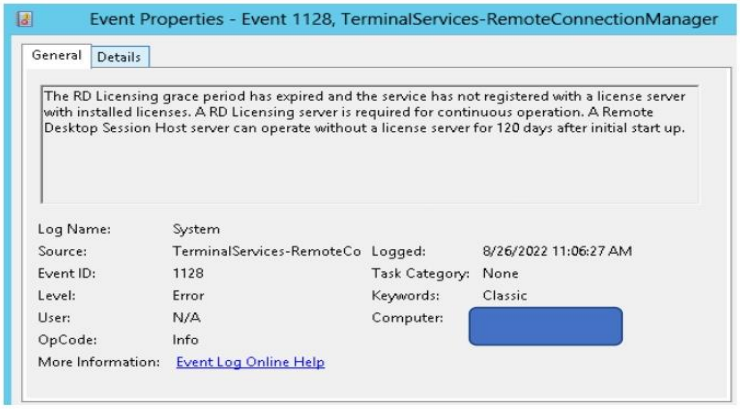
b) Evidencia 1 – Tarjeta de red desconectada.



c) Evidencia 2 – Tarjeta de red conectada



Evidencia 4 – Licencia RD expirada.



ANEXO 2
FORMATOS DEL PLAN DE CONTINGENCIA INFORMÁTICO Y RESTAURACIÓN DE SERVICIOS DE TIC

1. FORMATO EVENTO TERREMOTO/SISMO

SIS Seguro Integral de Salud	FORMATO EVENTO SISMOS	Código formato ----
		Código documento: XXXX -00X
		Página 1 de 1

1. ANTES

a. Descripción del evento

Evento natural no detectable en el largo plazo, se genera al interior de manto terrestre y genera una repentina liberación de energía que propaga energía en forma de ondas provocando el movimiento de las capas superiores de la tierra.

EL entorno del evento afecta a:

- Infraestructura de centro de datos
- Infraestructura de área de operaciones de OGTI
- Infraestructura de equipos de computo de usuarios de la OGTI
- Recursos humanos de la OGTI
- Infraestructura de la sede central del SIS.
- Ciudad de Lima

b. Objetivo

Establece ejercicios con el fin de, en momento de un siniestro, minimizar el tiempo de interrupción de las operaciones del SIS y evitar la exposición l riesgo de los trabajadores de la OGTI.

c. Personal encargado

Es el equipo conjunto de la OGTI como equipo de respuesta ante incidentes, siguiendo el lineamiento de jerarquía propuesto por la directriz del plan de contingencia. Según su jerarquía establecen los lineamientos que deben cumplir cada parte del equipo.

Condición para prevenir el riesgo

- Simulacros de evacuación continua y capacitación de la misma, en coordinación con todas las oficinas del SIS para hacer ejercicio del plan de evacuación. (brigada de emergencia)
- Inspección continua de seguridad
- Revisión y mantenimiento continuo de señalética y equipos de emergencia (luces, salidas, etc)
- Definición de puntos de reunión en caso de evacuación y horario de comunicación post siniestro.
- Estudio de tiempo de reacción de apagado de emergencia de centro de datos, centro de energía y red eléctrica de la oficina.
- Establecer, ejecutar y supervisar los procedimientos de respaldo y restauración de servicios.
- Mantener un inventario del centro de datos y equipo de OGTI detallado continuo.

- Establece, ejecutar y supervisar los planes de mantenimiento al centro de datos, sistema de back up, grupo electrógeno, central de energía, comunicaciones y equipos de cómputo de la OGTI.

2. DURANTE

a. Activación de contingencia

Al ocurrir un sismo. Se activa de manera inmediata sin desprecio del grado telúrico. El líder de continuidad activa la contingencia.

b. Actividades

Se ejecuta la evacuación del personal previo apagado completo de emergencia del centro de datos y equipos de OGTI. (botón de pánico)

c. Personal encargado

Personal de nivel operativo del plan.

d. Actividades en la activación de plan de contingencia.

- Desconectar el suministro eléctrico de la oficina usando el botón de pánico.
- Evacuar las oficinas de acuerdo a los brigadistas de evacuación usando las rutas establecidas en el ejercicio de los simulacros. Deben y tienen que hacer seguimiento de las disposiciones de los brigadistas elegidos.
- Alejarse de cualquier material que pueda desprenderse de la infraestructura del edificio (ventanas, techo técnico, etc.)
- Al retirarse de las instalaciones en el punto de reunión establecido, pasar lista de los asistentes de la oficina, de faltar alguno se deberá brindar la alerta de persona faltante.
- La ayuda medica en caso se necesite deberá ser atendida por el personal designado
- La evacuación debe de ser calmada y dentro de los tiempos establecidos por los simulacros previos.
- El tiempo evento total será determinado por el grado del sismo y probabilidad de replicas y daños a la infraestructura.
- Esperar al llamado de calma.

3. DESPUÉS

El personal encargado son los gestores del plan de contingencia de la OGTI

a. Actividades

Las actividades deben de estar orientadas según el ejercicio que tengan y en el menor tiempo posible y si el nivel de afectación es crítica en el centro de datos, la responsabilidad de la actividad es monitoreada por los gestores del plan.

En caso que el evento sea de considerable magnitud, se deberá:

- Solo se retorna después del llamado de calma y/o por recomendación de las autoridades o el responsable de brigada.
- Al retornar a las oficinas solo el personal encargado podrá encender los equipos de la OGTI (centro de datos, comunicaciones, central de energía,

etc). Cuando el llamado de calma se manifieste y según evaluación técnica de mantenimiento por posibles cortos eléctricos.

- El personal de nivel operativo deberá de realizar una evaluación de daños en la infraestructura técnica de la OGTI y demás oficinas afectadas.
- EL personal de nivel operativo debe de realizar el inventario de los equipos según su responsabilidad.
- Se debe realizar inventario de la documentación
- Considerar limpieza y orden de las áreas afectadas si en caso se requieran. Esta acción se debe coordinar con el personal de mantenimiento.
- Revisar la disponibilidad de los recursos después del inventario (manuales técnicos, hardware y copias de respaldo)
- De tener un centro alterno, proceder con la activación inmediata después del llamado de calma, solicitar y mover las cintas de respaldo al sitio.
- Mantener el contacto con los proveedores de servicios clave y terceros para instrucciones y notificación de requisitos de ayuda.
- Supervisar el progreso de recuperación
- Recuperación en sitio alterno: si la infraestructura de la OGTI está comprometida, el equipo encargado de la restauración deberá migrar a un sitio alterno con todas las facilidades que se exijan para el cumplimiento de las restauraciones, sus tareas serán las siguientes:
  - Ejecutar los procesos de recuperación del centro de datos en los sistemas afectados
  - Verificar que las aplicaciones restauradas y estén en pleno funcionamiento
  - Documentar y confirmar los puntos de recuperación
  - Reportar el nivel de perdida de datos desde la última restauración
  - Verificar que los equipos periféricos básicos de oficina estén funcionando.
- Finalizando la actividad de restauración retornar al sitio original
- Informar la perdida de infraestructura y solicitar la reposición.

b. Reportes

Los gestores del Plan de Contingencia de la OGTI deben de presentar un informe al responsable del plan de contingencia de la OGTI.

c. Desactivación del plan de contingencias.

El líder del plan de contingencia anuncia la desactivación.

d. Actualización.

Los registros se usan como base de conocimiento para la actualización del plan.

2. FORMATO EVENTO FALLA DE SUMINISTRO ELECTRICO

SIS Seguro Integral de Salud	FORMATO FALLA DE SUMINISTRO ELECTRICO	Código formato ----
		Código documento: XXXX -00X
		Página 1 de 1

1. ANTES

a. Descripción del evento

El corte del suministro de energía eléctrica del centro de datos o en la sede central de la entidad.

EL entorno del evento afecta a:

- Parque de computo
- Centro de datos
- Equipos de comunicaciones.
- UPS
- Aire acondicionado
- Grupo electrógeno

b. Objetivo

Restablecer la operatividad de los equipos y servicios que brinda la OGTI después de restablecer la energía eléctrica y detener la amenaza.

c. Personal encargado

Es el equipo gestor del plan de contingencia de la OGTI como equipo de respuesta ante incidentes, siguiendo el lineamiento de jerarquía propuesto por la directriz del plan de contingencia. Según su jerarquía establecen los lineamientos que deben cumplir cada parte del equipo.

Condición para prevenir el riesgo

- Plan de mantenimiento preventivo y correctivo a los equipos UPS y a la infraestructura que lo alberga, este plan debe de ser revisado anualmente.
- Plan de mantenimiento preventivo y correctivo al grupo electrógeno y sistema eléctrico (cableado, cuchillas, bypass, ATS)
- Realizar pruebas periódicas de los equipos UPS.
- Asegurar que la autonomía de energía de los UPS par el centro de datos no sea menor a 30 min.
- Asegurar que se cuente con respaldo de energía los periféricos del centro de datos como aire acondicionado, puerta de seguridad, cámaras de vigilancia, etc.
- Asegurar que existan líneas de alimentación continua al personal estratégico de la OGTI, con el fin de realizar los respaldos y apagado seguro del centro de datos.
- Revisión del cableado eléctrico de la OGTI y las demás oficinas del SIS.
- Revisión del pozo a tierra anualmente.
- Revisión de equipos de luces de emergencia.
- Se debe de realizar simulaciones de apagado y corte de energía del centro de daos.

2. DURANTE

a. Activación de contingencia

Al ocurrir un corte de servicio por algún evento. Se activa de manera inmediata. El líder de continuidad activa la contingencia.

b. Personal encargado

Personal de nivel operativo del plan.

c. Actividades en la activación de plan de contingencia.

