

## RESOLUCIÓN N° 085 -2014-INVERMET-SGP

Lima, 24 ABR 2014

### VISTO:

El Memorando N° 030-2014-INVERMET-OPP de la Oficina de Planificación y Presupuesto, los Informes Nos 019 y 039-2014-INVERMET/OPP/INF del Área de Informática y el Informe N° 021-2014-INVERMET-OAJ de la Oficina de Asesoría Jurídica, y;

### CONSIDERANDO:

Que, mediante la Resolución Ministerial N° 246-2007- PCM, de 22 de agosto de 2007, se aprueba la aplicación y uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática, con la finalidad de coadyuvar a la creación de la infraestructura de Gobierno Electrónico, por considerar la seguridad de la información, como un componente importante para dicho objetivo;

Que, la referida norma técnica ofrece recomendaciones, procedimientos y actividades que deben seguir las entidades públicas para implantar un sistema de gestión de seguridad de la información, entre las cuales figura la "Gestión de Respaldo y Recuperación" que tiene por objetivo establecer los lineamientos y procedimientos que debe seguir una entidad con el fin de salvaguardar y garantizar la seguridad de la información esencial del negocio y del software, en concordancia con la política de recuperación diseñada, incidiendo en la provisión de servicios de respaldo que garanticen la seguridad de la información que la entidad considere esencial, siendo necesario definir el nivel de importancia de la información a recuperar, sometiendo a pruebas rutinarias sus procedimientos, para asegurar la eficacia y oportunidad en la recuperación de la información;

Que, el Área de Informática de la Oficina de Planificación y Presupuesto, a través de los Informes Nos 019 y 039-2014-INVERMET/OPP/INF de fecha 29 de enero y 17 de marzo de 2014, propone el documento denominado "Plan de Recuperación ante Desastres de Tecnología de Información del Sistema SIGA.NET", precisando que para su elaboración se aplicaron los lineamientos y procedimientos establecidos en la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI y la Norma Técnica Peruana NTP-ISO/IEC 27001:2008 EDI "Código de buenas prácticas para la gestión de seguridad", además de haber alineado dicho plan a las Técnicas Estándar Internacional ISO/IEC 22301 "Sistema de Gestión de la Continuidad del Negocio", ISO/IEC 31000:2009 "Gestión de Riesgos", así como las Buenas Prácticas del Business Continuity Institute (BCI) y el Disaster Recovery Institute (DRI), en la parte pertinente de procedimientos de recuperación de información, derivado de desastre, específicamente producido por incendio o sismo, sin considerar las etapas de gestión ni de continuidad del negocio;

Que, a efectos de establecer los procedimientos requeridos para la recuperación de tecnología de información del sistema que utiliza el Fondo Metropolitano de Inversiones – INVERMET, resulta necesario emitir el acto de administración que apruebe el documento denominado "Plan de Recuperación de Tecnología de



Información ante Desastres del Sistema SIGA.NET", conforme lo propuesto por el Área de Informática;

En uso de las facultades conferidas en el literal o) del artículo 20° del Reglamento del INVERMET, aprobado mediante Acuerdo de Concejo N° 083 de la Municipalidad Metropolitana de Lima; y,

Con el visado de la Oficina de Planificación y Presupuesto, de la Oficina de Asesoría Jurídica y del Área de Informática;

**SE RESUELVE:**

**Artículo Primero.-** Aprobar el documento denominado "Plan de Recuperación de Tecnología de Información ante Desastres del Sistema SIGA.NET" del Fondo Metropolitano de Inversiones – INVERMET, el mismo que en Anexo forma parte integrante de la presente resolución.

**Artículo Segundo.-** Encargar al Área de Informática, el registro del Plan señalado en el artículo precedente, en el Portal del Estado Peruano, Oficina de Gobierno Electrónico e Informático de la Presidencia del Consejo de Ministros.

**Artículo Tercero.-** Disponer que el Área de Informática adopte las medidas que correspondan con el objeto de aplicar de manera eficiente y oportuna el Plan que por esta resolución se aprueba.

**Artículo Cuarto.-** Encargar al responsable de la página web, la publicación de la presente resolución, en el portal web institucional ([www.invermet.gob.pe](http://www.invermet.gob.pe)).

**Regístrese y Comuníquese.**

 MUNICIPALIDAD METROPOLITANA DE LIMA  
Fondo Metropolitano de Inversiones INVERMET

  
LUIS ARTURO GARCIA COSSIO  
SECRETARIO GENERAL PERMANENTE (e)





# Plan de Recuperación de Tecnología de Información Ante Desastres del Sistema SIGA.NET

Febrero 2014

## RESUMEN

El presente Plan tiene por objetivo Recuperar Información del Sistema SIGA.Net con que cuenta INVERMET, así como establecer los procedimientos e implementar planes de contingencia tendientes a restaurar dicho Sistema ante un desastre de Sismo o Incendio.

Las Normas Técnicas Peruanas "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2da Edición y "NTP-ISO/IEC 27001: 2008 EDI Código de buenas prácticas para la gestión de la seguridad de la información" establecen los lineamientos que obligatoriamente deben tener en cuentas las entidades públicas para los casos de desastres informáticos, fallas de seguridad y pérdidas de servicio, puedan recuperar la información, restablecer el sistema y determinar la continuidad de negocio.

En el marco de la citada normatividad, se desarrolló el Plan de Recuperación de Tecnología de Información Ante Desastres del Sistema SIGA.NET, ante las contingencias que se pudieran generar, así como el procedimiento a seguir para restaurar el dicho Sistema, asociando aplicaciones y/o servicios y recursos necesarios para recuperar la información de datos del sistema SIGA.NET ante un desastre de sismo o incendio, previendo un plazo de 72 horas de ocurrido el desastre informático, para el restablecimiento del sistema.

Los alcances del presente Plan no comprenden el nivel de fallas de seguridad, de pérdidas de servicio y la disponibilidad de servicio, debido a que la entidad en la actualidad no cuenta formalmente con un manual de procedimientos.

Para elaborar este plan, se alinea al estándar internacional "ISO/IEC 22301: Sistemas de gestión de la continuidad del negocio" y a las buenas prácticas del Business Continuity Institute (BCI) y el del Disaster Recovery institute (DRI).

De dicho estándar, para desarrollar el presente plan solo se viene tomando la fase de implementación y la actividad del Plan de Recuperación ante Desastres, que establece las pautas para desarrollar un plan de contingencias de desastres informáticos derivados Incendio o Sismos debido a que las otras fases y actividades son para otros tipos de escenarios que se presenten o afecten la Continuidad de Negocio.



## PROPÓSITO

El propósito de este Plan de Recuperación de Tecnología de Información ante Desastres (DRP del inglés Disaster Recovery Plan) es recuperar la información del Sistema SIGA.NET y eventualmente restaurar y reestablecer dicho Sistemas, para cuyo efecto se establecen procedimientos y actividades que se deben seguir para cuando ocurra un sismo o incendio, a fin de garantizar el éxito y viabilidad del presente plan y así conseguir el objetivo de recuperar la información de establecer la continuidad de negocio del dicho Sistema.



Con el propósito de restaurar las aplicaciones y/o servicios y recursos necesarios para recuperar la información de datos del sistema SIGA.NET ante un desastre de sismo o incendio, el plan contempla un periodo de 72 horas de ocurrida el desastre informático, para el restablecimiento del sistema.



Así mismo el plan identifica los componentes claves requeridos para recuperar la información y dentro de las limitaciones, continuar con las Operaciones de Negocio del Sistema SIGA.NET luego de un incidente de Sismo o Incendio, dentro de estos componentes se encuentran:

- Involucrados en la recuperación.
- Recursos asociados.
- Análisis de Riesgos.
- Estrategias.
- Roles de Recuperación del Sistema SIGA.NET y TI.
- Fase de Actividades y de Restauración.
- Lista de Proveedores.

## ALCANCE

El alcance del presente Plan de Recuperación de Tecnología de Información Ante Desastres del Sistema SIGA.NET, es conseguir la recuperación oportuna de la información del Sistema SIGA.NET y buscar la restauración del mismo, para cuyo efecto se está considerando los siguientes aspectos:

- ✓ Estrategias de recuperación según la criticidad de los servicios de TI relacionados.
- ✓ Grupos y roles de recuperación.
- ✓ Actividades de Preparación, Respuesta, Operación Alternativa, Restauración y Retorno.
- ✓ Identificación de Personal Alternativo/Primario por cada Rol de Recuperación.
- ✓ Árbol de Llamadas del Plan de Recuperación ante Desastres (DRP).
- ✓ Recursos e insumos mínimos para la recuperación.
- ✓ Registros vitales y documentación de soporte indispensables para la recuperación.
- ✓ Dependencia de servicios y los recursos asociados.





## ÍNDICE

1. Introducción.....	6
2. Definiciones técnicas .....	9
3. Alcance del Plan .....	11
4. Estrategias .....	25
5. Equipos y Roles de Recuperación.....	31
6. FASE ANTES: Actividades de Preparación.....	35
7. FASE DURANTE: Actividades de Respuesta y de Operación Alternativa .....	38
8. FASE DESPUÉS: Actividades de Restauración y Retorno.....	41
9. Empleados asociados por Rol .....	43
10. Árbol de Llamadas .....	44
11. Recursos asociados al área.....	44
12. Lista de Proveedores .....	46
13. Lista de documentos de consulta .....	48
14. Recomendaciones .....	49
15. Factores críticos de éxito .....	51
16. Cuellos de Botella .....	51
Anexos .....	52
1. Formato de árbol de llamadas .....	52
2. Formato de Requerimiento .....	53



## PLAN DE RECUPERACIÓN ANTE DESASTRES DE TECNOLOGÍA DE INFORMACIÓN DEL SISTEMA SIGA.NET

### 1. Introducción

El presente Plan establece los procedimientos para la recuperación de información que contiene el sistema Interno de INVERMET denominado SIGA.NET en caso de sismo o incendio. Así como los procedimientos que se deben seguir para restaurar dicho Sistema, estableciendo las aplicaciones y/o servicios y los recursos asociados al sistema SIGA.NET para la recuperación ante un desastre de sismo o incendio, cuyo proceso de restablecimiento se ejecutará en un plazo de 72 horas.

En el desarrollo del presente Plan se han tomado en consideración las Normas Técnicas Peruanas "NTP-ISO/IEC 17799:2007 EDI Código de buenas prácticas para la gestión de la seguridad de la información. 2da Edición" y la "NTP-ISO/IEC 27001: 2008 EDI Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información"; asimismo se viene aplicando la norma estándar internacional "ISO/IEC 22301: Sistemas de Gestión de la Continuidad del Negocio" y la norma "ISO/IEC 31000:2009 Gestión de Riesgos", todos ellos en la parte pertinente que es aplicable, a los alcances del presente plan, es decir a la recuperación de la información del sistema SIGA NET y la probabilidad de la restauración del mismo en un periodo corto.

Al respecto, de la norma técnica peruana "NTP-ISO/IEC 17799:2007 EDI, se está tomando como referencia el inciso 10.5.1, referida a la "Gestión de Respaldo y Recuperación", la misma que tiene por objetivo establecer los lineamientos y procedimiento que una entidad debe seguir, con el fin de salvaguardar y garantizar la seguridad de toda la información esencial del negocio y del software, en concordancia con la política de recuperación diseñada, incidiendo en la provisión de servicios de respaldo que garanticen la seguridad de la información que la entidad considere esencial, por lo que es necesario definir el nivel necesario de recuperación de la información, debiéndose comprobar y probar regularmente dichos procedimientos de recuperación para asegurar que son eficaces y que pueden cumplirse en el tiempo establecido por los procedimientos operativos de recuperación a fin de mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación, es decir recomienda como estrategia de respaldo, el desarrollo de procedimientos rutinarios.

