GOBIERNO REGIONAL DE UCAYALI

GOBERNACION REGIONAL

"Año de la unidad, la paz y el desarrollo"

RESOLUCION EJECUTIVA REGIONAL N° 511 - 2023-GRU-GR

Pucallpa, 24 OCT. 2023

VISTO; El OFICIO N° 0202-2023-GRU-SG-OTI, INFORME N° 048-2023-GRU-GRPP-SGDI/WEMM; INFORME N° 232-2023-GRU-GRPP-SGDI, INFORME LEGAL N° 068-2023-GRU-GGR-ORAJ/TTC; y el texto de la Directiva, y;

CONSIDERANDO:

Que, de conformidad con el Artículo 191° de la Constitución Política del Perú, concordante con el Artículo 2° de la Ley N° 27867 – Ley Orgánica de Gobiernos Regionales, establece que los Gobiernos Regionales, son personas jurídicas de derecho público, con autonomía política, económica y administrativa en asuntos de su competencia;

Que, el Artículo 2º de la Ley Nº 28551 – Ley que establece la Obligación de Elaborar y Presentar Planes de Contingencia, define los planes de contingencia como instrumentos de gestión que definen los objetivos, estrategias y programas que orientan las actividades institucionales para la prevención, reducción de riesgos, permitiendo disminuir o minimizar los daños tecnológicos;

Que, mediante Ley Nº 28716, Ley de Control Interno de las Entidades del Estado se establecen las normas para regular la elaboración, aprobación, implantación, funcionamiento, perfeccionamiento y evaluación del control interno en las entidades del Estado, con el propósito de cautelar y fortalecer los sistemas administrativos y operativos con acciones y actividades de control previo, simultáneo y posterior, contra los actos y prácticas indebidas o de corrupción, propendiendo al debido y transparente logro de los fines, objetivos y metas institucionales;

Que, el acápite 07 del numeral 3.10 de la Resolución de Contraloría Nº 320- 2006-CG, que aprueba las Normas de Control Interno, señala que "*Para el adecuado ambiente de control en los sistemas informáticos, se requiere que éstos sean preparados y programados con anticipación para mantener la continuidad del servicio. Para ello se debe elaborar, mantener y actualizar periódicamente un plan de contingencia debidamente autorizado y aprobado por el titular o funcionario designado donde se estipule procedimientos previstos para la recuperación de datos con el fin de afrontar situaciones de emergencia*";

Que, el numeral 4.1 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, aprobada mediante Resolución Ministerial Nº 246-2007-PCM, señala que "*La evaluación de riesgos debe identificar, cuantificar y priorizar riesgos contra el criterio para la aceptación del riesgo y los objetivos relevantes para la organización. Los resultados deben guiar y determinar la apropiada acción de gestión y las prioridades para manejar la información de los riesgos de seguridad y para implementar controles seleccionados para proteger estos riesgos. El proceso de evaluación de riesgos y de seleccionar controles puede requerir que sea realizado un número de veces con el fin de cubrir diferentes partes de la organización o sistemas de información individuales*";

Que, mediante Resolución Ministerial N° 004-2016-PCM, se 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;

Que, en el marco de las disposiciones contenidas en las normas precedentemente acotadas, la Oficina de Tecnologías de la información mediante OFICIO N° 0202-2023-GRU-SG-OTI de fecha 22 de setiembre de 2023, presenta la propuesta de la *Directiva de Plan de Contingencia Informático del Gobierno Regional de Ucayali*, actualizado, que tiene por objeto, garantizar la continuidad de los Servicios de Tecnologías de la Información y Comunicaciones y asegurar la disponibilidad de la información generada y almacenada por los diferentes recursos y servicios digitales del Gobierno Regional de Ucayali, ante la ocurrencia de alguna contingencia que interrumpa parcial o totalmente su funcionamiento; propuesta normativa que ha sido revisada por la Subgerencia de Desarrollo Institucional, conforme se corrobora con el INFORME N° 232-2023-GRU-GRPP-SGDI de fecha 03 de octubre de 2023;

Que, mediante INFORME LEGAL Nº 068-2023-GRU-GGR-ORAJ/TTC de fecha 16 de octubre de 2023, la Oficina Regional de Asesoría Jurídica; concluye: Estando con los informes del área usuaria, el órgano encargado de la formulación de instrumentos de gestión; corresponde al Titular de la entidad, aprobar la Directiva propuesta, mediante Resolución Ejecutiva Regional, con la finalidad de dar cumplimiento a lo dispuesto en las Normas de Control Interno, aprobadas por Resolución de Contraloría Nº 320-2006- CG y la Resolución Ministerial N° 004-2016-PCM;

Que, en uso de las facultades conferidas por la Ley 27867 – Ley Orgánica de Gobiernos Regionales y sus modificatorias; contando con las visaciones de la Gerencia General Regional, Gerencia Regional de Planeamiento y Presupuesto, Oficina Regional de Administración, Oficina Regional de Asesoría Jurídica, Sub Gerencia de Desarrollo Institucional, Secretaría General, y;

SE RESUELVE:

ARTÍCULO PRIMERO: APROBAR la **Directiva N° 023-2023-GRU-GR-GGR-GRPP-SGDI "*DIRECTIVA DE PLAN DE CONTINGENCIA INFORMÁTICO DEL GOBIERNO REGIONAL DE UCAYALI*"**, cuyo texto completo forma parte de la presente Resolución.

ARTICULO SEGUNDO: ENCARGAR a la Oficina de Tecnologías de la Información y Comunicaciones, la implementación, supervisión y ejecución del Plan de Contingencia Informático.

ARTÍCULO TERCERO: DISPONER a la Oficina de Tecnologías de la Información, la publicación en el portal de transparencia del Gobierno Regional de Ucayali (*www.regionucayali.gob.pe*) la presente resolución y la Directiva.

ARTÍCULO CUARTO: DISPONER a la Secretaría General, la notificación del presente acto resolutivo a todas las Unidades Orgánicas de la Sede Central del Gobierno Regional de Ucayali, para los fines de su competencia.

REGÍSTRESE, COMUNÍQUESE Y CÚMPLASE.

GOBIERNO REGIONAL DE UCAYALI
Manuel Gambini Rupay
GOBERNADOR REGIONAL

DIRECTIVA N° 023-2023-GRU-GR-GGR-GRPP-SGDI

"DIRECTIVA DE PLAN DE CONTINGENCIA INFORMATICO DEL GOBIERNO REGIONAL DE UCAYALI"

I. OBJETIVO.

- Definir las actividades de planeamiento, preparación y ejecución de tareas destinadas a proteger la información contra los daños y perjuicios producidos por corte de servicios, fallas técnicas o humanos.
- Garantizar la continuidad de las operaciones de los principales elementos que componen los Sistemas de Información.
- Realizar y cumplir fielmente el respaldo de los datos en dispositivos externos, a fin de reducir el tiempo de recuperación para las actividades principales (critico).

II. FINALIDAD.

Garantizar la continuidad de los servicios de Tecnologías de la Información y Comunicaciones del Gobierno Regional de Ucayali, a fin de que se restablezcan en un periodo de tiempo mínimo, ante la ocurrencia de alguna contingencia que interrumpa parcial o totalmente su normal funcionamiento.

III. ALCANCE.

El Plan de Contingencia del Gobierno Regional de Ucayali, tiene cobertura a la infraestructura, los sistemas software, equipos, recursos humanos, servicios y demás relacionados, que ayudaran a mitigar riesgos imprevistos que pudieran alterar las condiciones normales de operación de los procesos informáticos. Así mismo, tendrá alcance a todas las unidades orgánicas de la sede institucional y sedes remotas.

La tabla N° 01 muestra a las diferentes sedes administrativas remotas que incluye a la Sede Central.

N°	DIRECCION (Jirón, Calle, Avenida, Pasaje)	SEDE ADMINISTRATIVA
1	Jr. Raymondi N°220	**Central:** - Despacho: Gobernador Regional. - Gerencia General Regional. - Oficina Regional de Administración. - Oficina de Logística. - Oficina de Contabilidad.

		- Oficina de Tesorería. - Oficina de Gestión de las Personas. - Gerencia Regional de Infraestructura. - Sub Gerencia de Estudios. - Sub Gerencia de Obras. - Oficina Regional de Asesoría Jurídica. - Gerencia Regional de Planeamiento, Presupuesto. - Sub Gerencia de Programación Multianual de Inversiones. - Sub Gerencia de Planificación y Estadística. - Sub Gerencia de Presupuesto. - Sub Gerencia de Desarrollo Institucional. - Sub Gerencia de Seguimiento y Evaluación. - Gerencia Regional de Desarrollo Social. - Sub Gerencia de Promoción y Desarrollo Humano e Inclusión Social. - Oficina de Control Institucional Regional. - Secretaria General. - Oficina de Imagen Institucional. - Oficina de Enlace Lima. - Oficina de Tramite Documentario. - Oficina de Tecnologías de la Información.
2	Jr. Mariscal Cáceres N° 795	**Sede Ex - Inpe:** - Oficina de Gestión Patrimonial. - Almacén Central. - Oficina del Programa de Desarrollo Comunal. - Archivo Institucional. - Archivo Regional. - Gerencia Regional de Pueblos Indígenas. - Archivo de Tesorería. - Archivo Gerencia Regional de Infraestructura - GRI. - Oficina de Liquidaciones GRI.
3	Jr. Apurímac N° 460	**Sede Apurímac:** - Secretaria del Consejo Regional. - Despacho: Vice Gobernador Regional. - Gerencia Regional de Desarrollo Económico. - Sub Gerencia de Promoción de Inversiones y Competitividad Regional. - Sub Gerencia de Políticas, Seguimiento y Evaluación. - Autoridad Regional de Ucayali - ARAU.

		- Dirección de Gestión del Territorio. - Dirección de Gestión Ambiental. - Procuraduría Publica Regional. - Dirección Regional de Energía y Minas (Unidad Operativa). - Dirección Regional de vivienda y Construcción (Unidad Operativa). - Oficina de Cooperación Técnica y Relaciones Internacionales. - Secretaria Técnica de Procesos Administrativos Disciplinarios.
4	Av. Centenario Km. 3.500, interior	- Oficina Regional de Defensa Nacional. - Proyecto Regional de Infraestructura Multisectorial - PRIM.
5	Av. Centenario Km.2.500	- Gerencia Regional Forestal y de Fauna Silvestre.

Tabla N° 01: Sedes Remotas del Gobierno Regional de Ucayali.

IV. BASE LEGAL.

- Ley N°27867, Ley Orgánica de Gobiernos Regionales y sus modificatorias.
- Decreto Supremo N° 004-2019-JUS, que aprueba el Texto Único Ordenado de la Ley N° 27444, Ley de Procedimiento Administrativo General.
- Resolución Ministerial N° 188-2015-PCM, Aprobación de los Lineamientos para la Formulación y Aprobación de Planes de Contingencia.
- Resolución Ministerial N° 028-2015-PCM, Aprueba los lineamientos para la gestión de la continuidad operativa de las Entidades Públicas entre los tres niveles de gobierno.
- Resolución Ministerial N° 004-2016-PCM, 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.
- Decreto Supremo N° 066-2011-PCM que aprueba el "Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 2.0",y que en su objetivo N° 7, establece la necesidad de promover una Administración Pública de calidad orientada a la población, y la necesidad de contar con una Estrategia Nacional de Ciberseguridad, con el objetivo de minimizar los riesgos en caso de sufrir algún tipo de incidente en los recursos informáticos del Estado, así como, la disuasión

del crimen cibernético, que se producen mediante el uso de redes teleinformáticas, entre otros.

- Decreto de Urgencia N° 007-2020, que aprueba el marco de confianza digital.
- Resolución Ministerial N° 246-2007-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI Tecnologías de la Información, Código de Buenas Prácticas para la Gestión de Seguridad de la Información 2da Edición en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Directoral N° 0022-2022-INACAL/DN, que aprueba la Norma Técnica Peruana NTP-ISO/IEC 27001:2022 Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos. 3ra. Edición.
- Ordenanza Regional N°002-2018-GRU-CR – Aprueba el Reglamento de Organización y Funciones - ROF del Gobierno Regional de Ucayali.
- Ordenanza Regional N°003-2019-GRU-CR – Aprueba la modificación estructural del Reglamento de Organización y Funciones – ROF del Gobierno Regional de Ucayali, aprobado mediante Ordenanza Regional N°002-2018-GRU-CR, por la creación de la Gerencia Regional Forestal y de Fauna Silvestre.

V. DISPOSICIONES GENERALES.

El Plan de Contingencia Informático, es fundamental para poder continuar con las actividades críticas del Gobierno Regional de Ucayali, ante un evento inesperado e imprevisible. El presente plan contiene atributos de detalle y de complejidad, independiente o como marco del entorno tecnológico y probablemente conteniendo un conjunto de acciones criticas destinadas a lograr una recuperación dentro de los tiempos esperados.

Para que el Plan de Contingencia tenga éxito, se evaluará y analizará todos los procesos y no limitarse exclusivamente a los recursos e infraestructura asociado a los sistemas de información o software institucional.

La evaluación de riesgo analizará la naturaleza de la ocurrencia de los eventos inesperados, su impacto y la probabilidad de que estos eventos afecten el normal desempeño de los procesos críticos de la entidad.

5.1 Responsabilidades del Plan.

Conforme al Reglamento de Organizaciones y Funciones del Gobierno Regional de Ucayali aprobado con Ordenanza Regional N° 002-2018-GRU-CR, se especifica que una de las funciones de la Oficina de Tecnologías de la Información es proponer y mantener actualizados los Planes de Contingencia y Seguridad Informática de la Institución, en

concordancia con lo dispuesto por la Secretaria de Gobierno Digital (SeGDi) como ente rector del Sistema Nacional de Transformación Digital.

5.2 Actualización del Plan.

El presente plan de contingencia requiere su actualización periódica una vez al año, dicha actualización estará a cargo de la Oficina de Tecnologías de la Información de la entidad.

5.3 Difusión del Documento de Plan de Contingencia

a) Difusión.

La oficina de Tecnologías de la Información del GRU, definirá el mecanismo adecuado para que el personal del área y de las diferentes Unidades Orgánicas puedan acceder al Plan para su conocimiento y aplicación cuando sea necesario.

5.4 Flujo del Plan de Contingencias.

El Plan de Contingencia se rige sobre un proceso iterativo denominado PDCA (Planificar, Hacer, Comprobar y Actuar). Esto inicia con el análisis de riesgos desde donde otras amenazas se identifican y que podría afectar a la continuidad de los procesos. Luego de determinar el impacto en la entidad y la priorización de los procesos críticos, se seleccionan las acciones más importantes para hacer eficiente y eficaz la aplicación del Plan de Contingencia.

El presente Plan deberá ser revisado continuamente, comenzando por realizar un nuevo análisis de riesgos. Es importante resaltar que el Plan de Contingencia siempre requiere estar actualizado y monitoreado ya que nuevas amenazas podrían ocasionar algún tipo de vulnerabilidades que pudieran afectar los procesos internos y/o externos de la entidad. En ese sentido con el objeto de anticipar a una inminente amenaza, es necesario considerar los siguientes casos:

- ✓ Si la amenaza estaba prevista y las acciones ejecutadas fueron eficaces; se corrigen únicamente aspectos menores para mejorar la eficiencia.
- ✓ Si la amenaza estaba prevista y las acciones ejecutadas fueron ineficientes, se deberá analizar el origen de la falla y proponer nuevas acciones que garanticen una mejor medida correctiva/reactiva.
- ✓ Si la amenaza no estaba prevista, se debe actuar inmediatamente para realizar un nuevo análisis de riesgos. Es posible que las acciones adoptadas sean eficaces para una amenaza no prevista. No obstante, que de todas formas se debe realizar el análisis del suceso.

Finalmente, se modifica el Plan de Contingencia siempre que las revisiones estén aprobadas, para luego reiniciar el flujo.

Con la intensión de conocer el flujo antes descrito, se observa en la siguiente figura el flujo general del ciclo de vida del Plan de Contingencia Informático de la entidad:

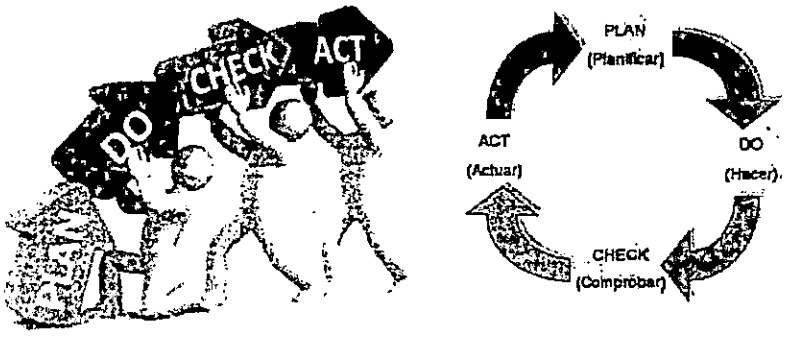


Figura N° 01: Modelo del Ciclo de Vida del Plan
Fuente: Web de ITIL Foundation.

5.5 Declaración de Contingencia.

La ejecución de una declaración de contingencia tiene su origen en cualquier escenario sobre las distintas sedes remotas hoy disponibles, en ese sentido se toma en consideración los siguientes criterios.

5.5.1 Criterios para declarar la Contingencia.

Según la naturaleza de las amenazas, este puede provocar, diferentes consecuencias previsibles y no previsible. Para el presente Plan de Contingencia, el Gobierno Regional de Ucayali ha definido las siguientes amenazas:

a) Incendio o Fuego.

En la Sede Central del Gobierno Regional de Ucayali, existen mayores probabilidades de ocurrencia de siniestro producto de un incendio, ya que la infraestructura del local es de material inflamable sumado a esto el deficiente sistema eléctrico con que cuenta dicha sede. Por lo tanto, es nuestra obligación estar preparados ante una situación de grandes magnitudes que

podría generar graves consecuencias y pérdidas cuantiosas que afectarían la operativa de la entidad.

b) Sismo.
Este evento es el más imprevisible de todos, por lo que se deberá tomar la precaución del caso para que su efecto no traiga consecuencias graves que altere el normal funcionamiento de las labores en la entidad.

c) Inundaciones por Lluvias Torrenciales.
Producto de las constantes lluvias que muchas veces se extiende por más de una hora, podría generar inundaciones que permitiría el ingreso masivo de agua a las instalaciones de la Entidad, sobre todo en la Sede Central que se encuentra en una zona orográfica baja.

d) Interrupción del Suministro o Fluido Eléctrico.
La interrupción del fluido eléctrico por un tiempo prolongado ocasionará la suspensión de las actividades administrativas normales que ejecuta la entidad, dando lugar a una posible pérdida de datos y fallas graves en los procesos críticos que pudieran afectar su continuidad.

e) Interrupción del Servicio de Internet.
El servicio de internet de la entidad es provisto por la empresa Optical Networks, quien actualmente nos provee de 01 línea de internet dedicado con fibra óptica de 100 MB de velocidad para soportar los servicios, sistemas web y el consumo del servicio de internet por parte de los usuarios de la red institucional. En el supuesto que se interrumpa el servicio de Internet, se procederá a comunicar al servicio de atención al cliente indicándole la situación actual para generar un ticket de asistencia, a fin de reestablecer el servicio en el corto plazo.

f) Robo o Pérdida de Archivos.
El Robo o Pérdida de archivos es inminente en sus diferentes modalidades, el robo o pérdida de archivos podría ser atribuido a los propios usuarios, ya que son ellos los administradores de sus propios equipos computacionales.
Ante ello se podría generar una serie de procedimientos para salvaguardar y poner a buen recaudo los archivos de interés institucional.

g) Falla en el Sistema de Alimentación Ininterrumpida (SAI) del Cuarto de Servidores (Data Center).
El Cuarto de Servidores (Data Center) del Gobierno Regional de Ucayali, es el espacio físico más crítico, porque es desde allí

que se gestionan y controlan todos los procesos informáticos y de comunicaciones que la entidad realiza.

Siendo así, corresponde mantener un nivel de redundancia optimo que ayude a minimizar con mayor precisión las interrupciones de los servicios informáticos. El Sistema Alimentación Ininterrumpida (SAI o UPS) es fundamental su operatividad para proteger los equipos, servicios e información alojada en el DC, ante una eventual contingencia por interrupción del fluido eléctrico u otro imprevisto.

h) Falla por recalentamiento del Tablero General.

El Gobierno Regional de Ucayali, cuenta hoy en día con un Tablero de Distribución General que se conecta a la línea pública de energía eléctrica y distribuye a través de sus canales fluido eléctrico a las diferentes unidades orgánicas de la Sede Central del GRU.

Es importante llevar a cabo el adecuado mantenimiento del tablero para evitar cualquier siniestro que termine ocasionando cortos circuitos con consecuencia de incendio.

i) Fallas en los Sistemas de Radioenlaces.

El Gobierno Regional de Ucayali, actualmente interconecta a la mayoría de sus sedes remotas vía sistemas de radioenlace (conectividad inalámbrica vía frecuencias de radio), que ha permitido ahorrar grandemente la inversión de conectividad para aquellas sedes, a fin de que puedan acceder a los principales servicios de la entidad.

Los sistemas inalámbricos sobre radioenlaces, proporciona un alto nivel de seguridad para proteger los datos que se empaquetan y transmiten entre sedes.

Por ello es prescindible considerar que dichos sistemas deben someterse a una revisión periódica para mantener su confiabilidad y desempeño funcional.

j) Fallas en los Equipos de Computo.

Los equipos de cómputo (Desktop y Laptop) del Parque Informático Institucional son las principales fuentes de desarrollo de las actividades de los usuarios en las unidades orgánicas del GRU. Razón por la cual dichos equipos deben estar disponibles la mayor cantidad de tiempo, para evitarse afecte el normal funcionamiento de las labores administrativas hecha por los usuarios de equipos de cómputo.

Ante una eventual caída o desperfecto en la operativa de los equipos de cómputo, se hace necesario considerar la

disponibilidad presupuestal para lograr la ejecución del Plan de Mantenimiento de Equipos preventivo/reactivo para garantizar la ampliación de su ciclo de vida.

k) Fallas en los Equipos de Servidores de Datos

Los Servidores de Información, son pieza clave de la disponibilidad y continuidad de los servicios informáticos del GRU, ya que son estos equipos que permiten el registro, procesamiento, almacenamiento y recuperación de la información en tiempo real y de forma transparente al usuario.

Cualquier anomalía en estos equipos debería de alertar significativamente a la entidad, más aún si no se cuenta con una solución alterna que permita redundar los procesos ante una eventual falla en cadena, que es poco probable que suceda, sin embargo, hay que estar alertas para poder actuar ante cualquier suceso.

l) Fallas en los Sistemas de Base y de Información.

Sistemas Base:

Los sistemas base (Sistemas Operativos), deben estar permanentemente bien vigilados, ya que como plataforma principal para poder soportar todas las demás aplicaciones deben estar en condiciones lógicas de funcionalidad con la gestión de parches y/o actualizaciones de ser el caso para un mejor rendimiento.

En caso de fallas se deberá actuar de manera rápida para restablecer su funcionalidad, aplicando todos los mecanismos posibles para una pronta solución.

Sistemas de Información:

Los sistemas de información de la entidad, como aplicaciones software que automatizan los procesos de la entidad, son susceptible de colapsar por varios motivos, y una de las amenazas más frecuentes y de mayor probabilidad de que se materialice son los propios desarrolladores de software, ya que son ellos los que conocen la lógica del negocio, su arquitectura y su mantenimiento. Para ello se tendrá que considerar la elaboración de un mecanismo automático o no que ayude a garantizar la integridad y disponibilidad documentada de las aplicaciones de propiedad intelectual de la entidad.

m) Falla en el Motor de Base de Datos.

Las Bases de Datos son una de las plataformas más críticas y que deberían tener redundancia absoluta para mantener y poner a buen recaudo la información que desde allí se

administran. El responsable de las copias de seguridad deberá realizar periódicamente un diagnóstico de la funcionalidad del Motor y demás recursos.

n) Falla de la Plataforma de Correo Electrónico.
El correo corporativo institucional del GRU es una plataforma corporativa importante que permite mantener comunicados para interactuar con los principales órganos del gobierno nacional, regional y local, así como también con los diversos agentes públicos privados a nivel mundial. Cualquier evento que atente contra el normal funcionamiento de la plataforma de correo, se atribuye a la suite ZIMBRA, quien es nuestro proveedor actual para dicho servicio. Se prevé el restablecimiento inmediato del servicio por considerarse una plataforma de mucha demanda con alcance global.

o) Falla en el Equipo de Seguridad Firewall.
El equipo de seguridad es un dispositivo que ayuda a controlar, supervisar y gestionar los accesos, roles y políticas para usuarios y grupos de usuarios. Este dispositivo permite además aislar nuestra red LAN local de la red Externa (Internet), impidiendo accesos no autorizados y bajo demanda.
De fallar el Equipo Firewall, afectaría la seguridad primaria de nuestra red LAN y la de nuestras Sistemas, Bases de Datos, archivos y provocaría el uso desmedido del Servicio de Internet por parte de los usuarios, generando un alto riesgo de colapsar y suspender los servicios de la entidad.

p) Falla en el Sistema de Red de Datos LAN.
Hoy en día el Sistema de Red de Datos LAN (Cableado Estructurado) de la Sede Central, es uno de los más deficientes que existen, por cuanto su despliegue, equipamiento y funcionalidad no garantiza un adecuado rendimiento operativo, encontrándose una serie de anomalías que afecten los procesos al usar los diferentes sistemas y aplicaciones (Sistema de Gestión Documentaria, Sistema de Mesa de Partes Virtual, Agenda Institucional, Solicitud de Acceso a la Información Pública, Libro de Reclamaciones, etc.) y del orden nacional (SIAF, SIGA, entre otros).
Al tener una caída en la Red de Datos LAN de la entidad, restringiendo el acceso a los sistemas, recursos y demás componentes informáticos usados por los usuarios, se debería considerar una reestructuración pronta para obtener una mayor confiabilidad.

q) Ausencia del Personal de la Oficina de Tecnologías de la Información.
La disponibilidad del personal informático para realizar las debidas asistencias técnicas a los usuarios que lo requieran es importante, más aún frente a situaciones de contingencia, procesos que ejecutan las distintas unidades orgánicas de la entidad. En ese sentido es también fundamental considerar los mecanismos para que el personal de soporte informático se mantenga expectante ante cualquier evento que active una determinada contingencia.

r) Robo o Pérdida de Equipos.
Es inminente la sustracción o pérdida de algún bien de la entidad, ya que como activo institucional puede ocasionar atrasos con consecuente perdidas de información imprevista. Bajo esa premisa este evento deber ser cuidadosamente protegido por el personal de cada área usuaria.

s) Intrusión.
Este suceso crece cada vez con mayor fuerza, ya que en un mundo donde existe un gran nivel de interoperabilidad e interacción a través de internet, las personas encuentran gran cantidad de mecanismos para acceder a información confidencial y no autorizada.

t) Sabotaje.
El sabotaje hoy en día está teniendo mayores casos en los diferentes sectores, ya que es ocasionado por empleados o ex empleados en contra de la propia entidad como actos de venganzas o incompatibilidad laboral. A esta amenaza debe darse mayor importancia ya que podría desencadenar consecuencias graves que afectarían los activos de información de la entidad.

u) Accesos No Autorizados.
Los accesos sin autorización previa a los ambientes sobre todo de la Oficina de Tecnologías de la Información (Data Center) del Gobierno Regional de Ucayali, supone que la información e infraestructura podrían quedar expuestos para que personal ajeno realice cualquier acto vandálico o forzado que atente contra la integridad, confidencialidad y disponibilidad de la información institucional.

v) Acción de Códigos Maliciosos.
La ejecución de los códigos maliciosos en sus diferentes variantes (virus, troyanos, gusanos, spyware, etc.) representa a

una de las amenazas más peligrosas que afectan la seguridad informática de la entidad, cada variante puede tener objetivos similares o distintos, lo que significa que los atributos y mecanismos de defensa de un software antivirus deben ser los más eficientes posibles. Es inminente la infección por alguna variante de código malicioso externo, sin embargo, es poco probable que una de aquellas amenazas vulnera nuestra infraestructura ya que contamos con sistema de gestión que controlan y supervisan las entradas y salidas de datos desde nuestro Centro de Datos.