- Dependiendo del evento se recomienda la evacuación del personal si en caso exista un siniestro usando el botón de pánico para detener todos los servicios de la OGTI
- Si el evento es menor el personal deberá monitorear el pase inmediato de energía de los UPS al centro de datos, deberá dirigirse al cuarto de maquinas donde alberga el grupo electrógeno para monitorear su encendido.
- Se debe de mantener con combustible al grupo electrógeno hasta que retorne el fluido eléctrico de no ser así, si es necesario el apagado del centro de datos, se debe recurrir a la actividad de apagado seguro del centro de datos.
- Informar al responsable del plan para que se comunique con la oficina de abastecimiento del problema presentado y también de necesitar combustible para el grupo electrógeno.
- Comunicar a la empresa prestadora de servicios de energía eléctrica la falta de fluido eléctrico.

3. DESPUÉS

El personal encargado son los gestores del plan de contingencia de la OGTI, definirán la responsabilidad de las actividades según corresponda su función.

a. Actividades

- Se debe de confirmar con el proveedor de fluido eléctrico la no existencia de nuevos cortes o fluctuación de energía.
- Encender el centro de datos siguiendo el procedimiento apagado y encendido del centro de datos.
- Reiniciar todos los servicios del centro de datos
- El equipo de soporte deberá revisar si existen equipos afectados por el corte de fluido y proceder a su reparación
- Registrar los eventos para bitácora
- Comunicar el restablecimiento de los servicios informáticos del SIS.

b. Reportes

Los gestores del Plan de Contingencia de la OGTI deben de presentar un informe al responsable del plan de contingencia de la OGTI.

c. Desactivación del plan de contingencias.

El líder del plan de contingencia anuncia la desactivación.

d. Actualización.

Los registros se usan como base de conocimiento para la actualización del plan.

3. FORMATO EVENTO DELITO INFORMÁTICO

SIS Seguro Integral de Salud	FORMATO DELITO INFORMÁTICO	Código formato ----
		Código documento: XXXX -00X
		Página 1 de 1

1. ANTES

a. Descripción del evento

Alteración de los datos de los sistemas de información causados por un agente externo como un ataque cibernético o malware (código malicioso) .

EL entorno del evento afecta a:

- Infraestructura lógica del centro de datos
- Infraestructura lógica del área de operaciones de OGTI
- Infraestructura lógica de equipos de computo de usuarios de la OGTI

b. Objetivo

Restablecer la operatividad de los equipos y servicios que brinda la OGTI después de restablecer los sistemas de información y detener la amenaza.

c. Personal encargado

Es el equipo gestor del plan de contingencia de la OGTI como equipo de respuesta ante incidentes, siguiendo el lineamiento de jerarquía propuesto por la directriz del plan de contingencia. Según su jerarquía establecen los lineamientos que deben cumplir cada parte del equipo.

Condición para prevenir el riesgo

- Mantener actualizado con los parches de seguridad en los equipos de cómputo y servidores del centro de datos
- Establecer políticas de seguridad de acceso a los sistemas de información.
- Filtros de acceso a los servicios de correo en los exploradores de navegación de internet.
- Filtros de acceso y control de navegación en internet.
- Mantener actualizado el antivirus de los equipos de computo y centro de datos
- Contar con herramientas activas de búsqueda de malware en la red del SIS
- Contar con herramientas de prevención de fuga de datos en la red y equipos de cómputo del SIS.
- Deshabilitar los puertos de acceso a la totalidad de los trabajadores del SIS
- Habilitar las restricciones de uso de dispositivos de salida como grabadoras de CD.
- Concientización al personal del SIS sobre seguridad de la información y seguridad de las TIC
- Realizar un análisis de hackeo ético por periodos no mayores a 6 meses
- Contar con políticas y procedimientos de seguridad y responsabilidad de los usuarios ante los equipos de computo y servicios del SIS.
- Contar con personal especializado en seguridad informática y de información de manera permanente.

- Contar con metodología de desarrollo seguro y de análisis de seguridad de aplicaciones.
- Mantener las actualizaciones de respaldo de datos en cintas
- Llevar control de versiones de fuentes de los sistemas de información y portales de la entidad.
- Realizar pruebas continuas de restauración.
- Documentar todas las pruebas,

2. DURANTE

a. Activación de contingencia

Al ocurrir un incidente de delito informático. (mensajes de error, encriptación de datos, falla o caída de aplicaciones sin alertas) Se activa de manera inmediata. El líder de continuidad activa la contingencia.

b. Actividades

Se ejecuta la evacuación del personal previo apagado completo de emergencia del centro de datos y equipos de OGTI. (botón de pánico)

c. Personal encargado

Personal de nivel operativo del plan.

d. Actividades en la activación de plan de contingencia.

- Ante ataques por malware, el o los equipos detectados deberán ser desconectados físicamente y retirados para su análisis y desinfección por parte de soporte técnico.
- Soporte verifica e identifica el atacante de la maquina infectada, usando la herramienta de muestreo de amenazas del proveedor de antivirus, deberá guardar una copia y entregarla al proveedor, luego elimina la infección y reporta a los involucrados.
- Los sistemas de información afectados por un malware deberán de ser eliminados y restaurados para asegurar la continuidad.
- Usar la ultima copia de cintas para la restauración de datos en caso se necesite en caso de un atraque de encriptación de datos.
- Probar el sistema.
- Ante ataque de externos, el especialista de redes deberá de detectar los puertos más afectados y bloquearlos hasta que finalice el ataque. Deberá recomendar el análisis contra virus en toda la red y equipos del SIS.

3. DESPUÉS

El personal encargado son los gestores del plan de contingencia de la OGTI

a. Actividades

- Se realiza la concientización sobre seguridad al usuario afectado
- Se deberá mantener un registro sobre la eficacia de la herramienta de antivirus.
- Se mantiene un registro de eventos siguiendo el formato de incidentes

b. Reportes

Los gestores del Plan de Contingencia de la OGTI deben de presentar un informe al responsable del plan de contingencia de la OGTI.

c. Desactivación del plan de contingencias.

El líder del plan de contingencia anuncia la desactivación.

d. Actualización.

Los registros se usan como base de conocimiento para la actualización del plan.

4. FORMATO EVENTO FALLA DE HARDWARE Y SOFTWARE

SIS Seguro Integral de Salud	FORMATO FALLA DE HARDWARE Y SOFTWARE	Código formato ----
		Código documento: XXXX -00X
		Página 1 de 1

1. ANTES

a. Descripción del evento

Herramienta de uso de los trabajadores del SIS para el ejercicio de sus actividades dentro de la institución. Las fallas existentes no pueden ser lejanas al día a día, estos afectan a la continuidad de los servicios y de la información que estos procesan.

EL entorno del evento afecta a:

- Parque de computo o centro de datos del SIS

b. Objetivo

Restablecer la operatividad de los equipos y servicios que brinda la OGTI después de restablecer los equipos y detener la amenaza.

c. Personal encargado

Es el equipo gestor del plan de contingencia de la OGTI como equipo de respuesta ante incidentes, siguiendo el lineamiento de jerarquía propuesto por la directriz del plan de contingencia. Según su jerarquía establecen los lineamientos que deben cumplir cada parte del equipo.

Condición para prevenir el riesgo

- Plan de mantenimiento preventivo y correctivo a los equipos de cómputo y periféricos, estos deben de ser revisados por lo menos 1 vez al año.
- Plan de mantenimiento al centro de datos, este debe de ser revisado por lo menos 1 vez al año.
- Revisión continua de los logs de los servidores para prevenir mal funcionamiento de los mismos
- Realizar respaldo de las carpetas compartidas de los usuarios
- Disponer de un pequeño parque de equipos de computo y periféricos de respaldo en caso de fallas que no se puedan reparar.
- Disponer de equipos de contingencia dentro del centro de datos.
- Se debe cumplir con un calendario de respaldos
- Mantener actualizado el inventario de hardware y software del centro de datos, equipos de computo y periféricos de la OGTI.
- Disponer de herramientas de monitoreo para el centro de datos.
- Realizar planes de revisión de obsolescencia tecnológica del centro de datos y licencias de la OGTI.
- Documentar todas las pruebas,

2. DURANTE

a. Activación de contingencia

Al ocurrir fallas de conexión por indisponibilidad de equipos o sistemas de información

Se activa de manera inmediata. El líder de continuidad activa la contingencia.

b. Actividades

Se ejecuta la evacuación del personal previo apagado completo de emergencia del centro de datos y equipos de OGTI. (botón de pánico)

c. Personal encargado

Personal de nivel operativo del plan.

d. Actividades en la activación de plan de contingencia.

- Revisar el equipo averiado, se debe de buscar un reemplazo
- Si el equipo cuenta con garantía, se solicita el cambio o reparación del mismo
- Si es un servidor el que falla, se debe de migrar toda su infraestructura lógica a un servicio virtual temporal, en caso requiera una restauración por cintas se procede con la actividad de respaldo.
- Si es un equipo de computo personal el que falla, el personal de soporte deberá de reparar la falla según el alcance de sus herramientas, disponibilidad de partes de repuesto y software.
- Los tiempos de restauración dependerán de la disponibilidad de equipos de respaldo.

3. DESPUÉS

El personal encargado son los gestores del plan de contingencia de la OGTI, definirán la responsabilidad de las actividades según corresponda su función.

a. Actividades

- Revisión de operaciones de los equipos restaurados
- Seguimiento de la ejecución de la garantía de los equipos que lo tengan.
- Registrar en la documentación de eventos
- Comunicar al personal afectado de la reanudación de servicios en caso fuesen afectados

b. Reportes

Los gestores del Plan de Contingencia de la OGTI deben de presentar un informe al responsable del plan de contingencia de la OGTI.

c. Desactivación del plan de contingencias.

El líder del plan de contingencia anuncia la desactivación.

d. Actualización.

Los registros se usan como base de conocimiento para la actualización del plan.