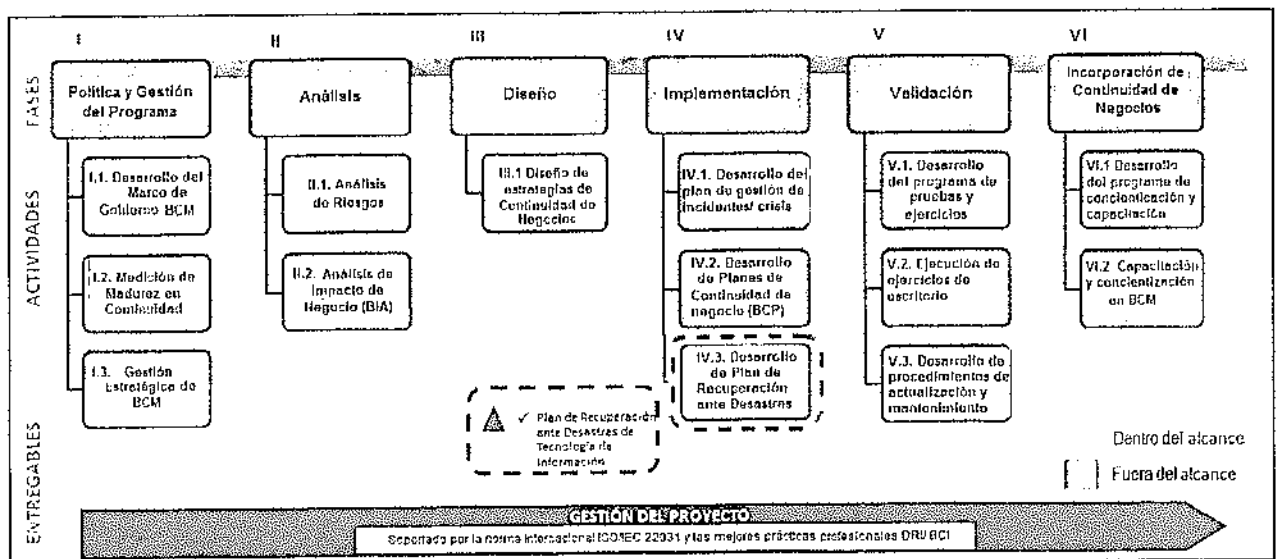


Del mismo modo el inciso 14.1 de la Normas Técnicas Peruanas "NTP-ISO/IEC 17799:2007 EDI, "Código de buenas prácticas para la gestión de la seguridad de la información. 2da Edición", en relación a "Aspectos de Gestión de Continuidad del Negocio", precisa que se debe implementar un proceso de gestión de continuidad de negocio para reducir, a niveles aceptables, la interrupción causada por desastres y fallas de seguridad, concordando con lo recomendado en la norma "NTP-ISO/IEC 27001: 2008 EDI Técnicas de Seguridad. Sistemas de gestión de seguridad de la Información ",

Los alcances del presente Plan no comprenden el nivel de fallas de seguridad, debido a que la entidad en la actualidad no cuenta formalmente con manual de procedimientos.

Este documento muestra el plan de recuperación de información, aplicaciones del SIGA.NET y recursos asociados a éste, ante desastres provenientes de sismo e incendio, el cual está alineado al estándar internacional ISO/IEC 22301 y a las buenas prácticas del *Business Continuity Institute (BCI)* y del *Disaster Recovery Institute (DRI)*.

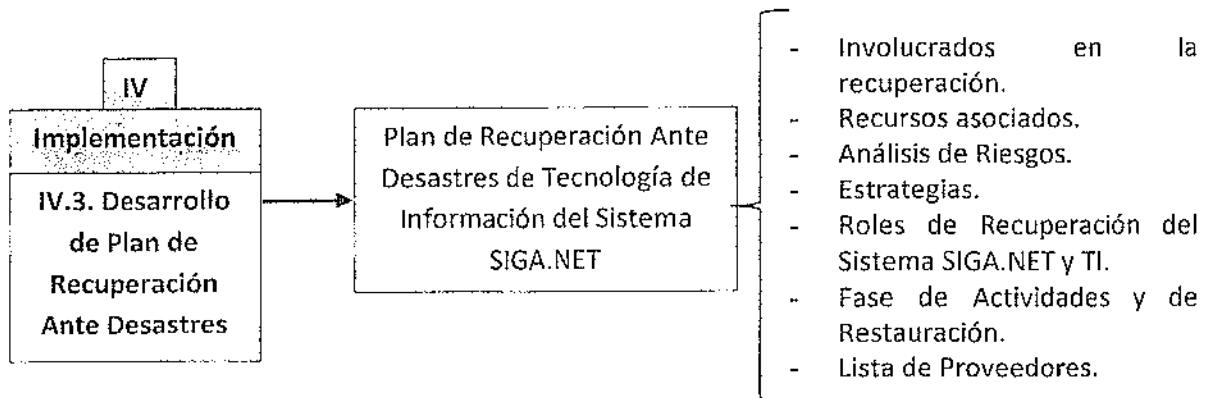
El estándar internacional ISO/IEC 22301 y a las buenas prácticas del *Business Continuity Institute (BCI)* y del *Disaster Recovery Institute (DRI)* que establecen las pautas de cómo se debe desarrollar el plan para el fin propuesto, determinando los alcances del mismo y los objetivos esperados. Por ello, que en el siguiente gráfico se muestra el alcance del Plan de Recuperación ante Desastres de Tecnología de Información del sistema SIGA.NET, estableciendo en líneas punteadas dentro de la fase IV de Implementación, el nivel IV.3 que corresponde al Desarrollo de Plan de Recuperación ante Desastres de Tecnología de Información, que es el marco conceptual y de realización del presente plan, sin comprender en ella, las etapas de gestión ni de continuidad del negocio a que se refieren los niveles IV.1 y IV.2, que serán desarrollados más adelante.



--- Situación Actual

Dicho estándar se tomara la fase de implementación y la actividad del Plan de Recuperación ante Desastres para realizar nuestro Plan de Recuperación de Tecnología de Información Ante Desastres del Sistema SIGA.NET. Las otras fases y actividades son para otros tipos de escenarios en la Continuidad de Negocio.

Para implementar nuestro Plan de Recuperación de Desastres de Tecnología de Información del Sistema SIGA.NET tomaremos la fase y la actividad que nos muestra en la figura del estándar internacional "ISO/IEC 22301:



En el Plan Recuperación de Desastres de Tecnología de Información del Sistema SIGA.NET se elaboró un análisis de Riesgo siguiendo la metodología del estándar "ISO/IEC 31000:2009: Gestión de Riesgos" donde muestra la identificación, gestión y control de los principales riesgos que existen en los procesos críticos relacionados al Sistema SIGA.NET de INVERMET, y estrategia en un escenario de sismo o incendio, para la recuperación de las aplicaciones y/o servicios de TI.

- Esta norma proporciona directrices genéricas para el diseño, implementación y mantenimiento de los procesos de gestión de riesgos. Este enfoque de la formalización de las prácticas de gestión del riesgo facilitará una mayor adopción de una gestión de riesgos del Sistema SIGA.NET. Esta norma, también se adapta a múltiples sistemas de gestión en el ámbito de aplicación de este enfoque a la gestión de riesgos es permitir a todas las tareas estratégicas, de gestión y de funcionamiento de una organización a lo largo de los proyectos, funciones y procesos para ser alineados a un conjunto común de objetivos de gestión de riesgos.

Se realizó un Plan de Recuperación de Tecnología de Información ante Desastres del Sistema SIGA.NET que se ejecutara para restablecerlo en 72 Horas, y que involucra lo siguiente:

- ✓ Contabilidad.
- ✓ Presupuesto.
- ✓ Tramite Documentario.
- ✓ Logistico.
- ✓ Tesoreria.
- ✓ Activo Fijo.

Así mismo como los recursos asociados a la recuperación son:

- ✓ Recursos Humanos.
- ✓ Infraestructura.
- ✓ Tecnología.
- ✓ Información de Proveedores.



Se formó equipos y roles de recuperación del Sistema SIGA.NET y TI con sus roles principales y funciones básicas. Las fases durante las actividades de respuestas y de operación del personal, infraestructura, tecnología e información de proveedores.



## 2. Definiciones técnicas

Término	Definición
<p><b>BCM (Gestión del Programa de Continuidad de Negocios)</b></p>	<p>Es un proceso holístico (integral) que identifica posibles debilidades que impactan la continuidad de las operaciones de la organización. Permite obtener una capacidad de respuesta efectiva, con lo cual, salvaguarda principalmente al personal, los intereses, la reputación, imagen o nombre y, el valor de la empresa. BCM es un proceso continuo, "vivo" dentro de la organización ya que se da de manera permanente, con el objetivo de mantener preparado al negocio en los momentos más difíciles como son los desastres.</p>
<p><b>BCP (Plan de Continuidad del Negocio)</b></p>	<p>Un plan o documento claramente definido a ser utilizado en una situación de emergencia, incidente, desastre o crisis. Usualmente un plan considera la recuperación de procesos, recursos y servicios a través de acciones específicas a realizar, con personal clave previamente capacitado.</p>

Término	Definición
<b>BIA (Análisis de Impacto al Negocio)</b>	<p>Es un análisis a nivel ejecutivo por medio de la cual una organización determina de manera cuantitativa y cualitativa impactos, efectos, y pérdidas que podrían resultar si la organización sufre una interrupción seria en sus operaciones. Establece las funciones y procesos críticos, sus prioridades de recuperación e interdependencias a fin de determinar tiempos de recuperación objetivo (RTO) y puntos objetivos de recuperación (RPO).</p> <p>Los resultados son utilizados para la toma de decisiones respecto a las estrategias de recuperación, y son la base para realizar los planes.</p>
<b>Crisis</b>	<p>Una ocurrencia o percepción que amenaza las operaciones, personal, marca, reputación, confianza, y/o cualquier riesgo estratégico que afecte los objetivos del negocio.</p>
<b>Desastre</b>	<p>Un evento catastrófico repentino no planeado que causa daños o pérdidas irreparables. Un evento que compromete la disponibilidad de funciones críticas, procesos o servicios por un periodo de tiempo de manera no aceptable. Un evento donde la alta dirección de una organización activa su plan de continuidad.</p>
<b>Posible Desastre</b>	<p>Ha ocurrido una falla en el área que ha paralizado el proceso, pero todavía está en evolución – es una alerta”, solo se pide que se informe de la situación actual, no se moviliza personal.</p>
<b>Alerta de Desastre</b>	<p>El RTO más crítico está por vencerse, de manera preventiva se solicita a los Áreas de soporte iniciar las coordinaciones para el transporte del personal y habilitación de centro alternativo, recursos, registros vitales, proveedores y Áreas de las que se depende.</p>
<b>Declaración de Desastre</b>	<p>Es un hecho que el RTO se vence, antes de ello, se decide activar los planes, para lo cual se da inicio a la movilización del personal al centro alternativo y a las pruebas preliminares de los recursos a utilizar.</p>
<b>DRP (Plan de Recuperación ante Desastres)</b>	<p>Un plan de continuidad (BCP) enfocado a la recuperación de los servicios ofrecidos por los Áreas de tecnología; Sistemas TI, Centro de Control y, Telecomunicaciones; y a la recuperación del área y a sus procesos en sí.</p>
<b>Registro Vital</b>	<p>Cualquier documento o recurso difícilmente sustituible sin el cual no es posible la recuperación de un servicio de tecnología, proceso o función del negocio.</p>
<b>MTPD (Período Máximo Tolerable de Interrupción)</b>	<p>Es el periodo de tiempo después del cual la viabilidad de una organización se verá amenazada de forma irrevocable si no puede reiniciar la entrega de un producto, proceso o servicio específico.</p>



Término	Definición
RTO (Tiempo Objetivo de Recuperación)	Uno de los resultados clave del BIA que identifica el tiempo en el cual las actividades críticas y/o sus dependencias deben ser recuperadas para que la viabilidad de la Organización no se vea amenazada, este tiempo comienza a partir de la invocación del plan. El RTO debe asegurar que no se excede el MTPD.
RPO (Punto Objetivo de Recuperación)	Es el tiempo transcurrido desde el que la información debe ser restaurada (última copia de respaldo) antes de ocurrido el evento serio o desastre que permite la operación de una actividad una vez que ésta se haya reiniciado. Desde la perspectiva de tecnología se refiere a la frecuencia de las copias de respaldo.
Sitio alternativo de Negocio (SAN)	Es un sitio mantenido en espera para ser utilizado cuando ocurra en evento serio o desastre, con el objetivo de mantener la continuidad del negocio a través de las actividades de misión crítica. En el caso de Tecnología de Información el término que aplica se llama Centro de Cómputo Alterno. Los tipos de sitios alternos son: HOT, WARM, y COLD (mientras más caliente, más costoso ya que los recursos críticos están duplicados y sincronizados).
Centro Alterno de Operaciones (CCA)	Se refiere al centro alternativo de procesamiento, almacenamiento y/o de comunicaciones el cual se mantiene listo para ser utilizado en caso ocurra una interrupción seria en el centro primario. Su principal objetivo consiste en minimizar la interrupción de los servicios y aplicaciones críticas que las áreas del negocio demandan.