VI. DISPOSICIONES ESPECIFICAS.

6.1 Estructura del Plan

Mediante los Planes de Contingencia somos capaces de detectar sobre los efectos económicos, legales y de imagen que pueden llegar a ocasionar la paralización de los procesos o la violación de la confidencialidad de la información del Gobierno Regional de Ucayali. En ese sentido para un adecuado y efectivo desarrollo del plan se ha diseñado la siguiente estructura, en donde se han definido las responsabilidades para cada agente involucrado.

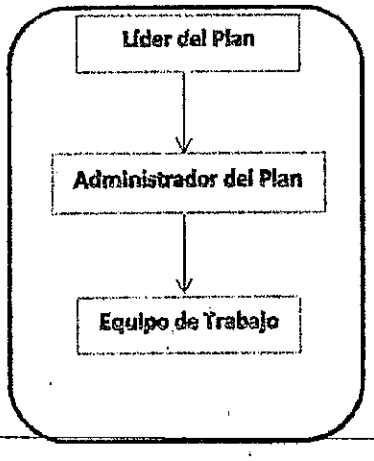


Figura N° 02: Estructura Organizativa del Plan de Contingencia Informático GRU
Fuente: Elaboración Propia

***Evento o incidente;** será entendido como la interrupción de las condiciones normales de operación en cualquier proceso informático dentro del Gobierno Regional de Ucayali.*

En ese sentido dado que existen diferentes niveles de toma de decisiones y acciones de respuesta ante cualquier evento o incidente que demande la ejecución de procedimientos de contingencia, es necesario aprender a tomar decisiones que no dependan de consultas adicionales.

Por ello es importante definir un Estructura para cumplir y hacer cumplir fielmente lo que indica el presente Plan de Contingencia ante cualquier incidente de tipo informático que pudiera impactar negativamente en el funcionamiento y operativa de los servicios informáticos en la entidad.

Por ello la estructura propuesta del Plan de Contingencia tendría las funciones de supervisar, y evaluar la eficiencia y eficacia del Plan de Contingencia.

Quedando conformado de la siguiente manera:

- Líder del Plan: Gerente Regional de Administración.
- Administrador del Plan: Director de la Oficina de Tecnologías de la Información.
- Equipo de Trabajo: Soporte Informático Institucional, Unidades Orgánicas involucradas y de ser el caso la Procuraduría Publica Regional.

El Gerente Regional de Administración y el Jefe de la Oficina de Tecnologías de la Información tienen las funciones de supervisar y evaluar el desarrollo del Plan, así como verificar el cumplimiento de las tareas en caso de una contingencia.

6.2 Equipo de Trabajo.

El equipo de trabajo se encargará de ejecutar el desarrollo del Plan de Contingencia en el extremo de sus competencias, organizando asimismo equipos de trabajo complementarios para afrontar de manera eficiente el antes, durante y después de materializada y controlada una contingencia (evento o incidente).

6.3 Conformación de los Equipos de Trabajo

La conformación de los equipos estará a cargo de la Oficina de Tecnologías de la Información, quien coordinará con las demás áreas usuarias para que sean agentes participantes ante un evento de contingencia determinado.

El aspecto más importante de una organización para hacer frente a contingencias es la creación y entrenamiento de los equipos de trabajo definidos. Dentro del diseño, coordinación, ejecución y desarrollo de pruebas del Plan de Contingencia en necesario contar con varios equipos de trabajo, el mismo que depende del tamaño de la organización y de los recursos existentes como recursos humanos, procesos, equipos eléctricos y/o electrónicos.

Los equipos de trabajo a considerar en este plan se conformarán de acuerdo a las condiciones y escenarios presentados en la contingencia; es decir dependiendo del tipo de evento o incidente expuesto.
En adelante se muestra el cuadro con los equipos de trabajo responsables de ejecutar el Plan de Contingencia Informático, el mismo que estará agrupado por factores de riesgo a fin de segmentar los eventos de contingencias. Estos son:

- Contingencias de tipo Siniestros.
- Contingencias de tipo de Sistemas de Información.
- Contingencias de tipo de Recursos Humanos.
- Contingencias de tipo de Seguridad Interna y Externa.

Contingencia: Siniestros		
Código	**Descripción del Evento de Contingencia**	**Equipo de Trabajo**
CG_01	Incendio o Fuego	Oficina Regional de Administración, Oficina de Tecnologías de la Información, Oficina Regional de Defensa Nacional.
CG_02	Sismo	Todas las áreas de la Sede Central y Sedes Descentralizadas.
CG_03	Inundaciones por Lluvias Torrenciales	Gerencia Regional de Infraestructura, Oficina de Tecnologías de la Información, Oficina Regional de Defensa Nacional.
CG_04	Interrupción del Suministro o Fluido Eléctrico	Oficina Regional de Administración.
CG_05	Falla por recalentamiento del Tablero General	Oficina Regional de Administración y la Gerencia Regional de Infraestructura.
CG_06	Interrupción del Servicio de Internet	Oficina Regional de Administración, Oficina de Tecnologías de la Información.
Contingencias: Sistemas de Información		
CG_07	Robo o pérdida de Información	Oficina Regional de Administración, Oficina de Tecnologías de la Información, Oficina Regional

		de Asesoría Jurídica, Procuraduría Pública Regional.
CG_08	Falla en el Sistema de Alimentación Ininterrumpida (SAI) Principal	Oficina Regional de Administración, Oficina de Tecnologías de la Información.
CG_09	Fallas en los Sistemas de Radioenlaces	Oficina de Tecnologías de la Información.
CG_10	Falla en los Equipos de Computo	Oficina de Tecnologías de la Información.
CG_11	Fallas en los Equipos Servidores de Información	Oficina de Tecnologías de la Información.
CG_12	Fallas en los Sistemas Base y de Información	Oficina de Tecnologías de la Información.
CG_13	Falla en el Motor de Bases de Datos	Oficina de Tecnologías de la Información.
CG_14	Falla en la Plataforma de Correo Electrónico	Oficina de Tecnologías de la Información.
CG_15	Falla del Equipo de Seguridad Firewall	Oficina de Tecnologías de la Información.
CG_16	Falla en el Sistema de Red de Datos Local LAN	Oficina de Tecnologías de la Información.
CG_17	Accesos No Autorizados	Oficina de Tecnologías de la Información.
CG_18	Acción de Código Malicioso	Oficina de Tecnologías de la Información.
Contingencia: Recursos Humanos		
CG_19	Ausencia del Personal de la Oficina de Tecnologías de la Información	Oficina de Tecnologías de la Información, Oficina de Gestión de las Personas.
CG_20	Ausencia de personal Directivo para la Toma de Decisiones ante eventos de contingencias o riesgo inminente	Gerencia General Regional, Oficina Regional de Administración.
Contingencia: Seguridad Interna y Externa		
CG_21	Robo o Pérdida de Equipos	Oficina Regional de Administración, Oficina de Tecnologías de la Información, Oficina Regional de Asesoría Jurídica, Procuraduría Pública Regional.

CG_22	Intrusión	Oficina Regional de Administración, Oficina de Tecnologías de la Información.
CG_23	Sabotaje	Oficina Regional de Administración, Oficina de Tecnologías de la Información, Procuraduría Pública Regional.

Tabla N° 02: Equipos de Trabajo para la Ejecución del Plan de Contingencias.

6.4 Gestión del Riesgo

El riesgo como tal es un suceso imprevisible que puede presentarse en cualquier circunstancia, el mismo que puede generar diferentes impactos para todos los escenarios posibles.

Riesgo; es la probabilidad de ocurrencia de un evento inesperado. Proximidad a un daño, contingencia, peligro, inseguridad o exposición. Proceso Crítico; Proceso considerado indispensable para la continuidad de las operaciones y servicios del Gobierno Regional de Ucayali - RU, y cuya falta o ejecución deficiente puede tener un impacto operacional o de imagen significativo para la Entidad.

6.4.1 Análisis del Riesgo:

Producto del análisis del riesgo, se genera información valiosa para identificar y cuantificar la criticidad de los eventos de contingencia, el mismo que sirve para tomar las mejoras de decisiones. En ese sentido se consideran 3 elementos que permiten aproximar un valor objetivo del riesgo, entre los que tenemos: la Probabilidad, el Impacto y la Exposición al Riesgo. Estos elementos permitirán gestionar con mayor eficiencia y detalle los tiempos en la administración de los riesgos que podrían generar más impacto.

6.4.2 Probabilidad del Riesgo:

Es el afecto inminente de que un evento de contingencia se materialice. La probabilidad del riesgo debe ser superior a cero, caso contrario se presume una amenaza al servicio. Asimismo, la probabilidad debe ser inferior al 100% o el riesgo será una certeza; dicho de otro modo, es un problema conocido.

La probabilidad se puede entender también como la posibilidad de la consecuencia, porque si la condición se produce se supone que la probabilidad de la consecuencia será del 100%.

6.4.3 Impacto del Riesgo:

El impacto del riesgo se mide por la gravedad de los efectos producto de una amenaza. El mismo que ayuda a determinar el nivel del impacto en relación al grado de afectación del nivel del servicio. Cuanto mayor sea el valor, mayor será el impacto, para el caso nuestro clasificaremos el impacto con escala del 1 al 3.

6.4.4 Exposición al Riesgo:

Esta definición es la resultante de multiplicar la probabilidad por el impacto. Es así que aquellos riesgos que tienen un alto nivel de probabilidad y de impacto son los que mayor atención deben tener, pues son los que generan mayores valores de exposición.

6.4.5 Eventos Con Control y Sin Control:

En razón de identificar a los riesgos, estos deben ser clasificados en función de las acciones de prevención, y que pueden ser definidos por la entidad. Considerando que habrá eventos que no se pueden identificar por ser impredecibles. En ese sentido se tienen la siguiente clasificación.

a) **Eventos con Control**

Son aquellos que al identificarlos nos permite ejecutar acciones que eviten su materialización o minimicen el impacto.

b) **Eventos sin Control**

Son aquellos en los que su ocurrencia es impredecible, motivo por el cual solo ejecutaremos acciones que minimicen su impacto.

6.4.6 Matriz del Riesgo:

Todo suceso de un evento de contingencia trae consecuencias sobre las actividades propias de la entidad, por lo que es importante identificar su impacto. En ese sentido resulta fundamental su cuantificación con la finalidad de obtener un mejor análisis. El valor numérico asignado es directamente proporcional con respecto al impacto o gravedad que su ocurrencia pueda generar a los servicios, los impactos se clasificaran según la Tabla N° 03, donde una actividad crítica se encuentra clasificada dependiendo de la importancia dentro de los procesos TI.

Impacto	Detalle	Valor Numérico
Bajo impacto	Se considera que una actividad crítica tiene un impacto bajo, cuando la falla de esta, no tiene un impacto en la continuidad de las operaciones.	1
Medio Impacto	Se considera que una actividad critica tiene un impacto medio cuando la falla de esta	2

	ocasiona una interrupción en las operaciones del GRU por un tiempo mínimo de tolerancia.	
Alto Impacto	Se considera que una actividad crítica tiene un impacto alto sobre las operaciones del GRU, cuando ante un evento inesperado las funciones normales son interrumpidas en su totalidad.	3

Tabla N° 03: Cuadro de Impactos

Probabilidad de Ocurrencia	Detalle
Frecuente	Evento repetido
Ocasional	Suceso de alguna vez
Remoto	Impracticable que suceda

Tabla N°04: Cuadro de Probabilidad de Ocurrencias

La probabilidad de ocurrencia de un evento resulta fundamental para determinar la posibilidad de que dicho evento de contingencia se concentre. La determinación de esta probabilidad se recogerá de la información obtenida de planes de contingencias implementados en diferentes organizaciones.
Que se entienda técnicamente lo siguiente; ***Exposición = Impacto x Probabilidad.***

	Bajo	Medio	Alto
Frecuente			
Ocasional			
Remoto			

Tabla N° 05: Exposición al Riesgo

Todo evento cuyo valor numérico sea "3" o cuya calificación sea de "Alto Impacto", es considerado un evento critico dentro del Plan de Contingencia, lo que significa que se pondrá mayor atención sobre dichos eventos.
Así mismo cualquier evento cuya exposición al riesgo sea igual o mayor al promedio de 0.15, tendrá también la denominación de evento de contingencia "Crítico".
En la matriz de Riesgo de Contingencia serán considerados los eventos susceptibles de entrar en contingencia, indicando su valor y su clasificación (Con Control/Sin Control).

6.5 Elementos Identificados como Críticos para Generar eventos de Contingencias

Como parte de la identificación de los aspectos que forman parte del servicio informático y de comunicaciones del Gobierno Regional de Ucayali, resulta fundamental considerar todos los elementos susceptibles de generar eventos que suponen la activación de una contingencia. Sobre ello se tienen los siguientes elementos que serán sospesados para su respectiva evaluación.

- HARDWARE
  - Servidores de Información.
  - Equipo de Cómputo (Desktop y Portátiles).
  - Impresoras, fotocopiadoras y Escáner.
  - Equipos de Radioenlaces.
  - Equipos Multimedia.
- SOFTWARE
  - Software Base (Sistemas Operativos y de Ofimática).
  - Sistemas de Información en producción dentro de la entidad.
  - Software de Base de Datos.
  - Software Antivirus.
  - Software de aplicación específica para las diferentes áreas.
- COMUNICACIONES
  - Equipos Conmutadores (Switch).
  - Equipos Router.
  - Equipos Cortafuegos.
  - Equipos de Radio Enlaces.
- SISTEMAS DE INFORMACION
  - Respaldo de Información generada con Software Base y Ofimática.
  - Respaldo de los Sistemas Informáticos puestos en producción dentro de la entidad.
  - Respaldo de Bases de Datos de los sistemas de información.
  - Configuración de Servidores de Información.
- EQUIPOS AUTONOMOS, DE EFRIAMIENTO Y OTROS.
  - Sistema de Climatización de precisión.
  - Sistemas de Alimentación Ininterrumpida-SAI del Centro de Datos y de los Equipos de Cómputo.
  - Sistemas de Aire Acondicionado de Confort.
  - Tablero General.
- INFRAESTRUCTURA INSTITUCIONAL
  - Sede Central.

- Sedes Remotas (Ex Inpe, Apurímac, Defensa Nacional/Seguridad Ciudadana/Defensa Civil, Gerencia Regional Forestal y de Fauna Silvestre).

- PROVEEDORES DE SERVICIOS ANALOGOS Y DIGITALES
  - Internet.
  - Suministro Eléctrico.
- CAPITAL HUMANO
  - Personal Directivo con predisposición y compromiso para actuar ante eventos de contingencias.
  - Personal administrativo en sus diferentes niveles.

6.6 Desarrollo del Plan de Contingencias

Cuando se haya identificado los eventos de contingencia y los elementos superferolíticos causantes de los mismos, se iniciará la ejecución del Plan de Contingencia. En síntesis, la secuencia general a desarrollar cuando se presente un evento de contingencia sería el siguiente:

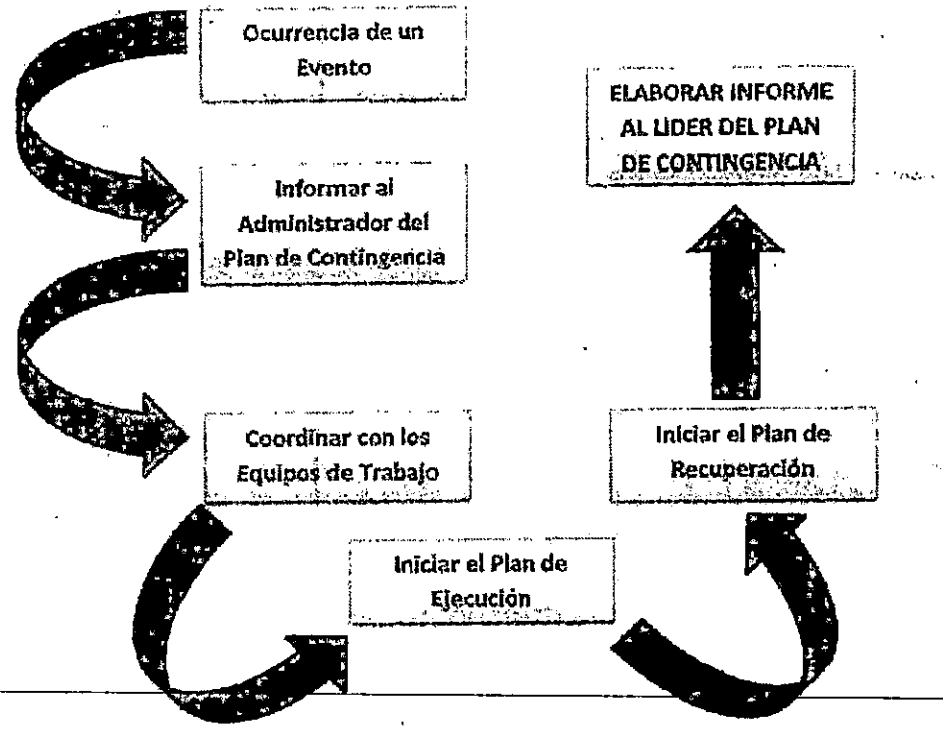


Figura N° 03: Flujo General de la Ejecución del Plan de Contingencia
Fuente: Elaboración Propia.

6.7 Plan de Pruebas.

6.7.1 Introducción.

Una de las medidas para minimizar los riesgos de la tecnología son las PRUEBAS. Cada componente de un sistema de información, equipos informáticos, equipos de comunicaciones y software en

general debe ser aprobado cuidadosamente antes de utilizarlo para un evento.

Todos los planes de contingencia deben ser probados para demostrar su habilidad de mantener la continuidad de los procesos críticos de la entidad.

Cuando se desarrollan pruebas al plan de contingencias, se descubren elementos operacionales que requieren ajustes para asegurar y/o garantizar el éxito en la ejecución del plan, de tal forma que dichos ajustes perfeccionen los planes preestablecidos.

6.7.2 Objetivos.

- Determinar si el Plan de Contingencias es capaz de proporcionar el nivel deseado de apoyo a la sección o a los procesos críticos del GRU, probando la efectividad de los procedimientos expuestos en el Plan de Contingencias.
- Las pruebas permitirán ejecutar una valoración detallada de los costos de operación al momento de la ocurrencia de un evento de contingencia.

6.7.3 Procedimientos de Pruebas del Plan de Contingencias.

En este caso se recomienda 2 niveles de pruebas:

- Pruebas en pequeñas Unidades Orgánicas.
- Pruebas a nivel Gerencial.

La idea es iniciar la prueba en las Unidades Orgánicas más pequeñas, para luego extender el alcance al nivel gerencial.

6.7.4 Métodos para realizar Pruebas del Plan de Contingencias.

a) Prueba Específica.

Consiste en probar una sola actividad, entrenando al personal en una función específica, basándose en los procedimientos estándar definidos en el Plan de Contingencia. De esta manera el personal tendrá una tarea bien definida y desarrollará la habilidad para cumplirla.

b) Prueba de Escritorio.

Implica el desarrollo de un Plan de Pruebas a través de una serie de preguntas estructurales.

Atributos y/o Esquema:

- Se usará un formato estándar.
- Está dirigido al equipo de recuperación de contingencias.
- Permite probar habilidades gerenciales del personal que tiene una mayor responsabilidad en sus funciones.

Las preguntas de escritorio son ejecutadas por el encargado de la prueba y el personal responsable de poner el plan de contingencias en ejecución que en la mayoría de los casos será personal de la Oficina de Tecnologías de la Información, en una situación hipotética de contingencia.

Un conjunto de preguntas se pedirá resuelva el personal.

El encargado y el personal utilizarán el plan de contingencias para resolver las respuestas a cada situación. El encargado contestará a las preguntas que se relacionan con la disponibilidad del personal entrenado, suficiencia de los recursos, suficiencia de máquinas, y si los requerimientos necesarios están de la mano. Los ajustes serán hechos al plan o al ambiente determinado durante esta fase si cualquier parte del plan no cumple con los objetivos propuestos.

c) Simulación en Tiempo Real.

Las pruebas de simulación real en la Unidad Orgánica a nivel de Gerencia en el GRU, estará dirigido a una situación de contingencia por un periodo de tiempo definido.

- Las pruebas se harán en tiempo real (durante el día o considerando una situación o escenario lo más real posible).
- Son usadas para probar partes específicas del plan.
- Permiten medir las habilidades de acción y ejecución en equipo de los grupos asignados para afrontar contingencias.

6.7.5 Preparaciones PRE Prueba.

- Verificar el Plan de Contingencias.
- Verificar si se han asignado las respectivas responsabilidades.
- Entrenar a todo el personal involucrado, incluyendo orientación completa de los objetivos del plan, roles, responsabilidades y la apreciación global del proceso.
- Establecer la fecha y hora para la ejecución de la prueba.
- Desarrollar un documento que indique los objetivos, alcances y metas de la prueba y distribuirlo antes de su ejecución.
- Asegurar la disponibilidad del ambiente donde se hará la prueba y del personal esencial durante tiempo que tomará la ejecución de dichas pruebas.
- No dejar de lado los resultados obtenidos, la meta es aprender y descubrir las vulnerabilidades, no generar fracaso y frustración.
- La prueba inicial se enfoca principalmente en entrenar al equipo que ejecutará con éxito el plan de contingencias, solucionando el problema y restableciendo a la normalidad las actividades realizadas.
- Enfocar los procesos críticos que dependen de sistemas específicos o compañías externas donde se asume que hay problemas.
- Definir el ambiente donde se realizarán las reuniones del equipo de recuperación de contingencias.

- Distribuir una copia de la parte del Plan de Contingencias a ser ejecutado.

6.7.6 Comprobación del Plan de Contingencias

El resultado final debe ser una prueba integrada que involucre secciones múltiples del Plan de Contingencia de la entidad. La capacidad funcional del Plan de Contingencia radica en el hecho de que tan cerca se encuentren los resultados de la prueba con las metas planteadas.

6.7.7 Flujo del Plan de Pruebas.

A continuación, se muestra la ejecución de las pruebas del Plan de Contingencias. Continúa en la página siguiente:

GOBIERNO REGIONAL DE UCAYALI V°B° GOBERNACIÓN

GOBIERNO REGIONAL DE UCAYALI V°B° GERENCIA GENERAL

OFICINA REGIONAL DE ADMINISTRACIÓN V°B° G.R.U.

Gerencia Regional de Planeamiento y Pres. V°B° G.R.U.

OFICINA REGIONAL DE ASESORÍA JURÍDICA V°B° G.R.U.