ANEXO 3
FORMATO DE CONTROL Y CERTIFICACION DE LAS PRUEBAS

CONTROL Y CERTIFICACIÓN DE PRUEBAS DE CONTINGENCIA

PRUEBA N°

Escenario de Prueba: (Descripción del escenario a probar/certificar)

Área Responsable: (Área responsable del escenario de prueba a probar/certificar)

INFORMACION DEL PROCESO

Metodología: (Detallar lo que se va a hacer en la prueba)

Alcance: (Definir hasta donde va a abarcar)

Condiciones de Ejecución

Equipo: Nombre Servidor/PC de prueba

Ubicación: Lugar de prueba

Aplicación/Software:

Fecha de Backup: / /

RESULTADO DE LA PRUEBA

Resultado: Satisfactorio: ☐ Satisfactorio con Observaciones: ☐ Deficiente: ☐

Observaciones: (En el caso de haber observaciones o que la prueba haya sido deficiente, se indicarán los motivos, y resultados

ACTUALIZACION EN EL PLAN DE CONTINGENCIA

Cambios o actualizaciones en el Plan de Contingencia: (Se indicarán los cambios que se deben realizar al Plan de Contingencia como consecuencia de las observaciones detectadas en las pruebas correspondientes)

ACTUALIZACION PARTICIPANTES

Participante	Cargo	Firma

ANEXO 4
MATRIZ DE RIESGOS

AI-1 SALA DE SERVIDORES

Código del Activo	Nombre del Activo d	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Recomendaciones
AI-1	Sala de servidores	Infraestructura Física del centro de datos que cuenta con gabinetes de servidores, gabinetes de UPS, gabinete	Incendio	Mantenimiento insuficiente	Incendio en la Sala de servidores por mantenimiento insuficiente	5	1	Mediano	Se deberá de realizar mantenimiento periódicamente a la Sala de servidores
				Capacitación de seguridad insuficiente	Incendio en la Sala de servidores por capacitación de seguridad insuficiente	5	1	Mediano	Se deberá de capacitar al personal sobre medidas de seguridad y manipulación de extintores
				Error humano	Incendio en la Sala de servidores por error humano	5	1	Mediano	Se deberá de capacitar al personal sobre medidas de seguridad y manipulación de extintores
				Falta del sistema contra incendios	Incendio en la Sala de servidores por falta del sistema contra incendios	5	1	Mediano	Se deberá implementar un sistema contra incendios y realizar un plan de mantenimiento.

		de comunicaciones, aire acondicionado, cableado de datos, cableado eléctrico, puerta de seguridad.		Falta de técnicas apropiadas para controlar algún evento catastrófico	Incendio en la Sala de servidores por falta de técnicas apropiadas para controlar algún evento catastrófico	5	1	Mediano	Se deberá de capacitar al personal sobre medidas de seguridad y manipulación de extintores
			Inundación	Mantenimiento insuficiente	Inundación en la Sala de servidores por mantenimiento insuficiente	4	1	Bajo	Coordinación con el área de mantenimiento para la realización de planes de revisión y mantenimiento de tuberías de agua
				Inadecuado ambiente físico	Inundación en la Sala de servidores por Inadecuado ambiente físico	4	1	Bajo	Coordinación con el área de mantenimiento para la realización de planes de revisión y mantenimiento de tuberías de agua
				Falta de técnicas apropiadas para controlar algún evento catastrófico	Inundación en la Sala de servidores por falta de técnicas apropiadas para controlar algún evento catastrófico	4	1	Bajo	Coordinación con el área de mantenimiento para la realización de planes de revisión y mantenimiento de tuberías de agua
			Acceso no autorizado a la información	Falta de procedimiento formal de Ingreso a la Sala de servidores	Acceso indebido a la Sala de servidores por falta de procedimiento formal de Ingreso a la Sala de servidores	3	3	Alto	Se deberá de desarrollar una directiva donde se indique el procedimiento para gestionar los accesos a la Sala de servidores y las medidas de seguridad que se deberán cumplir
				Asignación	Acceso indebido a la Sala de	3	2	Mediano	Se deberá de desarrollar una directiva

				equivocada de derechos de acceso	servidores por asignación equivocada de derechos de acceso				donde se indique el procedimiento para gestionar los accesos a la Sala de servidores y las medidas de seguridad que se deberán cumplir
				Insuficientes mecanismos de supervisión/monitoreo	Acceso indebido a la Sala de servidores por insuficientes mecanismos de supervisión/monitoreo	4	2	Mediano	Se deberá de desarrollar una directiva donde se indique el procedimiento para gestionar los accesos a la Sala de servidores y las medidas de seguridad que se deberán cumplir
				Falta de procedimiento de retiro de accesos	Acceso indebido a la Sala de servidores por falta de procedimiento de retiro de accesos	4	2	Mediano	Se deberá de desarrollar una directiva donde se indique el procedimiento para gestionar los accesos a la Sala de servidores y las medidas de seguridad que se deberán cumplir
			Daño por fenómeno sísmico	Falta de técnicas apropiadas para controlar algún evento catastrófico	Daño por fenómeno sísmico en la Sala de servidores debido a la falta de técnicas apropiadas para controlar algún evento catastrófico	4	1	Bajo	Se deberá realizar una revisión del centro de datos sobre su infraestructura para soporte ante fenómenos sísmicos
			Saturación de humedad en	Mantenimiento insuficiente	Fallas en el control de temperatura y humedad de la Sala de servidores por mantenimiento insuficiente	5	1	Mediano	Se deberá de realizar mantenimiento periódicamente al sistema de aire acondicionado

			ambientes	Uso incorrecto del software y hardware	Fallas en el control de temperatura y humedad de la Sala de servidores por uso incorrecto del software y hardware	4	1	Bajo	Se deberá crear un plan o integrar al plan de mantenimiento una actividad que contemple la revisión de los sensores de humedad o el reemplazo del mismo.
			Fallas del sistema de aire acondicionado	Mantenimiento insuficiente	Fallas del sistema de aire acondicionado de la Sala de servidores por mantenimiento insuficiente	5	1	Mediano	Se deberá de realizar mantenimiento periódicamente al sistema de aire acondicionado. Se debe considerar adquirir un sistema de aire acondicionado de precisión junto al desarrollo de un plan de mantenimiento del sistema.
				Uso incorrecto del software y hardware	Fallas del sistema de aire acondicionado de la Sala de servidores por uso incorrecto del software y hardware	4	1	Bajo	Se deberá integrar al plan de mantenimiento o desarrollar una actividad que contemple la revisión periódica de los equipos y la capacitación al personal quien estará a cargo del control o administración del centro de datos. Se debe considerar adquirir un sistema de aire acondicionado de precisión junto al desarrollo de un plan de mantenimiento del sistema.
			Pérdida del suministro de electricidad	Red inestable de energía eléctrica	Pérdida del suministro de electricidad en la Sala de servidores por red inestable de energía eléctrica	3	1	Bajo	Se deberá programar mantenimiento de las estaciones de red eléctrica.

				Dependencia de proveedor de servicio público	Pérdida del suministro de electricidad en la Sala de servidores por dependencia de proveedor de servicio público	5	1	Mediano	Se deberá de tener UPS y/o grupo electrógeno y se deberá de verificar que cuenten con mantenimiento
				Falta de redundancia de fuentes de energía	Pérdida del suministro de electricidad en la Sala de servidores por falta de redundancia de fuentes de energía	5	1	Mediano	Se deberá de tener UPS y/o grupo electrógeno y se deberá de verificar que cuenten con mantenimiento

AI-2 Sistema de almacenamiento de Datos de respaldo del centro de datos.

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
AI-2	Sistema de almacenamiento de Datos de Respaldo del Centro de Datos.	Es el sistema adquirido por SIS con responsabilidad de los operarios del centro de datos y de propiedad de la OGEI, este sistema tiene como función principal de agrupar los diferentes archivos de los sistemas a respaldar,	Mal funcionamiento del sistema	Mantenimiento insuficiente	Mal funcionamiento del sistema de almacenamiento de los Servidores por Mantenimiento insuficiente	5	2	Alto	Se deberá de tener un plan de mantenimiento para los Servidores
				Susceptibilidad a la humedad, al polvo y a la suciedad	Mal funcionamiento del sistema de almacenamiento de los Servidores por susceptibilidad a la humedad, al polvo y a la suciedad	4	2	Mediano	Se deberá de tener un plan de mantenimiento para los Servidores
				Incorrecta configuración	Mal funcionamiento del sistema de almacenamiento de los Servidores por Incorrecta configuración	5	2	Alto	Se deberá de verificar que solo el personal capacitado tenga acceso a los Servidores
				Error humano	Mal funcionamiento del sistema de almacenamiento de los Servidores y Servidores por Error humano	5	1	Mediano	Se deberá de verificar que solo el personal capacitado tenga acceso a los

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
		estos archivos cuentan con una encriptación propia para ser copiados a cintas							Servidores
				Obsolescencia Tecnológica	Mal funcionamiento del sistema de almacenamiento de los Servidores por Obsolescencia Tecnológica	5	1	Mediano	Se deberá de tener un plan de mantenimiento para los Servidores
				Falta actualización del Software de Servidores (parche)	Mal funcionamiento del sistema de almacenamiento de los Servidores por Falta actualización del Software de Servidores (parche)	5	1	Mediano	Se deberá de verificar la instalación de Parches y Actualizaciones en los Servidores
			Uso no autorizado del equipo	Mala administración de la contraseña del equipo	Uso no autorizado del sistema de almacenamiento de los Servidores por Mala administración de la contraseña del equipo	5	1	Mediano	Se deberá de verificar el cumplimiento de la directiva de contraseñas
				Error humano	Uso no autorizado del sistema de almacenamiento de los	5	1	Mediano	Se deberá de verificar que solo el