### 3. Alcance del Plan

- **BIA (Indicadores de Continuidad)**

Las aplicaciones del Sistema SIGA.NET involucrados en la recuperación son:

Módulos de SIGA.NET	Funcionalidades Principales	RTO	RPO
Contabilidad	<ul style="list-style-type: none"> <li>• Emisión de Documentos de Pago (Bienes y Servicios, Consultorías, RRHH)</li> <li>• Certificaciones</li> </ul>	12 horas	24 horas
Presupuesto	<ul style="list-style-type: none"> <li>• Modificaciones Presupuestarias (internas y entre específicas)</li> <li>• Reportes</li> </ul>	24 horas	72 horas

Módulos de SIGA.NET	Funcionalidades Principales	RTO	RPO
Trámite Documentario	<ul style="list-style-type: none"> <li>Administración y Seguimiento de Trámites documentarios internos y externos.</li> <li>Reportes</li> </ul>	24 horas	24 horas
Logística	<p><b>Compras:</b></p> <ul style="list-style-type: none"> <li>Formulación de Requerimientos</li> <li>Certificación Presupuestal</li> <li>Emisión de Orden de Compra</li> <li>Emisión de Orden de Servicio</li> </ul> <p><b>Almacén:</b></p> <ul style="list-style-type: none"> <li>Internamiento</li> <li>Despacho de productos</li> </ul>	24 horas	48 horas
Tesorería	<ul style="list-style-type: none"> <li>Emisión de Documentos de Pago.</li> <li>Emisión de Cartas Fianzas</li> </ul>	24 horas	72 horas
Activo Fijo	<ul style="list-style-type: none"> <li>Registro, Modificación, Eliminación y Seguimiento de Activos Fijos.</li> </ul>	72 horas	72 horas

MTPD: 72 horas

• **Recursos Asociados a la recuperación**

A continuación, se muestra la lista de recursos asociados a la recuperación de los servicios, asumiendo que sólo se cuenta con el personal principal:

Tipo	Módulo	Nombre de recurso
Recursos humanos	Contabilidad	Dos (2) especialistas en contabilidad
	Presupuesto	Dos (2) especialistas presupuestales
	Logística	Tres (3) encargados de servicios generales y almacén.
	Trámite documentario	Un (1) encargado de trámites internos y externos.
	Tesorería	Dos (2) encargados de ingresos y egresos
	Activo Fijo	Un (1) encargado de administración de activos
Infraestructura	Todos los Módulos	Oficinas de operación



Tipo	Módulo	Nombre de recurso
Tecnología	Todos los Módulos	Teléfonos / celulares (Mínimo seis ) Computadoras / laptop (Mínimo once) Impresoras / Fotocopiadoras (Mínimo dos)
		Servidores: ✓ Servidor de Base de Datos, Servidor de aplicaciones, Domain controler y Check Point 4000 Appliances.
		Redes: ✓ Radio enlace (primera opción) ✓ Dos (2) Switchs (de 24 y 48 puertos respectivamente) ✓ Un (1) Access point ✓ Router
		Correo electrónico de dominio de INVERMET; es decir, el institucional. ✓ Sistema SIGA.NET
Información	Todos los Módulos	<ul style="list-style-type: none"> <li>✓ Información de proyectos</li> <li>✓ Información de activos</li> <li>✓ Órdenes de pago</li> <li>✓ Órdenes de compra</li> <li>✓ Órdenes de Servicio</li> <li>✓ Información de Certificaciones</li> <li>✓ Información de trámites documentarios internos y externos.</li> </ul>
Proveedores	Todos los Módulos	<ul style="list-style-type: none"> <li>✓ Optical Networks (Servicio de Internet dedicado)</li> <li>✓ Telefónica del Perú (Servicio de telefonía física y celular)</li> <li>✓ Hermes (Custodia de backup)</li> <li>✓ Propietario de Edificio (Housing del DataCenter)</li> <li>✓ PMS ( Actualización y soporte especializado al sistema de seguridad firewall checkpoint)</li> <li>✓ Luz del sur (Fluido eléctrico)</li> </ul>

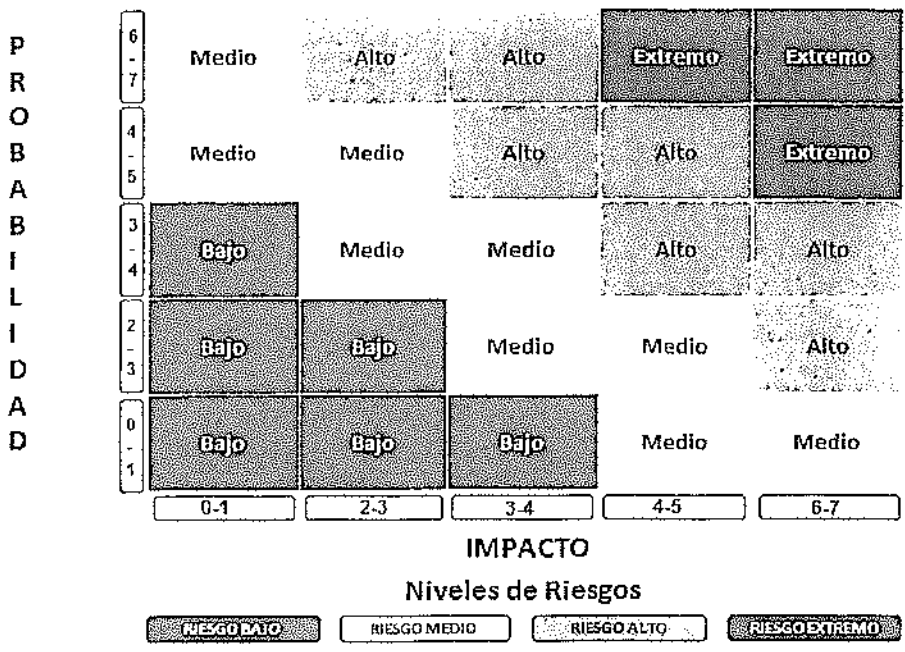


• **Análisis de Riesgos**

Se elaboró siguiendo la metodología del estándar internacional "ISO/IEC 31000: 2009: Gestión de Riesgos", que proporciona principios y directrices sobre la gestión de riesgos.

A continuación, se presenta la identificación, gestión y control de los principales riesgos que existen en los procesos críticos relacionados al Sistema SIGA.NET de INVERMET.

Para poder obtener gráficamente la severidad de los riesgos identificados, se utiliza la siguiente escala.





Leyenda:

FRECUENCIA	Descripción
PERM	Permanente
PERIO	Periódico
OCA	Ocasional

TIPO DE CONTROL	Descripción
PM	Preventivo Manual
PA	Preventivo Automático
DM	Detectivo Manual
DA	Detectivo Automático
CM	Correctivo Manual
CA	Correctivo Automático







Activo		Vulnerabilidad		Amenaza		Riesgos			Controles efectivos			Evaluación de Riesgos Controlados				
Descripción	Descripción	Descripción	ID	Descripción	Evento	Causa	ID	Descripción	Responsable	Tipo de Control	Nivel de Control	Frecuencia	Impacto	Probabilidad	Nivel de Riesgo	Criticidad
Sede Central de INVERMET	Centro ubicado en una zona sísmica (Ilima), rodeada de centros empresariales y negocios.	Incendios o terremotos que destruyan el local o lo dejen en todo caso inhabilitado parcialmente		Pérdida parcial o total de infraestructura de sede central de INVERMET.	Sismo/ Incendio	Falta de espacio físico para operar		(grifos, gabinetes de manga, extinguidores). Mantenimiento y conservación de los equipos contra incendios. Señalización de: Rutas de escape, puertas y escaleras de emergencia; así como las tareas de seguridad.	Área de informática	PM	Regular	PERIO	5	4	9	
									Mantenimiento	PM	Regular	PERM				
									Área de informática	PM	Regular	PERM				
									Formación de brigadas de evacuación.	Área de informática	PM	Regular	PERM			

A  
L  
T  
O



Activo		Vulnerabilidad		Amenaza		Riesgos			Controles efectivos			Evaluación de Riesgos Controlados					
Descripción	Descripción	Descripción	ID	Descripción	Escenario	Evento	Causa	ID	Descripción	Responsable	Tipo de Control	Nivel de Control	Frecuencia	Impacto	Probabilidad	Nivel de Riesgo	Criticidad
Personal Crítico de INVERMET	No cuentan con personal alternativo para ningún puesto	Incendios o terremotos que inhabiliten completamente al personal crítico	R03	No definir personal alternativo en caso de no contar con el directo.	Sismo/ Incendio	Error	Falla de personal	C11	Realizar simulacros de evacuación	RRHH	PM	Regular	PERM	3	4	7	M E D I O
Data Center compartido de INVERMET	Se encuentra en el Octavo piso del mismo edificio con servicio tercerizado	Pérdida Total o Parcial de los equipos e infraestructura del Data Center	R04	Daño en el Data center compartido	Incendio	Error de respaldo	Respaldo y Control inadecuado	C12	Establecer personal alternativo para las actividades críticas del proceso de identificación Contar con Centro de Cómputo de Operaciones de Respaldo donde, en caso de la infraestructura compartida este intacta, se pueda reoperar en este sin mayor complicación Contar con un servidor backup, de	Área de Contabilidad	PA	Regular	PERM	7	5	12	E V A L U A D O
								C13		Área de Contabilidad	PA	Regular	PERM				

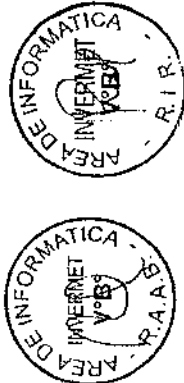


Activo	Vulnerabilidad	Amenaza	Riesgos	Controles efectivos	Evaluación de Riesgos Controlados
--------	----------------	---------	---------	---------------------	-----------------------------------

Descripción	Descripción	Descripción	ID	Descripción	Evento	Escenario	Causa	ID	Descripción	Responsable	Tipo de Control	Nivel de Control	Frecuencia	Impacto	Probabilidad	Nivel de Riesgo	Críticidad
Registros vitales	No se manejan copias de respaldo	No existe revisión periódica de conexiones de redes en caso cortos circuitos		Pérdidas de registros vitales (planos de red, software, Sistema SIGA.NET, hardware, bases de datos, etc.),	Error de respaldo y backup	Incendio	Falla de disponibilidad de procesos relevantes	C14	idénticas características que respalden en caso de pérdida total en el Data Center Manejo de copias de respaldo en caso de información relevante y backup de equipos críticos, de base de datos en Centro Alterno de Operaciones Realizar revisiones de hardware y conexiones de redes para evitar cortos circuitos.	Área de Informática	PA	Regular	PERM	4	4	8	ALTO
								C15		Soporte	PM	Regular	PERIO				



Activo	Vulnerabilidad	Amenaza	Riesgos				Controles efectivos				Evaluación de Riesgos Controlados				
Descripción	Descripción	Descripción	Descripción	Escenario	Evento	Causa	ID	Descripción	Responsable	Tipo de Control	Frecuencia	Impacto	Probabilidad	Nivel de Riesgo	Criticidad
Cables de energía del edificio de INVERMET	Son compartidos y la energía es brindada por un proveedor	Ocurrencia de cortos circuitos	Daño en la Infraestructura Administrativa por los cables de energía del edificio y daño en el centro de cómputo, a causa de una sobrecarga de energía por parte del proveedor externo que abastece energía	Incendio	Error de cableado y conectividad	Proceso y control inadecuado	C16	Contar con interruptores termomagnéticos en la sub-estación eléctrica, que no permite el paso de sobretensión y cortocircuito. Contar con servicios de mantenimiento preventivo a la sub-estación eléctrica e interruptores termomagnéticos.	Soporte	PA Regular	PERIO	6	6	12	ALTO
Equipos de Comunicación	No se cuenta con equipos de respaldo ni se realiza pruebas de disponibilidad de comunicación en caso ocurra un incidente	Sismo que inhabilita todo equipo de comunicación principal	Daño a la infraestructura de telecomunicaciones (interrupción del servicio de voz (telefonía) y/o datos, cualquier problema físico que detenga las operaciones de los equipos de	Sismo	Error de respaldo	Respaldo y Control inadecuado	C13	Contar con Centro de Cómputo de Respaldo (en otra ubicación física con igual número de equipos y de idénticas características a los del Centro de Cómputo Principal.	Gerente de Finanzas	PA Regular	PERM	4	5	9	ALTO



Activo	Vulnerabilidad	Amenaza	Riesgos				Controles efectivos				Evaluación de Riesgos Controlados						
Descripción	Descripción	Descripción	ID	Descripción	Escenario	Evento	Causa	ID	Descripción	Responsable	Tipo de Control	Nivel de Control	Frecuencia	Impacto	Probabilidad	Nivel de Riesgo	Criticidad

				comunicación entre áreas para el buen manejo del proceso o afecte el medio de transmisión).													
			C14	Poseer doble fuente de alimentación de energía (diferentes UPS) en todos los Equipos Críticos (de Comunicación, Servidores, etc.) en ambos Centros de Cómputo. Contar con idénticas características en los Enlaces de						Soporte	PA	Regular	PERM				
			C15	de los principales proveedores de telecomunicaciones. Realizar pruebas periódicas de disponibilidad de comunicación.						Soporte	PA	Regular	PERM				
			C16							Soporte	PA	Regular	PERIO				
			C17						El sistema de comunicación.	Área	PA	Regular	PERM	6	5	11	

No se tiene un

Proveedor

R Información de

Sismo

Incumplí

Desempeño.