GOBIERNO REGIONAL DE UCAYALI V°B° SECRETARÍA GENERAL

SUB GERENCIA DE DESARROLLO INSTITUCIONAL V°B° GRPP

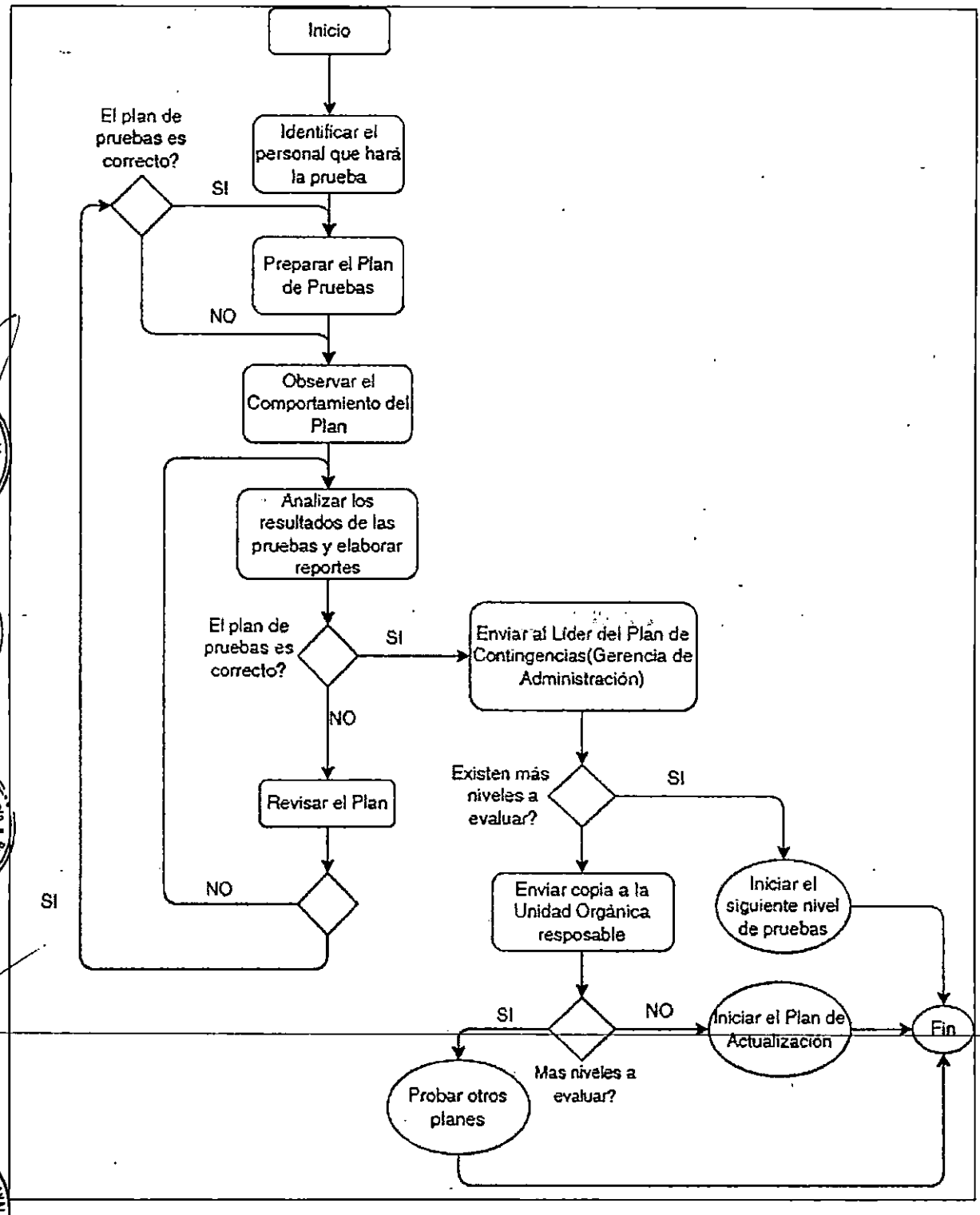


Figura N° 04: Flujo de Ejecución de las Pruebas del Plan de Contingencia.

6.8 Plan de Respaldo y Recuperación.

6.8.1 Objetivo.

Establecer procedimientos para el funcionamiento de los servicios y la administración de las copias de seguridad de información de los diferentes Sistemas de Información, Base de Datos e Información Crítica que cuenta el Gobierno Regional de Ucayali, la cual se encuentran en proceso de producción.

6.8.2 Alcance.

Se aplica para todos los Sistemas de Información, Base de Datos e Información Crítica en producción alojados en los servidores de datos y servicios de red de la entidad.

6.8.3 Servicios y Servidores que deben contar con Respaldo y su pronta Restauración

- Copia de seguridad de la base de datos de los sistemas de información (SISGEDO, SIAF, SIGAM MEF, SIGA PLANILA, AGENDA VIRTUAL, CONVOCATORIAS, MESA DE PARTES VIRTUAL, SOLICITUD A LA INFORMACION PUBLICA, SISTEMA DE LIBRO DE RECLAMACIONES, ASISTENCIA, SISMORE).
- Copia de seguridad del código fuente de los sistemas de información (SISGEDO, SIAF, SIGA MEF, SIGA PLANILA, AGENDA VIRTUAL, CONVOCATORIAS, MESA DE PARTES VIRTUAL, SOLICITUD A LA INFORMACION PUBLICA, SISTEMA DE LIBRO DE RECLAMACIONES, ASISTENCIA, SISMORE).
- Copia de seguridad del Servidor de Correo Institucional.
- Copia de seguridad de las máquinas virtuales.
- Copia de seguridad del Firewall.
- Copia de seguridad del Directorio Activo (Dominio).
- Copia de seguridad de la Información Crítica que se encuentran en los servidores.

6.8.4 Estrategias de Respaldo y Recuperación

Para la correcta elaboración de las copias de seguridad y pronta recuperación de la información, se debe designar formalmente a las personas responsables de esta función.

Para el Respaldo de la información

- Respaldo Local

  En este tipo de respaldo existen diversos dispositivos la cual se pueden usar:
  - Servidor de Respaldo
  - Disco Duro externo en Red o USB
  - CD's y DVD's
  - Cintas Magnéticas

La desventaja de utilizar estos medios de respaldo es que ante cualquier eventualidad que se suscite en la sede donde se encuentren estos equipos se verán afectados.

- Respaldo Remoto
  En este tipo de respaldo se diferencia por la ventaja de que nuestra información pueda estar a salvo ante eventualidades que pueda suceder en la sede principal en donde se encuentran nuestros equipos tecnológicos, entre los tipos tenemos:
  - Servidor de Respaldo remotos

    Si en caso la entidad tuviera diferentes sedes separadas geográficamente se pudiera instalar uno o varios servidores distribuidos, para la generación de copias de seguridad de la información a través de la red con una conexión optima y segura. De esa manera si llegara a suceder alguna eventualidad en una de las sedes de la entidad, la información podría ser recuperada inmediatamente.

  - Servicios de Respaldo Remoto
    Existen empresas que ofrecen los servicios de servidores dedicados o servicios de respaldo, en donde la entidad solo alquila el espacio o el equipamiento que necesite para el respaldo de su información, teniendo en cuenta que la empresa ofrezca una buena política de seguridad, privacidad y la garantía de la integridad de la información. Estos servicios son conocidos popularmente como servicios en la nube.

Frecuencia de la ejecución de las copias de seguridad
La frecuencia dependerá del tipo de copia de seguridad a ejecutar, a continuación, se detalla:

- Copia de seguridad de Base de Datos:
  Se debe realizar de manera diaria, semanal y mensual.
- Copia de seguridad de Firewall:
  Se debe realizar mensualmente.
- Copia de seguridad de servicios
  Se debe realizar de manera diaria, semanal y mensual, siempre que éstos actualicen de su versión.

Ubicación de las copias de seguridad.

En caso del Gobierno Regional de Ucayali, el almacenamiento de las Copias de Seguridad se realiza en tres dispositivos diferentes, servidor de datos, Disco Duro externo de 2 Tb con conexión USB 3.0 y un Disco Duro externo de 16 TeraBytes con conexión USB 3.0 de alta velocidad, la cual se encuentra conectado a uno de los servidores físicos ubicado dentro del Centro de Datos de la Entidad.

Registros de las copias de seguridad

Se realiza el llenado de la bitácora de Copia de Seguridad del Gobierno Regional de Ucayali del Anexo N° 03, de manera diaria. A su vez, se remite un informe a la Oficina Regional de Administración de manera semanal, validando las copias de seguridad.

Al momento de realizar la copia de seguridad, se debe respetar la siguiente estructura:

BK_NombreCopiaDeSeguridad_Dia_Mes_Año
Ejemplo: BK_SISGEDO_20_10_2023.

Para la Recuperación de la Información

Ante cualquier eventualidad que la entidad presente, la continuidad de los servicios informáticos puede lograrse mediante acciones preventivas, evitando la paralización y logrando poner en marcha nuevamente en el menor tiempo posible.

Dentro de los procedimientos de recuperación de la información, se tiene los siguientes tipos:

- Recuperación Gradual o en Frío
  Implica la restauración de la copia de seguridad de manera progresiva, en donde la entidad no se vea afectada por un plazo de 72 horas como máximo sin el restablecimiento de los servicios informáticos.
- Recuperación Intermedia o Templada
  Implica la restauración de las copias de seguridad y el restablecimiento de los servicios informáticos por un periodo de 24 horas como máximo.
- Recuperación Inmediata o Caliente
  Implica la restauración de las copias de seguridad y el restablecimiento de los servicios informáticos de manera inmediata, proporcionando un ambiente de producción espejo.

Para la recuperación del Centro de Datos

Ante cualquier desastre natural o provocado por el ser humano, no solo se debe salvaguardar la información sino también el espacio y equipamiento en donde se alojan, por ello es muy importante tener en claro los procedimientos para la recuperación del Centro de Datos ante cualquier evento que afecte directamente.

Para esto es importante contar con un Centro de Datos Redundante (CDR), teniendo en cuenta el estricto cumplimiento de las medidas de seguridad y prevención ante desastres, logrando así que éste no se vea afectado.

Procedimiento de Recuperación:

En caso de desastres en el centro de Datos de la Sede Principal

- Comunicar al personal encargado y al Oficial de Seguridad y Confianza Digital de la Oficina de Tecnologías de la Información la activación del Centro de Datos Redundante.
- Instalar y configurar software Base en los servidores del Centro de Datos Redundante.
- Instalar y configurar las estaciones de trabajo y los equipos de telecomunicaciones.
- Comunicar al Personal Responsable de la generación de las Copias de Seguridad, la restauración de la misma en el centro de Datos Redundantes para el restablecimiento inmediato de los servicios informáticos de la entidad.
- Verificar el correcto funcionamiento de los equipos del Centro de Datos Redundante y los servicios informáticos de la entidad.

Para la reestructuración y retorno al centro de Datos en la Sede Principal.

- Verificar y realizar el control de daños de los equipos e instalaciones que resultaron comprometidos durante el desastre suscitado en la Sede Principal para su pronta restauración o en caso extremo la sustitución.
- Priorizar la adquisición o restauración de los bienes afectados.
- Una vez adquirido los bienes solicitados, supervisar la instalación y/o montaje de los mismos.

- Realizar la configuración de los equipos, el entorno de trabajo y los equipos de telecomunicaciones del Centro de Datos.
- Restaurar la información y los servicios informáticos en el Centro de Datos de la sede principal.
- Desactivar el Centro de Datos Redundante.

6.9 Identificación de Aplicaciones Críticas

La tabla N° 06 muestra la Matriz del Riesgo de Contingencia ponderado, de acuerdo a los valores de riesgo e impacto en los distintos procesos corporativos, usando el conocimiento y la experiencia en Sistemas de Información y de Comunicaciones.

Orden	Descripción del riesgo	Probabilidad	Impacto	Ponderación	Alerta	clasificación
CONTINGENCIA: Riesgos relacionados a Siniestros						
	INFRAESTRUCTURA INSTITUCIONAL					
1	Incendio o Fuego	0.04	3	0.16	3	CC
2	Sismo	0.10	3	0.30	3	SC
3	Inundación por desperfecto de servicios sanitarios y/lluvias torrenciales	0.02	2	0.04	2	CC
	PROVEEDORES DE SERVICIOS					
4	Interrupción del suministro o Fluido Eléctrico.	0.10	3	0.20	3	CC
5	interrupción del Servicio de Telefonía	0.02	1	0.02	1	SC
6	Interrupción en el servicio de Internet.	0.10	1	0.02	1	SC
	EQUIPO					
7	Falla en el Sistema de Alimentación Ininterrumpida SAI Principal.	0.02	3	0.06	3	CC
8	Falla por recalentamiento del Tablero General.	0.10	3	0.20	3	CC
CONTINGENCIA: Riesgos relacionados a Sistemas de Información						

	INFORMACION					
9	Robo o Pérdida de Archivos	0.03	2	0.06	2	CC
	SOFTWARE					
10	Acción de Códigos Maliciosos	0.05	3	0.20	3	CC
11	Falla en los Sistemas Base y de Información.	0.05	3	0.20	3	CC
12	Falla en la Plataforma de Correo Electrónico.	0.10	3	0.20	3	SC
13	Falla del Motor de Base de Datos.	0.04	3	0.16	3	CC
	COMUNICACIONES					
14	Falla en el Sistema de Red de Datos LAN.	0.04	3	0.16	3	CC
	HARDWARE					
15	Fallas de equipos de Cómputo (Desktop y Portátiles).	0.03	2	0.06	2	CC
16	Fallas en los Equipos Servidores de Información.	0.04	3	0.20	3	CC
17	Falla en el Equipo de Seguridad Firewall.	0.03	3	0.12	3	CC
CONTINGENCIA: Riesgos relacionados a Recursos Humanos						
18	Ausencia del personal de la Oficina de Tecnologías de la Información	0.04	3	0.16	3	CC
19	Ausencia de personal Directivo para la Toma de Decisiones ante eventos de	0.03	3	0.09	3	CC

	contingencias o riesgo inminente					
CONTINGENCIA: Riesgos relacionados a la Seguridad Interna y Externa						
	INFRAESTRUCTURA INSTITUCIONAL					
20	Robo o Pérdida de Equipos.	0.03	3	0.09	3	CC
21	Intrusión	0.03	3	0.12	3	SC
22	Sabotaje	0.01	3	0.03	3	SC
23	Accesos no Autorizados	0.01	3	0.03	3	CC

Tabla N° 06: Matriz de Riesgo de Contingencia

El valor "3" en la columna "Alerta" significa que el evento es de un "ALTO IMPACTO", por lo que deberá ser controlado con cualquier mecanismo o proceso adecuado.
En la columna "Clasificación" se identifican a todos los eventos "Con Control (CC) o Sin Control (SC)".

En la tabla N° 07 y la Tabla N° 08 se tiene la sinopsis de los eventos de acuerdo a su clasificación.

Numeración del Cuadro N°	Eventos Con Control
1	Incendio o Fuego
3	Inundaciones por Lluvias Torrenciales
4	Interrupción del Suministro o Fluido Eléctrico
7	Falla en el Sistema de Alimentación Ininterrumpida – SAI Principal.
8	Falla por recalentamiento del Tablero General
9	Robo o Pérdida de Archivos
10	Acción de Códigos Maliciosos.
11	Falla en los Sistemas Base y de Información.
13	Falla del Motor de Base de Datos.
14	Falla en el Sistema de Red de Datos LAN.
16	Falla en los Equipos de Cómputo.
17	Fallas en los Equipos Servidores de Información.
18	Falla en el Equipo de Seguridad Firewall.
19	Ausencia del Personal de la Oficina de Tecnologías de la Información
20	Ausencia de Personal Directivo para la Toma de Decisiones ante eventos de contingencias o riesgo inminente.
21	Robo o Pérdida de Equipos.
24	Accesos No Autorizados.

Tabla N° 07: Eventos Con Control (CC)

Numeración del Cuadro N°	Eventos Sin Control (SC)
2	Sismo
5	Interrupción del Servicio de Telefonía
6	Interrupción del Servicio de Internet
12	Falla en la Plataforma de Correo Electrónico
22	Intrusión
23	Sabotaje

Tabla N° 08: Eventos Sin Control (SC)

Luego de identificar los eventos de contingencia, presentamos la Tabla N° 09 denominado Elementos vs Contingencia, donde se muestran la relación existente entre los elementos mínimos definidos por la Oficina de Tecnologías de la Información, indicando a que contingencia especificada pertenecen.

ELEMENTO	PLAN DE CONTINGENCA DESARROLLADO		
	CODIGO	ALCANCE	CONTINGENCIA
HARDWARE			
SERVIDORES	CG-01	INFRAESTRUCTURA INSTITUCIONAL	Siniestros
	CG-03	INFRAESTRUCTURA INSTITUCIONAL	Siniestros
	CG-04	INFRAESTRUCTURA INSTITUCIONAL	Siniestros
	CG-05	EQUIPO	Siniestros
	CG-08	EQUIPO	Sistemas de Información
	CG-11	HARDWARE	Sistemas de Información
	CG-13	SOFTWARE	Sistemas de Información
	CG-19	SOFTWARE	Sistemas de Información
	CG-23	INFRAESTRUCTURA INSTITUCIONAL	Seguridad Interna y Externa
	CG-24	INFRAESTRUCTURA INSTITUCIONAL	Seguridad Interna y Externa
Estaciones de Cómputo (Desktop y Portátiles)	CG-01	INFRAESTRUCTURA INSTITUCIONAL	Siniestros
	CG-03	INFRAESTRUCTURA INSTITUCIONAL	Siniestros
	CG-04	PROVEEDORES DE SERVICIOS	Siniestros
	CG-05	PROVEEDORES DE SERVICIOS	Siniestros

	CG-07	INFORMACION	Sistemas de Información
	CG-10	HARDWARE	Sistemas de Información
	CG-12	SOFTWARE	Sistemas de Información
	CG-19	SOFTWARE	Sistemas de Información
	CG-20	INFORMACION	Recursos Humanos
	CG-22	INFRAESTRUCTURA INSTITUCIONAL	Seguridad Interna y Externa
	CG-23	INFRAESTRUCTURA INSTITUCIONAL	Seguridad Interna y Externa
	CG-24	INFRAESTRUCTURA INSTITUCIONAL	Seguridad Interna y Externa
Equipos de Radioenlaces	CG-04	PROVEEDORES DE SERVICIOS	Siniestros
	CG-16	COMUNICACIONES	Sistemas de Información
	CG-23	INFRAESTRUCTURA INSTITUCIONAL	Seguridad Interna y Externa
	CG-24	INFRAESTRUCTURA INSTITUCIONAL	Seguridad Interna y Externa
SOFTWARE			
Motor de Base de Datos	CG-08	EQUIPO	Siniestros
	CG-11	SOFTWARE	Sistemas de Información
	CG-12	SOFTWARE	Sistemas de Información
	CG-13	SOFTWARE	Sistemas de Información
	CG-19	SOFTWARE	Sistemas de Información
	CG-23	INFRAESTRUCTURA INSTITUCIONAL	Seguridad Interna y Externa
	CG-24	INFRAESTRUCTURA INSTITUCIONAL	Seguridad Interna y Externa
Sistemas de Información en Producción	CG-04	INFRAESTRUCTURA INSTITUCIONAL	Siniestro
	CG-07	INFORMACION	Sistemas de Información
	CG-11	HARDWARE	Sistemas de Información
	CG-13	SOFTWARE	Sistemas de Información
	CG-18	INFRAESTRUCTURA INSTITUCIONAL	Sistemas de Información

	CG-19	SOFTWARE	Sistemas de Información
	CG-23	INFRAESTRUCTURA INSTITUCIONAL	Seguridad Interna y Externa
	CG-24	INFRAESTRUCTURA INSTITUCIONAL	Seguridad Interna y Externa
Software Base (Sistemas Operativos y Ofimática)	CG-10	HARDWARE	Sistemas de Información
	CG-20	RECURSOS HUMANOS	Sistemas de Información
	CG-22	INFRAESTRUCTURA INSTITUCIONAL	Seguridad Interna y Externa
	CG-23	INFRAESTRUCTURA INSTITUCIONAL	Seguridad Interna y Externa
	CG-24	INFRAESTRUCTURA INSTITUCIONAL	Seguridad Interna y Externa
Software Antivirus para Servidores y Equipos de Cómputo	CG-08	EQUIPO	Siniestro
	CG-10	HARDWARE	Sistemas de Información
	CG-11	HARDWARE	Sistemas de Información
	CG-23	INFRAESTRUCTURA INSTITUCIONAL	Seguridad Interna y Externa
COMUNICACIONES			
Equipos de Conmutación LAN	CG-04	INFRAESTRUCTURA INSTITUCIONAL	Sistemas de Información
	CG-23	INFRAESTRUCTURA INSTITUCIONAL	Seguridad Interna y Externa
	CG-24	INFRAESTRUCTURA INSTITUCIONAL	Seguridad Interna y Externa
Equipos Router WAN	CG-04	COMUNICACIONES	Sistemas de Información
Equipo de Seguridad Cortafuego (Firewall)	CG-15	COMUNICACIONES	Sistemas de Información
SISTEMAS DE INFORMACION (SOFTWARE)			
Base de Datos usados por los Sistemas Software	CG-11	HARDWARE	Sistemas de Información
	CG-12	SOFTWARE	Sistemas de Información
	CG-13	SOFTWARE	Sistemas de Información
	CG-22	SOFTWARE	Sistemas de Información
Respaldo de Información	CG-11	SOFTWARE	Sistemas de Información

Generada con Software Base y Ofimática	CG-13	SOFTWARE	Sistemas de Información
Respaldo de los Sistemas Software	CG-11	SOFTWARE	Sistemas de Información
	CG-23	INFRAESTRUCTURA	Seguridad Interna y Externa
Respaldo de Base de Datos	CG-11	SOFTWARE	Sistemas de Información
	CG-13	SOFTWARE	Sistemas de Información
	CG-23	INFRAESTRUCTURA	Seguridad Interna y Externa
Respaldos de Información y Configuración de Servidores de Información	CG-11	SOFTWARE	Sistemas de Información
	CG-13	SOFTWARE	Sistemas de Información
EQUIPOS DE AUTONOMIA Y OTROS			
Sistema de Climatización de Precisión	CG-01	INFRAESTRUCTURA INSTITUCIONAL	Siniestros
	CG-24	INFRAESTRUCTURA INSTITUCIONAL	Seguridad Interna y Externa
Sistema de Alimentación Ininterrumpida (SAI/UPS)	CG-01	INFRAESTRUCTURA INSTITUCIONAL	Siniestros
	CG-24	INFRAESTRUCTURA INSTITUCIONAL	Seguridad Interna y Externa
Aire Acondicionado	CG-04	INFRAESTRUCTURA INSTITUCIONAL	Siniestros
Tablero General	CG-05	INFRAESTRUCTURA INSTITUCIONAL	Siniestros
INFRAESTRUCTURA FISICA			
Sede Central – GRU	CG-01	INFRAESTRUCTURA INSTITUCIONAL	Siniestros
	CG-02	INFRAESTRUCTURA INSTITUCIONAL	Siniestros
	CG-03	INFRAESTRUCTURA INSTITUCIONAL	Siniestros
	CG-04	INFRAESTRUCTURA INSTITUCIONAL	Siniestros
	CG-09	COMUNICACIONES	Sistemas de Información
	CG-24	INFRAESTRUCTURA INSTITUCIONAL	Seguridad Interna y Externa
	CG-01	INFRAESTRUCTURA INSTITUCIONAL	Siniestros

Sedes Descentralizadas-GRU	CG-02	INFRAESTRUCTURA INSTITUCIONAL	Siniestros
	CG-04	INFRAESTRUCTURA INSTITUCIONAL	Siniestros
	CG-09	COMUNICACIONES	Sistemas de Información
	CG-24	INFRAESTRUCTURA INSTITUCIONAL	Seguridad Interna y Externa
PROVEEDORES DE SERVICIOS			
Suministro de Energía Eléctrica	CG-04	PROVEEDORES DE SERVICIOS	Siniestros
Servicio de Telefonía Fija e Internet	CG-06	PROVEEDORES DE SERVICIOS	Siniestros
RECUROS HUMANOS			
Disponibilidad de Personal Directivo	CG-21	RECURSOS HUMANOS	Recursos Humanos
	CG-24	INFRAESTRUCTURA INSTITUCIONAL	Seguridad Interna y Externa
Disponibilidad de Personal Operativo	CG-20	RECURSOS HUMANOS	Recursos Humanos
	CG-24	INFRAESTRUCTURA INSTITUCIONAL	Seguridad Interna y Externa

Tabla N° 09: Elementos Vs. Contingencias

En adelante se procederá a desarrollar los Planes de Contingencia según el análisis previo descrito líneas arriba, y considerado además los eventos más críticos que requieren de una importante atención, pero sobre todo de una inmediata respuesta ante eventos de contingencia que pudieran afectar la operativa del Gobierno Regional de Ucayali.

6.10 Secuencia de Acción de Contingencias

Todos y cada uno de los eventos de contingencias, serán enfrentados en base a un conjunto de acciones de Mitigación, Emergencia y Recuperación

6.10.1 Contingencia: Eventos de Siniestros

Un evento de siniestro es aquella originada por el hombre en algunos casos, y en otros por la naturaleza, casi siempre imprevisible.

a) Objetivo

Determinar y validar en el Plan de Contingencia todos los eventos relacionados a siniestros que permita generar un conjunto de acciones destinadas a planificar, organizar, preparar, controlar y mitigar una emergencia que se presente en la Sede Central o en las Sedes Remotas de la entidad, con la finalidad de reducir al mínimo cualquier impacto negativo o perjudicial.

b) Cobertura

Todo evento de contingencia o emergencias que pudieran afectar, paralizar o dañar las instalaciones, el personal o los recursos de Tecnologías de la Información y Comunicaciones puede tener cobertura en toda la institución.

Así mismo es necesario saber que la ocurrencia de un siniestro que inhabilite total o parcialmente la operatividad del "Centro de Datos", es que se debe realizar las gestiones inmediatas con la Gerencia General del Gobierno Regional de Ucayali para determinar el uso de un ambiente alterno para la continuidad de las operaciones, hasta que se restablezca el funcionamiento normal.

Por otro lado, se considera necesario que, como parte del desarrollo de la contingencia por Siniestros, se debe incluir los elementos relativos a Proveedores de Servicios, por afectar o ser consecuencia de siniestros que pudieran presentarse:

La interrupción de Energía Eléctrica: al momento de restablecerse la energía eléctrica, puede generar cargas altas que pudieran ocasionar algún tipo de siniestros, afectando la seguridad física de la infraestructura y la de los equipos.

El siguiente cuadro muestra la Matriz de Riesgos, el mismo que define las contingencias del tipo siniestros.

Código del Formato	Descripción del Riesgo	Probabilidad de Ocurrencia	Impacto	Ponderación	Alerta
CONTINGENCIA: SINIESTROS					
INFRAESTRUCTURA INSTITUCIONAL					
CG-01	Incendio	0.04	3	0.16	3
CG-02	Sismo	0.10	3	0.30	3
CG-03	Inundación por lluvias torrenciales	0.02	2	0.04	2
PROVEEDORES DE SERVICIOS					
CG-04	Interrupción del suministro o fluido eléctrico	0.10	3	0.20	3
EQUIPO					
CG-05	Falla por recalentamiento del Tablero General	0.10	3	0.20	3

Tabla N° 10: Matriz de Riesgos-Contingencia Siniestros.

c) Plan de Pruebas.
El presente Plan de Pruebas se ejecutará en base a lo definido en la columna "Descripción del Riesgo" de la contingencia Siniestros. La ejecución del Plan de Pruebas se llevará a cabo, una vez el Líder o Administrador del Plan tengan la autorización de la Alta Dirección.

d) Descripción del Plan.
En adelante se desarrollarán los Planes de Contingencia de los eventos de mayor impacto identificados en la matriz de Riesgos de la Contingencia Siniestros.