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
					Servidores por Error humano				personal capacitado manipule los Servidores
				El equipo no exige el cambio periódico de contraseña	Uso no autorizado del sistema de almacenamiento de los Servidores por que el Servidor no exige el cambio periódico de contraseña	5	1	Mediano	Se deberá de implementar una política en el Active Directory que exija el cambio de contraseñas.
				Falta de conciencia de seguridad	Uso no autorizado del sistema de almacenamiento de los Servidores por falta de conciencia de seguridad	5	1	Mediano	Se deberá de verificar que solo el personal capacitado tenga acceso a los Servidores
				Ausencia o insuficiencia de lineamientos	Uso no autorizado de los Servidores por ausencia o insuficiencia de lineamientos de seguridad	5	1	Mediano	Se deberá de establecer los lineamientos de seguridad para el uso de equipos
				Falta de mecanismos	Uso no autorizado de los	5	1	Mediano	Se deberá de

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
				de monitoreo	Servidores por falta de mecanismos de monitoreo				verificar que se cuenten con logs de auditoría, los cuales deberán ser revisados en periodos programados.
				Incorrecta configuración	Uso no autorizado de los Servidores por incorrecta configuración	5	1	Mediano	Se deberá de realizar análisis de la configuración de los Servidores
				Falta de procedimiento formal de altas, bajas y modificaciones de usuario	Uso no autorizado de los Servidores por falta de procedimiento formal de altas, bajas y modificaciones de usuario	5	1	Mediano	Se deberá elaborar lineamientos que indiquen la verificación de los usuarios con acceso al VPN
				Falta de ejecución del procedimiento formal de altas, bajas y	Uso no autorizado de los Servidores por Falta de ejecución del procedimiento	5	1	Mediano	Se deberá de verificar que solo el personal autorizado

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
				modificaciones de usuario	formal de altas, bajas y modificaciones de usuario				tenga acceso a los Servidores
			Hacking	Incorrecta configuración	Hacking de los Servidores por Incorrecta configuración	5	1	Mediano	Se deberá de realizar análisis de la configuración de los Servidores
				Falta de mecanismos de configuración de seguridad del equipo	Hacking de los Servidores por Falta de mecanismos de configuración de seguridad del equipo	5	1	Mediano	Se deberá de realizar análisis de la configuración de los Servidores
				Falta de afinamiento en los mecanismos de seguridad del equipamiento de seguridad perimetral	Hacking de los Servidores por falta de afinamiento en los mecanismos de seguridad perimetral	5	1	Mediano	Se deberá de realizar análisis de la configuración de los equipos de seguridad perimetral
				Falta actualización del Sistema	Hacking de los Servidores por Falta actualización del Sistema	5	1	Mediano	Se deberá de verificar que los Servidores se encuentren con los parches

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
									actualizados
			Indisponibilidad del equipo	Red inestable de energía eléctrica	Indisponibilidad de los Servidores por Red inestable de energía eléctrica	5	1	Mediano	Se deberá de contar con un UPS para asegurar la continuidad de los Servidores
				Falta de redundancia activa	Indisponibilidad de los Servidores por Falta de redundancia activa	5	2	Alto	Se deberá de tener contingencia de los Servidores para asegurar la disponibilidad de la información
				Insuficientes mecanismos de supervisión/monitoreo	Indisponibilidad de los Servidores por Insuficientes mecanismos de supervisión/monitoreo	5	1	Mediano	Se deberá de monitorear 24*7 la operatividad de los Servidores
				Mantenimiento insuficiente	Indisponibilidad de los Servidores por Mantenimiento insuficiente	5	1	Mediano	Se deberá contar con un plan de mantenimiento de los Servidores

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
			Pérdida de información	Falta de copias de respaldo	Pérdida de información de los Servidores por falta de copias de respaldo	5	1	Mediano	Se deberá de verificar que se estén realizando copias de respaldo de los Servidores
				Falta de pruebas periódicas de restauración	Pérdida de información de los Servidores por falta de pruebas periódicas de restauración	5	2	Alto	Se deberá de verificar que se estén realizando pruebas de restauración de las copias de respaldo de los Servidores
				Error humano	Pérdida de información de los Servidores por Error humano	5	1	Mediano	Se deberá de verificar que solo el personal capacitado manipule los Servidores
			Códigos maliciosos (ej. Virus, bomba	Falta actualización del Software de Servidores (parche)	Infección de códigos maliciosos (ej. Virus, bomba lógica, troyano) en los Servidores por	5	1	Mediano	Se deberá de verificar la instalación de

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
			lógica, troyano)		falta actualización del Software de Servidores (parche)				Parches y Actualizaciones en los Servidores
				Falta de antivirus	Infección de códigos maliciosos (ej. Virus, bomba lógica, troyano) en los Servidores por falta de antivirus	5	1	Mediano	Se deberá de verificar que los Servidores cuenten con antivirus
				Falta de antivirus actualizado	Infección de códigos maliciosos (ej. Virus, bomba lógica, troyano) en los Servidores por Falta de antivirus actualizado	5	1	Mediano	Se deberá de monitorear la actualización de los Servidores
				Falta de conciencia de seguridad	Infección de códigos maliciosos (ej. Virus, bomba lógica, troyano) en los Servidores por Falta de conciencia de seguridad	5	1	Mediano	Se deberá capacitar al personal sobre seguridad de la información
			Fuga de información	Error humano	Fuga de información de los Servidores por Error humano	5	1	Mediano	Se deberá de verificar que solo el personal capacitado tenga acceso a los

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
									Servidores
				Falta de conciencia de seguridad	Fuga de información de los Servidores por Falta de conciencia de seguridad	5	1	Mediano	Se deberá capacitar al personal sobre seguridad de la información
				Asignación equivocada de derechos de acceso	Fuga de información de los Servidores por Asignación equivocada de derechos de acceso	5	1	Mediano	Se deberá de verificar que solo el personal autorizados tengan acceso a los Servidores
				Mala administración de claves	Fuga de información de los Servidores por Mala administración de claves	5	2	Alto	Se deberá de capacitar al personal sobre la directiva de contraseñas y la política de seguridad de la información
				Asignación equivocada de derechos de acceso	Fuga de información de los Servidores por Asignación equivocada de derechos de acceso	5	2	Alto	Se deberá de verificar que solo el personal capacitado tenga acceso a los

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
									Servidores
				Falta de procedimiento formal de altas, bajas y modificaciones de usuario	Fuga de información de los Servidores por Falta de procedimiento formal de altas, bajas y modificaciones de usuario	5	1	Mediano	Se deberá elaborar lineamientos que indiquen la verificación de los usuarios con acceso al Servidores

AI-3 Datos de Respaldo (Cintas Back up)

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
AI-3	Datos de Respaldo	Son los archivos comprimidos que se usaran como dispositivos de respaldo, que estarán resguardados en dispositivos físicos del centro de datos y en cintas magnéticas	Robo de cintas	Falta de mecanismos de monitoreo	Robo de cintas por falta de mecanismos de monitoreo	5	1	Mediano	Se deberá restringir el acceso a maletines u algún objeto capaz de almacenar cintas
				Falta de conciencia de seguridad	Robo de cintas por falta de conciencia de seguridad	5	1	Mediano	Se deberá de capacitar al personal sobre la política de seguridad de la información
				Falta de protección física del edificio, puertas y ventanas	Robo de cintas por falta de protección física del edificio, puertas y ventanas	5	1	Mediano	Se deberá de verificar que solo el personal autorizado tenga acceso (en el marcador biométrico) al área

		que serán enviadas a un almacén para su correcto cuidado, las cintas se solicitaran como envío y entrega siguiendo los parámetros de seguridad del proveedor de servicios de almacén de cintas.		Lineamientos inexistentes o insuficientes	Robo de cintas por Lineamientos inexistentes o insuficientes	5	1	Mediano	Se deberá de contar con una directiva para el retiro de equipos que almacenen cintas
				Falta de política formal sobre el uso de computadoras portátiles	Robo de datos de respaldo por falta de política formal sobre el uso de computadoras portátiles	5	1	Mediano	Se deberá de establecer los lineamientos de seguridad para el uso de equipos portátiles.
				Almacenamiento no protegido	Robo de cintas por Almacenamiento no protegido	5	1	Mediano	Se deberá verificar el retiro de equipos informáticos
				Falta de procedimientos de acceso a las instalaciones de procesamiento de la información	Robo de cintas por Falta de procedimientos de acceso a las instalaciones de procesamiento de la información	5	1	Mediano	Se deberá verificar el retiro de equipos informáticos
			Pérdida de información	Falta de copias de respaldo	Pérdida de información por Falta de copias de respaldo	4	1	Bajo	Se deberá crear y respetar el plan de respaldo y asignar un presupuesto

									inamovible sobre estos mismos
				Falta de pruebas periódicas de restauración	Pérdida de información de las estaciones de trabajo por Falta de pruebas periódicas de restauración	4	1	Bajo	Se deberá crear y respetar el plan de respaldo y asignar un presupuesto inamovible sobre estos mismos
				Error humano	Pérdida de copias de respaldo por Error humano	5	1	Mediano	Se deberá de asignar responsabilidades al personal para el correcto almacenamiento de las cintas y las copias digitales de respaldo
			Mal uso de información	Ausencia o insuficiencia de lineamientos (concernientes a la seguridad de la información en contratos con empleados)	Mal uso de información de las estaciones de trabajo que cuentan los archivos de las cintas por Ausencia o insuficiencia de lineamientos (concernientes a la	5	1	Mediano	Se deberá colocar cláusulas de seguridad en los contratos y hacer firmar acuerdos de confidencialidad a todos los empleados

					seguridad de la información en contratos con empleados)				
				Falta de procedimiento de rehúso y eliminación segura de equipos y medios	Mal uso de información de las estaciones de trabajo que contienen copias de respaldo digitales para las cintas de respaldo por falta de procedimiento de rehúso y eliminación segura de equipos y medios	5	2	Alto	Se deberá de implementar una directiva de rehúso y eliminación segura de medios.
				Falta de procedimientos para manejo de la información clasificada	Mal uso de información de las estaciones de trabajo que contienen copias de respaldo digitales para las cintas de respaldo por Falta de	5	1	Mediano	Se deberá capacitar al personal sobre seguridad de la información

					procedimientos para manejo de la información clasificada				
				Mala administración de la contraseña del equipo	Mal uso de información de las estaciones de trabajo que contienen copias de respaldo digitales para las cintas de respaldo por Mala administración de la contraseña del equipo	5	2	Alto	Se deberá de verificar el cumplimiento de la directiva de contraseñas
				Reutilización de equipos sin borrar apropiadamente la información	Mal uso de información de las estaciones de trabajo que contienen copias de respaldo digitales para las cintas de respaldo por Reutilización de equipos sin borrar apropiadamente la información	5	2	Alto	Se deberá de implementar una directiva de rehúso y eliminación segura de medios.