C17



EXPREDO

Activo	Vulnerabilidad	Amenaza	ID	Descripción	Escenario	Evento	Causa	ID	Descripción	Responsable	Tipo de Control	Nivel de Control	Frecuencia	Impacto	Probabilidad	Nivel de Riesgo	Criticidad
			Riesgos			Controles efectivos			Evaluación de Riesgos Controlados								
Data Crítica	SLA con el proveedor de backup que asegure la contingencia de la información brindada	perdida la información porque no la tiene respaldada	08	proyectos, presupuesto, inventarios, solicitudes de Compra y de servicio, que no sean accesibles para el personal por falta o error en el backup	Sismo	mimiento de responsabilidad es y respaldado	respaldado y proceso inadecuado		genera una copia de respaldo al gestor de hechos vitales en un sistema backup alternativo, diferente al brindado al proveedor. Contar con proveedores de emergencia para casos de interrupciones o falta de disponibilidad de proveedores principales. Garantizar continuidad de negocios en los SLA establecidos con los proveedores involucrados. Al realizar una solicitud de activos de respaldo, considerar en	de informática	Control	Regular	PERM	4	3	7	
Telefonía, Firewall e Internet	No se cuenta con el servicio de proveedores alternos	Proveedores principales inhabilitados	09	Falla en prestación de servicios tercerizados (internet, hosting, firewall, telefonía)	Sismo	Error de Servicio	Falta de disponibilidad de proveedor	C18	Logística	Logística	PM	Regular	PERM	4	3	7	M E D I O
Activos Relevantes	No hay priorización de activos en caso desastre	Pérdida parcial o total de activos relevantes	10	No definir activos relevantes del proceso para ser respaldados	Sismo/ Incendio	Error de manejo de datos	Mantenimiento o carga	C20	Cada Área involucrada	Cada Área involucrada	PM	Regular	PERM	6	5	11	E X T R E M O





Activo		Vulnerabilidad		Amenaza		Riesgos				Controles efectivos				Evaluación de Riesgos		Controlados	
Descripción	Descripción	Descripción	ID	Descripción	Escenario	Evento	Causa	ID	Descripción	Responsable	Tipo de Control	Frecuencia	Impacto	Probabilidad	Nivel de Riesgo	Criticidad	
		no respaldados por otros		y/o duplicados en el Centro Alterno de Operación.													
Personal Alterno	No se cuenta con personal alternativo capacitado para realizar tareas primarias	Terremoto o incendio que inhabilita a personal capacitado	R 1 1	Personal alternativo (en caso se defina) no capacitado para restauración de operaciones.	Sismo/ Incendio	Incumplimiento de roles y capacitaciones	Desempeño y Control inadecuado	C21	ella una sección de respaldo y recuperación donde se detalla las pautas que se deben tener en cuenta para la definición de activos a respaldar. Realizar capacitaciones, entrenamiento de las principales funciones y manejo de sistema para personal alternativo.	RRHH	PM	PERM	2	2	4		
CD/DVD de backup	La información respaldada no es administrada en la nube	Información protegida por el proveedor inhabilitada o pérdida	R 1 2	Soporte físico para CD/DVD de backup sin copia de respaldo	Sismo/ Incendio	Incumplimiento de responsabilidades y respaldo	Fallas en respaldo de disco	C22	información que se almacena en el CD, primero esté en archivos	Almac enarmento	PA	PERM	4	3	7		

B  
A  
J  
O

M  
E  
D  
I  
O







#### 4. Estrategias

Las estrategias planteadas fueron diseñadas a partir de distintas capacidades con las que cuenta la entidad tales como presupuesto, personal, estructura y cultura organizacional.

La recuperación de las aplicaciones y/o servicios de TI están en función a la disponibilidad de los componentes mencionados a continuación:

**Escenario: Sismo o Incendio**

Componente	Definición de la estrategia
  <p data-bbox="279 1019 550 1086"><b>Infraestructura de TI (servidores)</b></p>	<p><b>Situación actual:</b></p> <ul data-bbox="651 716 1369 1086" style="list-style-type: none"> <li>• El servicio de respaldo es brindado por un proveedor externo (Hermes).</li> <li>• La frecuencia de respaldo de los servidores es semanal de acuerdo a la cantidad de transacciones que se realicen.</li> <li>• El servicio de seguridad y vigilancia al Centro de Datos principal lo realiza Protransporte como parte del servicio de alquiler de un espacio para un rack de servidores, este centro de datos está ubicado en el 8vo Piso del edificio de Protransporte.</li> </ul> <p><b>Estrategia propuesta:</b></p> <ul data-bbox="651 1120 1369 1411" style="list-style-type: none"> <li>• Ajustar las políticas de respaldo con el proveedor, con el fin de poder cumplir el RPO definido para los procesos críticos de continuidad ya que, actualmente estos valores son iguales poniendo a la entidad en una situación límite con grandes probabilidades de no cumplir los objetivos de recuperación.</li> <li>• Contar con un Centro de Datos alternativo que cuente con base de datos y servidores con replicación en línea.</li> </ul>
<p data-bbox="247 1579 590 1646"><b>Infraestructura de Comunicaciones (enlaces)</b></p>	<p><b>Situación actual:</b></p> <ul data-bbox="651 1456 1369 1601" style="list-style-type: none"> <li>• Enlaces de comunicación que soportan el acceso de usuarios autorizados a través de internet desde el centro alternativo de operaciones (sede) al centro de datos desde un punto de acceso a través de internet.</li> </ul> <p><b>Estrategia propuesta:</b></p> <ul data-bbox="651 1646 1369 1780" style="list-style-type: none"> <li>• Implementar un enlace de comunicación dedicado entre el centro alternativo de operaciones y de datos con el objetivo de asegurar un mejor tiempo de recuperación y el acceso adecuado de los usuarios a la red.</li> </ul>



Componente	Definición de la estrategia
<p><b>Medios de Transporte</b></p>	<p><b>Situación actual:</b></p> <ul style="list-style-type: none"> <li>• Los medios de transporte en caso de activación de un centro alternativo de operaciones no están contemplados.</li> </ul> <p><b>Estrategia propuesta:</b></p> <ul style="list-style-type: none"> <li>• Considerando la ubicación y los posibles obstáculos de acceso que se puedan generar después de ocurrido el sismo (como cierre de calles u obstaculización de pistas), se pueden plantear diferentes alternativas como:           <ul style="list-style-type: none"> <li>✓ Transporte de buses particulares para la entidad.</li> <li>✓ Entrega de "vales por concepto de transporte" que cubran un porcentaje del gasto de transporte extra que genere la nueva ubicación.</li> </ul> </li> </ul>
<p><b>Personal Alterno</b></p>	<p><b>Situación actual:</b></p> <ul style="list-style-type: none"> <li>• La entidad no cuenta con personal informático alerno en otros locales especializado Tecnologías de Información.</li> </ul> <p><b>Estrategia propuesta:</b></p> <ul style="list-style-type: none"> <li>• Designar personal titular y alerno considerando los siguientes aspectos:           <ul style="list-style-type: none"> <li>✓ Deberán vivir como mínimo en diferentes zonas o distritos de Lima.</li> <li>✓ No deberán realizar las mismas actividades en un mismo instante de tiempo para no generar cuellos de botella y retrasos.</li> </ul> </li> <li>• En caso el titular y el alerno se encuentren ausentes, se deberá contactar al proveedor de RRHH, con quien previamente se establecieron acuerdos para poder cumplir con los requerimientos de continuidad. Dicho agente deberá proporcionar al personal pertinente de acuerdo al perfil solicitado.</li> <li>• El personal alerno deberá contar con un manual de funciones detallando las principales tareas y responsabilidades que deberá cumplir, disminuyendo las dependencias a una sola persona.</li> </ul>
<p><b>Medios de comunicación</b></p>	<p><b>Situación actual:</b></p> <ul style="list-style-type: none"> <li>• Cuentan con correo electrónico.</li> <li>• Algunas personas cuentan con Blackberry, Smartphones, RPM o RPC.</li> </ul>



Componente	Definición de la estrategia
	<p><b>Estrategia propuesta:</b></p> <ul style="list-style-type: none"> <li>Mantener el uso de teléfonos móviles como Blackberry o Smartphones para asegurar el acceso al correo electrónico interno.</li> <li>Asignar teléfonos al personal clave en el proceso de recuperación con el fin de no interrumpir las comunicaciones de coordinación.</li> </ul> <p><b>Situación actual:</b></p> <ul style="list-style-type: none"> <li>El soporte a usuarios es responsabilidad directa del Área de Informática a través del correo interno o de Manuales de Usuario.</li> </ul>
<p><b>Soporte a Usuarios / Mesa de Ayuda</b></p>	<p><b>Estrategia propuesta:</b></p> <ul style="list-style-type: none"> <li>Asegurar la presencia de personal titular o alternativo de TI necesario para colaborar con los requerimientos técnicos y de sistemas que se requieran durante el proceso de recuperación y operación en contingencia.</li> </ul> <p><b>Situación actual:</b></p> <ul style="list-style-type: none"> <li>Información física: <ul style="list-style-type: none"> <li>✓ La información original necesaria para realizar las operaciones críticas se encuentra almacenada en files en la misma oficina.</li> <li>✓ Las copias se encuentran bajo custodia del personal respectivo dependiendo de la operación.</li> <li>✓ El proveedor brindará la información requerida según solicitud de la entidad.</li> </ul> </li> </ul>
<p><b>Información (física o digital)</b></p>	<ul style="list-style-type: none"> <li>Información digital: <ul style="list-style-type: none"> <li>✓ Los documentos físicos que son digitalizados son enviados vía correo electrónico. Por ende, los documentos sólo son guardados en el servidor de correo ocasionando que, para la recuperación, el usuario tenga que hacer una búsqueda manual en su correo, lo cual pone en riesgo la probabilidad de cumplimiento del RPO del proceso, producto o servicio.</li> </ul> </li> </ul>



Componente	Definición de la estrategia
------------	-----------------------------

**Estrategia propuesta:**

- Información física:
  - ✓ Optar por la tercerización de documentos críticos, tomando en cuenta las consideraciones de Servicio de Proveedores.
- Información Digital:
  - ✓ Asignar un servidor específico para el almacenamiento de los principales documentos manejados por los procesos críticos, de modo que se prescindiera de la búsqueda manual de documentos digitales en el correo electrónico por el usuario en caso de la ocurrencia de una crisis.

Coordinar con el proveedor de TI para asegurar el correcto respaldo y contingencia del servidor en mención.

Es de vital importancia elaborar una lista de requerimientos mínimos de equipos de cómputo (cantidad, tipo y características técnicas) y de oficina que estarán ubicados en el sitio alterno e inventariar aplicaciones del sistema SIGA.NET considerando la siguiente información: Nombre de aplicación, procesos, productos o servicios que soporta, infraestructura mínima, Usuarios, administrador de sistema, versión y fecha de último mantenimiento.

Finalmente, es relevante mencionar que toda información sea física o digital debe estar replicada en línea.

**Situación actual:**

- No se cuenta con ningún tipo de recurso de operación en el centro alterno.

**Estrategia propuesta:**

- Contar con PCs mínimas necesarias, mobiliario, laptops, materiales de oficina como papel, toners, lapiceros entre otros para ejecutar el proceso de recuperación.

Recursos de Operación (UPS, PCs, mobiliario, etc.)