EVENTO: INCENDIO	CODIGO DEL EVENTO	CG-01

1. PLAN DE MITIGACION

a) Descripción del Evento
Un incendio es una ocurrencia de fuego no controlada que puede abrasar algo que no está destinado a quemarse. Puede afectar a estructuras y a seres vivos. La exposición de los seres vivos a un incendio puede producir daños muy graves hasta la muerte, generalmente por inhalación de humo o por desvanecimiento producido por la intoxicación y posteriormente quemaduras graves. Se producen en materiales sólidos, líquidos combustibles inflamables, equipos e instalaciones bajo carga eléctrica entre otros. Este evento incluye los siguientes elementos mínimos identificados por el Gobierno Regional de Ucayali, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:
Infraestructura
Data Center de la Sede Central.
Centro de Comunicaciones de la Sede Apurímac.
Sede Central en su totalidad (provisto de material altamente inflamable).
Recursos Humanos
Personal debidamente entrenado para afrontar el evento

b) Objetivo
Establecer las acciones que se ejecutaran ante un incendio a fin de minimizar el tiempo de interrupción de las operaciones del Gobierno Regional de Ucayali, sin exponer la seguridad de las personas y la infraestructura tecnológica.

c) Criticidad
El Gobierno Regional de Ucayali, determina que el presente evento tiene un nivel de gran impacto en el servicio y se define como CRITICO.

d) Entorno
Este evento se puede presentar en cualquiera de las oficinas de la Sede Central, ya que su infraestructura antigua de madera y el deficiente sistema eléctrico hace más probable la ocurrencia de evento de este tipo.

e) Personal Encargado
El Gerente o Director del área, es el encargado de dar estricto cumplimiento a lo especificado en las condiciones de prevención de Riesgo del presente Plan.

f) Condiciones de Prevención de Riesgo
- Programar y ejecutar inspecciones periódicas.
- Realizar la renovación total de las conexiones eléctricas a fin de asegurar su mejor rendimiento y despliegue.
- Realizar charlas sobre el uso y manejo de extintores a todo el personal de la entidad.
- Responder a las recomendaciones de INDECI, en torno del evento.
- Disponer de una lista de contacto de emergencia que incluya a bomberos, hospitales, clínicas y del personal de la entidad responsable de las acciones de prevención y ejecución de la contingencia.
  Del mismo modo deberá contar con elementos para detección y extinción de un posible incendio, los cuales cubrirán el ambiente del DATA CENTER y de la Oficina de Tecnologías de la Información.
- Implementar detectores de humo y sistema de extinción en el DATA CENTER.
- Mantener actualizado los extintores de las diferentes Oficinas y verificar que el extintor del Data Center contenga la fórmula adecuada para equipos electrónicos.

2.PLAN DE EMERGENCIA

a) Eventos que activan la contingencia
La contingencia se activará al ocurrir el incendio.
El proceso de contingencia se activará inmediatamente después de ocurrir el evento.

b) Procesos relacionados antes del evento.
- Identificar las ubicaciones de los extintores.
- Conocer el número de emergencia de la Compañía General de Bomberos.
- Conocer los números telefónicos del personal de la Oficina de Tecnologías de la Información.
- Conocer el número de teléfono de los bomberos.

c) Personal que autoriza la contingencia
Cada responsable de área o empleado que identifique algún indicio de incendio cercano, pueden activar la contingencia.

d) Descripción de las actividades después de activar la contingencia
- Tratar de apagar el incendio con extintores o cualquier mecanismo para tal fin.
- Evacuar el área.

Luego de extinguido el incendio, se deberá realizar las siguientes actividades:
- Evaluación de daños ocasionados al personal, bienes, equipos e instalaciones.
- En caso de daños a la salud física del personal, prestar atención medica inmediata.
- Realizar un inventario general de la documentación, personal, equipos y demás recursos afectados, indicando su estado.

- De encontrarse bienes afectados como consecuencia del evento, se evaluará para determinar la reposición o restauración parcial o total según sea el caso.

El líder del Plan de Contingencias deberá coordinar con la Alta Dirección del GRU, la posibilidad de instalar ambientes provisionales para aquellas áreas que fueron afectadas por el evento.

e) Duración

La duración de la contingencia dependerá del tiempo que demande controlar el incendio.

3.PLAN DE RECUPERACIÓN

a) Personal Encargado

El personal encargado del Plan de Recuperación es la Gerencia Regional de Administración y el equipo de Tecnologías de información, cuyo rol principal es asegurar el normal desarrollo de las operaciones dentro de la entidad.

b) Descripción

El plan de recuperación estará orientado a recuperar en el menor tiempo posible las actividades afectadas durante la interrupción del servicio, esto dependiendo de la magnitud del siniestro.

c) Mecanismos de Comprobación

El responsable del área afectada presentará un informe al Líder del Plan de Contingencia explicando que parte de las actividades u operaciones han sido afectadas y cuáles son las acciones o sugerencias inmediatas a realizar.

d) Mecanismos de Recuperación

Deberá ejecutarse de acuerdo a lo definido en el punto a) y siguiendo el Plan de Recuperación descrita el numeral 6.8 del presente documento.

e) Desactivación del Plan de Contingencia

El administrador del Plan de Contingencia desactivará el Plan una vez que se hayan tomado las acciones descritas en la Descripción del Plan de Recuperación, mediante una comunicación al Líder del Plan.

f) Proceso de Actualización

El proceso de actualización será en base al informe presentado por el Administrador del Plan luego de lo cual se determinará las acciones a tomar.

Tabla 11: Plan de Contingencia-Evento Incendio

EVENTO: SISMO	CODIGO DEL EVENTO	CG-02

1.PLAN DE MITIGACION

a) Descripción del Evento

Serie de vibraciones de la superficie terrestre generadas por un movimiento brusco y repentino de las capas internas (corteza y manto).

Este evento incluye los siguientes elementos mínimos identificados por el GRU, los mismos que por la naturaleza de su impacto a causa de la contingencia, se representan de la siguiente manera:

Infraestructura

Sede Central del GRU

Sedes Descentralizadas del GRU.

Recursos Humanos

Totalidad del Personal activo.

b) Objetivo
Establecer las acciones que se ejecutarán ante un sismo a fin de minimizar el tiempo de interrupción de las operaciones de la entidad sin exponer la seguridad de los empleados.

c) Criticidad
El Gobierno Regional de Ucayali determina que el presente evento tiene un nivel de gran impacto en el servicio y se define como CRITICO.

d) Entorno
Este evento se puede presentar en las diferentes en la Sede Central y todas las Sedes Externas que dependen de la Entidad.

e) Personal Encargado
El responsable de área, es el encargado de dar estricto cumplimiento a lo especificado en las coordinaciones de prevención de Riesgo del presente Plan.

f) Condiciones de Prevención de Riesgo
- Disponer de un Plan de evacuación de las instalaciones del Gobierno Regional de Ucayali, el mismo que debe ser de conocimiento de todo el personal que labora en la entidad.
- Coordinar con la Oficina de Defensa Nacional, Seguridad Ciudadana y Defensa Civil la programación de simulacros de evacuación con la participación masiva del personal institucional al menos 2 veces por trimestre.
- Mantener las salidas libres de obstáculos.
- Señalizar adecuadamente las zonas seguras y de evacuación.
- Determinar las zonas de concentración segura cuando existan evacuación.

2.PLAN DE EMERGENCIA

a) Eventos que activan la contingencia
El proceso de contingencia se activará inmediatamente después de ocurrir el evento.

b) Procesos relacionados antes del evento
- Disponer la relación de todos los empleados por áreas de la entidad.
- Sugerir a la Gerencia Regional de Administración para que, en coordinación con la Oficina de Defensa Nacional, Seguridad Ciudadana y Defensa Civil, realice inspecciones diarias de seguridad interna.
- Realizar inspecciones trimestrales de seguridad externa.
- Programar los simulacros en horarios que no afecten las actividades regulares del personal institucional.

c) Personal que autoriza la contingencia
Cualquier empleado en sano juicio, puede activar la contingencia.

d) Descripción de las actividades después de activar la contingencia.
- Desconectar el fluido eléctrico y cerrar las llaves de repositorios que contengan elementos inflamables.
- Evacuar las oficinas de acuerdo a las disposiciones del personal de Defensa Civil o el que haga de sus veces, utilizando las rutas establecidas durante los simulacros. El personal empleado de la entidad deber considerar la señalización de ruta, zonas seguras entre otros.

- Verificar que todo el personal institucional se encuentre físicamente bien.
- Brindar los primeros auxilios al personal afectado de ser el caso.
- Alejarse de las ventanas de vidrio para evitar sufrir cualquier corte por desprendimientos imprevistos.
- Evaluar los daños ocasionados por el sismo sobre las instalaciones físicas, ambientes de trabajo, instalaciones eléctricas, equipos, archivos, etc.
- Realizar un inventario general de la documentación, personal, equipos y demás recursos afectados, indicando su estado de operatividad.

El líder del Plan de Contingencias deberá coordinar con la Alta Dirección de la entidad, la disposición de ambientes provisionales para aquellas áreas que fueron afectadas por el evento.

e) Duración

La evacuación del personal institucional se realizará bajo estricta calma con un máximo de 5 minutos de duración.

La duración de la contingencia dependerá del grado de intensidad y de daños ocasionados.

3.PLAN DE RECUPERACION

a) Personal Encargado

El personal encargado del Plan de Recuperación es el Área y el equipo del área afectada, cuyo rol principal es asegurar el normal desarrollo de las operaciones del Gobierno Regional de Ucayali.

b) Descripción

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

c) Mecanismos de Comprobación.

El Gerente o jefe del área afectada presentará un informe al Líder del Plan de Contingencia explicando qué parte de las actividades u operaciones ha sido afectadas y cuáles son las acciones tomadas.

d) Mecanismos de Recuperación

Deberá ejecutarse de acuerdo al Plan de Recuperación descrita el numeral 6.8 del presente documento.

e) Desactivación del Plan de Contingencia

El Administrador del Plan de Contingencia desactivará el Plan una vez que se hayan tomado las acciones descritas en la Descripción del Plan de Recuperación, mediante una comunicación al Líder del Plan.

f) Proceso de Actualización

El proceso de actualización será en base al informe presentado por el Administrador del Plan luego del cual determinará las accions a seguir.

Tabla N° 12: Plan de Contingencia-Evento Sismo.

INUNDACION POR LLUVIAS TORRENCIALES	CODIGO DEL EVENTO:	CG-03
1.PLAN DE MITIGACION		
a) Descripción de Evento		

Las lluvias torrenciales son fenómenos atmosféricos producidos por la condensación de las nubes. Consiste en la precipitación de gotas de agua líquida o sobre enfriada, cuyo diámetro es mayor a los 0.5 milímetros.
Este evento incluye los siguientes elementos mínimos identificados por el GRU, los mismos que por su naturaleza de impacto a causa de la contingencia, se representan de la siguiente manera:
Infraestructura
Sede Central del GRU.
Algunas Sedes Descentralizadas del GRU.
Operativo
Archivos y documentos corporativa.
Equipos Diversos
Data Center, Equipos de cómputo, de Impresión, Aire Acondicionado, etc.

b) Objetivo
Establecer acciones ante una inundación con el objetivo de minimizar el tiempo de interrupción de la operativa de la entidad sin exponer la seguridad de los empleados institucionales.

c) Criticidad
El Gobierno Regional de Ucayali define que el presente evento tiene un nivel de gran impacto en el servicio y se identifica como CRITICO.

d) Entorno
Este evento se puede presentar en las diferentes oficinas de la sede central y en sus Sedes Externas.

e) Personal Encargado
El responsable de área, es el encargado de dar estricto cumplimiento a lo especificado en las condiciones de prevención de Riesgo del presente Plan.

f) Condiciones de Prevención de Riesgo
- Planificar acciones ante los pronósticos de tiempo que oficializa el Servicio Nacional de Meteorología e Hidrología del Perú SENAMHI.
- Realizar con periodicidad bimensual la verificación de la infraestructura (techo, cielo raso, paredes, pisos) a fin de identificar posibles filtraciones hacia el interior de las oficinas.
- Asegurar que los equipos electrónicos como equipos de cómputo, impresoras, scanner, UPS y demás similares se encuentran fuera del alcance de la inundación.

2.PLAN DE EMERGENCIA

a) Eventos que activan la contingencia
Este evento se activa cuando la lluvia es intensa y supera los 5 minutos después de iniciado el mismo.
El proceso de contingencia se activará inmediatamente después de ocurrir el evento.

b) Procesos relacionados antes del evento
Todo proceso relacionado con la operativa normal del Gobierno Regional de Ucayali.

c) Personal que autoriza la contingencia
El responsable que autoriza la contingencia es el Administrador del Plan.

d) Descripción de las actividades después de activar la contingencia

- Realizar el Correcto apagado del Centro de Datos de la entidad de acuerdo a lo indicado en el Anexo N° 04 del presente documento.
- Desconectar el fluido eléctrico y bajar todas las llaves mecánicas y termo magnéticas instaladas en las diferentes oficinas de la entidad.
- Verificar permanentemente el despliegue del agua a su paso por la Sede Central y las sedes externas.
- Evaluación de los daños ocasionados por la inundación sobre las instalaciones físicas, ambientes de trabajo, instalaciones eléctricas, archivos de documentos, etc.
- Realizar un inventario general de la documentación, personal, equipos y demás recursos afectados, indicando su estado de operatividad.

El Líder del Plan de Contingencias deberá coordinar con la Alta Dirección de la entidad, la disposición de ambientes provisionales para aquellas áreas que fueron afectadas por el evento.

e) Duración
La duración de la contingencia dependerá del grado de intensidad y de daños ocasionados.

3.PLAN DE RECUPERACION

a) Personal Encargado
El personal encargado del Plan de Recuperación es el Área y el equipo del área afectada, cuyo rol principal es asegurar el estado de su entorno de trabajo para poder continuar con el normal desarrollo de sus actividades.

b) Descripción
El plan de recuperación estará orientado a recuperar en el menor tiempo posible las actividades afectadas durante la interrupción del servicio.

c) Mecanismos de Comprobación
El responsable del área afectada presentará un informe al Administrador del Plan explicando qué parte de las actividades u operaciones ha sido afectada y cuáles son las acciones tomadas.

d) Mecanismos de Recuperación
Deberá ejecutarse de acuerdo al Plan de Recuperación descrita el numeral 6.8 del presente documento.

e) Desactivación del Plan de Contingencia
El Administrador del Plan de Contingencia desactivará el Plan una vez que se hayan tomado las acciones descritas en la Descripción del Plan Recuperación, mediante una comunicación al Líder del Plan.

f) Proceso de Actualización
El proceso de actualización será en base al informe presentado por el Administrador del Plan luego de lo cual se determinará las acciones a tomar.

Tabla N° 13: Plan de Contingencia-Evento Inundación por Lluvias Torrenciales.

ITERRUPCION DEL SUMINISTRO O FLUIDO ELECTRICO	CODIGO DE EVENTO	CG-04
1.PLAN DE MITIGACION		
a) Descripción del Evento		

Falla general del suministro de energía eléctrica. Este evento incluye los siguientes elementos mínimos identificados por el GRU, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de contingencia:

Proveedores de Servicios

Suministro de energía eléctrica.

Hardware

Servidores y Equipos de Cómputo.

Equipos

Sistema de Protección Ininterrumpida UPS.

b) Objetivo

Restablecer las operaciones consideradas como críticas para el servicio.

c) Criticidad

El GRU define el presente evento como de gran impacto en el servicio e identifica como CRITICO.

d) Entorno

Este evento se puede presentar en las diferentes oficinas de la Sede Central y en las Sedes Externas de la Entidad, afectando el normal funcionamiento de los principales servicios.

e) Personal Encargado

El responsable del área, es el encargado de dar estricto cumplimiento a lo especificado en las condiciones de prevención de Riesgo del presente Plan.

f) Condiciones de Prevención de Riesgo

- Las actividades diarias que realiza el Gobierno Regional de Ucayali, pondrán en funcionamiento continuo los UPS de los equipos de cómputo en las áreas consideradas como críticas.
- Realizar periódicamente el mantenimiento de los UPS para asegurar la autonomía de energía eléctrica de las estaciones de trabajo con un máximo de 10 minutos.
- Realizar el mantenimiento periódico del Sistema de Alimentación Ininterrumpida SAI/UPS, para garantizar la autonomía eléctrica de los Servidores Centrales, el tiempo de autonomía no debe ser menor a 30 minutos.
- Implementar con equipos de luces de emergencia con tolerancia no menor a 15 minutos, en los ambientes considerados como críticos.

2.PLAN DE EMERGENCIA

a) Eventos que activan la contingencia

La interrupción del suministro de energía eléctrica en los ambientes del Gobierno Regional de Ucayali (Sede Central y sus Sedes Externas).

b) Procesos relacionados antes del evento

Toda acción relacionada a la operativa y funcionalidad normal del Gobierno Regional de Ucayali.

c) Personal que autoriza la contingencia

El responsable que autoriza la contingencia es el Administrador del Plan.

d) Descripción de las actividades después de activar la contingencia

- Informar al Gerente Regional de Administración y al Director de la Oficina de Tecnologías de la Información.

- Aquellos equipos de cómputo que operan con dispositivos UPS, deberán ser verificados por el propio usuario para controlar su tiempo de autonomía, a fin de evitar un apagado brusco del equipo de computo
- En caso la interrupción de energía sea mayor a 10 minutos, se procederá a apagar los servidores de datos y demás equipos críticos siguiendo las instrucciones del Anexo 04, hasta que el fluido eléctrico sea restablecido en su totalidad.

e) Duración
El tiempo máximo de la interrupción del suministro fluido eléctrico dependerá de la situación que dio origen a dicho evento, pudiendo ser atribuido a posibles agentes externos.

3.PLAN DE RECUPERACION

a) Personal Encargado
El personal encargado del Plan de Recuperación es el Director de la Oficina de Tecnologías de la Información y el Gerente Regional de Administración del Gobierno Regional de Ucayali.

b) Descripción
Se procederá a informar al Líder del Plan sobre el evento presentado y que procedimiento se llevará a cabo para su atención.

c) Mecanismos de Comprobación
El responsable del área afectada presentará un informe al Administrador del Plan de Contingencia detallando que equipo y actividades han sido afectados y cuáles son las acciones correctivas a seguir.

d) Mecanismos de Recuperación
Deberá ejecutarse de acuerdo al Plan de Recuperación descrita el numeral 6.8 del presente documento.

e) Desactivación del Plan de Contingencia
El Gerente Regional de Administración o el Director de la Oficina de Tecnologías de la Información podrán desactivar el Plan una vez se recuperen las funcionalidades básicas de trabajo con los sistemas software o cualquier otro componente que amerite el reinicio de las operaciones normales de la entidad.

f) Proceso de Actualización
El proceso de actualización será en base al informe presentado por el Administrador del Plan luego del cual podrá determinar las acciones a seguir.

Tabla N° 14: Plan de Contingencia-Evento Interrupción del Suministro o Fluido Eléctrico.

FALLA POR RECALENTAMIENTO DEL TABLERO ELECTRICO GENERAL	CODIGO DEL EVENTO	CG-05

1.PLAN DE MITIGACION

a) Descripción del Evento
El Tablero Eléctrico General es la parte principal de la instalación eléctrica, en el mismo se encuentran todos los dispositivos de seguridad y maniobra de los circuitos eléctricos de la instalación. Consiste en una caja donde se montan los interruptores automáticos respectivos, cortacircuitos y fusibles,

y el medidor de consumo. Este evento incluye los siguientes elementos mínimos identificados por el GRU, los mismos que por naturaleza pueden ser considerados como parte afectada o causa de contingencia:

Proveedores de Servicios

Suministro de energía eléctrica

Hardware

Servidores y Equipos de Cómputo

Equipos

Sistema de Protección Ininterrumpida UPS

b) Objetivo

Restablecer las operaciones consideradas como críticas para el servicio.

c) Criticidad

El GRU define el presente evento teniendo en cuenta que es de gran impacto en el servicio y se identifica como CRITICO.

d) Entorno

Este evento solo se puede presentar en la Sede Central y en la Sede Apurímac de la Entidad, el mismo que pudiera afectar el normal funcionamiento de los principales servicios.

e) Personal Encargado

El responsable será el personal electricista o quien haga sus veces de dar estricto cumplimiento a lo especificado en las condiciones de prevención de Riesgo del presente Plan.

f) Condiciones de Prevención de Riesgo

- Las actividades diarias que realiza el Gobierno Regional de Ucayali, pondrán en funcionamiento continuo del UPS de los de cómputo en las áreas consideradas como críticas.
- Realizar periódicamente al menos 1 vez al mes el mantenimiento preventivo/correctivo del Tablero para asegurar la integridad de operatividad y performance.
- Sugerir si el caso amerita y teniendo en cuenta la cantidad de equipos electrónicos que hoy consumen el servicio eléctrico dentro de la Sede Central, la renovación de dicho Tablero acompañado del Sistema Eléctrico en su totalidad debe ser prioridad.

2.PLAN DE EMERGENCIA

a) Eventos que activan la contingencia

Falla del Tablero Eléctrico por una sobrecarga de tensión, con consecuente de inminente corto circuito.

b) Procesos relacionados antes del evento

Toda acción relacionada a la operativa y funcionalidad normal del Gobierno Regional de Ucayali.

c) Personal que autoriza la contingencia

El responsable que autoriza la contingencia es el personal Eléctrico cuya tarea tiene asignado la correcta operación del Tablero.

d) Descripción de las actividades después de activar la contingencia

- Informar al Gerente Regional de Administración.
- Aquellos equipos de cómputo que operan con dispositivos UPS, deberán ser verificados por el propio usuario para controlar su tiempo

de autonomía, a fin de evitar un apagado brusco del equipo de cómputo. • En caso la interrupción de energía producto de la falla en el Tablero supere los 10 minutos, por seguridad física y lógica se procederá a apagar los servidores de datos y demás equipos críticos siguiendo las instrucciones del Anexo 04 hasta que la operatividad del Tablero sea restablecida en su totalidad. e) Duración El tiempo máximo del evento, dependerá del tiempo que dure su composición.
3.PLAN DE RECUPERACION a) Personal Encargado El personal encargado del Plan de Recuperación es el Gerente Regional de Administración (Líder del Plan) del Gobierno Regional de Ucayali. b) Descripción Se procederá a informar al Líder del Plan sobre el evento presentado y que procedimiento se llevará a cabo para su atención. c) Mecanismos de Comprobación En caso de comprobar la existencia de alguna falla en algunas de las áreas, producto de la anomalía en el Tablero, el responsable del área afectada informará al Gerente Regional de Administración para coordinar que acciones correctivas serán ejecutadas. d) Mecanismos de Recuperación Deberá ejecutarse de acuerdo al Plan de Recuperación descrita el numeral 6.8 del presente documento. e) Desactivación del Plan de Contingencia El Gerente Regional de Administración podrá desactivar el Plan, una vez que se recuperen la operatividad funcional del Tablero, procediendo al reinicio de las operaciones normales de la entidad. f) Proceso de Actualización El proceso de actualización será en base al informe presentado por el Administrador del Plan luego del cual podrá determinar las acciones a seguir.

Tabla N° 15: Plan de Contingencia-Evento Falla por Recalentamiento del Tablero Eléctrico General.

6.10.2 Contingencia: Evento de Sistemas de Información

Se puede definir como el conjunto de procesos, procedimientos, recursos físicos, técnicos y humanos que interactúan ante la presencia de un siniestro, teniendo como finalidad garantizar la continuidad de las operaciones automatizadas para reducir su nivel de impacto.

a) Objetivo.

Proveer una solución para mantener operativo los sistemas de información principales de la institución, que permitan reducir el impacto en las operaciones normales cuando son interrumpido o paralizados por contingencias que afectan parcial o totalmente las

instalaciones donde se procesan las aplicaciones automatizadas y los servicios de procesamiento de datos.

b) Cobertura.

El desarrollo del Plan de Contingencia sobre el evento de sistemas de información del GRU, está relacionada con el impacto potencial que provoca la interrupción de los servicios de procesamiento informático, que afecta el normal desarrollo de las actividades y procesos institucionales, tales como:

- Disponibilidad de los servicios de sistemas de Información (SIAF MEF. SIGA MEF, SISGEDO, SIGA PLANILLA, SISMORE, AGENDA VIRTUAL, etc.)
- Desarrollo de actividades mediante el Internet.

Así mismo, se consideran los riesgos y soluciones del ambiente físico, relacionados con la operación de los procesos principales del Centro de Datos (Data Center) de la entidad.

A continuación, se presenta la Matriz de Riesgos, tomando en cuenta las contingencias que mayor atención deben tener, para evitar o mitigar impactos severos.

Código del Evento	Descripción del Riesgo	Probabilidad de Ocurrencia	Impacto	Ponderación	Alerta
CONTINGENCIA: SISTEMAS DE INFORMACION					
INFORMACION					
CG-07	Robo o Pérdida de Archivos	0.03	3	0.06	3
SOFTWARE					
CG-12	Fallas en los Sistemas Base y de Información	0.05	3	0.20	3
CG-13	Falla en el Motor de Base de Datos.	0.04	3	0.16	3
CG-19	Acción de Código Malicioso	0.05	3	0.20	3
COMUNICACIONES					
CG-16	Falla en el Sistema de Red de Datos Local LAN	0.04	3	0.16	3
HARDWARE					
CG-11	Falla en los Equipos Servidores de Información	0.04	3	0.20	3

Tabla N°16: Matriz Riesgos-Contingencia Sistemas de Información

c) Plan de Pruebas

El presente Plan de Pruebas se ejecutará en base a lo definido en la columna "Descripción del Riesgo" de la contingencia Sistemas de Información.

La ejecución del Plan de Pruebas se llevará a cabo, una vez el Líder o Administrador del Plan tengan la autorización de la Alta Dirección.

La simulación del Plan de Pruebas ejecutará de manera trimestral.

d) Descripción del Plan

A continuación, se detallan los Planes de contingencia definidos en la Matriz de Riesgos de contingencia de Sistemas de Información.