			Infección de códigos maliciosos (ej. Virus, bomba lógica, troyano)	Falta actualización del Software de Servidores (parche)	Infección de Códigos maliciosos (ej. Virus, bomba lógica, troyano) en estaciones de trabajo que contienen copias de respaldo digitales para las cintas de respaldo por Falta actualización del Software de Servidores (parche)	5	1	Mediano	Se deberá de verificar la instalación de Parches en las estaciones de trabajo que contienen copias de respaldo digitales para las cintas de respaldo.
				Falta de antivirus	Infección de Códigos maliciosos (ej. Virus, bomba lógica, troyano) en estaciones de trabajo que contienen copias de respaldo digitales para las cintas de respaldo por Falta de antivirus	5	1	Mediano	Se deberá de verificar que las estaciones de trabajo que contienen copias de respaldo digitales para las cintas de respaldo cuenten con antivirus

				Falta de antivirus actualizado	Infección de Códigos maliciosos (ej. Virus, bomba lógica, troyano) en estaciones de trabajo que contienen copias de respaldo digitales para las cintas de respaldo por Falta de antivirus actualizado	4	2	Mediano	Se deberá de monitorear la actualización del antivirus en las estaciones de trabajo que contienen copias de respaldo digitales para las cintas de respaldo
				Falta de conciencia de seguridad	Infección de Códigos maliciosos (ej. Virus, bomba lógica, troyano) en estaciones de trabajo que contienen copias de respaldo digitales para las cintas de respaldo por Falta de conciencia de seguridad	5	2	Alto	Se deberá capacitar al personal sobre seguridad de la información
			Mal funcionamiento del equipo	Susceptibilidad a la humedad, al polvo y a la suciedad	Mal funcionamiento de las estaciones de trabajo que contienen copias de respaldo digitales para las	5	1	Mediano	Se deberá de tener un plan de mantenimiento de las estaciones de trabajo que contienen copias

					cintas de respaldo por Susceptibilidad a la humedad, al polvo y a la suciedad				de respaldo digitales para las cintas de respaldo
				Incorrecta configuración	Mal funcionamiento de las estaciones de trabajo que contienen copias de respaldo digitales para las cintas de respaldo por Incorrecta configuración	5	1	Mediano	Se deberá de tener un plan de mantenimiento de las estaciones de trabajo que contienen copias de respaldo digitales para las cintas de respaldo
				Error humano	Mal funcionamiento de las estaciones de trabajo que contienen copias de respaldo digitales para las cintas de respaldo por Error humano	5	2	Alto	Se deberá capacitar al personal sobre seguridad de la información
				Obsolescencia Tecnológica	Mal funcionamiento de las estaciones de trabajo que contienen copias de respaldo digitales para las cintas de respaldo por Obsolescencia	5	1	Mediano	Se deberá de tener un plan de mantenimiento de las estaciones de trabajo que contienen copias de respaldo digitales para las cintas de

					Tecnológica				respaldo
			Uso no autorizado de las estaciones de trabajo	Mala administración de la contraseña del equipo	Uso no autorizado de las estaciones de trabajo que contienen copias de respaldo digitales para las cintas de respaldo por Mala administración de la contraseña del equipo	5	1	Mediano	Se deberá de verificar el cumplimiento de la directiva de contraseñas
				Error humano	Uso no autorizado de las estaciones de trabajo que contienen copias de respaldo digitales para las cintas de respaldo por Error humano	5	1	Mediano	Se deberá capacitar al personal sobre seguridad de la información
				No hacer "logout" cuando se sale de la estación de trabajo	Uso no autorizado de las estaciones de trabajo que contienen copias de respaldo digitales para las	5	1	Mediano	Se deberá de implementar una Política en el AD, la cual bloquee las estaciones de trabajo

					cintas de respaldo por No hacer "logout" cuando se sale de la estación de trabajo				que contienen copias de respaldo digitales para las cintas de respaldo a los 5 min de inoperatividad
				Las estaciones de trabajo que contienen copias de respaldo digitales para las cintas de respaldo no exigen el cambio periódico de contraseña	Uso no autorizado de las estaciones de trabajo que contienen copias de respaldo digitales para las cintas de respaldo por no exige el cambio periódico de contraseña	5	1	Mediano	Se deberá de implementar una política en el Active Directory que exija el cambio de contraseñas.
				Falta de conciencia de seguridad	Uso no autorizado de las estaciones de trabajo que copias de respaldo digitales para las cintas de respaldo por Falta de conciencia de seguridad	5	1	Mediano	Se deberá capacitar al personal sobre seguridad de la información
				Ausencia o insuficiencia de lineamientos (concernientes a la	Uso no autorizado de las estaciones de trabajo que contienen copias de respaldo	5	1	Mediano	Se deberá capacitar al personal sobre seguridad de la información

				seguridad de la información en contratos con empleados)	digitales para las cintas de respaldo por Ausencia o insuficiencia de lineamientos				
				Falta de procedimiento formal de altas, bajas y modificaciones de usuario	Uso no autorizado de las estaciones de trabajo que contienen copias de respaldo digitales para las cintas de respaldo por Falta de procedimiento formal de altas, bajas y modificaciones de usuario	5	1	Mediano	Se deberá elaborar lineamientos que indiquen la verificación de los usuarios con acceso a las estaciones de trabajo
			Fuga de información	Error humano	Fuga de información de las estaciones de trabajo que contienen copias de respaldo digitales para las cintas de respaldo por Error humano	5	1	Mediano	Se deberá capacitar al personal sobre seguridad de la información

				Falta de conciencia de seguridad	Fuga de información de las estaciones de trabajo que contienen copias de respaldo digitales para las cintas de respaldo por Falta de conciencia de seguridad	5	1	Mediano	Se deberá capacitar al personal sobre seguridad de la información
				Insuficientes mecanismos de supervisión/monitoreo	Fuga de información de las estaciones de trabajo por Insuficientes mecanismos de supervisión/monitoreo	5	1	Mediano	Se deberá implementar un medio de protección de información confidencial
				Asignación equivocada de derechos de acceso	Fuga de información de las estaciones de trabajo que contienen copias de respaldo digitales para las cintas de respaldo por Asignación equivocada de derechos de acceso	5	1	Mediano	Se deberá verificar periódicamente los permisos de acceso a las carpetas compartidas.

				Mala administración de claves	Fuga de información de las estaciones de trabajo que contienen copias de respaldo digitales para las cintas de respaldo por Mala administración de claves	5	1	Mediano	Se deberá de capacitar al personal sobre la directiva de contraseñas y la política de seguridad de la información
				Falta de procedimiento formal de altas, bajas y modificaciones de usuario	Fuga de información de las estaciones de trabajo que contienen copias de respaldo digitales para las cintas de respaldo por Falta de procedimiento formal de altas, bajas y modificaciones de usuario	5	1	Mediano	Se deberá elaborar lineamientos que indiquen la verificación de los usuarios con acceso a las estaciones de trabajo

AI-4 Sistema de autenticación de directorio activo.

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
AI-4	Sistema de autenticación de directorio activo.	Sistema que se encuentra alojado dentro de un servidor del centro de datos, este sistema tiene como función contener a todos los usuarios del directorio del SIS, para a su vez relacionarlo con los sistemas desarrollados por la entidad	Hacking	Incorrecta configuración	Hacking del Software de Servidores por incorrecta configuración	5	1	Mediano	Se deberá de realizar análisis de la configuración del Software de Servidores
				Falta de mecanismos de configuración de seguridad del equipo	Hacking del Software de Servidores por falta de mecanismos de configuración de seguridad del equipo	5	1	Mediano	Se deberá de realizar análisis de la configuración del Software de Servidores
				Falta de afinamiento en los mecanismos de seguridad del equipamiento de seguridad perimetral	Hacking del Software de Servidores por falta de afinamiento en los mecanismos de seguridad perimetral	5	1	Mediano	Se deberá de realizar análisis de la configuración de los equipos de seguridad perimetral
				Mala administración	Hacking del Software de Servidores por mala	5	1	Mediano	Se deberá de capacitar al personal sobre la directiva de

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
		y los adquiridos para las operaciones del SIS, esto garantiza que el usuario quien manipule la información dentro del proceso que involucre el alcance del SGSI, tenga los permisos adecuados para garantizar la seguridad de		de claves	administración de claves				contraseñas y la política de seguridad de la información
				Falta de conciencia de seguridad	Hacking del Software de Servidores por falta de conciencia de seguridad	5	1	Mediano	Se deberá de capacitar al personal sobre la política de seguridad de la información
				Falta actualización del Sistema	Hacking del Software de Servidores por falta actualización del Sistema	5	1	Mediano	Se deberá de verificar la instalación de Parches y Actualizaciones en el Software de Servidores
			Códigos maliciosos (ej. Virus, bomba lógica, troyano)	Falta actualización del Software de Servidores (parche)	Infección de códigos maliciosos (ej. Virus, bomba lógica, troyano) en el Software de Servidores por falta de actualización (parche)	5	2	Alto	Se deberá de verificar la instalación de Parches y Actualizaciones en el Software de Servidores
				Falta de antivirus	Infección de códigos maliciosos (ej. Virus, bomba lógica, troyano) en el Software de Servidores por falta de	5	1	Mediano	Se deberá de verificar la instalación del antivirus en el Software de Servidores.