Componente	Definición de la estrategia
------------	-----------------------------



**Servicios de Proveedores**

**Situación actual:**

- Se cuenta con los siguientes servicios asignados a proveedores en la sede principal:
  - ✓ Servicio de respaldo (CDs, DVDs).
  - ✓ Servicio de Housing para el DataCenter (Custodia).
  - ✓ Servicios básicos (luz, agua, teléfono, internet)
- Se cuenta con acuerdos establecidos, pero no con SLA definidos y conocidos por los principales interesados.
- No existe un procedimiento o medidas establecidas para asegurar que los proveedores cumplen con los objetivos estratégicos que requiere la organización, poniendo en riesgo la completa satisfacción de sus necesidades.
- No se cuenta con proveedores de los servicios mencionados para el Centro Alterno de Operaciones (CCA).

**Estrategia propuesta:**

- Establecer como mínimo los siguientes procedimientos:
  - ✓ Verificar que la priorización del proveedor respecto a la entidad permite el cumplimiento del RPO.
  - ✓ Verificar que el proveedor cumpla con un SGCN que asegure la integridad, confidencialidad y disponibilidad de la información en custodia.
  - ✓ Al manejar información sensible de los clientes se debe verificar que el proveedor cumpla con las directrices pertinentes conforme a la Ley de Protección de Datos Personales (Ley N° 29733).

Para el caso específico del proveedor de centro de datos, se debe verificar que este cumpla con las características de infraestructura adecuadas, haciendo revisiones periódicas.

Cabe mencionar, que es recomendable, una vez equipado el Centro Alterno de Operaciones (CCA), manejar los mismos procedimientos mencionados con los proveedores, para lograr que la entidad cuente con partes y accesorios de servidores y equipos de comunicación disponibles en el centro alternativo.

ESQUEMA GENERAL DE LA CONTINUIDAD DEL NEGOCIO (ESTRATEGIAS)

ANTES	DURANTE		DESPUES	LECCIONES APRENDIDAS	
<p>Preparación</p> <ul style="list-style-type: none"> <li>- Poner a punto la estrategia, antes que ocurra algún desastre</li> <li>- Preparación de sitios y centros alternos y los recursos necesarios para la operación alterna</li> <li>- Realizar ejercicios y simulacros de preparación</li> <li>- Se está a la espera de cualquier notificación de evento según las definiciones de escalamiento</li> </ul>	<p>Respuesta</p> <ul style="list-style-type: none"> <li>- Según evaluación del Comité se declara Posible Desastre</li> <li>- Se recibe notificación del estado</li> <li>- Se coordina evaluación en el sitio afectado</li> <li>- Según los informes de los grupos de emergencia y considerando la proximidad al vencimiento de RTOs se solicita la declaración de Alerta de Desastre para las áreas afectadas.</li> </ul>	<p>Respuesta</p> <ul style="list-style-type: none"> <li>- Según evaluación del Comité se declara Alerta de Desastre</li> <li>- Se recibe notificación del estado</li> <li>- Se coordina la movilización de recursos al esquema alterno</li> <li>- Se inician actividades de preparación a la operación alterna</li> <li>- Se evalúa permanentemente los procesos que requieren ser activados previo al vencimiento de sus RTO.</li> </ul>	<p>Operación Alterna</p> <ul style="list-style-type: none"> <li>- Se inicia la operación alterna, utilizando los Checklist de cada proceso</li> <li>- Se monitorea la operación alterna</li> <li>- Se informa al Comité sobre el avance de la recuperación</li> <li>- Se evalúa incorporar procesos a la operación alterna según sus RTO</li> <li>- Se confirma al Comité la recuperación de los procesos</li> </ul>	<p>Restauración y Retorno</p> <ul style="list-style-type: none"> <li>- El Comité declara el Desastre Controlado</li> <li>- Se coordina el Plan de Restauración</li> <li>- Se coordina el Plan de Retorno</li> <li>- Se retorna a la normalidad de las operaciones</li> <li>- Se coordina solicitar el estado de Fin de Desastre al Comité.</li> </ul>	<ul style="list-style-type: none"> <li>- El Comité declara el Fin del Desastre</li> <li>- El Comité se desactiva formalmente y da inicio a la etapa de mejoras.</li> <li>- Se evalúa las oportunidades de mejora</li> <li>- Se implementan las mejoras a las estrategias</li> <li>- Se actualizan los Planes de Continuidad y de Desastres.</li> </ul>
			(Cont.)	Fin del Desastre	
			Alerta de Desastre	Desastre Controlado	
			Evento Ocurrido	Desastre Declarado	
			Possible Desastre	Fin del Desastre	

>> Estados de respuesta de la Continuidad del Negocio.  
 >> Los estados mencionados marcan el inicio de cada etapa según el desenvolvimiento del evento o desastre presentado.





## 5. Equipos y Roles de Recuperación

A continuación, se muestra una estructura propuesta del Equipo de Recuperación Primario de Sistemas y TI con sus roles principales y las funciones básicas a desempeñar por rol.

<b>Legenda:</b>	
- Rol:	Posición o rol perteneciente al grupo.
- Prioridad:	Importancia de las posiciones: 1: Primero en ejecutar, dirigiendo las acciones de recuperación. 2: Ejecuta las acciones y realiza coordinaciones según las decisiones tomadas por los líderes. 3: Brinda soporte en el desarrollo de las actividades.



<b>Grupo:</b>	<b>Equipo de Recuperación Primario de Sistemas y TI</b>		
<b>Descripción:</b>	Responsables de Recuperar los servicios y aplicaciones de Sistemas TI, lo cual comprende principalmente a las plataformas, base de datos, comunicaciones y accesos a los sistemas.		
<b>Código</b>	<b>Rol</b>	<b>Prioridad</b>	
CTI	Coordinador de Recuperación de TI	1	
CIN	Coordinador de Infraestructura	1	
CBD	Coordinador de BD	1	
CNW	Coordinador de Networking	1	
CSI	Coordinador de Seguridad de Aplicaciones	2	
CAP	Coordinador de Aplicaciones (Soporte Help Desk)	2	

El líder de recuperación que es el Coordinador de Recuperación de TI y cada uno de los roles definidos en el plan, realizan actividades de coordinación con el personal de la entidad y los respectivos proveedores para la activación del DRP, lo cual permitirá recuperar los servicios y/o aplicaciones críticas del negocio. Cabe mencionar que el Coordinador de Recuperación de TI del plan actúa acorde a las instrucciones del Comité de Gestión de Crisis.





• **Habilidades por Rol**



A continuación, se presentan los las funciones y habilidades que cada rol debe cumplir:

Rol	Función	Habilidad
  <p><b>Líder de Recuperación</b></p>	<ol style="list-style-type: none"> <li>1. Establecer el protocolo para activar el sitio alternativo de operaciones.</li> <li>2. Gestión de la disponibilidad de los sistemas en producción y contingencia de sistemas</li> <li>3. Gestión de la seguridad informática de la compañía</li> <li>4. Gestión de proyectos de compra, migración y mejora de la performance de la infraestructura de tecnologías de la información.</li> <li>5. Identificación de soluciones que permitan el mejoramiento continuo y la optimización de recursos</li> <li>6. Conocer la arquitectura de los sistemas de la compañía.</li> </ol>	<ul style="list-style-type: none"> <li>• Liderazgo</li> <li>• Comunicación</li> <li>• Seguridad y confianza para manejar incidentes</li> <li>• Motivador e integrador de equipos de trabajo</li> <li>• Manejo de recursos humanos bajo presión.</li> </ul>
<p><b>Coordinador de Infraestructura</b></p>	<ol style="list-style-type: none"> <li>1. Gestión de infraestructura y servicios de TI.</li> <li>2. Implementación y mantenimiento de planes y políticas de la seguridad física.</li> <li>3. Supervisión de las instalaciones y condiciones físicas de los activos de TI de la organización.</li> <li>4. Administración del inventario de activos de sistemas.</li> <li>5. Mantener actualizada y segura la configuración en el centro alternativo de operaciones.</li> <li>6. Evaluar el daño en la plataforma tecnológica básica de la entidad, coordinar y dirigir las acciones necesarias para su recuperación en el centro alternativo y su restauración a condiciones normales.</li> <li>7. Instalar el hardware y software base, así como configurar las últimas versiones de los sistemas operativos, en los ambientes del centro alternativo de operaciones.</li> <li>8. Ejecutar los procedimientos de backup y restablecer los controles de operación en el centro alternativo luego de restablecidos los servicios en dicho ambiente.</li> </ol>	<p>Tener conocimientos de:</p> <ul style="list-style-type: none"> <li>• Hardware y software de servidores</li> <li>• Soluciones de almacenamiento</li> <li>• Gestión de incidentes de TI.</li> <li>• Documentación y control de cambios.</li> <li>• Infraestructura de negocios.</li> <li>• Hardware y software de servidores</li> </ul>



Rol	Función	Habilidad
 <p><b>Coordinador de Networking</b></p>	<ol style="list-style-type: none"> <li>1. Implementar y administrar las redes de comunicaciones.</li> <li>2. Monitorear los servicios de red.</li> <li>3. Evaluar el daño en las redes de comunicación de datos y coordinar las estrategias de recuperación con los proveedores de servicios.</li> <li>4. Mantener actualizado el diagrama actual de conexión de dispositivos, el diagrama alternativo y el inventario de equipos de telecomunicaciones a ser usado en caso de emergencia.</li> <li>5. Mantener, recuperar y/o restaurar los enlaces de red y comunicaciones entre la oficina central de INVERMET y el centro alternativo de operaciones.</li> </ol>	<ul style="list-style-type: none"> <li>• Capacidad de Trabajo en equipo.</li> <li>• Capacidad de trabajo bajo presión.</li> <li>• Administración de redes y comunicaciones.</li> <li>• Hardware y software y virtualización de servidores</li> <li>• Monitoreo de servicios de red</li> </ul>
 <p><b>Coordinador de Base de Datos</b></p>	<ol style="list-style-type: none"> <li>1. Monitoreo y mejora del rendimiento de las bases de datos.</li> <li>2. Gestión de proyectos de migración de bases de datos.</li> <li>3. Diseño de políticas de la seguridad e integridad de las bases de datos</li> <li>4. Diseño, implementación y supervisión de los procesos de respaldo de información.</li> <li>5. Restablecimiento de los servicios de base de datos, con la data restaurada, válida, íntegra, probada y disponible para los usuarios, en el centro alternativo de operaciones.</li> <li>6. Informar a los usuarios acerca de la cantidad de información que se ha perdido como consecuencia del desastre y que será necesario recuperar.</li> <li>7. Velar por el funcionamiento adecuado de las bases de datos.</li> </ol>	<ul style="list-style-type: none"> <li>• Vocación de Servicio.</li> <li>• Iniciativa.</li> <li>• Orden.</li> <li>• Capacidad de Trabajo en equipo.</li> <li>• Capacidad de trabajo bajo presión.</li> </ul>



Rol	Función	Habilidad
 <p><b>Coordinador de Seguridad de Información</b></p>	<ol style="list-style-type: none"> <li>1.Revisión y ejecución de los pases a producción</li> <li>2.Monitoreo de accesos a los sistemas y baja de usuarios que no cumplen con los criterios y derechos de accesos.</li> <li>3.Apoyo en el monitoreo y mejoras del rendimiento de las bases de datos.</li> <li>4.Apoyo en la documentación de las políticas de seguridad y procedimientos del área.</li> <li>5.Supervisar el cumplimiento de los controles que permitan asegurar la integridad, confidencialidad y disponibilidad de la información durante la situación de emergencia y recuperación.</li> </ol>	<ul style="list-style-type: none"> <li>• Vocación de Servicio.</li> <li>• Iniciativa.</li> <li>• Orden.</li> <li>• Capacidad de Trabajo en equipo.</li> <li>• Capacidad de trabajo bajo presión.</li> </ul>
 <p><b>Coordinador de Aplicaciones y Soporte</b></p>	<ol style="list-style-type: none"> <li>1.Apoyar en la instalación de sistemas y aplicaciones del centro alternativo de operaciones.</li> <li>2.Asistir a los usuarios en la reinstalación de los sistemas y aplicativos una vez superado el desastre.</li> <li>3.Asistir a los usuarios en la atención de incidentes de TI.</li> <li>4.Aprobar, con el coordinador de networking y base de datos, la puesta en marcha del centro alternativo de operaciones.</li> <li>5.Brindar apoyo y soporte al coordinador de networking y base de datos en la ejecución de algunas tareas, según lo requiera.</li> <li>6.Monitorear el desarrollo de las operaciones en contingencia y elaborar diagnósticos de su estado.</li> <li>7.Informar al coordinador de recuperación de TI las principales incidencias.</li> </ol>	<ul style="list-style-type: none"> <li>• Vocación de Servicio.</li> <li>• Iniciativa.</li> <li>• Orden.</li> <li>• Capacidad de Trabajo en equipo.</li> <li>• Capacidad de trabajo bajo presión.</li> <li>• Dominio de los sistemas y aplicaciones.</li> <li>• Capacidad de búsqueda de soluciones</li> </ul>

### 6. FASE ANTES: Actividades de Preparación

Esta fase determina las actividades previas que se deben realizar, a fin de garantizar el éxito y la viabilidad de la ejecución del presente plan.