ROBO O PERDIDA DE ARCHIVOS	CODIGO DEL EVENTO	CG-07

1. PLAN DE MITIGACION

a) Descripción del Evento

A medida que los datos se almacenan o se propagan por una gran cantidad de aplicación y dispositivos, la capacidad de ejecutar políticas de seguridad y cumplimiento de forma coherente se vuelve aún más crítica. En ese sentido el robo o pérdida de archivos genera mayor impacto en las organizaciones.

Software

Acción de Código Malicioso.

Hardware

Servidores y Equipos de Cómputo, Firewall.

Infraestructura Institucional

Intrusión, Accesos No Autorizados.

b) Objetivo

Aplicar los mecanismos necesarios para proteger de accesos no autorizados a los equipos y sistemas corporativos.

c) Criticidad

El GRU define el presente evento teniendo en cuenta que es de gran impacto en el servicio y se identifica como CRITICO.

d) Entorno

En la Sede Central y en las demás sedes de la Entidad.

e) Personal Encargado

Todo usuario de dominio o de equipo de cómputo, será responsable de poner a buen recaudo sus cuentas de acceso a su equipo y a los sistemas a donde tiene permisos, con la finalidad de no entorpecer la integridad y confidencialidad de la información institucional.

f) Condiciones de Prevención de Riesgo

- Mediante software, se deberán configurar los equipos para que sus unidades de lectura externa como (CD, DVD, USB, etc.) se encuentren deshabilitadas, siendo habilitadas las estrictamente necesarias a través de una autorización expresa del Director de área.

- Evitar que los usuarios de equipos de cómputo, dejen la sesión abierta de su equipo, ya que personas no autorizadas e inescrupulosas podrían acceder a copiar, alterar o eliminar información institucional.
- Mantener actualizado los certificados del Firewall (cortafuegos) de la Sede Central y la Sede Apurímac, a fin de evitar o reducir el número de colaciones e intrusiones desde el exterior a través de internet.
- Verificar el funcionamiento del UPS del equipo de cómputo, para evitar el apagado repentino ante un corte de fluido eléctrico.
- En caso del Centro de Datos realizar los mantenimientos oportunos del Sistema de Alimentación Ininterrumpida (SAI/UPS).

2.PLAN DE EMERGENCIA

a) Eventos que activan la contingencia
Falla del Tablero Eléctrico por una sobrecarga de tensión, con consecuente de inminente corto circuito.
Alteración o pérdida de los archivos de los equipos de cómputo y/o servidores.

b) Procesos relacionados antes del evento
Toda acción relacionada a la operativa y funcionalidad normal del Gobierno Regional de Ucayali.

c) Personal que autoriza la contingencia
El responsable que autoriza la contingencia es el personal Eléctrico cuya tarea tiene asignado la correcta operación del Tablero.

d) Descripción de las actividades después de activar la contingencia
- Informar al Gerente Regional de Administración.
- Aquellos equipos de cómputo que operan con dispositivos UPS, deberán ser verificados por el propio usuario para controlar su tiempo de autonomía, a fin de evitar un apagado brusco del equipo de cómputo.
- En caso la interrupción de energía producto de la falla en el Tablero supere los 5 minutos, por seguridad física y lógica se procederá a apagar los servidores de datos y demás equipos críticos hasta que la operatividad del Tablero sea restablecida en su totalidad.
- Si en caso exista alteración de los archivos, inmediatamente proceder con el análisis de antivirus que cuenta la entidad y mediante software la recuperación de los archivos.

e) Duración
El tiempo máximo del evento, dependerá del tiempo que dure su composición.

3.PLAN DE RECUPERCION

a) Personal Encargado
El personal encargado del Plan de Recuperación es el Gerente Regional de Administración (Líder del Plan) del Gobierno Regional de Ucayali.

b) Descripción
Se procederá a informar al Líder del Plan sobre el evento presentado y que procedimiento se llevará a cabo para su atención.

c) Mecanismos de Comprobación

En caso de comprobar la existencia de alguna falla en algunas de las áreas, producto de la anomalía en el Tablero, el responsable del área afectada informará al Gerente Regional de Administración para coordinar que acciones correctivas serán ejecutadas.

d) Mecanismos de Recuperación
Deberá ejecutarse de acuerdo al Plan de Recuperación descrita el numeral 6.8 del presente documento.

e) Desactivación del Plan de Contingencia
El Gerente Regional de Administración podrá desactivar el Plan, una vez que se recuperen la operatividad funcional del Tablero, procediendo al reinicio de las operaciones normales de la entidad.

f) Proceso de Actualización
El proceso de actualización será en base al informe presentado por el Administrador del Plan luego del cual podrá determinar las acciones a seguir.

Tabla N° 17: Plan de Contingencia-Evento Robo o Pérdida de Archivos.

FALLA EN LOS SISTEMAS BASE Y DE INFORMACION	CODIGO DEL EVENTO	CG-12

1.PLAN DE MITIGACION

a) Descripción del Evento
El Sistema Base y de Información es la plataforma que soporta, administra y controla las principales funcionalidades lógicas del Hardware de Servidores y de los equipos que operan los usuarios del dominio institucional.
Software
Acción de Código Malicioso, Falla en los sistemas base de información.
Hardware
Servidores y Equipos de Cómputo.
Infraestructura Institucional
Intrusión, Accesos No Autorizados.

b) Objetivo
Mantener la continuidad de las operaciones principales de nivel lógico que soportan los servidores y equipos de cómputo en la entidad.

c) Criticidad
El GRU define el presente evento teniendo en cuenta que es de gran impacto en el servicio y se identifica como CRITICO.

d) Entorno
En la Sede Central y en las demás sedes de la Entidad.

e) Personal Encargado
Director de la Oficina de Tecnologías de la Información y usuarios del dominio institucional, se encargarán de prever el normal funcionamiento y operación de los elementos base del hardware informático.

f) Condiciones de Prevención de Riesgo
- Realizar el mantenimiento preventivo y correctivo de forma periódica, el mismo que debe estimarse en razón de una (1) vez cada 6 meses.
- Entrenar a los usuarios del dominio a realizar el control y lectura básica de la operatividad funcional de sus sistemas base (sistema operativo).

2.PLAN DE EMERGENCIA

a) Eventos que activan la contingencia

Anomalías imprevistas en el Sistema Operativo de Servidor o Equipo terminal. b) Procesos relacionados antes del evento Acción proactiva para medir operación normal de los sistemas base en servidores y equipos terminales. c) Personal que autoriza la contingencia El responsable que autoriza la contingencia es el personal de la Oficina de Tecnologías de la Información, y cada usuario que detecte alguna anomalía en su sistema base (sistema operativo). d) Descripción de las actividades después de activar la contingencia • Informar vía medio electrónico al Gerente Regional de Administración, del evento acontecido. • Ejecutar la acción correctiva en el acto del evento presentado. e) Duración El tiempo máximo del evento, dependerá de la gravedad de los daños o anomalías producidas.
3.PLAN DE RECUPERACION a) Personal Encargado El personal encargado del Plan de Recuperación estará a cargo del Personal de Tecnologías de la Información. b) Descripción Se procederá a informar al Líder del Plan sobre el evento presentado y que procedimiento se llevará a cabo para su atención. c) Mecanismos de Comprobación Se desarrollará el formato de Ocurrencia de Eventos para luego remitirlo al Líder del Plan. d) Mecanismos de Recuperación Deberá ejecutarse de acuerdo al Plan de Recuperación descrita el numeral 6.8 del presente documento. e) Desactivación del Plan de Contingencia El Director de la Oficina de Tecnologías de la Información podrá desactivar el Plan, una vez que se restablezca la operatividad funcional del Sistema Base, procediendo al reinicio de las operaciones normales de la entidad. f) Proceso de Actualización El proceso de actualización será en base al informe presentado por el Director de la Oficina de Tecnologías de la Información luego del cual podrá determinar las acciones a seguir.

Tabla N° 18: Plan de Contingencia-Evento Falla en los Sistemas Base o de Información

FALLA EN EL MOTOR DE BASE DE DATOS	CODIGO DEL EVENTO	CG-13
1.PLAN DE MITIGACION		
a) Descripción del Evento Considerado uno de los servicios más importantes por cualquier organización, ya que realiza varias tareas criticas como registro,		

procesamiento, almacenamiento y recuperación de datos para gestión y toma de decisiones institucional.

Este evento incluye algunos elementos identificados por el Gobierno Regional de Ucayali, los mismos puedes ser considerados o sufrir alguna alteración por cauda aparente de contingencia, estos elementos son los siguientes.

Hardware

Servidores y Equipos de Cómputo.

Software

Motor de Base de Datos.

Información

Respaldo de Bases de Datos y Software Base.

b) Objetivo

Mantener la continuidad de los procesos de registro, almacenamiento y recuperación de los datos e información institucional.

c) Criticidad

El Gobierno Regional de Ucayali define el presente evento teniendo en cuenta que es de gran impacto en el servicio y se identifica como CRITICO.

d) Entorno

El servicio se administra desde el Centro de Datos del Gobierno Regional de Ucayali.

e) Personal Encargado

El responsable será el Administrador de Base de Datos, quien se encargará de gestionar, controlar y mantener el normal funcionamiento del servicio del Motor de Base de Datos institucional.

f) Condiciones de Prevención de Riesgo

- Realizar la revisión periódica de los logs de la Base de Datos, a fin de evitar posibles anomalías en la funcionalidad del motor de Base de Datos.
- Con las copias de seguridad, se debe asegurar la integridad de la información ante posibles contingencias. Las copias de respaldo se harán en base a requerimientos, antes o después de ejecutar un proceso.
- Mantener actualizado las funciones necesarias del Motor de Base de Datos.

2.PLAN DE EMERGENCIA

a) Eventos que activan la contingencia

- Fallas en el Sistema de Cableado Estructurado dentro de la LAN.
- Fallas o funciones anómalas en el Servidor de Base de Datos.
- Interrupción del servicio que impide el acceso normal a los sistemas software de la entidad.
- Acceso no autorizado a uno de los servicios del Motor de Base de Datos.

b) Procesos relacionados antes del evento

Activar el equipamiento redundante para garantizar la continuidad del servicio de base de datos.

c) Personal que autoriza la contingencia

El responsable que autoriza la contingencia es el Director de la Oficina de Tecnologías de la Información. d) Descripción de las actividades después de activar la contingencia • El Director de la Oficina de Tecnologías de la Información, delegará o coordinará el procedimiento correctivo para restablecer el o los servicios del Motor de Base de Datos. e) Duración La duración de la contingencia no debe ser mayor a 2 horas después de activado la contingencia.
3.PLAN DE RECUPERACION a) Personal Encargado El Director de la Oficina de Tecnologías de la Información del Gobierno Regional de Ucayali, es el responsable del Plan de Recuperación, el mismo que se encargará de comunicar y ordenar oficialmente el restablecimiento para usar normalmente cada uno de los sistemas de software integrados al Servidor de Bases de Datos de la entidad. b) Descripción • Se hará de conocimiento a Secretaría General con copia a la Gerencia General, la causa que generó la interrupción del servicio. • Seguidamente se tomarán las medidas preventivas del caso y se revisará el Plan de Contingencias. • Finalmente se enviará una alerta remota a todas las estaciones de trabajo indicando que pueden usar sus aplicaciones o sistemas con normalidad. c) Mecanismos de Comprobación Se completará el formato de ocurrencia de eventos y se remitirá al Líder del Plan de Contingencia. d) Mecanismos de Recuperación Deberá ejecutarse de acuerdo al Plan de Recuperación descrita el numeral 6.8 del presente documento. e) Desactivación del Plan de Contingencia El director de la Oficina de Tecnologías de la Información será el responsable de comunicar y desactivar el presente plan una vez recuperado totalmente la funcionalidad de la Base de Datos. f) Proceso de Actualización Todo procedimiento que haya provocado alguna contingencia será incluido en el Plan de Contingencias para prevenir eventos imprevistos.

Tabla N° 19: Plan de Contingencias-Evento Falla en el Motor de Base de Datos.

ACCION DE CODIGO MALICIOSO	CODIGO DEL EVENTO	CG-19
1.PLAN DE MITIGACION		
a) Descripción del Evento Los Códigos Maliciosos en sus diferentes variantes, tienen por objeto violar y/o alterar el normal funcionamiento de los sistemas hardware y software. Habitualmente reemplazan archivos ejecutables por otros infectados con el		

código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.

Este evento incluye algunos elementos identificados por el Gobierno Regional de Ucayali, los mismos que pueden ser considerables a sufrir algún cambio imprevisto o no autorizado, estos elementos son los siguientes:

Hardware

Servidores y Equipos de Cómputo.

Software

Software Base y Sistemas Software implantados en la entidad.

b) Objetivo

Restablecer las operaciones de los equipos y sistemas después de ejecutar los procedimientos necesarios para depurar e interrumpir cualquier ataque que vulnere la funcionalidad normal de los equipos y sistemas.

c) Criticidad

El Gobierno Regional de Ucayali define el presente evento teniendo en cuenta que es de gran impacto en el servicio y se identifica como CRITICO.

d) Entorno

Los Servidores de Datos y Equipos de Cómputo que se encuentran en la Sede Central y los equipos de cómputo que se encuentra en las sedes descentralizadas.

e) Personal Encargado

El Director de la Oficina de Tecnologías de la Información es el responsable de supervisar el correcto funcionamiento de los Equipos de Cómputo y de los Servidores de Datos de la institución.

f) Condiciones de Prevención de Riesgo

- Definir políticas de seguridad para impedir el uso de aplicaciones y/o herramientas software no autorizadas en los equipos de cómputo que operan los usuarios de dominio.
- Crear políticas de acceso a internet según las necesidades y permisos autorizados a los usuarios del dominio de equipos de cómputo.
- Evaluar la necesidad de eliminar definitivamente las unidades extraíbles de lectura y escritura instaladas en los equipos de cómputo.
- Bloquear los puertos USB de los Equipos de Cómputo que por su uso no lo requieran, y dejar solo a los que estrictamente lo necesitan previa autorización de su jefe inmediato.
- Mantener actualizado el sistema de protección antimalware en todos los Equipos de Cómputo.
- Configurar una solución de almacenamiento masivo de los archivos más críticos que los usuarios de las áreas pudieran solicitar, a fin de respaldar y custodiar la información de interés institucional.

2.PLAN DE EMERGENCIA

a) Eventos que activan la contingencia

- Comportamiento anómalo del hardware durante la ejecución de algún software.
- Los accesos a los recursos y sistemas informáticos se hacen lentos.
- Fallas continuas en los Servidores y Equipos de Cómputo.

b) Procesos relacionados antes del evento
Cualquier proceso relacionado con el uso de aplicaciones por parte de los equipos de cómputo y también de parte de los servidores.

c) Personal que autoriza la contingencia
El responsable que autoriza la contingencia es el Director de la Oficina de Tecnologías de la Información, extendiéndose al personal del Área de Soporte Informático si el caso lo amerita.

d) Descripción de las actividades después de activar la contingencia
- Desconectar inmediatamente el Equipo de Cómputo y/o servidor de la Red de Datos Corporativa, a fin de evitar una posible propagación de alguna variante de código malicioso.
- Evaluar y determinar si el equipo de cómputo y/o servidor ha sido infectado, usando el antivirus instalado en dicho equipo.
- Detectar y evaluar la fuente de la infección.
- Eliminar o congelar la acción del virus del sistema.
- Probar la funcionalidad del sistema.
- De no solucionarse el problema de infección; se respaldar la información y luego formatear el disco duro del equipo, ejecutando el respaldo de información para la seguridad e integridad de los datos.
- Reiniciar la conexión a la red de datos de la entidad.
- Efectuar las pruebas de operatividad funcional del equipo de cómputo con el usuario.
- Suscribir la conformidad con el usuario del equipo.

e) Duración
La duración de la contingencia no debe ser mayor a 2 horas en caso se confirme la presencia de algún código malicioso en cualquiera de sus variantes.

3.PLAN DE RECUPERACION

a) Personal Encargado
Personal de soporte informático de la Oficina de Tecnologías de la Información.

b) Descripción
- Personal de soporte informático informara al Director de la Oficina de Tecnologías de la Información el tipo de virus encontrado y el procedimiento usado para eliminarlo.
- Seguidamente el evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

c) Mecanismos de Comprobación
Se completará el formato de ocurrencia de eventos y se remitirá al Líder del Plan de Contingencia.

d) Mecanismos de Recuperación
Deberá ejecutarse de acuerdo al Plan de Recuperación descrita el numeral 6.8 del presente documento.

e) Desactivación del Plan de Contingencia
Personal de soporte informático informara al Director de la Oficina de Tecnologías de la Información para que se proceda a desactivar el plan.

f) Proceso de Actualización La infección por virus o códigos maliciosos de cualquier variante, no exime detener la aplicación de actualización de datos en los sistemas software del Gobierno Regional de Ucayali.

Tabla N° 20: Plan de Contingencias-Evento Acción de Códigos Maliciosos.

FALLA EN EL SISTEMA DE RED DE DATOS LAN	CODIGO DEL EVENTO	CG-16
1.PLAN DE MITIGACION		
a) Descripción del Evento El cableado estructurado de Datos LAN corporativo, soporta toda la conectividad por medios guiados (cables), el mismo que debe estar en constante y dinámico monitoreo y control operativo, ya que la infraestructura sobre todo en la Sede Central y el despliegue del medio de transporte (cable ethernet) no son los adecuados, corrompiendo toda norma de conexión y configuración sobre los elementos montados en la red de datos. En ese sentido, se estima conveniente considerar los siguientes componentes que podrían ser fuente y medios vulnerables de percibir algún tipo de contingencia: ***Comunicaciones*** Falla en el Switch de Core (Conmutador Principal). ***Proveedor de Servicios*** Interrupción del Suministro o Fluido Eléctrico. ***Infraestructura Institucional*** Robo o pérdida de equipos. b) Objetivo Mantener el Sistema de Cableado Estructurado en condiciones de funcionalidad y operación normales, para garantizar que la conectividad no se vea afectada, a fin de evitar interrupciones de los servicios y recursos de información de la intranet y hacia el exterior. c) Criticidad El Gobierno Regional de Ucayali define el presente evento teniendo en cuenta que es de gran impacto en el servicio y se identifica como CRITICO. d) Entorno La conectividad se desprende del Sistema de Cableado Estructurado de la entidad, el cual tiene alcance a toda la sede Central con independencia física más no lógica para el acceso a los servicios en las diferentes sedes remotas. e) Personal Encargado El Director de la Oficina de Tecnologías de la Información será el responsable de asegurar el correcto funcionamiento de la Red de Datos LAN de la entidad. f) Condiciones de Prevención de Riesgo • Programar acciones de mantenimiento preventivo y correctivo, que permita minimizar o mitigar cualquier contingencia que afecte a la Red de Datos Organizacional.		
2.PLAN DE EMERGENCIA		

a) Eventos que activan la contingencia
   - Bloqueo de accesos a los recursos de la Intranet y/o perdida de la conectividad.
   - Evento de tipo incendio cerca a los conmutadores de borde que distribuyen y extienden la conectividad a los usuarios del dominio por toda la entidad.

b) Procesos relacionados antes del evento
   Mantenimiento contiguo del cableado y de los equipos para impedir un mayor impacto ante una contingencia.

c) Personal que autoriza la contingencia
   Será el Director de la Oficina de Tecnologías de la Información o personal de Soporte Informático con la autorización expresa del director de dicha oficina.

d) Descripción de las actividades después de activar la contingencia
   - Verificar la operativa del cableado estructurado y los equipos que la componen, para identificar posibles fallas internas.
   - Verificar las condiciones operativas del entorno como el fluido eléctrico, precipitaciones a causa de lluvias intensas, Accesos no autorizados a los nodos donde se encuentra instalados los conmutadores de borde y otros según corresponda.

e) Duración
   La duración de la contingencia no debe ser mayor a 1 hora después de haber activado la contingencia.

3.PLAN DE RECUPERACION

a) Personal Encargado
   El Director de la Oficina de Tecnologías de la Información o personal de Soporte Informático autorizado, serán los responsables del Plan de Recuperación.

b) Descripción
   - Se hará de conocimiento al Director de la Oficina de Tecnologías de la Información, la fuente que originó la contingencia, así como el mecanismo a emplear para su solución.

c) Mecanismos de Comprobación
   Se completará el formato de ocurrencia de eventos y se remitirá al Líder del Plan de Contingencia.

d) Mecanismos de Recuperación
   Deberá ejecutarse de acuerdo al Plan de Recuperación descrita el numeral 6.8 del presente documento.

e) Desactivación del Plan de Contingencia
   El Director de la Oficina de Tecnologías de Información o el personal de Soporte Informático autorizado serán responsables de comunicar y desactivar el plan.

f) Proceso de Actualización
   De ser el caso, si no se ha considerado algún procedimiento que haya provocado alguna contingencia será incluido en el plan de contingencias para prevenir eventos futuros.

Tabla N° 21: Plan de Contingencia-Evento Falla en el Sistema de Red de Datos LAN.

FALLA EN LOS EQUIPOS SERVIDORES DE DATOS	CODIGO DEL EVENTO	CG-11

1.PLAN DE MITIGACION

a) Descripción del Evento

La seguridad de los servidores es tan importante como la seguridad en la red de datos, debido a que los servidores usualmente procesan y almacenan una gran cantidad de información vital para la entidad. Por ello se deben implementar mecanismos que garanticen la continuidad de los procesos y de los servicios corporativos.

En ese sentido, se estima conveniente considerar los siguientes componentes que podrían ser fuentes y medios vulnerables de percibir algún tipo de contingencia:

Comunicaciones

Falla en el Switch de Core (Conmutador Principal).

Hardware

Falla en algún elemento critico de los equipos servidores.

Falla en el Sistema de Alimentación Ininterrumpida – SAI principal.

b) Objetivo

Mantener los tiempos de indisponibilidad al mínimo por parte de los equipos servidores de datos de la entidad.

c) Criticidad

El Gobierno Regional de Ucayali define el presente evento teniendo en cuenta que es de gran impacto en el servicio y se identifica como CRITICO.

Teniendo en cuenta el detalle impacto

d) Entorno

La plataforma tecnológica que forma parte del parque informático institucional (equipos de cómputo, conmutadores y servidores).

e) Personal Encargado

El Director de la Oficina de Tecnologías de la Información será el responsable de asegurar el correcto funcionamiento de los Equipos Servidores de Datos.

f) Condiciones de Prevención de Riesgo

- Realizar el mantenimiento preventivo y correctivo, que permita minimizar el impacto de cualquier contingencia que afecte el normal funcionamiento operativo de los equipos servidores.

2.PLAN DE EMERGENCIA

a) Eventos que activan la contingencia

- Sectores afectados en los discos duros de los Servidores de Datos.
- Error de Memoria RAM.
- Error de Tarjeta(s) Controladora(s).
- Error de Tarjeta Controladora RAID.
- Comportamiento anómalo del Sistema Operativo del Servidor, que impide el normal funcionamiento de los componentes hardware.
- Falla en el Sistema de Alimentación Ininterrumpida (SAI/UPS), que da lugar a un apagado imprevisto de los Servidores.

b) Procesos relacionados antes del evento

Plan de Mantenimientos de los equipos servidores de datos para mitigar o reducir el impacto producto de una contingencia.

c) Personal que autoriza la contingencia
El Director de la Oficina de Tecnologías de la Información o personal de Soporte Informático con la autorización expresa del director de dicha oficina.

d) Descripción de las actividades después de activar la contingencia
- Verificar inmediatamente el estado operativo de los servidores, dependiendo del evento se deberá planificar una acción correctiva en caso de falla.
- Proceder a las acciones correctivas ante la detección del evento:

Ante Sectores afectados en los discos duros de los Servidores de Datos
- Verificar los discos afectados.
- Apagar el servidor y reemplazar con otros discos del mismo tipo.
- Generar la partición adecuada y formatearlo.
- Restaurar la última copia de seguridad de los sistemas de información generada.
- Ejecutar y verificar el correcto funcionamiento de los sistemas de información que se encontraban en dicho servidor.

Ante errores de memoria RAM
- Verificar las memorias dañadas.
- Retirar las memorias y reemplazarlos por otras iguales o similares.
- Encender el servidor y verificar su funcionamiento.

Ante error de Tarjeta(s) Controladora(s)
- Apagar correctamente el servidor.
- Ubicar la tarjeta de red controladora.
- Retirar la tarjeta de red dañada y reemplazarlo por una similar.
- Encender el servidor y verificar su correcto funcionamiento.

Ante error de tarjeta controladora RAID
- Verificar el error.
- Apagar correctamente el servidor de datos.
- Ubicar y cambiar la tarjeta controladora RAID por una similar o igual.
- Encender el servidor y configurar los arreglos de los discos RAID.
- Verificar el correcto funcionamiento del servidor de datos.

Ante Comportamiento anómalo del Sistema Operativo del Servidor
- Diagnosticar el estado del sistema operativo.
- Realizar la copia de seguridad.
- Reparar o instalar nuevamente el sistema operativo con las particiones de almacenamiento adecuados.
- Configurar el entorno de trabajo.
- Restaurar la copia de seguridad generada.
- Verificar el correcto funcionamiento del sistema operativo en el servidor.

Ante Falla en el Sistema de Alimentación Ininterrumpida (SAI/UPS)
- Realizar la copia de seguridad de los servidores de datos.
- Realizar el correcto apagado de los servidores de datos.

- Verificar el estado del Sistema de Alimentación Interrumpida (SAI/UPS) y apagarlo correctamente. - Encender correctamente el SAI/UPS seguido del servidor de datos y verificar su funcionamiento. • Informar a la Gerencia Regional de Administración, las acciones correctivas a ejecutar para lograr restablecer la operatividad de los servicios en el menor tiempo posible. e) Duración La duración de la contingencia no debe ser mayor a 1 hora después de haber activado la contingencia.
3.PLAN DE RECUPERACION
a) Personal Encargado El Director de la Oficina de Tecnologías de la Información o personal de Soporte Informático autorizado, serán los responsables del Plan de Recuperación. b) Descripción Se hará de conocimiento al Director de la Oficina de Tecnologías de la Información, la fuente que originó la contingencia, así como el mecanismo a emplear para su solución. c) Mecanismos de Comprobación Se completará el formato de ocurrencia de eventos y se remitirá al Líder del Plan de Contingencia. d) Mecanismos de Recuperación Deberá ejecutarse de acuerdo al Plan de Recuperación descrita el numeral 6.8 del presente documento. e) Desactivación del Plan de Contingencia El Director de la Oficina de Tecnologías de Información o el personal de Soporte Informático autorizado serán responsables de comunicar y desactivar el plan. f) Proceso de Actualización De ser el caso, si no se ha considerado algún procedimiento que haya provocado alguna contingencia será incluido en el plan de contingencias para prevenir eventos futuros.