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
		la información.			antivirus				
				Falta de antivirus actualizado	Infección de códigos maliciosos (ej. Virus, bomba lógica, troyano) en el Software de Servidores por falta de antivirus actualizado	5	1	Mediano	Se deberá de verificar la instalación del antivirus en el Software de Servidores.
				Falta de conciencia de seguridad	Infección de códigos maliciosos (ej. Virus, bomba lógica, troyano) en el Software de Servidores por falta de conciencia de seguridad	5	1	Mediano	Se deberá de capacitar al personal sobre la política de seguridad de la información
			Mal funcionamiento del software	Error humano	Mal funcionamiento del Software de Servidores por error humano	5	1	Mediano	Se deberá de verificar que solo el personal capacitado tenga acceso a la administración del Software de Servidores
				Parche no instalado	Mal funcionamiento del Software de Servidores	5	2	Alto	Se deberá de verificar la instalación de Parches y

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
				correctamente	por parche no instalado correctamente				Actualizaciones en el Software de Servidores
				Software desfasado por vigencia tecnológica y sin soporte por parte del fabricante	Mal funcionamiento del Software de Servidores por software desfasado por vigencia tecnológica y sin soporte por parte del fabricante	5	2	Alto	Se deberá de verificar las versiones del Software de Servidores y de encontrarse alguno que se encuentre desfasado tecnológicamente, se deberá de migrar.
			Fuga de información	Error humano	Fuga de información del Software de Servidores por error humano	5	1	Mediano	Se deberá de verificar que solo el personal capacitado tenga acceso a el Software de Servidores
				Falta de conciencia de seguridad	Fuga de información del Software de Servidores por falta de conciencia de seguridad	5	1	Mediano	Se deberá de verificar que solo el personal capacitado tenga acceso a el Software de Servidores
				Asignación equivocada de derechos de	Fuga de información del Software de Servidores por Asignación	5	1	Mediano	Se deberá verificar periódicamente los permisos de acceso a el Software de

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
				acceso	equivocada de derechos de acceso				Servidores
				Mala administración de claves	Fuga de información del Software de Servidores por mala administración de claves	5	1	Mediano	Se deberá de capacitar al personal sobre la directiva de contraseñas y la política de seguridad de la información
				Asignación equivocada de derechos de acceso	Fuga de información del Software de Servidores por asignación equivocada de derechos de acceso	5	1	Mediano	Se deberá verificar periódicamente los permisos de acceso a el Software de Servidores
				Falta de procedimiento formal de altas, bajas y modificaciones de usuario	Fuga de información del Software de Servidores por falta de procedimiento formal de altas, bajas y modificaciones de usuario	5	1	Mediano	Se deberá elaborar lineamientos que indiquen la verificación de los usuarios con acceso al software de los servidores

AI-5 Información digital del Personal de la OGTI.

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
AI-5	Información digital del Personal.	Es la información con la que trabajan los profesionales de la unidad de sistemas y UIT, consta de sistemas y credenciales de acceso a todos los servidores del centro de datos, así como las aplicaciones y herramientas cuales ellos administren, administran	Mal funcionamiento del software	Error humano	Mal funcionamiento del Software de Aplicaciones por error humano	5	1	Mediano	Se deberá de verificar que solo el personal capacitado tenga acceso al Software de Aplicaciones
				Software desfasado por vigencia tecnológica y sin soporte por parte del fabricante	Mal funcionamiento del Software de Aplicaciones por software desfasado por vigencia tecnológica y sin soporte por parte del fabricante	5	2	Alto	Se deberá de verificar las versiones del Software de Aplicaciones y de encontrarse alguno que se encuentre desfasado tecnológicamente, se deberá de migrar.
			Indisponibilidad del Software	Software obsoleto	Indisponibilidad del Software de Aplicaciones por Software obsoleto	4	1	Bajo	Se deberá crear un plan de mantenimiento que contemple la renovación de los equipos y licencias dentro de un tiempo analizado que

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
		también la red de comunicaciones del SIS y su seguridad perimetral.							determine la obsolescencia de un equipo de cómputo y/o de las licencias que contiene.
				Software desfasado por vigencia tecnológica y sin soporte por parte del fabricante	Indisponibilidad del Software de Aplicaciones por software desfasado por vigencia tecnológica y sin soporte por parte del fabricante	4	1	Bajo	Se deberá crear un plan de mantenimiento que contemple la renovación de los equipos y licencias dentro de un tiempo analizado que determine la obsolescencia de un equipo de cómputo y/o de las licencias que contiene
				Error humano	Indisponibilidad del Software de Aplicaciones por error humano	5	1	Mediano	Se deberá de verificar que solo el personal capacitado y autorizado tenga acceso al Software de

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
									Aplicaciones
				Uso incorrecto del software	Indisponibilidad del Software de Aplicaciones por uso incorrecto del software	5	1	Mediano	Se deberá de verificar que solo el personal capacitado y autorizado tenga acceso al Software de Aplicaciones
			Acceso no autorizado al sistema	Error humano	Acceso no autorizado al Software de Aplicaciones por error humano	5	1	Mediano	Se deberá de verificar que solo el personal autorizado tenga acceso al Software de Aplicaciones
				Incorrecta configuración	Acceso no autorizado al Software de Aplicaciones por incorrecta configuración	5	1	Mediano	Se deberá de verificar que solo el personal autorizado tenga acceso al Software de Aplicaciones
				Falta de eliminación y	Acceso no autorizado al	5	1	Mediano	Se deberá de verificar que solo el personal

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
				modificación de accesos del personal	Software de Aplicaciones por falta de eliminación y modificación de accesos del personal				autorizado tenga acceso al Software de Aplicaciones

AI-6 Infraestructura del área de OGTI.

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
AI-6	Infraestructura de área de Operadores y de Centro de datos.	Son los equipos de cómputo, periféricos, herramientas y mobiliario de los trabajadores la unidad de Sistemas y UIT que es responsable de ellos.	Mal funcionamiento del software	Error humano	Mal funcionamiento del Software de Aplicaciones por error humano	5	1	Mediano	Se deberá de verificar que solo el personal capacitado tenga acceso al Software de Aplicaciones
				Software desfasado por vigencia tecnológica y sin soporte por parte del fabricante	Mal funcionamiento del Software de Aplicaciones por software desfasado por vigencia tecnológica y sin soporte por parte del fabricante	5	2	Alto	Se deberá de verificar las versiones del Software de Aplicaciones y de encontrarse alguno que se encuentre desfasado tecnológicamente, se deberá de migrar.
			Indisponibilidad del Software	Software obsoleto	Indisponibilidad del Software de Aplicaciones por Software obsoleto	4	1	Bajo	Se deberá crear un plan de mantenimiento que contemple la renovación de los equipos y licencias dentro de un tiempo analizado que determine

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
									la obsolescencia de un equipo de cómputo y/o de las licencias que contiene
				Software desfasado por vigencia tecnológica y sin soporte por parte del fabricante	Indisponibilidad del Software de Aplicaciones por software desfasado por vigencia tecnológica y sin soporte por parte del fabricante	4	1	Bajo	Se deberá crear un plan de mantenimiento que contemple la renovación de los equipos y licencias dentro de un tiempo analizado que determine la obsolescencia de un equipo de cómputo y/o de las licencias que contiene
				Error humano	Indisponibilidad del Software de Aplicaciones por error humano	5	1	Mediano	Se deberá de verificar que solo el personal capacitado y autorizado tenga acceso al Software de Aplicaciones
				Uso incorrecto del software	Indisponibilidad del Software de Aplicaciones por uso incorrecto del software	5	1	Mediano	Se deberá de verificar que solo el personal capacitado y autorizado tenga acceso al Software

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
									de Aplicaciones
			Acceso no autorizado al sistema	Error humano	Acceso no autorizado al Software de Aplicaciones por error humano	5	1	Mediano	Se deberá de verificar que solo el personal autorizado tenga acceso al Software de Aplicaciones
				Incorrecta configuración	Acceso no autorizado al Software de Aplicaciones por incorrecta configuración	5	1	Mediano	Se deberá de verificar que solo el personal autorizado tenga acceso al Software de Aplicaciones
				Falta de eliminación y modificación de accesos del personal	Acceso no autorizado al Software de Aplicaciones por falta de eliminación y modificación de accesos del personal	5	1	Mediano	Se deberá de verificar que solo el personal autorizado tenga acceso al Software de Aplicaciones
			Robo de equipos o de sus	Almacenamiento no protegido	Equipos de cómputo y periféricos no asegurados con	5	1	Mediano	Se deberá de verificar que solo el personal autorizado tenga acceso

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
			componentes		dispositivos de seguridad como candados.				al área de operaciones
				Uso inadecuado o negligente del control de acceso físico a edificios y ambientes	Indisponibilidad de control de vigilancia perimetral de parte del proveedor de servicios de vigilancia de personal	5	1	Mediano	Se deberá de verificar que solo el personal autorizado tenga acceso al área de operaciones
				Falta de protección física del edificio, puertas y ventanas	Indisponibilidad de seguros adicionales y dispositivos de refuerzo de seguridad en puertas y ventanas.	5	1	Mediano	Se deberá de verificar que solo el personal autorizado tenga acceso al área de operaciones
				Falta de proceso formal para revisar el derecho de acceso	Indisponibilidad de control de vigilancia perimetral de parte del proveedor de servicios de vigilancia de	5	1	Mediano	Se deberá de verificar que solo el personal autorizado tenga acceso al área de operaciones