Leyenda:	
- N°:	Número correlativo de la tarea
- Tarea, descripción:	Descripción de la tarea o actividad
- Frecuencia:	Frecuencia de ejecución de las tareas, los posibles valores son: Diaria, Semanal, Quincenal, Mensual, Bimestral, Trimestral, Cuatrimestral, Semestral, Anual, Bianaual, Un día en particular (especificar el día).
- CTI, CIN, CBD, ..., CAP:	Roles responsables, miembros del grupo de recuperación del presente plan.

N°	Tarea, descripción	Frecuencia	CTI	CIN	CBD	CN	CS	CA
----	--------------------	------------	-----	-----	-----	----	----	----

#### Respecto a recursos y materiales aplicados a las infraestructura del centro alterno:

Efectuar visitas o auditorías al centro alterno de operaciones una vez establecido y validar la existencia y funcionamiento de:

- Servidores y sus componentes
- Equipos de operación (laptop, terminales, consolas, etc.)
- Utilitarios básicos
- Registros vitales (CDs y DVDs de respaldo, scripts de configuración, contraseñas no personales, etc.)
- Materiales de operación (CD/DVD, cables, repuestos, etc.)

1. Anual X X X X

#### Respecto a la preparación y actualización de información requerida:

2. Validar replica de información en sitio alterno de contingencia

Diaria X



Nros.	Tarea-descripción	Frecuencia	CTI	GIN	CBD	CN	CS I	GA P	
3.	Asegurar que los registros vitales estén disponibles en el centro alterno.	Trimestral	X						
4.	Actualizar los registros vitales y coordinar con persona responsable de los registros vitales a fin de reemplazar los disponibles en el centro alternos y equipar un almacén de documentos off site con los registros más vigentes. (incluye DRP presente)	Trimestral		X	X	X	X	X	
5.	Realizar pruebas periódicas de traslado y disposición de la información desde la sede principal hasta el centro alterno de operaciones.	Semestral	X	X					
<b>Respecto a la disponibilidad del personal:</b>									
6.	Validar el plan respecto a la vigencia del personal existente y definir personal alterno para roles críticos	Mensual	X						
7.	Validar que roles primario y alterno de un mismo rol no estén ausentes en periodos similares	Bimestral	X						
<b>Respecto al esquema interno de notificación:</b>									
Efectuar pruebas de comunicación entre el personal a fin de:									
8.	- Validar la vigencia de la información de contacto registrada en el plan. - Evaluar la efectividad de los recursos asignados para las comunicaciones (correos, celulares y teléfonos en caso aplique).	Trimestral	X	X	X	X	X	X	
<b>Respecto a proveedores:</b>									
9.	Validar funcionamiento de los números de teléfono de los proveedores externos clave	Trimestral	X		X			X	
<b>Respecto a reportes e indicadores:</b>									
10.	Realizar seguimiento a los indicadores de continuidad del área en base a pruebas periódicas	Semestral	X	X	X	X	X	X	



### Visita a sede de Jesús María de INVERMET

El día 5 de Diciembre a las 3.00 pm se visitó las instalaciones del local de INVERMET ubicado en Húsares de Junín 893, Jesús María, contactando con el Sr. Robinson Martínez, quién guio la visita. La misma se realizó con la finalidad de conocer el local y definir si el mismo puede ser empleado en un futuro como el Centro Alterno de Operaciones y Sitio Alterno de Negocios. A partir de dicha visita, se ha identificado lo siguiente:

#### • Ventajas

- ✓ Local ubicado en zona segura y no está rodeado de centros empresariales ni de mucha congestión vehicular o peatonal.
- ✓ Se cuenta con ambientes libres para ser equipados y puestos a operación en caso de un incidente.
- ✓ Ambientes con ventilación y sin ventilación (sin ventanas) para uso específico de almacenamiento de Servidores.
- ✓ Se tiene LAN habilitada en todo el local.
- ✓ Se cuenta con periféricos básicos (impresoras, fotocopiadoras y plotters).
- ✓ Se tiene como plan a futuro, adquirir el local como propio, reconstruirlo y renovarlo para uso de INVERMET.

#### • Desventajas

- ✓ El local no cuenta con pozo a tierra.
- ✓ Si bien en el local algunas estaciones de trabajo cuentan con estabilizador propio, la energía no está estabilizada en general.
- ✓ Existen paneles y ventanas de vidrio catedral que, en caso de un sismo, son de alto riesgo por su posible destrucción y daño consiguiente.
- ✓ Existen conexiones antiguas y desordenadas en algunos ambientes.
- ✓ En algunos ambientes, hay sobrecarga de personal debido al trabajo realizado, lo que, en caso de sismo es una amenaza latente.

A partir de lo analizado y luego de la visita al local de INVERMET, se concluye que, el local cuenta con algunas desventajas no críticas; es decir, que se pueden corregir a corto y mediano plazo y por ello, se puede implementar en el mismo el Sitio Alterno de Negocios (para personal clave) y el Centro Alterno de Operaciones (para tecnología de información que soporta las operaciones) en caso ocurra un incidente que paralice e inhabilite el local principal de INVERMET, de acuerdo a las ventajas mencionadas. Además es importante recalcar que previamente se deben evaluar e implementar las estrategias y controles recomendados.





## 7. FASE DURANTE: Actividades de Respuesta y de Operación Alterna

En esta fase, se plantean las principales actividades en respuesta al sismo o incendio para poder llevar a cabo la recuperación de los principales sistemas y aplicaciones de TI. Dichas actividades serán ordenadas cronológicamente estimando la duración aproximada de las mismas:

Leyenda:	
- N°:	Número correlativo de la tarea
- Tarea, descripción:	Descripción de la tarea o actividad
- Duración:	Tiempo de ejecución o demora de la tarea, aquí algunos posibles valores: HH:MM, De inmediato, Indeterminado, N/A

N°	Tarea, descripción	Tiempo de Inicio
<b>RESPUESTA AL INCIDENTE: Define las actividades necesarias para escalar el evento catalogado como ALERTA DE DESASTRE y luego de la evaluación correspondiente decidir si se declara el evento como DESASTRE, solo se pide que se informe de la situación actual, no se moviliza personal, a excepción del Líder</b>		
<b>A. Estado de la Situación: Evento Ocurrido</b>		
1.	El coordinador de recuperación de TI debe recibir la notificación de parte del Equipo de Gestión de Crisis sobre el estado actual de "Evento Ocurrido".	No aplica
2.	Notificar a los miembros del equipo sobre el estado actual.	00:10
3.	El coordinador de recuperación de TI debe evaluar el estado y cantidad de personal afectado.	00:30
4.	El coordinador de infraestructura debe solicitar información al equipo de manejo de emergencias sobre el estado de la infraestructura del edificio principal para obtener un diagnóstico inicial.	00:30
<b>Estado de la Situación: Posible Desastre</b>		
5.	Recibir notificación de parte del Comité de Crisis sobre el estado actual de "Posible Desastre"	No aplica
6.	El coordinador de infraestructura debe recibir la información del equipo de manejo de emergencias y evaluar si la infraestructura ofrece las condiciones adecuadas para la recuperación garantizando la seguridad de las personas y los equipos.	01:00
7.	El coordinador de recuperación de TI, en colaboración con el coordinador de Infraestructura, coordinador de networking, coordinador de base de datos, coordinador de seguridad de información y el coordinador de aplicaciones y soporte deben evaluar los RTOs y el vencimiento de los mismo a fin de solicitar la declaración de "Posible Desastre"	02:00
8.	Comunicar al Equipo de Gestión de Crisis sobre los resultados obtenidos informando las decisiones tomadas a partir de ello.	02:30
<b>Estado de la Situación: Alerta de Desastre</b>		





Nº	Tarea, descripción	Tiempo de Inicio
9.	El <b>coordinador de recuperación de TI</b> debe recibir la notificación de parte del Equipo de Gestión de Crisis sobre el estado "Alerta de Desastre".	No Aplica
10.	El <b>coordinador de recuperación de TI</b> debe recibir la conformidad del Equipo de Gestión de Crisis para dar inicio a la activación del plan.	No Aplica
11.	Determinar, en conjunto con el <b>coordinador de infraestructura</b> la necesidad o no de activar el centro alternativo de operaciones.	00:30
12.	Determinar, en conjunto con el <b>coordinador de networking</b> y el <b>coordinador de base de datos</b> , el estado de los sistemas o aplicaciones para determinar el funcionamiento del centro de datos alternativo (ya que este se activa automáticamente frente a una interrupción).	01:00
13.	El <b>coordinador de recuperación de TI</b> deber notificar al personal titular y alternativo disponible del plan, sobre situación actual, con todos los datos coordinados con el resto del equipo y aprobados previamente con el Equipo de Gestión de Crisis, a fin de que se preparen para una eventual movilización al centro alternativo de operaciones.	03:00
14.	El <b>coordinador de recuperación de TI</b> y el <b>coordinador de infraestructura</b> deben realizar la validación de las condiciones del centro alternativo de operaciones.	03:00
15.	Comunicar al Equipo de Gestión de Crisis sobre el estado actual de los planes de acción tomados.	03:30
B.	<b>ACTIVACIÓN: Define las actividades a ser efectuadas luego de declarar el evento como DESASTRE y proceder a la activación del ambiente ALTERNO y a las pruebas preliminares de los recursos a utilizar</b>	

**Estado de la Situación: Desastre Declarado**

16.	El <b>coordinador de recuperación de TI</b> debe recibir notificación de parte del Comité de Crisis sobre el estado actual de "Desastre Declarado"	No aplica
17.	El <b>coordinador de recuperación de TI</b> , el <b>coordinador de networking</b> y el <b>coordinador de base de datos</b> deberán notificar al proveedor del centro de cómputo alternativo la activación del plan para que tomen las medidas y consideraciones necesarias.	00:30
18.	El <b>coordinador de infraestructura</b> debe coordinar con el proveedor respectivo la provisión de unidades de transporte para la movilización del personal necesario.	01:00
19.	El <b>coordinador de seguridad de información</b> debe coordinar con el proveedor correspondiente el traslado, en caso sea necesario, de la información física custodiada. Además deberá notificar el cambio de ubicación de operaciones para el almacenamiento de la información generada durante la operación en contingencia.	01:00
20.	El <b>coordinador de recuperación de TI</b> debe notificar al personal titular y alternativo del plan, sobre situación actual y comunicarles el punto de reunión para iniciar el traslado.	04:00
21.	Según llegue el personal: - Asignar colaborador al rol correspondiente. - Entregar parte del plan que le corresponde (desmembrar el plan	04:30