Tabla N° 22: Plan de Contingencia-Evento Falla en los Equipos Servidores de Datos.

6.10.3 Contingencia: Evento de Recursos Humanos

a) Objetivo
Definir y garantizar la participación de los recursos Humanos de la entidad, para actuar eficientemente ante un evento de contingencia que posibilite una acción de desastre humano o tecnológico.

b) Cobertura
El desarrollo del Plan de Contingencia sobre el evento de Recursos Humanos del Gobierno Regional de Ucayali, está relacionada con el impacto potencial que provoca la incapacidad

o factor imprevisto por parte de los recursos humanos para controlar y eliminar cualquier evento de contingencia. En ese sentido se hace mención de algunas causas relacionadas:

- Accidentes.
- Renuncia intempestiva y/o ceses.

Se sugiere que en los contratos se especifiquen las responsabilidades asignadas.

En adelante se presenta la Matriz de Riesgo, en la cual se han definido los que mayor atención deben poseer, a fin de evitar o limitar los daños.

Código del Evento	Descripción del Riesgo	Probabilidad de Ocurrencia	Impacto	Ponderación	Alerta
CONTINGENCIA: RECURSOS HUMANOS					
RECURSOS HUMANOS					
CG-19	Ausencia del Personal de la Oficina de Tecnologías de la Información	0.04	3	0.16	3

Tabla N°23: Matriz Riesgos-Contingencia Recursos Humanos

c) Descripción del Plan

A continuación, se detallan los Planes de contingencia definidos en la Matriz de Riesgos de contingencias de Recursos Humanos.

AUSENCIA DEL PERSONAL DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION	CODIGO DEL EVENTO	CG-11
1.PLAN DE MITIGACION		

a) Descripción del Evento

La disponibilidad y presencia del personal de la Oficina de Tecnologías de la Información (Soporte Informático) es fundamental para mitigar cualquier evento de contingencia que ponga en riesgo la continuidad de las operaciones críticas de la entidad, evaluando su alcance e impacto generado.

En ese sentido se deben aplicar mecanismos efectivos para mantener la presencia y reacción inmediata del capital humano que ayude a garantizar las acciones correctivas que pudieran afecta la integridad de la infraestructura de tecnologías de información y las operaciones o procesos organizacionales, para ello se ha identificado algunos elementos pasibles de sufrir algún comportamiento irregular anómalo, estos son los siguientes:

Recursos Humanos

Personal de la Oficina de Tecnologías de la Información.

b) Objetivo

Garantizar la continuidad de la operativa de los servicios informáticos del Gobierno Regional de Ucayali.

c) Criticidad
El Gobierno Regional de Ucayali define el presente evento en la clasificación de evento CRITICO.

d) Entorno
Se puede presentar en la Sede Central o en las sedes remotas del Gobierno Regional de Ucayali.

e) Personal Encargado
El Director de la Oficina de Tecnologías de la Información será el responsable de cumplir y hacer cumplir los procedimientos de mitigación, emergencia y recuperación ante una EVENTUAL contingencia definida en el Plan.

f) Condiciones de Prevención de Riesgo
- El Director de la Oficina de Tecnologías de la Información u otro personal autorizado entrenará a todo el personal del Área de Soporte Informático para que adquieran los conocimientos y habilidades necesarias y puedan actuar eficaz y eficientemente ante un evento que ponga en riesgo las operaciones sensibles de la entidad.
- El Director de la Oficina de Tecnologías de la Información, dispondrá de un mínimo a dos (2) personas de área de soporte informático y un (1) personal del área afectada de ser el caso.
- El personal de Soporte Informático debe hacer de conocimiento con anticipación a la Oficina de Tecnologías de la Información las razones de una inminente inasistencia al centro de labores, a fin de tomar las acciones necesarias para no afectar los requerimientos técnicos de los usuarios del dominio institucional.

2.PLAN DE EMERGENCIA

a) Eventos que activan la contingencia
- Interrupción de las funciones principales de los Equipos de Cómputo y de los Servidores de Datos.
- Mensajes continuos de errores o fallas en los servidores de Datos o en los Equipos de Cómputo de la Entidad.

b) Procesos relacionados antes del evento
Disponer los respaldos de los sistemas operativo de Equipos de Cómputo y Servidores.

c) Personal que autoriza la contingencia
El Director de la Oficina de Tecnologías de la Información o personal de Soporte Informático con la autorización expresa del director de dicha oficina.

d) Descripción de las actividades después de activar la contingencia
Para el caso de Equipos de Cómputo:
- Reportar por escrito al área de soporte informático.
- Efectuar la revisión y evaluación del Equipos de Cómputo para determinar la causa de falla.
- Escanear el equipo con el sistema antimalware o antivirus que cuenta la entidad a fin de bloquear y eliminar cualquier indicio de código malicioso.

• Identificar el origen de la infección (ejecutables, correo electrónico, dispositivos extraíbles, otros). • De no solucionarse el problema; formatear el disco duro del equipo y conectar a la red de datos corporativa. Para el caso de los Servidores de Dato: • De presentarse cualquier falla o comportamiento anómalo en los servidores, personal de la Oficina de Tecnologías de la Información actuará de inmediato para encontrar la solución al problema. • Poner de conocimiento a todas las áreas a través del servicio de mensajería interna las acciones a ejecutar y el tiempo de interrupción del servicio o servicios afectados. e) Duración La duración de la contingencia no debe ser mayor a 02 hora después de haber activado la contingencia.
3.PLAN DE RECUPERACION
a) Personal Encargado El Director de la Oficina de Tecnologías de la Información o personal designado por éste, serán los responsables del Plan de Recuperación. b) Descripción Personal del área de soporte informático informará al Director de la Oficina de Tecnologías de la Información, la causa que motivó el problema, así como también el procedimiento a seguir para resolverlo. Cuando se haya restablecido los servicios se enviará un aviso a través del sistema de mensajería remota a todos los usuarios del dominio para que puedan usar sus aplicaciones, sistemas o cualquier otro servicio configurado. c) Mecanismos de Comprobación Se completará el formato de ocurrencia de eventos y se remitirá al Líder del Plan de Contingencia. d) Desactivación del Plan de Contingencia El Director de la Oficina de Tecnologías de Información o el personal de Soporte Informático autorizado serán responsables de comunicar y desactivar el plan. e) Proceso de Actualización La actualización del presente evento se hará efectiva siempre y cuando existan escenarios que representan riesgo que pudiera afectar la continuidad de las operaciones de la entidad.

Tabla N° 24: Plan de Contingencia-Evento: Ausencia del Personal de la Oficina de Tecnologías de la Información.

6.10.4 Contingencia: Evento de Seguridad Interna y Externa.

a) Objetivo.

Mantener la integridad y buen recaudo de la infraestructura física, equipos, mobiliarios y demás recursos de información con que cuenta la entidad, en razón de eventos o fenómenos causados por fuente natural, tecnológica o humana.

b) Cobertura.

Desde el punto de vista de las posibles contingencias que engloban el evento de seguridad interna y externa, se toman en cuenta los siguientes aspectos:

- Despliegue de verificación de los ámbitos físicos.
- Gestión del control de accesos de los espacios restringidos definidos por la entidad, a fin de supervisar los ingresos y salidas del personal no autorizado (terceros u otros) a los ambientes críticos que son sensibles de sufrir alguna amenaza, poniendo un riesgo su integridad.
- Planificar acciones para que los actos de intrusión, sabotaje y cualquier acto delincuencial afecte el normal desempeño operativo de la entidad.

Habiendo detallado el objetivo y cobertura de acción que tendría el evento de contingencia interna y externa a nivel físico, se presenta a continuación la siguiente Matriz de Riesgos.

Código del Evento	Descripción del Riesgo	Probabilidad de Ocurrencia	Impacto	Ponderación	Alerta
CONTINGENCIA: SEGURIDAD INTERNA Y EXTERNA					
INFRAESTRUCTURA INSTITUCIONAL					
CG-21	Robo o perdida de equipos	0.03	3	0.09	3
CG-22	Intrusión	0.03	3	0.12	3
CG-23	Sabotaje	0.02	2	0.04	2

Tabla N° 25: Matriz de Riesgos-Contingencia Seguridad Interna y Externa

c) Plan de Pruebas

El presente Plan de Pruebas se ejecutará en base a lo definido en la columna "Descripción del Riesgo" de la contingencia Seguridad Interna y Externa.

La ejecución del Plan de Pruebas se llevará a cabo, una vez el Líder o Administrador del Plan tengan la autorización de la Alta Dirección.

d) Descripción del Plan

Visto la Matriz de Riesgos de Seguridad Interna y Externa, se observa que la ponderación de cada riesgo no alcanza el valor promedio equivalente a los 0.15 para considerarse en la clasificación de alerta como "Crítico" que corresponde al valor "3", por lo que no corresponde detallar un Plan de Mitigación, de Emergencia y de Recuperación respectivamente; quedando a disposición de su probable inclusión dentro del Plan de Contingencia en una próxima actualización.

e) Plan de Respaldo y Recuperación
Deberá ejecutarse de acuerdo al Plan de Respaldo y Recuperación descrita el numeral 6.8 del presente documento.

VII. DISPOSICIONES TRANSITORIAS COMPLEMENTARIAS FINALES

- El plan de contingencia del Gobierno Regional de Ucayali, tiene como objetivo primario salvaguardar la infraestructura de la Red y Sistemas de Información priorizando la ejecución de mecanismos de seguridad para protegernos y estar preparados ante una contingencia de cualquier índole.
- El Plan de Contingencia Informático del Gobierno Regional de Ucayali es la herramienta para implementar las habilidades y medios de respaldo a fin de mantener nuestras operaciones en condiciones normales, cuando un evento fuera del nuestro alcance e intente la interrupción parcial o total de las funciones organizacionales. Las políticas con respecto a la recuperación de desastres deben emanar de la máxima autoridad institucional, para garantizar su difusión y estricto cumplimiento.
- El Plan de Contingencia del Gobierno Regional de Ucayali está supeditado a la infraestructura física y a las funciones que realiza la Oficina de Tecnologías de la Información.
- Programar las actividades propuestas en el presente Plan de Contingencias.
- Hacer de conocimiento general el contenido del presente Plan de Contingencias, con la finalidad de incrementar las habilidades y destrezas al personal del GRU en el uso del presente Plan.
- Se debe orientar el Plan a proteger la infraestructura física, los recursos de información y los recursos humanos a nivel institucional, considerando que no se debe diseñar controles y políticas excesivas que conlleve a una gestión ineficiente.

VIII. TABLAS Y FIGURAS.

<u>TABLAS</u>

- <u>Tabla N° 01: Sedes Remotas del Gobierno Regional de Ucayali.</u>
- Tabla N° 02: Equipos de Trabajo del Plan de Contingencias.
- Tabla N° 03: Cuadros de Impactos.
- Tabla N° 04: Cuadro de Probabilidad de Ocurrencias.
- Tabla N° 05: Exposición del Riesgo.
- Tabla N° 06: Matriz de Riesgo de Contingencias.
- Tabla N° 07: Eventos Con Control (CC).
- Tabla N° 08: Eventos Sin Control (SC).
- Tabla N° 09: Elementos Vs Contingencias.
- Tabla N° 10: Matriz de Riesgos – Contingencias de Siniestros.

FIGURAS.

IX. ANEXOS.

ANEXO N° 01 FORMULARIO DE EVENTOS			
EVENTOS DE CONTINGENCIA – GOBIERNO REGIONAL DE UCAYALI			
CODIGO DEL EVENTO		FECHA	
DESCRIPCION DE LA OCURRENCIA			
PLAN DE MITIGACION - ACCIONES			
PLAN DE EMERGENCIA - ACCIONES			
PLAN DE RECUPERACION - ACCIONES			
LINEAS DE ACONTECIMIENTO: (opcional)			

GOBIERNO REGIONAL DE UCAYALI · V°B° · GOBERNACIÓN

GOBIERNO REGIONAL DE UCAYALI · V°B° · GERENCIA GENERAL

OFICINA REGIONAL DE ADMINISTRACIÓN · V°B° · G.R.U.

Gerencia Regional de Planeamiento y Pres. · V°B° · G.R.U.

OFICINA REGIONAL DE ASESORÍA JURÍDICA · V°B° · G.R.U.

GOBIERNO REGIONAL DE UCAYALI · V°B° · SECRETARÍA GENERAL

SUB GERENCIA DE DESARROLLO INSTITUCIONAL · V°B° · GRPP

ANEXO N° 02: FORMULARIO DEL PLAN DE PRUEBAS DE CONTINGENCIAS					
PLAN DE PRUEBA – GOBIERNO REGIONAL DE UCAYALI					
CODIGO N°	Código del plan				
PROCESO DE PRUEBA	Nombre del proceso de prueba				
AREA RESPONSABLE	Área responsable de llevar a cabo el proceso				
FECHA		**HORA INICIO**		**HORA FIN**	

INFORMACIÓN DEL PROCESO

METODOLOGIA Y ALCANCE:
Se especificará el procedimiento a seguir para el desarrollo de la prueba y su alcance

CONDICIONES DE EJECUCIÓN:

EQUIPO	Nombre del servidor, equipo de cómputo u otro dispositivo
APLICACIÓN	
VERSION	
FECHA DE BACKUP	

DE LA PRUEBA REALIZADA

RESULTADO DE LA PRUEBA: Marcar con una (x)

SATISFACTORIO	
SATISFACTORIO CON OBSERVACIONES	
DEFICIENTE	

OBSERVACIONES:
~~Se especifican las observaciones de las pruebas realizadas, así como los resultados de~~ las pruebas realizadas...

ACTUALIZACION DEL PLAN DE CONTINGENCIA

CAMBIOS EN EL PLAN DE CONTINGENCIA:

Se especifica que se implementará en el Plan de Contingencia como consecuencia de las observaciones encontradas en las pruebas realizadas.

MIEMBROS PARTICIPANTES

PARTICIPANTE	CARGO	FIRMA

GOBIERNO REGIONAL DE UCAYALI V°B° GOBERNACIÓN

GOBIERNO REGIONAL DE UCAYALI V°B° GERENCIA GENERAL

OFICINA REGIONAL DE ADMINISTRACIÓN V°B° G.R.U.

Gerencia Regional de Planeamiento y Presupuesto V°B° G.R.U.

OFICINA REGIONAL DE ASESORÍA JURÍDICA V°B° G.R.U.

GOBIERNO REGIONAL DE UCAYALI V°B° SECRETARÍA GENERAL

SUB GERENCIA DE DESARROLLO INSTITUCIONAL V°B° GRPP

ANEXO N° 03 – BITACORAS DE COPIA DE SEGURIDAD

OFICINA DE TECNOLOGIAS DE LA INFORMACION

BITACORA DE RESPALDO O COPIA DE SEGURIDAD DE LA INFORMACION DEL GOBIERNO REGIONAL DE UCAYALI

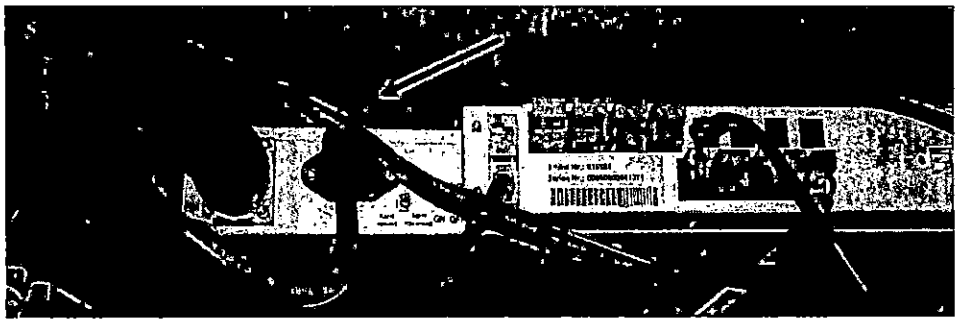
N°	Nombre de la Copia de Seguridad	Fecha de la Copia de Seguridad	Tiempo de Inicio - Fin de la Copia de Seguridad	Apellidos y Nombre	Cargo / Función	Información a respaldar	Ruta de Origen de la Copia de Seguridad	Sistema Operativo y Versión	Software Gestor y Versión	Dirección IP	Ruta Destino de la Copia de Seguridad	Estado del Servicio al momento de realizar la Copia de Seguridad	Tamaño de la Copia de Seguridad Generada (GB)

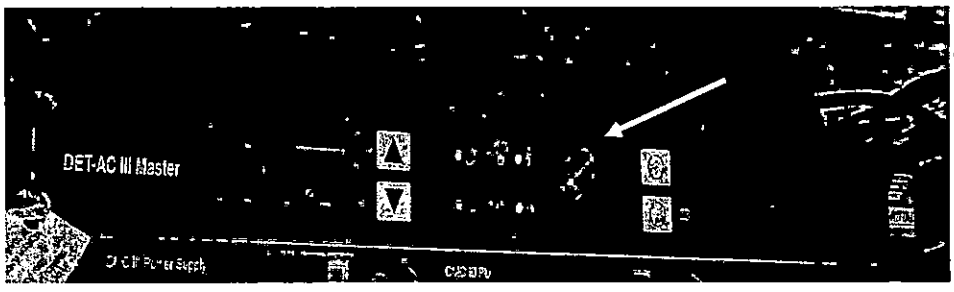
ANEXO N° 04

SECUENCIA DEL CORRECTO APAGADO Y ENCENDIDO DEL CENTRO DE DATOS, SISTEMA DE CLIMATIZACIÓN Y SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA (SAI/UPS).

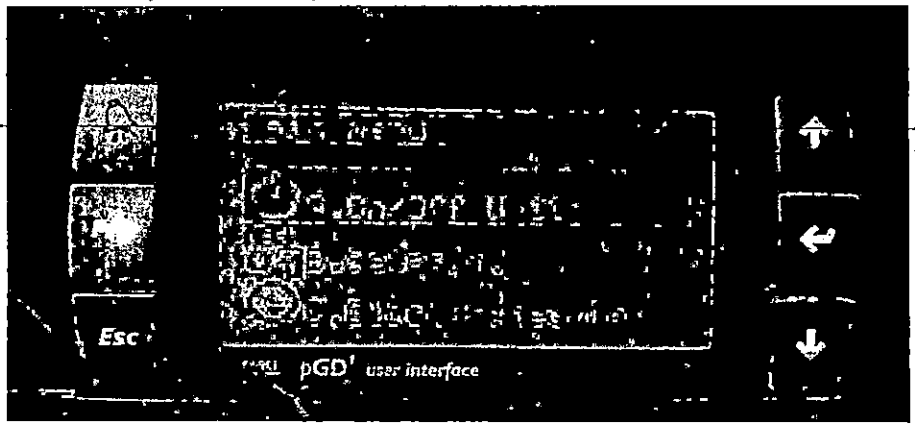
SECUENCIA DE APAGADO DEL SISTEMA DE CLIMATIZACION ANTE CUALQUIER EVENTUALIDAD EN EL GOBIERNO REGIONAL DE UCAYALI – DATA CENTER

1. Apagar el dispositivo **DETAC**, para ello se debe desconectar el cable de alimentación eléctrica, y, luego presionar el switch "OFF".

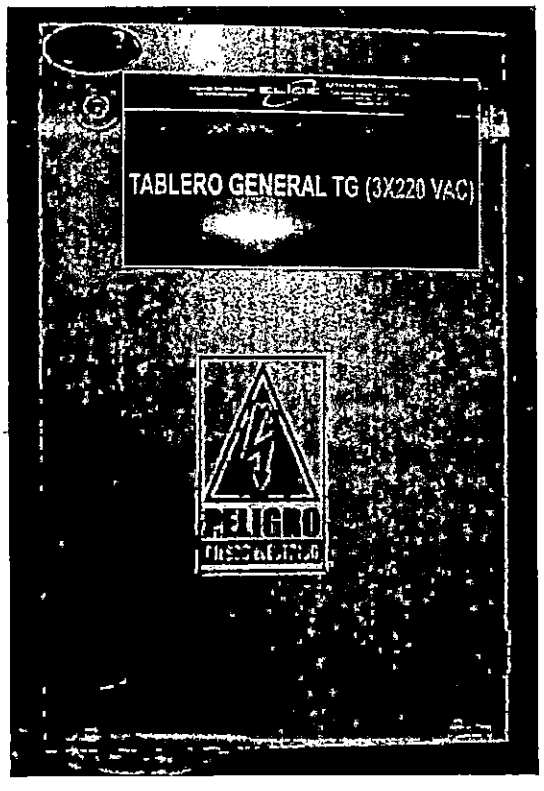


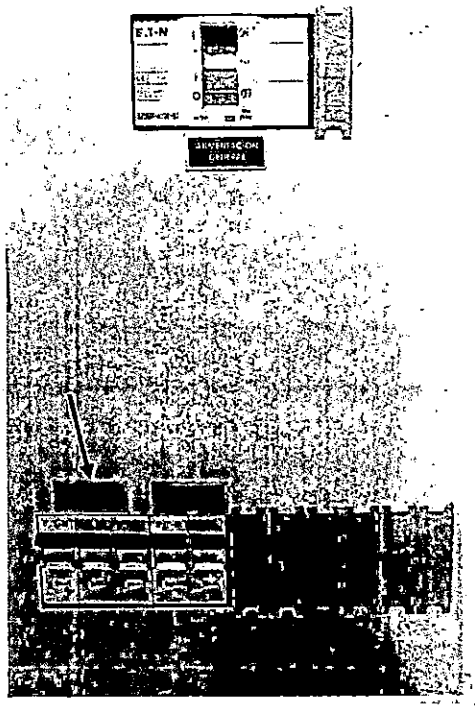


2. Apagar el **LCP** desde el panel de control frontal, presionando la tecla "**Prg**", luego seleccionar la opción **"On/Off Unit"**, presione la tecla "**ENTER**", seguidamente presionar sobre cualquiera de las teclas de desplazamiento (arriba o abajo) para cambiar a "**OFF**" y finalmente presionar "**ENTER**".

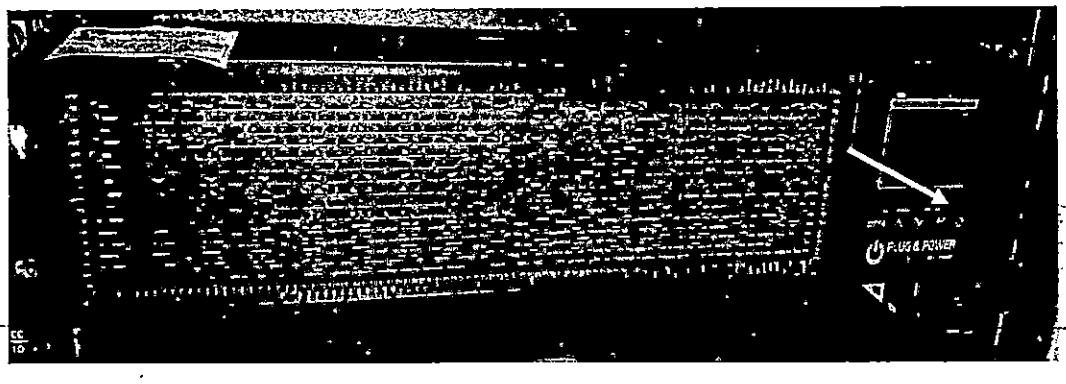


3. Ir al **TABLERO GENERAL TG (3X220 VAC);** y bajar las perillas del circuito **N° 01 o C1.**

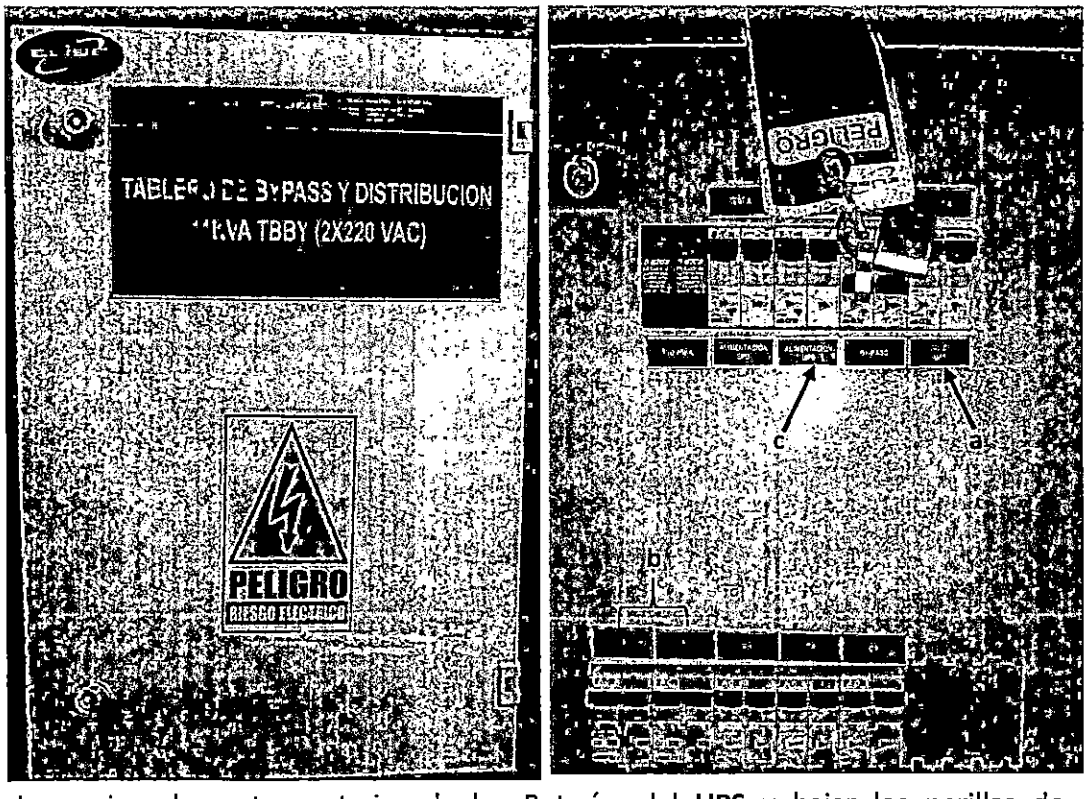




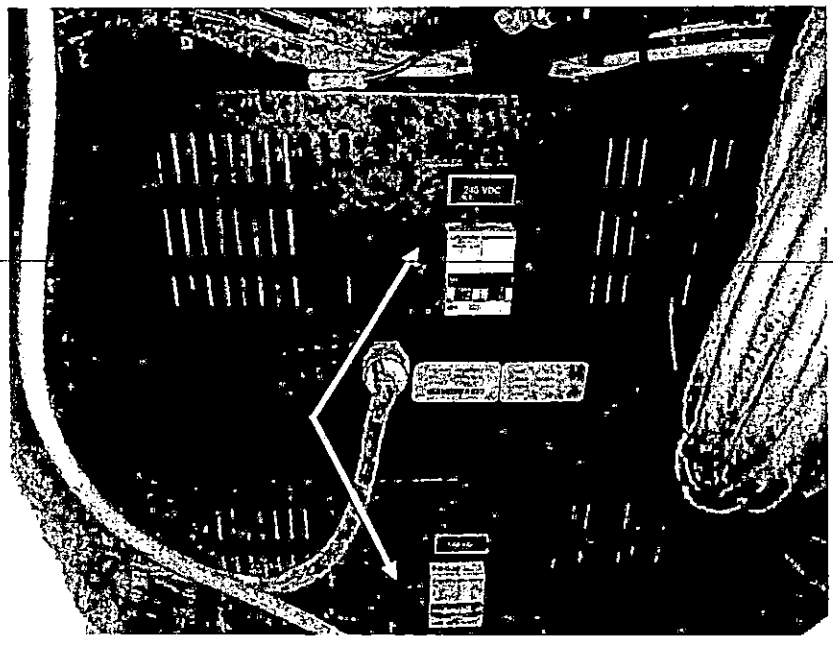
4. Ir al equipo de **UPS** y presione por unos segundos el botón de **"APAGADO"**; el equipo cambiará de estado a **"BYPASS"**.