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
					personal				
				Falta de mecanismos de monitoreo establecidos para las rupturas de la seguridad	Indisponibilidad de control de vigilancia perimetral de parte del proveedor de servicios de vigilancia de personal	5	1	Mediano	Se deberá de verificar que solo el personal autorizado tenga acceso al área de operaciones
			Uso inadecuado de los equipos	No hacer "logout" cuando se sale de la estación de trabajo	Uso no autorizado de las estaciones de trabajo que contienen copias de respaldo digitales para las cintas de respaldo por No hacer "logout" cuando se sale de la estación de trabajo	5	1	Mediano	Se deberá de implementar una Política en el AD, la cual bloquee las estaciones de trabajo que contienen copias de respaldo digitales para las cintas de respaldo a los 5 min de inoperatividad

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
				Descarga y uso incontrolado de software	Mal funcionamiento del Software de Aplicaciones por error humano	5	1	Mediano	Se deberá de realizar una política de seguridad para la descarga e instalación de software para los equipos de operaciones.
				Disposición o reutilización de medios de almacenamiento sin borrar apropiadamente	Mal uso de información de las estaciones de trabajo que contienen copias de respaldo digitales para las cintas de respaldo por Reutilización de equipos sin borrar apropiadamente la información	5	1	Mediano	Se deberá de implementar una directiva de rehúso y eliminación segura de medios.
				Ausencia de personal	No posibilidad de la administración del centro de datos por el personal responsable.	5	1	Mediano	Se deberá de asignar personal de reemplazo inmediato como contingencia previa coordinación con el

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
									equipo de operaciones.
			Obsolescencia de los componentes del equipo	Falta de esquemas de reemplazo periódicos	Fallas en el uso y administración de servicios y herramientas para la realización de copias de respaldo	5	1	Mediano	Se deberá crear un plan de renovación periódica de equipos.
				Equipo desfasado por vigencia tecnológica	Fallas en el uso y administración de servicios y herramientas para seguridad y protección de datos	5	1	Mediano	Se deberá crear un plan de renovación periódica de equipos.
			Corto circuito	Red inestable de energía eléctrica	Pérdida del suministro de electricidad en el área de operaciones por red inestable de energía eléctrica	3	1	Bajo	Se deberá programar mantenimiento de las estaciones de red eléctrica.

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
				Dependencia de proveedor de servicio público	Pérdida del suministro de electricidad en el área de operaciones por dependencia de proveedor de servicio público	5	1	Mediano	Se deberá de tener UPS y/o grupo electrógeno y se deberá de verificar que cuenten con mantenimiento
				Falta de redundancia de fuentes de energía	Pérdida del suministro de electricidad en el área de operaciones por falta de redundancia de fuentes de energía	5	1	Mediano	Se deberá de tener UPS y/o grupo electrógeno y se deberá de verificar que cuenten con mantenimiento

AI-7 Sistema de procesamiento de información.

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
AI-7	Sistema de procesamiento de información.	Son los sistemas alojados dentro del centro de datos quienes procesan la información de todas las áreas del SIS, estos sistemas pueden ser adquiridos o	Mal funcionamiento del software	Error humano	Mal funcionamiento del software de ingeniería por error humano	5	1	Mediano	Se deberá de verificar que solo el personal capacitado tenga acceso al software de ingeniería
				Software desfasado por vigencia tecnológica y sin soporte por parte del fabricante	Mal funcionamiento del software de ingeniería por software desfasado por vigencia tecnológica y sin soporte por parte del fabricante	5	2	Alto	Se deberá de verificar las versiones del software de ingeniería y de encontrarse alguno que se encuentre desfasado tecnológicamente, se deberá de migrar.
			Indisponibilidad del Software	Software obsoleto	Indisponibilidad del software de	4	1	Bajo	Se deberá crear un plan de mantenimiento que contemple

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
		desarrollados por el SIS.			ingeniería por Software obsoleto				la renovación de los equipos y licencias dentro de un tiempo analizado que determine la obsolescencia de un equipo de cómputo y/o de las licencias que contiene
				Software desfasado por vigencia tecnológica y sin soporte por parte del fabricante	Indisponibilidad del software de ingeniería por software desfasado por vigencia tecnológica y sin soporte por parte del fabricante	4	1	Bajo	Se deberá crear un plan de mantenimiento que contemple la renovación de los equipos y licencias dentro de un tiempo analizado que determine la obsolescencia de un equipo de cómputo y/o de las licencias que contiene
				Error humano	Indisponibilidad del software de ingeniería por error humano	5	1	Mediano	Se deberá de verificar que solo el personal capacitado y autorizado tenga acceso al software de ingeniería

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
				Uso incorrecto del software	Indisponibilidad del software de ingeniería por uso incorrecto del software	5	1	Mediano	Se deberá de verificar que solo el personal capacitado y autorizado tenga acceso al software de ingeniería
			Acceso no autorizado al sistema	Error humano	Acceso no autorizado al software de ingeniería por error humano	5	1	Mediano	Se deberá de verificar que solo el personal autorizado tenga acceso al software de ingeniería
				Incorrecta configuración	Acceso no autorizado al software de ingeniería por incorrecta configuración	5	1	Mediano	Se deberá de verificar que solo el personal autorizado tenga acceso al software de ingeniería
				Falta de eliminación y modificación de accesos del personal	Acceso no autorizado al software de ingeniería por falta de eliminación y	5	1	Mediano	Se deberá de verificar que solo el personal autorizado tenga acceso al software de ingeniería

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
					modificación de accesos del personal				

AI-8 Servicio de Energía Eléctrica.

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
AI-8	Servicio de Energía Eléctrica	Es el servicio público otorgado por el distribuidor de energía eléctrica, este servicio es administrado por la oficina de logística y	Pérdida del suministro de electricidad	Inexistencia o insuficiencia de acuerdo sobre el nivel de servicio	Pérdida del servicio de Energía Eléctrica por Inexistencia o insuficiencia de acuerdo	4	1	Bajo	Uso del grupo electrógeno, deberá existir un plan de rehabilitación de energía que se ponga en práctica según calendario, este debe de ser medido cada vez para que existan mantenimientos y

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
		el centro de datos es dependiente de ello.			sobre el nivel de servicio				adquisición de equipos adicionales o suministros de ser el caso.
				Problemas del proveedor respecto a los componentes del servicio	Pérdida del servicio de Energía Eléctrica por problemas del proveedor respecto a los componentes del servicio	4	1	Bajo	Uso del grupo electrógeno, deberá existir un plan de rehabilitación de energía que se ponga en práctica según calendario, este debe de ser medido cada vez para que existan mantenimientos y adquisición de equipos adicionales o suministros de ser el caso.
				Red inestable de energía eléctrica	Pérdida del servicio de Energía Eléctrica por Red inestable de energía	4	1	Bajo	Uso del grupo electrógeno, deberá existir un plan de rehabilitación de energía que se ponga en práctica según calendario, este debe de ser medido cada vez para que

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
					eléctrica				existan mantenimientos y adquisición de equipos adicionales o suministros de ser el caso.
			Fallas en el servicio de terceros	Problemas del proveedor respecto a los componentes del servicio	Fallas en el servicio de Energía Eléctrica por problemas del proveedor respecto a los componentes del servicio	4	1	Bajo	Uso del grupo electrógeno, deberá existir un plan de rehabilitación de energía que se ponga en práctica según calendario, este debe de ser medido cada vez para que existan mantenimientos y adquisición de equipos adicionales o suministros de ser el caso.
				No contar con otro enlace con proveedor diferente	Fallas en el servicio de Energía Eléctrica por no contar con otro enlace	4	1	Bajo	Uso del grupo electrógeno, deberá existir un plan de rehabilitación de energía que se ponga en práctica según calendario, este debe de ser medido cada vez para que

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
					con proveedor diferente				existan mantenimientos y adquisición de equipos adicionales o suministros de ser el caso.

AI-09 Grupo electrógeno.

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
AI-09	Grupo electrógeno	Es el equipo quien brinda de energía eléctrica al centro de datos en situaciones donde el proveedor de servicio no puede suministrarla, este equipo cubre temporalmente el	Indisponibilidad del equipo	Mantenimiento insuficiente	Indisponibilidad del equipo del Grupo Electrógeno por Mantenimiento insuficiente	5	1	Mediano	Se deberá contar con un plan de mantenimiento de la Grupo Electrógeno y se deberá de verificar periódicamente su ejecución
				Error humano	Indisponibilidad del	5	1	Mediano	Se deberá de verificar que

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
		suministro eléctrico de parte del proveedor. Este equipo tiene un encendido tardío y requiere de un sistema de continuidad eléctrica para cubrir su espera.			equipo del Grupo Electrógeno por Error humano				solo el personal capacitado tenga acceso al Grupo Electrógeno
				Obsolescencia Tecnológica	Indisponibilidad del equipo del Grupo Electrógeno por Obsolescencia Tecnológica	5	1	Mediano	Se deberá contar con un plan de mantenimiento de la Grupo Electrógeno y se deberá de verificar periódicamente su ejecución
			Mal funcionamiento del equipo	Mantenimiento insuficiente	Mal funcionamiento del equipo del Grupo Electrógeno por Mantenimiento insuficiente	5	1	Mediano	Se deberá contar con un plan de mantenimiento de la Grupo Electrógeno y se deberá de verificar periódicamente su ejecución
				Susceptibilidad a la humedad, al polvo y a la suciedad	Mal funcionamiento del equipo del Grupo Electrógeno por Susceptibilidad a la humedad, al	5	1	Mediano	Se deberá contar con un plan de mantenimiento de la Grupo Electrógeno y se deberá de verificar periódicamente su