Nº	Tarea, descripción	Tiempo de Inicio
	<p>impreso en caso sea necesario).</p> <ul style="list-style-type: none"> <li>- En caso de llegar más de un colaborador para el mismo rol, asignar a otros roles hasta completar los puestos de recuperación.</li> </ul> <p>El <b>coordinador de networking</b>, El <b>coordinador de base de datos</b> y el <b>coordinador de aplicaciones y soporte</b> deben trasladarse al centro alternativo de operaciones para:</p>	
22.	<ul style="list-style-type: none"> <li>- Preparar los equipos con las aplicaciones y sistemas necesarios.</li> <li>- Brindar los accesos correspondientes.</li> <li>- Verificar la correcta ejecución de las pruebas iniciales de los equipos en sitio alternativo (servidores, tape libraries, discos, SAN storage).</li> </ul> <p>Una vez que el personal haya llegado al centro alternativo de operaciones, el <b>coordinador de recuperación de TI</b> debe solicitar al personal lo siguiente:</p> <ul style="list-style-type: none"> <li>- Verificar validez de los equipos y materiales de operación</li> <li>- Verificar validez de los sistemas de tecnología (acceso y datos).</li> <li>- Verificar la existencia de la información física necesaria.</li> </ul>	04:30
23.	<p>El <b>coordinador de aplicaciones y soporte</b> debe monitorear y atender la ocurrencia de posibles incidentes de TI que pudieran ocurrir durante la estabilización y operación en contingencia.</p> <p>Comunicar al Equipo de Gestión de Crisis:</p> <ul style="list-style-type: none"> <li>- Resultados de pruebas iniciales.</li> <li>- Solicitar indicaciones de qué hacer con el personal sobrante.</li> <li>- Solicitar recursos y materiales adicionales en caso sea necesario.</li> </ul> <p>El <b>coordinador de recuperación de TI</b> debe, según indicaciones del Equipo de Gestión de Crisis coordinar la logística para la adquisición de los recursos adicionales</p>	06:30
24.	<p><b>C. OPERACIONES ALTERNA: Define las actividades de coordinación a ser efectuadas para reanudar la operación diaria.</b></p> <p><b>Estado de la Situación: Desastre Declarado (Cont.)</b></p> <p>El <b>coordinador de recuperación de TI</b>, en colaboración con el <b>coordinador de redes</b>, el <b>coordinador de base de datos</b> y el <b>coordinador de aplicaciones y soporte</b> deben monitorear la recuperación de procesos y actividades afectadas.</p>	07:00
25.	<p>El <b>coordinador de recuperación de TI</b> debe solicitar información sobre el estado de la recuperación de las instalaciones principales de la entidad para determinar en qué momento iniciar las actividades de normalización.</p>	11:00
26.	<p>El <b>coordinador de redes</b>, el <b>coordinador de base de datos</b> y el <b>coordinador de aplicaciones y soporte</b> deben gestionar y realizar revisiones en el local para asegurar que la infraestructura de red y comunicaciones sea la adecuada.</p>	12:00
27.	<p>Informar situación de avance al Equipo de Gestión de Crisis.</p>	12:00
28.	<p>El <b>coordinador de recuperación de TI</b> debe informar al Equipo de Gestión de Crisis la recuperación de las aplicaciones y/o servicios de TI cuando alcancen un estado aceptable.</p>	12:00
29.		15:00
30.		24:00



## 8. FASE DESPUÉS: Actividades de Restauración y Retorno

A continuación, se presentan las principales actividades a seguir una vez el Equipo de Gestión de Crisis ha desactivado la alerta de desastre debido a que las operaciones y las instalaciones ya se encuentran dentro de un nivel óptimo. Estas actividades estarán ordenadas cronológicamente estimando la duración aproximada de las mismas:

Leyenda:	
- N°:	Número correlativo de la tarea
- Tarea, descripción:	Descripción de la tarea o actividad
- Frecuencia:	Frecuencia de ejecución de la tareas, los posibles valores son: Diaria, Semanal, Quincenal, Mensual, Bimestral, Trimestral, Cuatrimestral, Semestral, Anual, Bianual, Un día en particular (especificar el día).
- CTI, CIN, CBD,...,CAP:	Roles responsables, miembros del grupo de recuperación del presente plan.

N°	Tarea, descripción	Duración
A.	<b>REPARACIÓN:</b> Define las actividades a ser efectuadas para realizar la reparación de los daños ocurridos al ambiente NORMAL y la preparación para dejar "a punto" el retorno a la normalidad	
	<b>Estado de la Situación:</b> Desastre Controlado	
1.	Recibir notificación de "DESASTRE CONTROLADO"	No aplica
2.	El <b>coordinador de recuperación de TI</b> debe recibir la notificación de parte del Equipo de Gestión de Crisis informando que el Desastre ha sido controlado.	No aplica
3.	El <b>coordinador de recuperación de TI</b> debe coordinar con el Equipo de Gestión de Crisis el esquema o plan de reparación del centro de cómputo dañado	48:00
4.	El <b>coordinador de recuperación de TI</b> , en coordinación con el resto del equipo, debe planificar la fecha de retorno considerando los recursos y la situación actual	120:00
	Preparar plan de acción para el retorno y asignar responsabilidades. Se debe considerar lo siguiente:	
5.	- El <b>coordinador de redes y de base de datos</b> debe verificar que las conexiones del local se encuentren adecuadamente instaladas y permitan condicionar los ambientes.	
	- El <b>coordinador de infraestructura</b> debe verificar que las instalaciones del local se encuentren en óptimas condiciones garantizando la seguridad de las personas y de los activos.	36:00
	- El <b>coordinador de seguridad de información</b> debe verificar y coordinar el traslado de la información necesaria al local y al proveedor.	



N°	Tarea, descripción	Duración
6.	Cada coordinador deber tomar puntos de control para la posterior verificación en el local (centro normal de operaciones).	24:00
B.	<b>VUELTA A LA NORMALIDAD:</b> Define las actividades a ser efectuadas para realizar el retorno a la normalidad, lo que implica desactivar el ambiente ALTERNO y activar el ambiente NORMAL.	
<b>Estado de la Situación: Fin del Desastre</b>		
7.	El <b>coordinador de infraestructura</b> con la aprobación del resto del equipo, solicita desactivar el centro alterno de operaciones.	24:00
8.	El equipo debe dirigir cada una de las actividades de retorno, cumpliendo las responsabilidades asignadas.	48:00
9.	El <b>coordinador de recuperación de TI</b> debe informar al Equipo de Gestión de Crisis el fin del proceso y esperar la notificación de "Fin de desastre".	01:00
10.	El <b>coordinador de recuperación de TI</b> debe coordinar reuniones posteriores con el Equipo de Gestión de Crisis para realizar el análisis de Lecciones Aprendidas.	02:00
11.	El equipo debe actualizar el Plan de Recuperación ante Desastres y documentación de soporte.	72:00



## 9. Empleados asociados por Rol

Identifica al personal con toda su información de contacto, quienes estarán asociados a cada Rol definido en este plan.

Leyenda:	
- Rol:	Rol del Colaborador
- N°:	Número correlativo del personal, se incrementa de uno en uno
- Apellido Paterno:	Apellido Paterno del colaborador
- Apellido Materno:	Apellido Materno del colaborador
- Nombres:	Nombres del colaborador
- P/A:	Determina si el colaborador es Primario o Alterno

**Rol:** Líder de Recuperación del plan

N°	Apellido Paterno	Apellido Materno	Nombres	P/A
1.	Inga	Ramirez	Rocio	P

**Rol:** Coordinador de Infraestructura

N°	Apellido Paterno	Apellido Materno	Nombres	P/A
1.	Valencia	Martínez	Robinson	P

**Rol:** Coordinador de Base de Datos

N°	Apellido Paterno	Apellido Materno	Nombres	P/A
1.	Inga	Ramirez	Rocio	P

**Rol:** Coordinador de Networking

N°	Apellido Paterno	Apellido Materno	Nombres	P/A
1.	Oliva	Guerrero	Edwin	P

**Rol:** Coordinador de Seguridad de Información

N°	Apellido Paterno	Apellido Materno	Nombres	P/A
1.	Alvites	Valladares	Andres Rusbel	P

**Rol:** Coordinador de Aplicaciones y Soporte

N°	Apellido Paterno	Apellido Materno	Nombres	P/A
1.	Loayza	Mota	Roberto	P

## 10. Árbol de Llamadas

**INICIA LLAMADA:** Líder de Recuperación del plan

Nº	Nombres (Apellidos, Nombres)	Tipo de Contacto	Propósito de la Llamada
1.	Oliva Guerrero, Edwin	Colaborador	Notificar situación actual
2.	Valencia Martinez, Robinson	Colaborador	Notificar situación actual

**CONTINUA LLAMANDO:** Loayza Motta, Roberto

Nº	Nombres (Apellidos, Nombres)	Tipo de Contacto	Propósito de la Llamada
3.	Obando, Roberto	Colaborador	Notificar situación actual
4.	Fairlie, Ernesto	Colaborador	Notificar situación actual
5.	Vargas, José	Colaborador	Notificar situación actual
6.	Jiménez, Humberto	Colaborador	Notificar situación actual
7.	Peña, Sonia	Colaborador	Notificar situación actual

**CONTINUA LLAMANDO:** Coordinador del Área de Logística

Nº	Nombres (Apellidos, Nombres)	Tipo de Contacto	Propósito de la Llamada
8.	Espinoza, Fernando	Proveedor	Notificar situación actual
9.	Ballesteros, José Luis	Proveedor	Notificar situación actual
10.	Ferruso, Pablo	Proveedor	Notificar situación actual

## 11. Recursos asociados al área

Identifique los recursos y materiales de operación, incluyendo la parte tecnológica, requeridos para la continuidad del área.

Leyenda:	
- Servidores	Descripción de Servidores asociados al área
- Equipamiento:	Nombre o Descripción del equipamiento y hardware requerido por los procesos del área
- Aplicación / Servicio:	Cantidad de licencias de software requerido por los procesos del área
- Insumos / Consumibles:	Consumibles y/o materiales adicionales requeridos por los procesos del área
- Registros Vitales:	Información digital, física o accesorios vitales requeridos para la recuperación de los procesos
- Cantidad:	Si aplica, cantidad necesaria del recurso. En caso de Aplicación este campo equivale al número de licencias.



No	Servidor	Sistema Operativo	Aplicación	RAM (MB)	Disco	Procesador	Prioridad (RTO)
1	Servidor de Aplicaciones	Windows 2008 R2 64X	Consola Antivirus, SPIJ, PROCOM, ACTISOFT	8 GB	3 discos de 300 GB en RAID5	E5 620 de 2.40 Ghz.	Hasta 24 Hrs
2	Domain Controller	Windows 2003 R2 86X	Servidor Dominio (AD,DC,DNS)	4 GB	1 disco de 160 GB + 2 discos de 1TB en RAID1	E5 405 de 2.00 Ghz.	Hasta 24 Hrs
3	Servidor BD	Windows 2008 R2 64X	BD MS SQL 2008, VISUAL STUDIO 2008, SIGA.NET	8 GB	3 discos de 300 GB en RAID5	E5 620 de 2.40 Ghz.	Hasta 24 Hrs
4	Servidor Web	CENTOS 6.5	PHP, MYSQL, JOOMLA	8 GB	2 discos de 300 GB en RAID1	E5 620 de 2.40 Ghz.	Hasta 48 Hrs
5	Check Point 4000 Appliances	CHECK POINT	FIREWALL CHECK POINT	4 GB	1 disco de 250gb	1.2 Ghz.	Hasta 24 Hrs

EQUIPAMIENTO Y RECURSOS	CANTIDAD POR RTO							Cantidad día-a-día
	Nombre del Equipamiento y/o Recursos	0hrs. (Inmediato)	12 Hrs.	24 Hrs.	48 Hrs.	1Sem.	2Sem.	
Laptops o PCs	2	4	8	11	12	20	20	-
Radio enlace	1	1	1	1	1	1	1	1
Impresoras láser/ fotocopiadoras compartidas	1	2	2	2	2	2	2	2

APLICACIÓN / SERVICIO	CANTIDAD DE ACCESOS POR RTO						
	Nombre de la Aplicación o Servicios de Sistemas TI	0hrs. (Inmediato)	12 Hrs.	24 Hrs.	48 Hrs.	1Sem.	2Sem.
SIGA.NET	0	2	8	11	20	20	20
Correo Electrónico institucional	0	2	8	11	20	20	20



REGISTROS VITALES (Nombre)	Ubicación Origen	¿Tiene Respaldo?	Ubicación
CD/DVD de respaldo	CD/ DVD en Offsite	No	-
Usuario Administrador	Directorio Sharepoint	Si	Backup Semanal de todo el servidor
Script	-	Si	Backup Semanal de todo el servidor
Archivos	File Server	Si	CD/DVD

## 12. Lista de Proveedores

Lista de proveedores críticos y sus contactos requeridos para la continuidad del área.