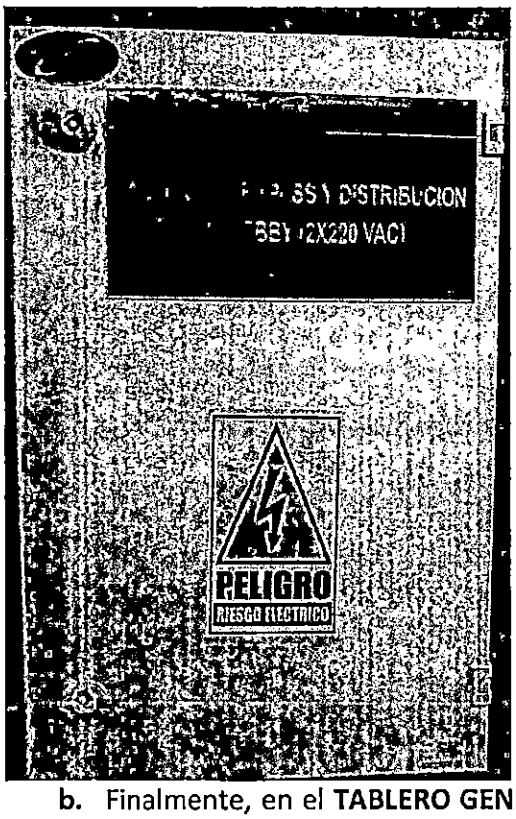
5. Ir al **TABLERO DE BYPASS Y DISTRIBUCION 11KVA TBBY (2X220 AC)**:
   a. Bajamos la perilla "**SALIDA UPS**" o "**ITM4**".
   b. Luego bajamos las perillas "**C1**", "**C2**".
   c. Después bajamos las perillas de "**ALIMENTACION UPS**" **O** "**ITM2**".

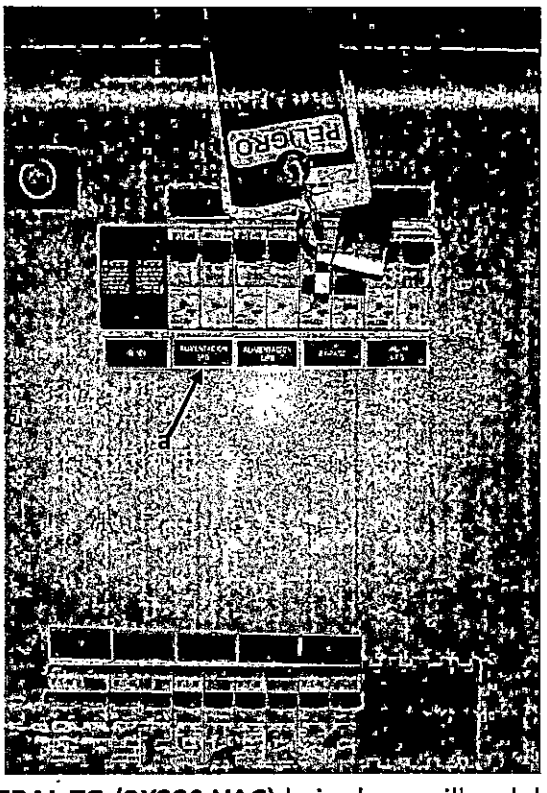


6. Luego ir a la parte posterior de las Baterías del **UPS** y bajar las perillas de alimentación por seguridad.

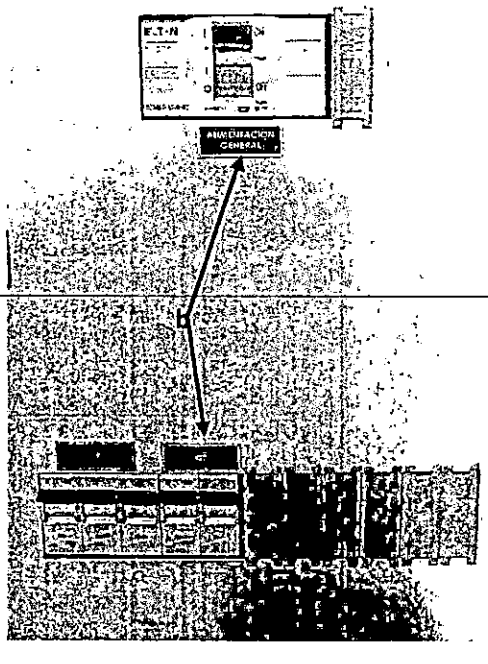


7. Después, en el **TABLERO DE BYPASS Y DISTRIBUCION 11KVA TBBY (2X220 VAC):**
   a. Bajar la perilla **"ALIMENTACION SPD"** o **"ITM I".**



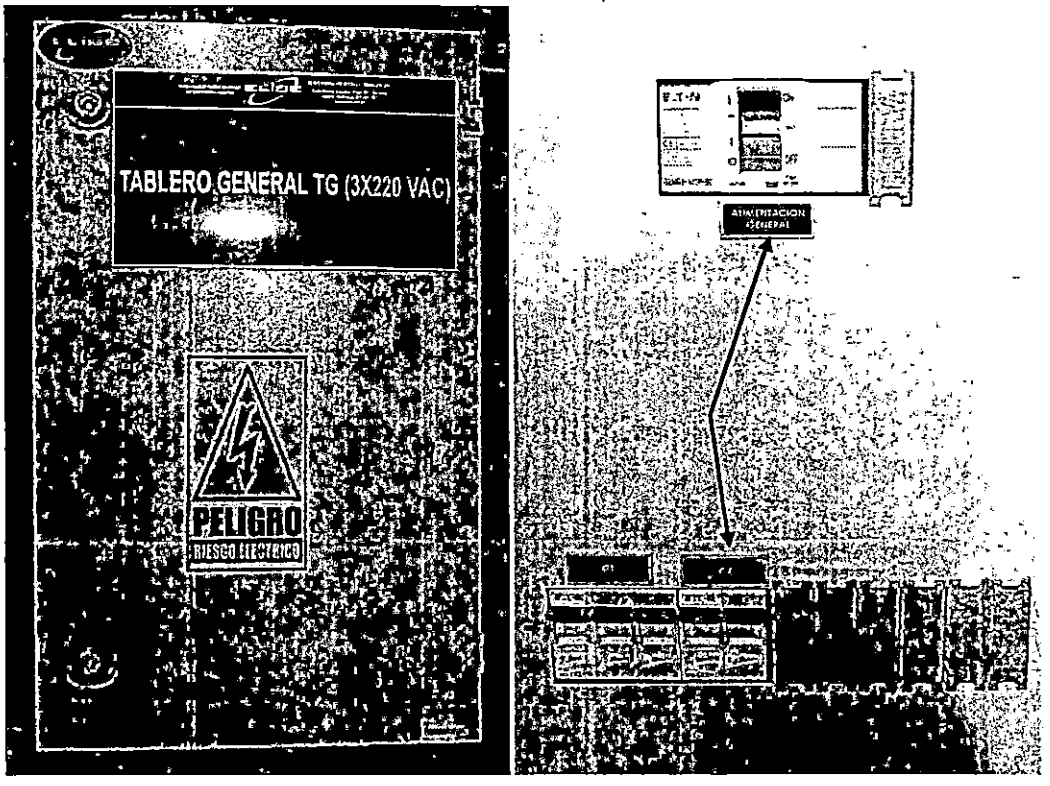


   b. Finalmente, en el **TABLERO GENERAL TG (3X220 VAC)** bajar las perillas del circuito **N° 02 o C2** y la perilla de **ALIMENTACION GENERAL.**

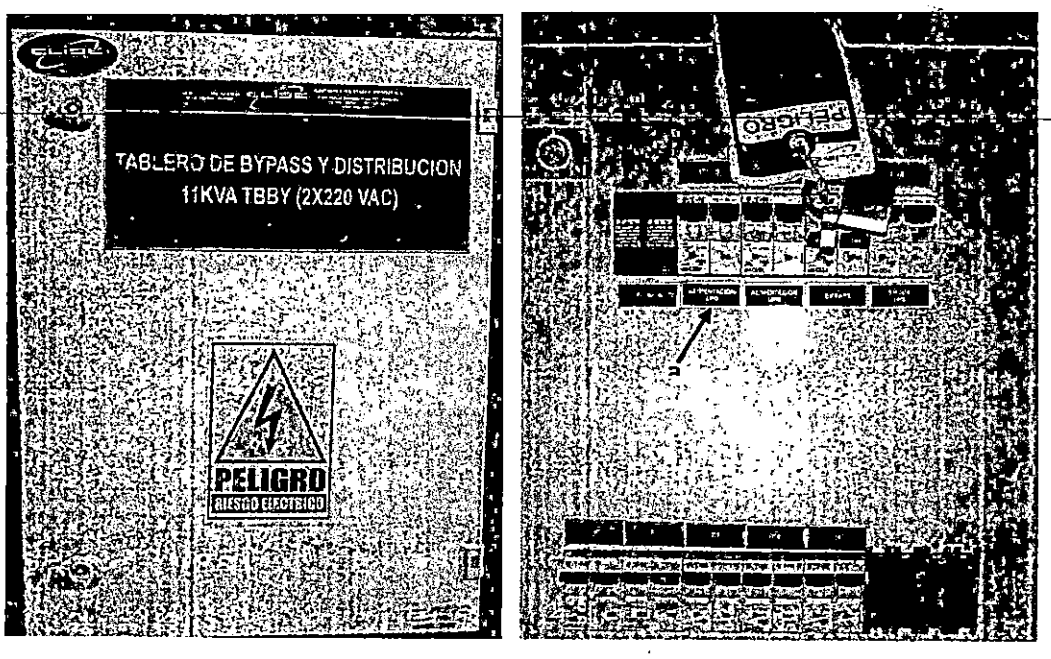


SECUENCIA DE ENCENDIDO DEL SISTEMA DE CLIMATIZACION ANTE CUALQUIER EVENTUALIDAD EN EL GOBIERNO REGIONAL DE UCAYALI – DATA CENTER

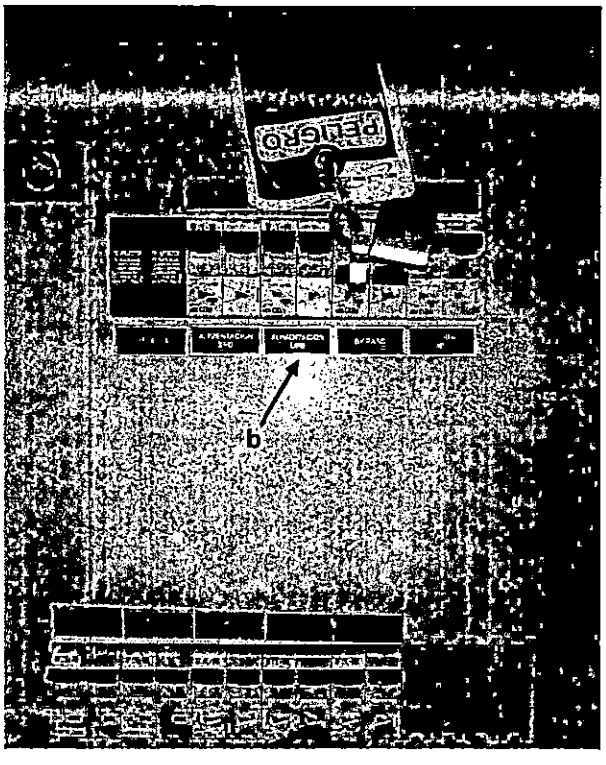
1. Nos dirigimos en el **TABLERO GENERAL TG (3X220 VAC)** y subir la perilla de **"ALIMENTACION GENERAL"** y luego de unos segundos subir la perilla de Circuito **N° 2 o "C2"**, el cual encenderá el Transformador de Aislamiento Monofásico.



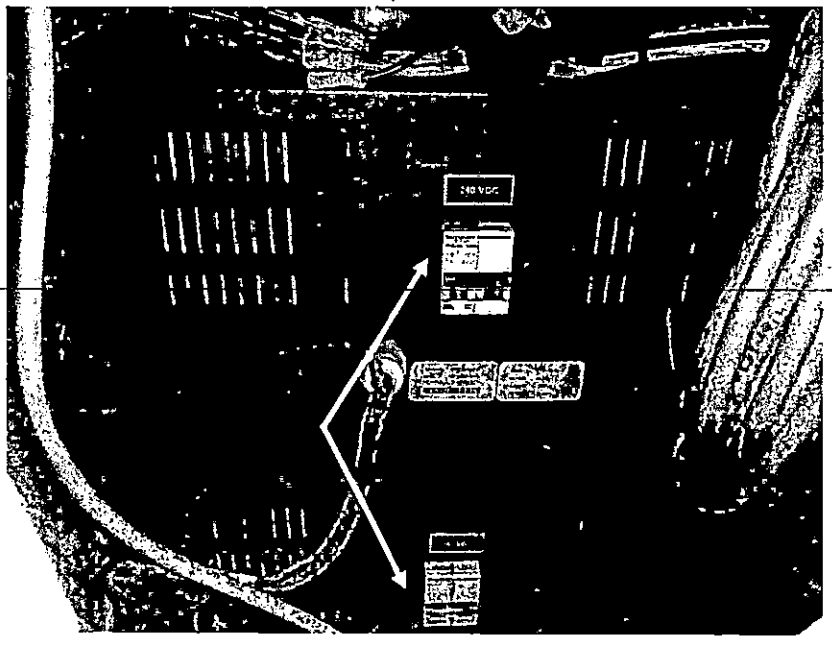
2. Luego, en el **TABLERO DE BYPASS Y DISTRIBUCION 11KVA TBBY (2X220 VAC):**
   a. Subir la perilla de **ALIMENTACION SPD o "ITM I".**



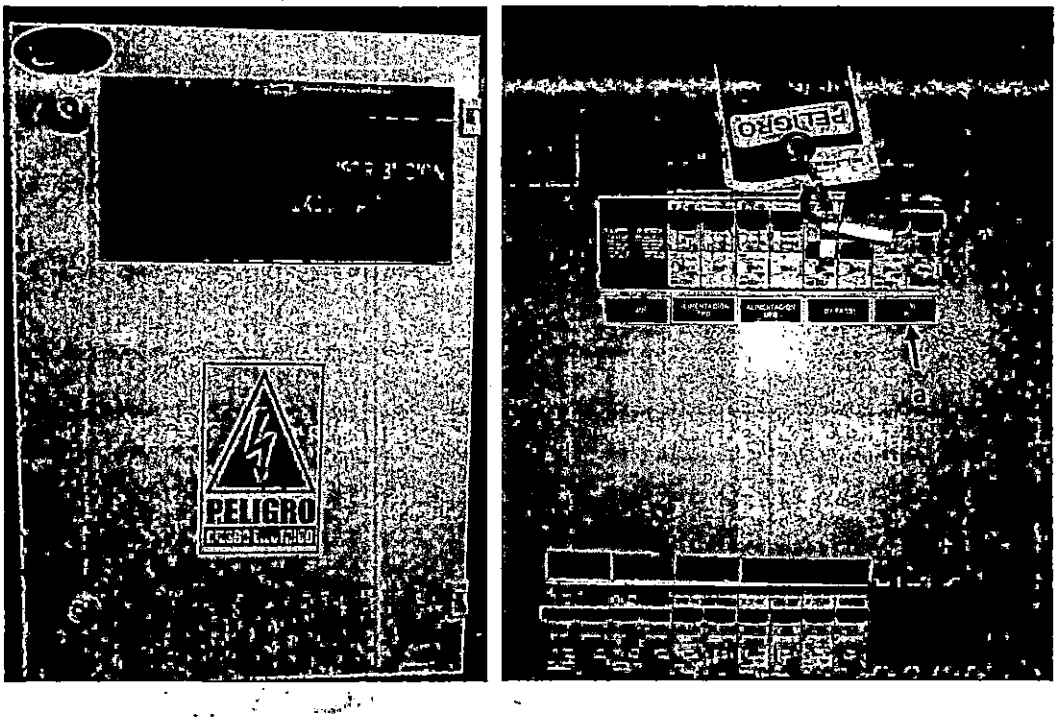
b. También, bajar la perilla de **"ALIMENTACION UPS" o "ITM2"**, con ello se carga el **UPS**.



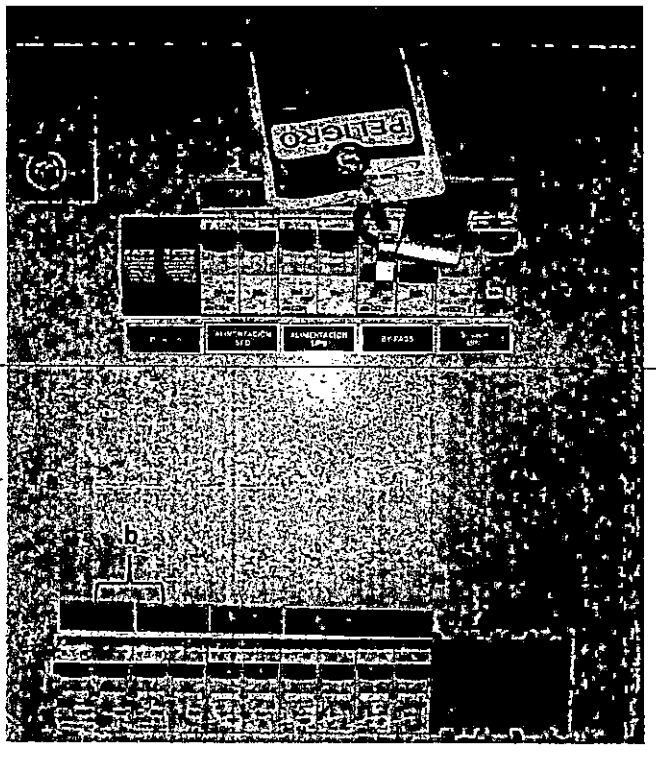
c. Procedemos a levantar las perillas de alimentación de las 02 baterías que están detrás de cada banco de baterías.



3. Seguido en el mismo **TABLERO DE BYPASS Y DISTRIBUCION 11KVA TBBY (2X220 VAC):**
   a. Levantamos la perilla de **"SALIDA DE UPS"** o **"ITM4"**.

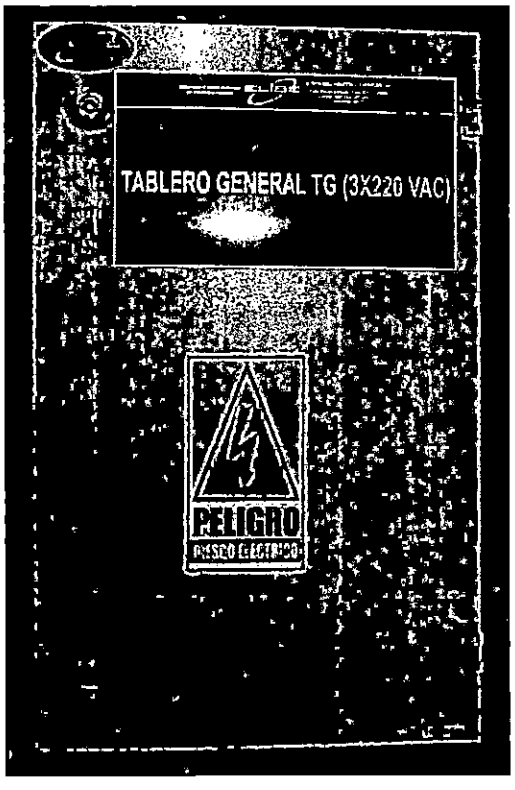


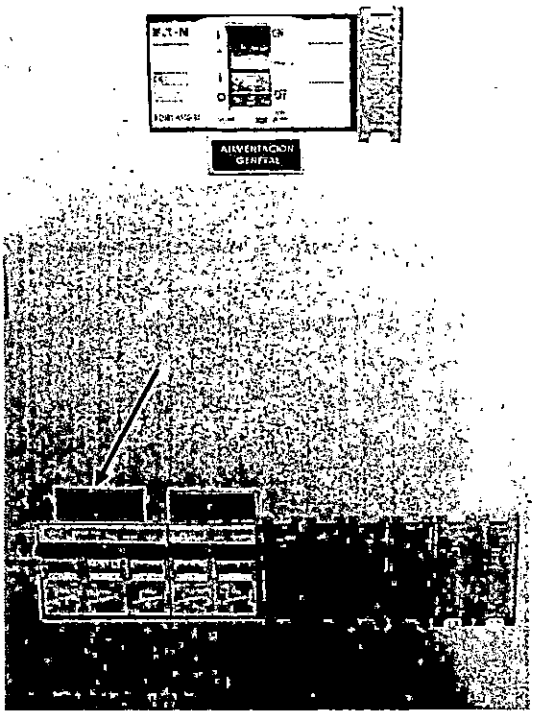
   b. También la perilla de los circuitos **"C1"** y **"C2"**, con estos energizamos los equipos "servidores" y "comunicaciones".

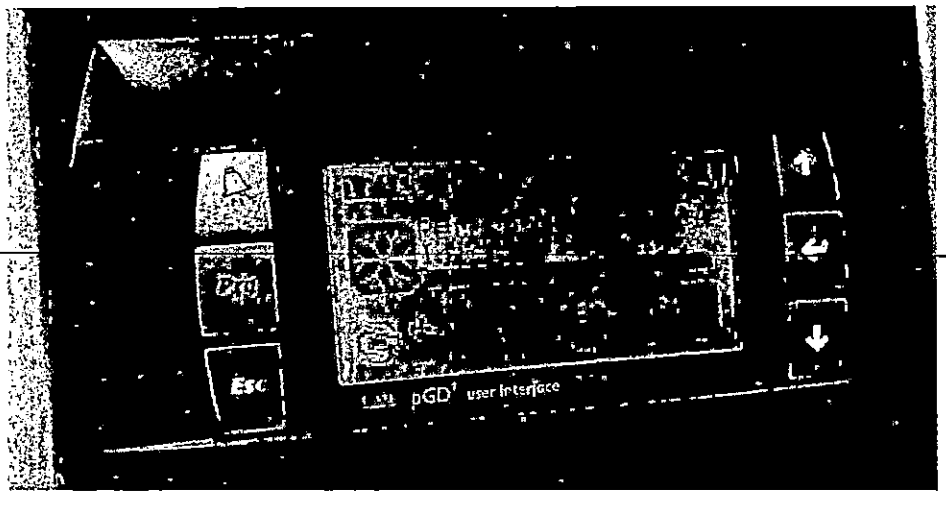


GOBIERNO REGIONAL DE UCAYALI · GOBERNACIÓN · V°B°
GOBIERNO REGIONAL DE UCAYALI · GERENCIA GENERAL · V°B°
OFICINA REGIONAL DE ADMINISTRACIÓN · G.R.U. · V°B°
Gerencia Regional de Planeamiento y Pres. · G.R.U. · V°B°
OFICINA REGIONAL DE ASESORÍA JURÍDICA · G.R.U. · V°B°
GOBIERNO REGIONAL DE UCAYALI · SECRETARÍA GENERAL · V°B°
SUB GERENCIA DE DESARROLLO INSTITUCIONAL · GRPP · V°B°

4. Ir al **TABLERO GENERAL TG (3X220 VAC)** y subir la perilla trifásica "**C1**", con ellos se enciende el "**LCP**" y arranca el evaporador (inicia con una temperatura no menor a **30°C** este valor es normal por el calor acumulado mientras estuvo apagado el **LCP** e inmediatamente procede a encender los 4 switch's de ventiladores del **LCP**.







GOBIERNO REGIONAL DE UCAYALI V°B° GOBERNACIÓN

GOBIERNO REGIONAL DE UCAYALI V°B° GERENCIA GENERAL

OFICINA REGIONAL DE ADMINISTRACIÓN V°B° G.R.U.