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
					polvo y a la suciedad				ejecución
				Falta de mecanismos de monitoreo	Mal funcionamiento del equipo del Grupo Electrógeno por Falta de mecanismos de monitoreo	5	1	Mediano	Se deberá de realizar pruebas periódicas del Grupo Electrógeno para verificar que se encuentran en buen estado.
				Error humano	Mal funcionamiento del equipo del Grupo Electrógeno por Error humano	5	1	Mediano	Se deberá de verificar que solo el personal capacitado tenga acceso al Grupo Electrógeno
				Obsolescencia Tecnológica	Mal funcionamiento del equipo del Grupo Electrógeno por Obsolescencia Tecnológica	5	1	Mediano	Se deberá contar con un plan de mantenimiento de la Grupo Electrógeno y se deberá de verificar periódicamente su ejecución

AI-10 UPS

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
AI-10	UPS	Es el equipo quien brinda de energía eléctrica al centro de datos en situaciones donde el proveedor de servicio no puede suministrarla, este equipo cubre temporalmente el suministro eléctrico de parte del proveedor. Este equipo tiene un encendido tardío y requiere de un sistema de continuidad eléctrica	Indisponibilidad del equipo	Mantenimiento insuficiente	Indisponibilidad del equipo UPS por Mantenimiento insuficiente	5	1	Mediano	Se deberá contar con un plan de mantenimiento del UPS y se deberá de verificar periódicamente su ejecución
				Error humano	Indisponibilidad del equipo UPS por Error humano	5	1	Mediano	Se deberá de verificar que solo el personal capacitado tenga acceso al UPS
				Obsolescencia Tecnológica	Indisponibilidad del equipo UPS por Obsolescencia Tecnológica	5	1	Mediano	Se deberá contar con un plan de mantenimiento del UPS y se deberá de verificar periódicamente su ejecución
			Mal funcionamiento del equipo	Mantenimiento insuficiente	Mal funcionamiento del equipo UPS	5	1	Mediano	Se deberá contar con un plan de mantenimiento del UPS y se deberá de verificar periódicamente su ejecución

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
		para cubrir su espera.			Electrógeno por Mantenimiento insuficiente				
				Susceptibilidad a la humedad, al polvo y a la suciedad	Mal funcionamiento del equipo UPS por Susceptibilidad a la humedad, al polvo y a la suciedad	5	1	Mediano	Se deberá contar con un plan de mantenimiento del UPS y se deberá de verificar periódicamente su ejecución
				Falta de mecanismos de monitoreo	Mal funcionamiento del equipo UPS Electrógeno por Falta de mecanismos de monitoreo	5	1	Mediano	Se deberá de realizar pruebas periódicas del UPS para verificar que se encuentran en buen estado.
				Error humano	Mal funcionamiento	5	1	Mediano	Se deberá de verificar que solo el personal capacitado tenga acceso al

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
					del equipo UPS por Error humano				UPS
				Obsolescencia Tecnológica	Mal funcionamiento del equipo UPS por Obsolescencia Tecnológica	5	1	Mediano	Se deberá contar con un plan de mantenimiento del UPS y se deberá de verificar periódicamente su ejecución

AI-11 Infraestructura de Red.

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
AI-11	Infraestructura de red	Conexión de la red interna	Obsolescencia de los componentes del equipo	Falta de esquemas de reemplazo periódicos	Fallas en el uso y administración de servicios y herramientas para el servicio de red	5	1	Mediano	Se deberá crear un plan de renovación periódica de equipos.
				Equipo desfasado por vigencia tecnológica	Fallas en el uso y administración de servicios y herramientas para el servicio de red	5	1	Mediano	Se deberá crear un plan de renovación periódica de equipos
			Falla mayor	Mantenimiento insuficiente	Falla mayor de la Infraestructura de red por Mantenimiento insuficiente	5	1	Mediano	Se deberá contar con un plan de mantenimiento de la Infraestructura de red y se deberá de verificar periódicamente su ejecución

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
				Mala estructura del cableado	Falla mayor de la Infraestructura de red por Mala estructura del cableado	5	2	Alto	Se deberá contar con un plan de mantenimiento de la Infraestructura de red y se deberá de verificar periódicamente su ejecución
				Error Humano	Falla mayor de la Infraestructura de red por Error Humano	5	1	Mediano	Se deberá de verificar que solo el personal capacitado manipule la Infraestructura de red
				Cableado desordenado sin rotulado	Falla mayor de la Infraestructura de red por Cableado desordenado sin rotulado	5	2	Alto	Se deberá contar con un plan de mantenimiento de la Infraestructura de red y se deberá de verificar periódicamente su ejecución
			Hacking	Mala estructura del cableado	Hacking de la Infraestructura de red por Mala estructura del cableado	5	2	Alto	Se deberá contar con un plan de mantenimiento de la Infraestructura de red y se deberá de verificar periódicamente su ejecución

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
				Arquitectura de red insegura	Hacking de la Infraestructura de red por Arquitectura de red insegura	5	2	Alto	Se deberá contar con un plan de mantenimiento de la Infraestructura de red y se deberá de verificar periódicamente su ejecución
				Falta de afinamiento en los mecanismos de seguridad del equipamiento	Hacking de la Infraestructura de red por Falta de afinamiento en los mecanismos de seguridad del equipamiento	5	2	Alto	Se deberá contar con un monitoreo de las conexiones que se encuentran en la infraestructura de red

AI-13 Sistema de seguridad de puertas de acceso a la sala de servidores.

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
AI-13	Sistema de seguridad de puertas de acceso al centro de operaciones y sala de servidores	Es el personal que se encarga de la administración y operación de la sala de servidores, ellos tienen la responsabilidad de mantener operativo el centro de datos, administran los servicios y equipos de comunicaciones, tienen la obligación de mantener la seguridad de la información ejecutando los planes de seguridad, mantenimiento y contingencia respectivos.	Indisponibilidad del equipo	Mantenimiento insuficiente	Indisponibilidad del equipo del Sistema de seguridad de puertas de acceso por Mantenimiento insuficiente	5	1	Mediano	Se deberá contar con un plan de mantenimiento al Sistema de seguridad de puertas de acceso y se deberá de verificar periódicamente su ejecución
				Error humano	Indisponibilidad del equipo del Sistema de seguridad de puertas de acceso por Error humano	5	1	Mediano	Se deberá de verificar que solo el personal capacitado tenga acceso al Sistema de seguridad de puertas de acceso
				Obsolescencia Tecnológica	Indisponibilidad del equipo del Sistema de seguridad de puertas de acceso por Obsolescencia Tecnológica	5	1	Mediano	Se deberá contar con un plan de mantenimiento al Sistema de seguridad de puertas de acceso y se deberá de verificar periódicamente su ejecución
			Mal	Mantenimiento	Mal funcionamiento	5	1	Mediano	Se deberá contar con un

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
			funcionamiento del equipo	insuficiente	del Sistema de seguridad de puertas de acceso por Mantenimiento insuficiente				plan de mantenimiento al Sistema de seguridad de puertas de acceso y se deberá de verificar periódicamente su ejecución
				Susceptibilidad a la humedad, al polvo y a la suciedad	Mal funcionamiento del Sistema de seguridad de puertas de acceso por Susceptibilidad a la humedad, al polvo y a la suciedad	5	1	Mediano	Se deberá contar con un plan de mantenimiento al Sistema de seguridad de puertas de acceso y se deberá de verificar periódicamente su ejecución
				Falta de mecanismos de monitoreo	Mal funcionamiento del Sistema de seguridad de puertas de acceso por Falta de mecanismos de monitoreo	5	1	Mediano	Se deberá de realizar pruebas periódicas al Sistema de seguridad de puertas de acceso para verificar que se encuentran en buen estado.

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
				Error humano	Mal funcionamiento del Sistema de seguridad de puertas de acceso por Error humano	5	1	Mediano	Se deberá de verificar que solo el personal capacitado tenga acceso al Sistema de seguridad de puertas de acceso
				Obsolescencia Tecnológica	Mal funcionamiento del Sistema de seguridad de puertas de acceso por Obsolescencia Tecnológica	5	1	Mediano	Se deberá contar con un plan de mantenimiento al Sistema de seguridad de puertas de acceso y se deberá de verificar periódicamente su ejecución

AI-14 Personal de operaciones de centro de datos.

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
AI-14	Profesionales	Es el personal que se encarga de la administración, operación y mantenimiento de los recursos informáticos de la OGTI y del SIS, ellos tienen la responsabilidad de mantener operativo el centro de datos, administran los servicios y equipos de comunicaciones, los recursos y servicios TI, tienen la obligación de mantener la seguridad de la información ejecutando los planes	Poco compromiso con la seguridad de la información	Capacitación de seguridad insuficiente	Poco compromiso con la seguridad de la información de los Profesionales por Capacitación de seguridad insuficiente	5	3	Extremo	Se deberá de capacitar al personal sobre temas relacionados a seguridad de la información
				Falta de conciencia de seguridad	Poco compromiso con la seguridad de la información de los Profesionales por Falta de conciencia de seguridad	5	3	Extremo	Se deberá de capacitar al personal sobre temas relacionados a seguridad de la información

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
		de seguridad, mantenimiento y contingencia respectivos..	Divulgación de información	Capacitación de seguridad insuficiente	Divulgación de información de los Profesionales por Capacitación de seguridad insuficiente	5	2	Alto	Se deberá de capacitar al personal sobre temas relacionados a seguridad de la información
			Ruptura en la disponibilidad del personal	Ausencia del personal	Ruptura en la disponibilidad de los Profesionales por Ausencia del personal (enfermedad, agotamiento, saturación, renuncia inmediata, abandono)	4	1	Bajo	Se deberá considerar que los profesionales deben de tener refuerzo con otro profesional adicional y que las tareas deben de estar documentadas.

Código del Activo	Nombre del Activo	Descripción del activo	Amenaza	Vulnerabilidad	Nombre del Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Controles
			Ingeniería social	Capacitación de seguridad insuficiente	Ingeniería social del Coordinador de los Profesionales por Capacitación de seguridad insuficiente	5	1	Mediano	Se deberá de capacitar al personal sobre temas relacionados a seguridad de la información