Leyenda:	
- SERVICIO DEL PROVEEDOR:	Nombre del servicio requerido a los proveedores (Ej. Servicio de Mantenimiento de Centrales Telefónicas)
- NOMBRE DEL PROVEEDOR:	Nombre o razón social de proveedor
- Dirección del Proveedor:	Dirección del proveedor, puede incluir referencias si es necesario
- Representante del Proveedor:	Nombre de contacto del proveedor, puede incluir varios representantes, a nivel Técnico, Administrativo, Político, etc.
- Telf. Oficina del proveedor:	Teléfono de oficina, incluir extensión, del representante del proveedor
- Celular del representante:	Teléfono celular del representante del proveedor
- E-Mail del representante:	Correo electrónico del representante del proveedor

<b>SERVICIO DEL PROVEEDOR:</b>	Internet Dedicado		
<b>NOMBRE DEL PROVEEDOR:</b>	OPTICAL NETWORK	<b>Dirección del Prov.:</b>	Calle Carlos Krumdieck 287
<b>Representante del Prov.</b>	<b>Telf. Oficina</b>	<b>Telf. Celular</b>	<b>E-Mail del Representante</b>
Pablo Ferruso	710-7500 Anexo: 7543	99427-6186 RPM: *0031758	pferruzo@optical.com.pe, noc@optical.com.pe



<b>SERVICIO DEL PROVEEDOR:</b>	Alquiler de Fotocopiadoras		
<b>NOMBRE DEL PROVEEDOR:</b>	COPYSERVICE	<b>Dirección del Prov.:</b>	Av. Javier Prado Este Nro 2436-2438, San Borja
<b>Representante del Prov.</b>	<b>Telf. Oficina</b>	<b>Telf. Celular</b>	<b>E-Mail del Representante</b>
	226-1222		
Angélica Mitacc R.	Anexos: 203 - 206 - 213 - 214	No cuenta	marketing@copiservice.com.pe



<b>SERVICIO DEL PROVEEDOR:</b>	Hosting Correo Institucional		
<b>NOMBRE DEL PROVEEDOR:</b>	Solución ORIÓN	<b>Dirección del Prov.:</b>	Av. Paseo de la República 3245 • Piso 4 Oficina B - San Isidro
<b>Representante del Prov.</b>	<b>Telf. Oficina</b>	<b>Telf. Celular</b>	<b>E-Mail del Representante</b>
Fernando Valverde	441-3783	98412-4450	fernando.valverde@solucionesorion.com

<b>SERVICIO DEL PROVEEDOR:</b>	Firewall		
<b>NOMBRE DEL PROVEEDOR:</b>	PMS	<b>Dirección del Prov.:</b>	Av. Faustino Sanchez Carrion 417 Of.203- Centro Empresarial Pershing – San Isidro
<b>Representante del Prov.</b>	<b>Telf. Oficina</b>	<b>Telf. Celular</b>	<b>E-Mail del Representante</b>
Fernando Espinoza	640-8098	No cuenta	fernando.espinoza@pms.com.pe

<b>SERVICIO DEL PROVEEDOR:</b>	Telefonía Fija y Celular		
<b>NOMBRE DEL PROVEEDOR:</b>	Telefónica del Perú	<b>Dirección del Prov.:</b>	Av. Alfredo Benavides N° 661, Piso 3, Miraflores
<b>Representante del Prov.</b>	<b>Telf. Oficina</b>	<b>Telf. Celular</b>	<b>E-Mail del Representante</b>
Jose Luis Ballesteros	210-9434	99878-6527 RPM:#582314	jose.ballesteros@telefonica.com

### 13. Lista de documentos de consulta

Especifique aquí los documentos de consulta o de soporte a utilizar en centro alterno.

Leyenda:	
- Nro:	Número correlativo de los documentos, se incrementa de uno en uno.
- Documento:	Nombre del documento
- Ubicación:	Especifique la ubicación electrónica del documento



Nº	Nombre del Documento	Ubicación física o fuente de origen del documento
1.	Manual de Usuario	\\serverbd\Siga_net\Manuales
2.	Manual de Instalación del SIGA.NET en el servidor y aplicativos	\\serverbd\Siga_net\Manuales



## 14. Recomendaciones

A partir del plan desarrollado y los diferentes hallazgos encontrados:

- Se recomienda documentar y definir adecuadamente (modelar) TODOS los procesos y funciones críticas del negocio; para lograr así el conocimiento a fondo del flujo de actividades claves o "core" del negocio.
- Se recomienda que una vez modelados y definidos los procesos críticos de negocio, se reajuste el presente plan de acuerdo a la prioridad de actividades identificadas.
- Se recomienda mantener siempre actualizado el Mapa de Riesgos del Negocio (no sólo tecnológico) en todas sus áreas, con el objetivo de lograr estar siempre alerta ante cualquier circunstancia, tomando en cuenta su impacto, probabilidad de ocurrencia e impacto, con la mitigación y medios de control respectivos; y actualizar, si es el caso, el presente plan.
- Se recomienda, establecer los tiempos críticos de operación y tiempos máximos de impacto tolerable en un determinado proceso, para posteriormente lograr la recuperación de todas las actividades críticas relacionadas al proceso.
- Se recomienda que anualmente se identifiquen períodos críticos en cada uno de los procesos del negocio, para identificar con mayor facilidad y detalle los diferentes incidentes que pueden ocurrir en la organización y el impacto en la recuperación de los procesos críticos, de acuerdo a una fecha y hora específica.
- Se recomienda establecer períodos de actualización de información, archivos, documentos críticos del negocio, para que con base de esta información se planteen nuevas estrategias de recuperación por áreas o procesos.
- Se recomienda adoptar en INVERMET, las estrategias propuestas para lograr una recuperación de las áreas implicadas garantizando que aplicaciones críticas se encuentren disponibles para uso en el Centro Alterno de Operaciones luego de ocurrido el desastre.
- Se recomienda, identificar todos los recursos asociados a cada actividad crítica de los procesos de negocio, de forma detallada, y presupuestarlos de acuerdo a su disponibilidad.



- Se sugiere tomar en cuenta los registros vitales, los cuales son documentos físicos o electrónicos relevantes para la organización, como hojas membretadas, procedimientos, formatos necesarios para llevar a cabo alguna tarea, documentos legales como contratos con proveedores, otros documentos importantes para el trabajo diario, CDs o DVDs de backup semanal; sin los cuales no es posible la recuperación de un proceso o función del negocio. Por ello será necesario resguardarlos por medio de políticas y procedimientos previamente establecidos que garanticen la recuperación de los registros vitales dentro del RTO establecido.
- Se recomienda, identificar y determinar ambientes o áreas alternas adecuadas para las operaciones en caso de incidentes (Sitio Alterno de Negocio y Centro Alterno de Operaciones); estos deben de contar con los recursos tangibles e intangibles necesarios para la activación del sitio. Asimismo, es necesario contar, estimar y mantener actualizado el personal indispensable para la operación alterna y no sólo contar con personal principal crítico.
- Clarificar los lineamientos sobre los cuales se debe actuar en caso de un incidente, pues las políticas de la organización ya están definidas aún en situaciones de crisis (Confidencialidad, relaciones con proveedores entre otros).
- Se recomienda, establecer una estrecha comunicación con los proveedores ante cualquier interrupción o incidente, ya que es de vital importancia al constituir fichas vitales para la restauración de operaciones específicas.
- Estimar impactos legales, en el país, respecto a la reputación e imagen, e igualmente a entes de regulación o control, al ambiente interno y la opinión pública en caso de no manejar una adecuada continuidad del negocio.
- Se recomienda diseñar un Sistema de Gestión de Continuidad de Negocios (SGCN) completo, no sólo enfocado al área de Informática, sino desarrollar los Planes de comunicación y gestión de crisis, Plan de emergencias, planes de continuidad de negocio y realizar prueba de los mismos, tanto Pruebas de escritorio (papel) como pruebas en caliente (simulación real de un desastre).
- Una vez diseñado y probado el SGCN se recomienda evaluar la adquisición de herramientas automatizadas para optimizar la gestión del SGCN, con el fin de facilitar las operaciones de actualización del mismo.





- Se recomienda realizar las pruebas al presente plan dos veces año para su respectivo ajuste y actualización según sea el caso.
- Se sugiere revisar el presente plan mínimo una vez al año para controles de cambio y actualizaciones según adquisiciones o alguna modificación relevante en la organización.

## 15. Factores críticos de éxito

Algunos factores críticos de éxito identificados son:

- Patrocinio para implementar y probar el presente Plan de Recuperación ante Desastres de la Tecnología de Información.
- Personal alternativo o de respaldo
- Equipamiento alternativo o de respaldo.
- Centro Alterno de Operaciones y Sitio Alterno de Negocios.
- Capacitación y concientización del personal.



## 16. Cuellos de Botella

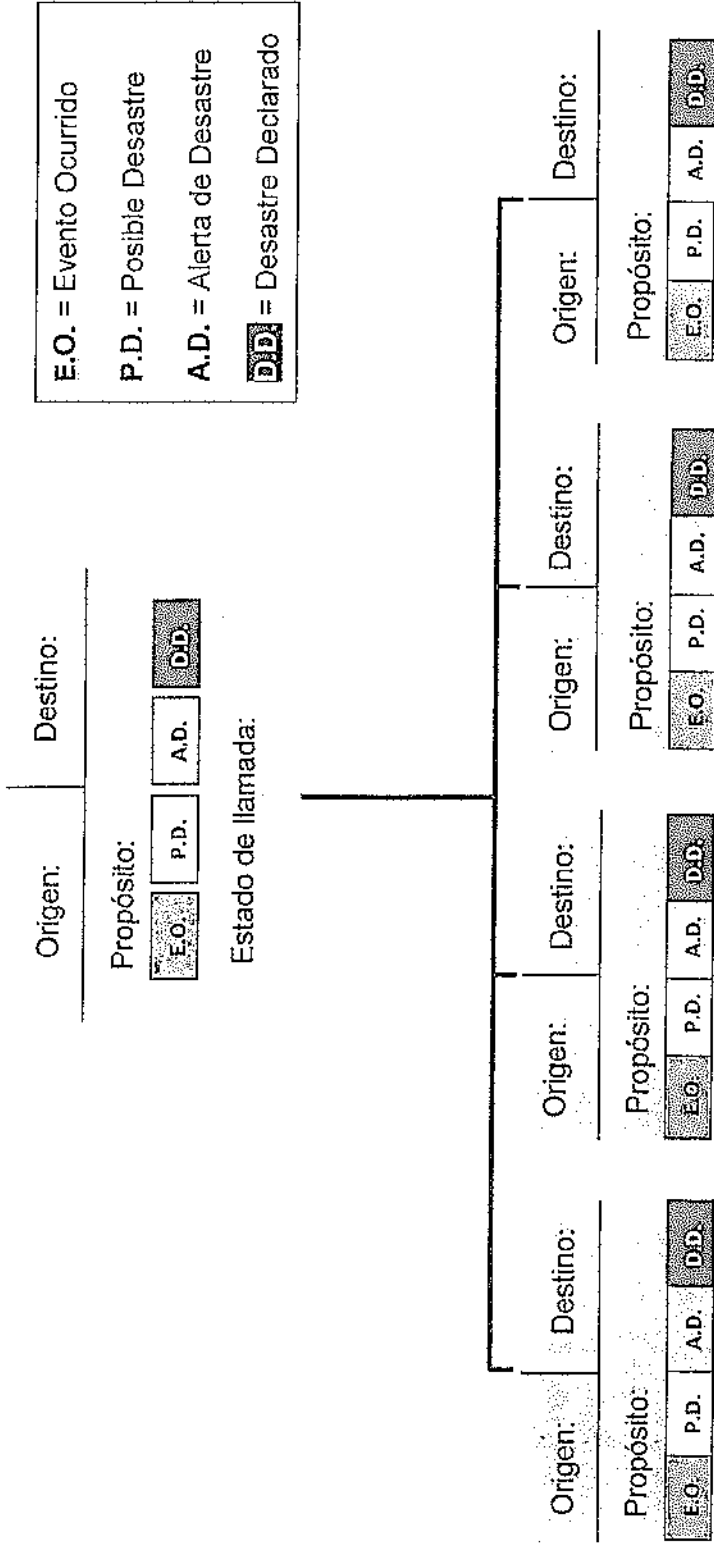
Algunos posibles cuellos de botella identificados son:

- Presupuesto
- Infraestructura
- Resistencia al cambio
- Sistema en vías de actualización e integración



**Anexos**

**1. Formato de árbol de llamadas**



## 2. Formato de Requerimiento

### Origen de la Solicitud

Hora del Requerimiento:	Hora de Recepción de Requerimiento:
Nombre del Plan:	Tiempo Máximo de Espera:
Nombre del Rol:	PIA:
Nombre de la persona:	
Solicitud de Requerimiento: (Pregunta, acción, información)	
Área a quien Solicita:	

### ENVIO DEL REQUERIMIENTO

### Respuesta a la Solicitud

Hora de Recepción de Solicitud:	Hora de Respuesta:
Plan de quien recibe:	
Nombre del Rol de Respuesta:	PIA:
Nombre de la Persona:	
Respuesta al Requerimiento: (acción a realizar, reporte o informe)	

Firma del Rol Solicitante

Firma del Rol de Respuesta