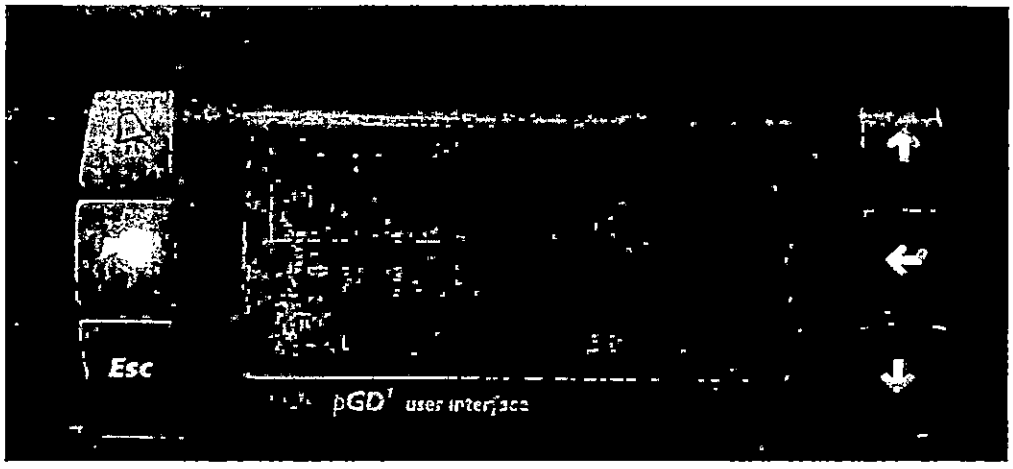
Gerencia Regional de Planeamiento y Pres. V°B° G.R.U

OFICINA REGIONAL DE ASESORÍA JURÍDICA V°B° G.R.U.

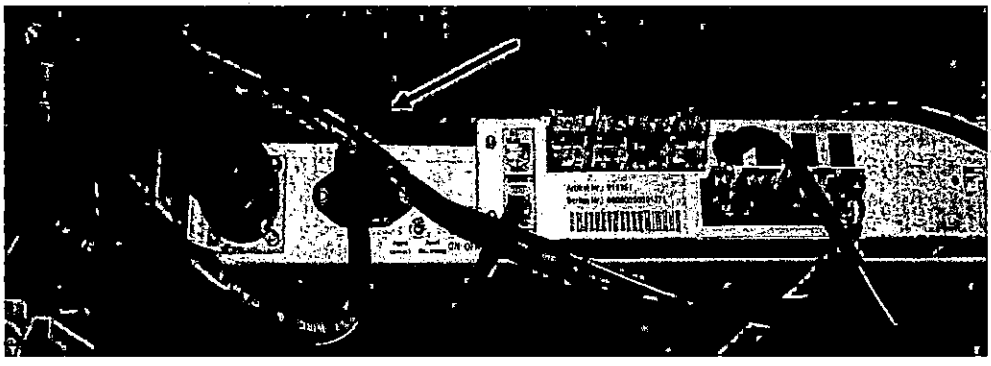
GOBIERNO REGIONAL DE UCAYALI V°B° SECRETARÍA GENERAL

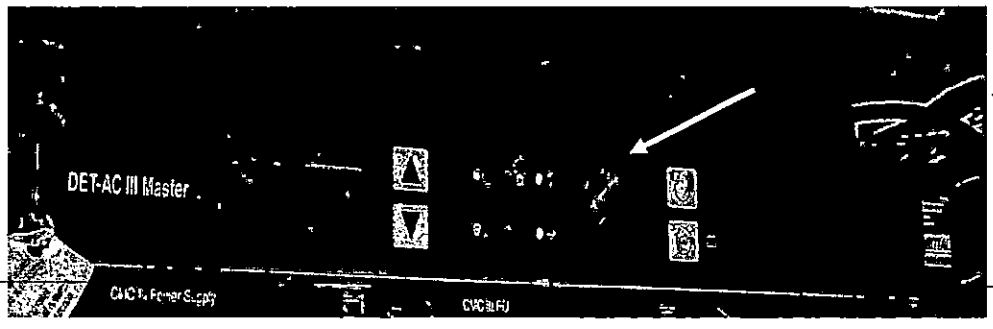
SUB GERENCIA DE DESARROLLO INSTITUCIONAL V°B° GRPP

5. Luego, en el panel del **LCP** cambiamos su estado de "**OFF**" a "**ON**".



6. Finalmente, cuando todo el sistema se encuentre energizado, conectamos el cable de alimentación del **DETAC.**





SECUENCIA DEL CORRECTO APAGADO DEL CENTRO DE DATOS ANTE CUALQUIER EVENTUALIDAD DE ELECTRICIDAD EN EL GOBIERNO REGIONAL DE UCAYALI

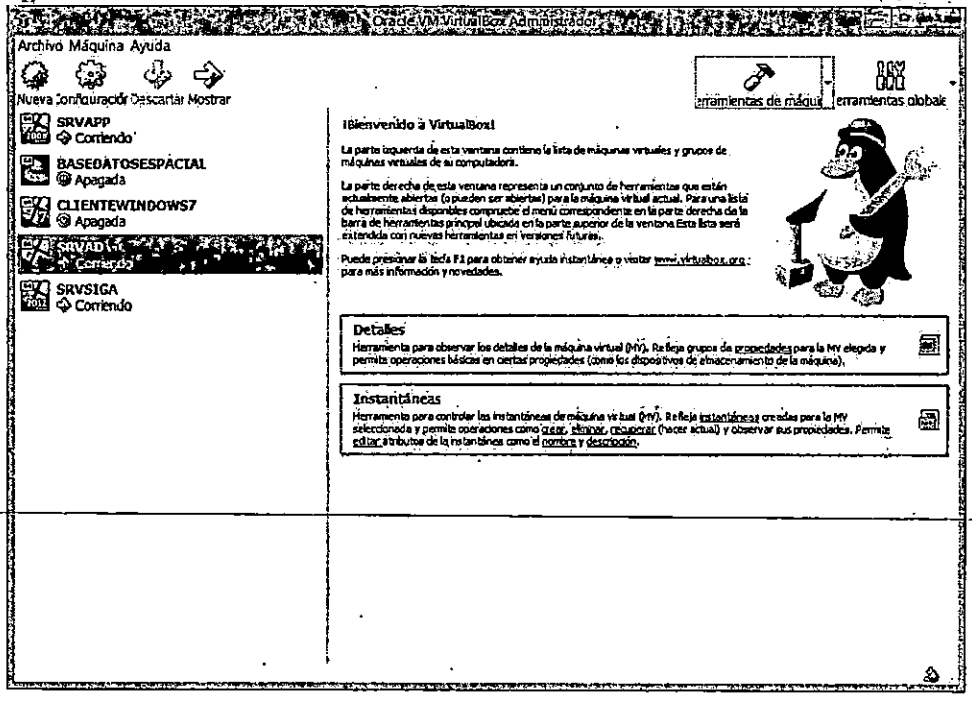
Al presentarse alguna interrupción o corte total de la energía eléctrica en la sede central del Gobierno Regional de Ucayali, lugar en donde se encuentra ubicado el **CENTRO DE DATOS,** se tiene un tiempo estimado de 10 a 15 minutos para poder realizar el correcto apagado de los equipos de servidores y de comunicación.

1. INGRESAR POR MEDIO DE ACCESO REMOTO AL 172.16.3.166 (SERVIDOR SIAF_ARCHIVOS), ABRIR EL PROGRAMA **ORACLE VM VIRTUALBOX ADMINISTRADOR E** INGRESAR A CADA **SERVIDOR VIRTUAL Y APAGAR DE MANERA CORRECTA**.

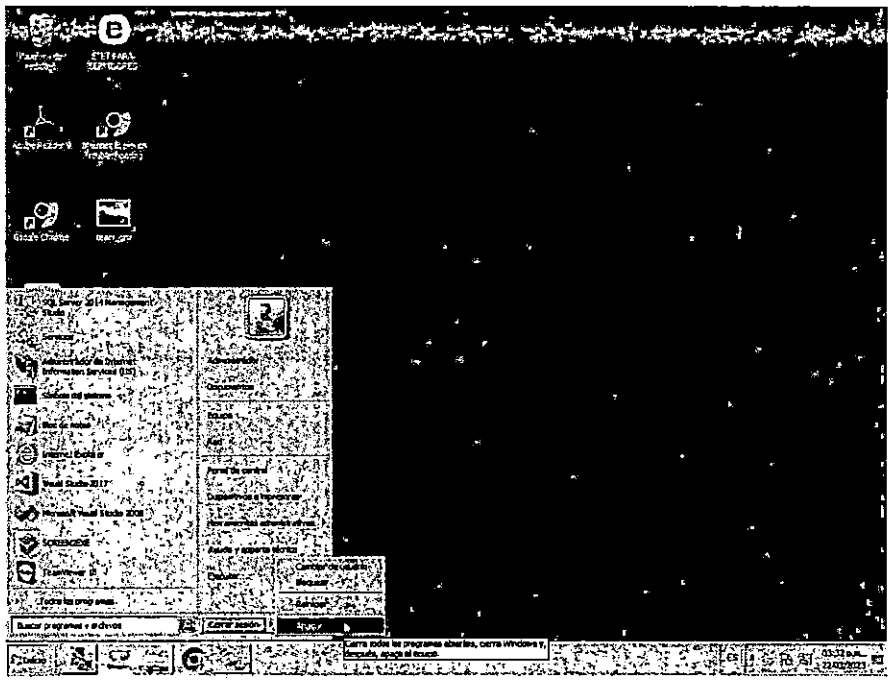
   a. SRVAPP : SERVIDOR VIRTUAL EN DONDE SE ENCUENTRAN LOS SISTEMAS DE INFORMACION DEL GOREU.

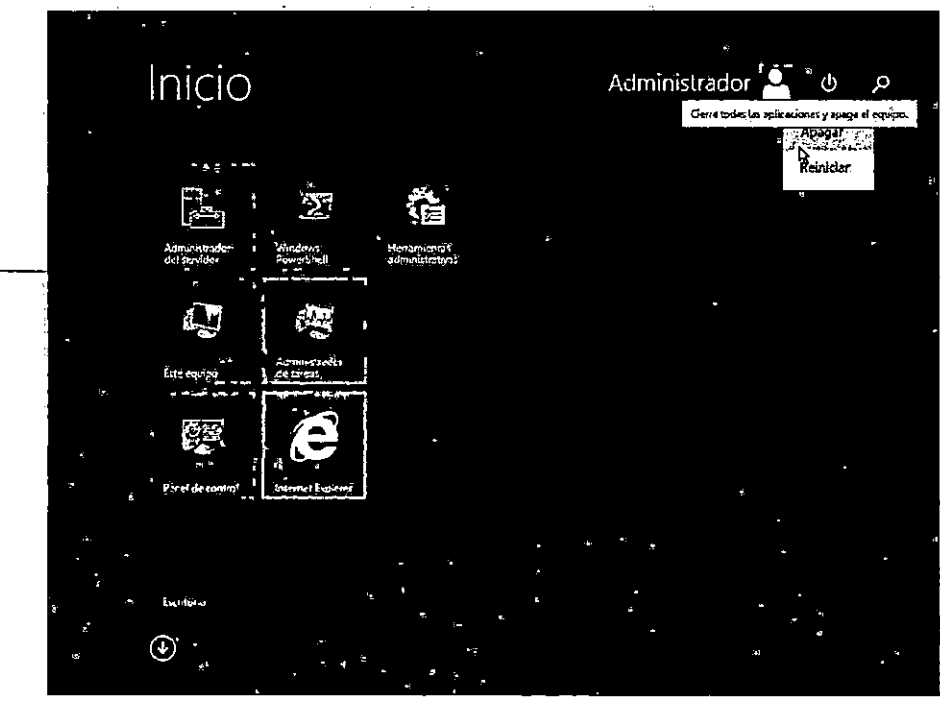
   b. SRVSIGA : SERVIDOR VIRTUAL EN DONDE SE ENCUENTRA LA BASE DE DATOS Y APLICACIÓN DEL SIGA MEF.

   c. EL SRVAD : SERVIDOR DE RESPALDO PARA EL ACTIVE DIRECTORY.



yuda





GOBIERNO REGIONAL DE UCAYALI V°B° GOBERNACIÓN

GOBIERNO REGIONAL DE UCAYALI V°B° GERENCIA GENERAL

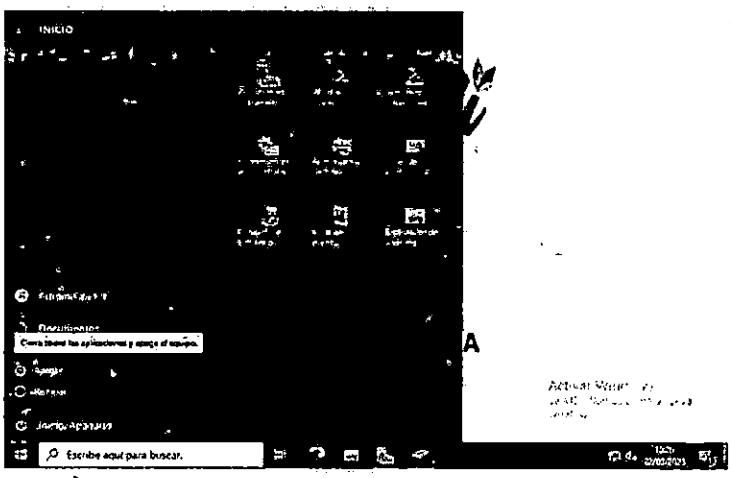
OFICINA REGIONAL DE ADMINISTRACIÓN V°B° G.R.U.

Gerencia Regional de Plan. V°B° G.R.U.

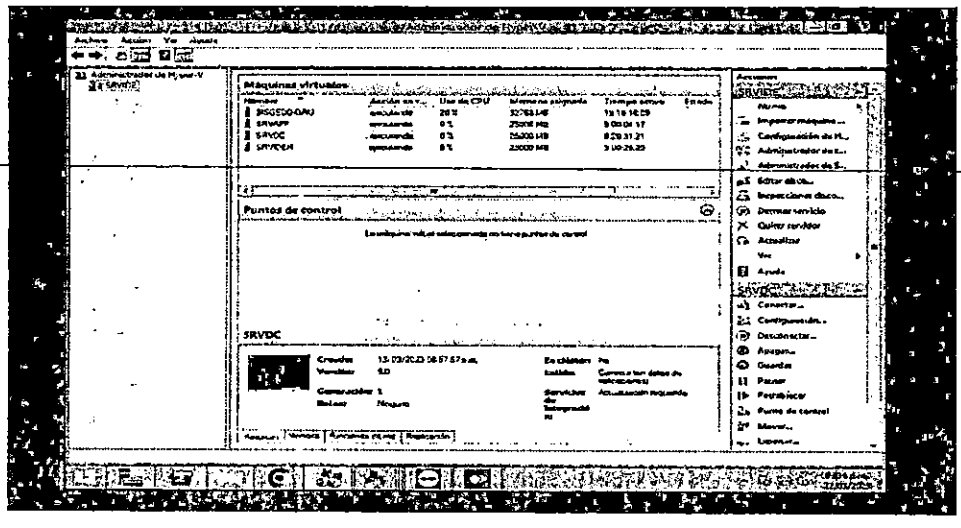
GOBIERNO REGIONAL DE ASESORÍA JURÍDICA V°B° G.R.U.

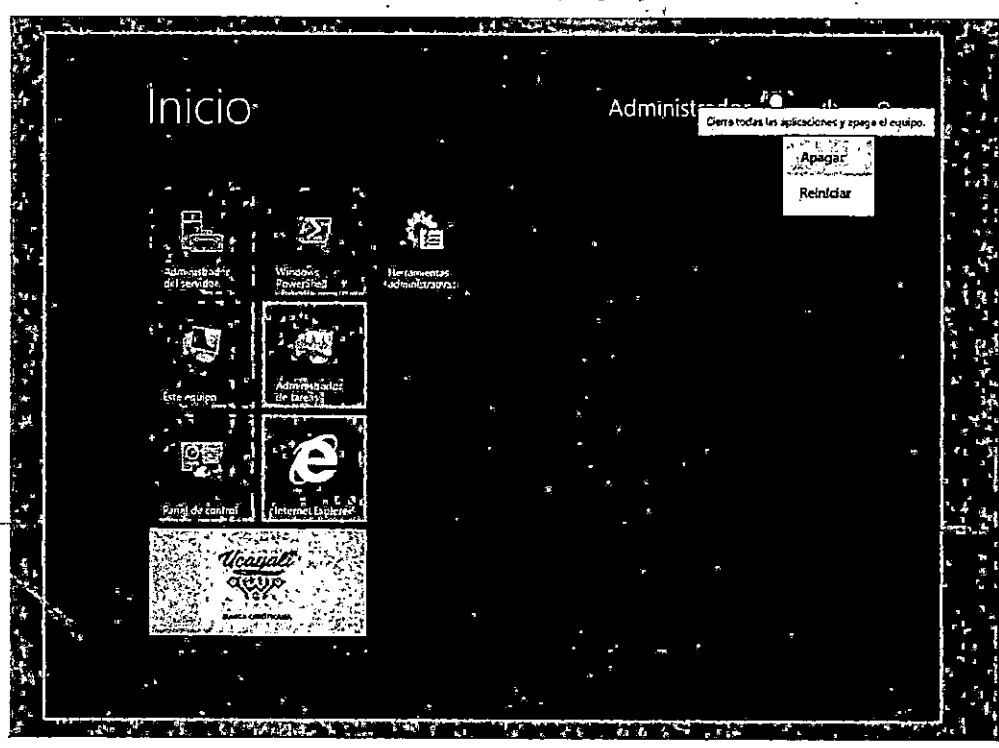
GOBIERNO REGIONAL DE UCAYALI V°B° SECRETARÍA GENERAL

GERENCIA DE DESARROLLO INSTITUCIONAL V°B° SUB GRPP



2. LUEGO INGRESAR POR ACCESO REMOTO AL 172.16.3.167 (SVR IDER), ABRIR EL ADMINISTRADOR DE HYPER-V E INGRESAR A CADA **SERVIDOR VIRTUAL** Y **APAGAR DE MANERA CORRECTA.**
   a. SISGEDO-GRU : SERVIDOR VIRTUAL CON ENTORNO LINUX EN DONDE SE ALOJA EL SISTEMA DE GESTION DOCUMENTARIA. PARA APAGAR SE UTILIZA EL COMANDO **"init 0"**
   b. SRVAPP: SERVIDOR VIRTUAL EN DONDE SE HARA LA MIGRACION DE LOS SISTEMAS DE INFORMACION.
   c. SRVDC : SERVIDOR VIRTUAL DE RESPALDO DEL ACTIVE DIRECTORY.
   d. SRVIDER : SERVIDOR VIRTUAL EN DONDE SE ENCUENTRA ALOJADO ARCHIVOS Y DOCUMENTOS DEL SISTEMA IDER.





GOBIERNO REGIONAL DE UCAYALI
V°B°
GOBERNACIÓN

GOBIERNO REGIONAL DE UCAYALI
V°B°
GERENCIA GENERAL

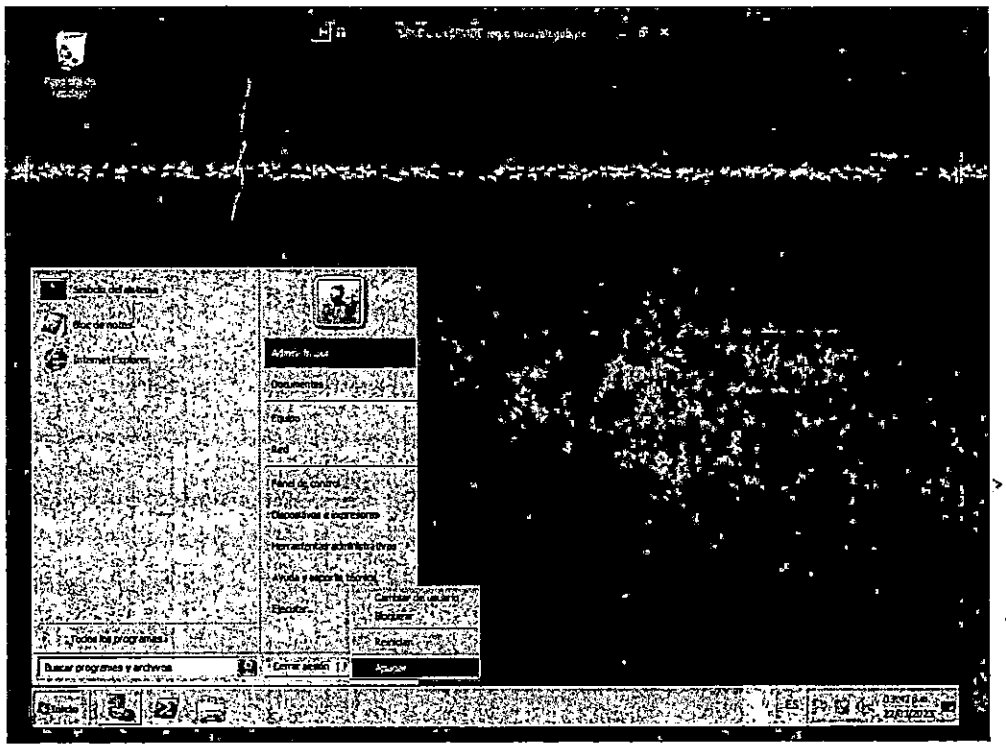
OFICINA REGIONAL DE ADMINISTRACIÓN
V°B°
G.R.U.

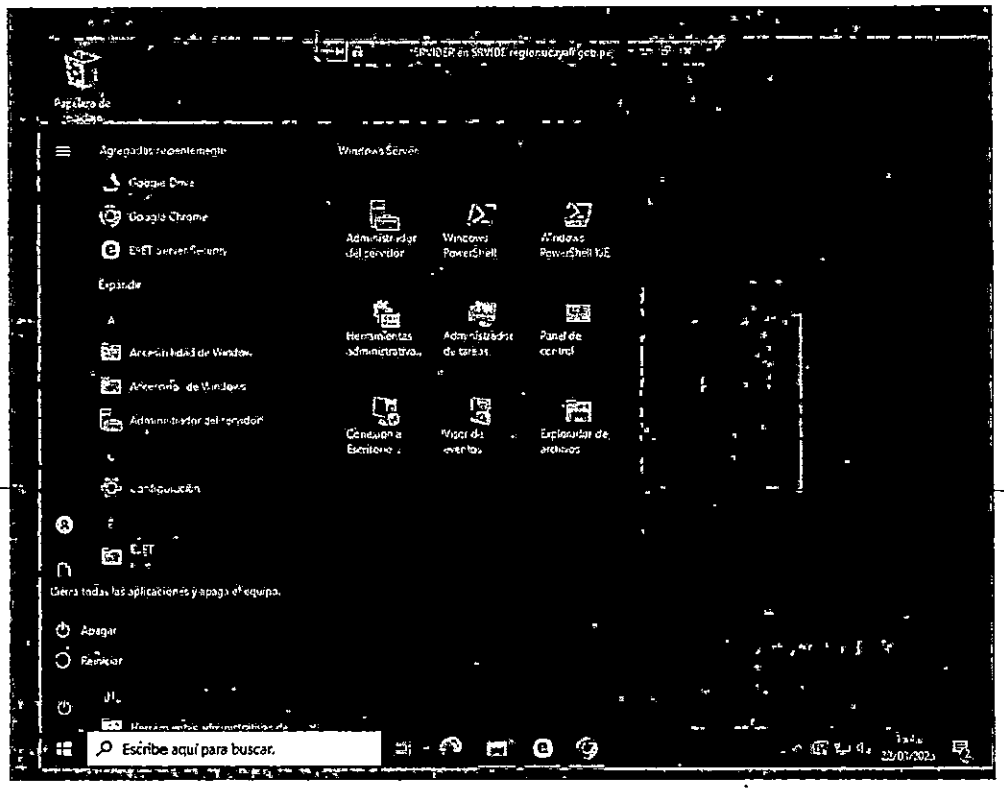
Gerencia Regional de Planeamiento y Presupuesto
V°B°
G.R.U.

OFICINA REGIONAL DE ASESORÍA JURÍDICA
V°B°
G.R.U.

GOBIERNO REGIONAL DE UCAYALI
V°B°
SECRETARÍA GENERAL

SUB GERENCIA DE DESARROLLO INSTITUCIONAL
V°B°
GRPP





GOBIERNO REGIONAL DE UCAYALI
V°B°
GOBERNACIÓN

GOBIERNO REGIONAL DE UCAYALI
V°B°
GERENCIA GENERAL

OFICINA REGIONAL DE ADMINISTRACIÓN
V°B°
G.R.U.

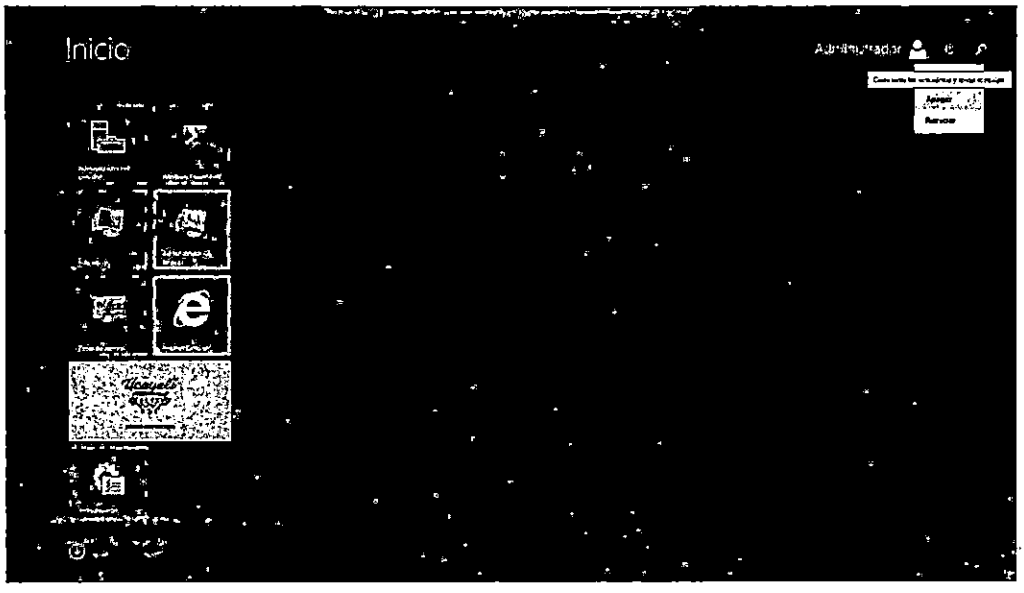
Gerencia Regional de Planeamiento y Pres.
V°B°
G.R.U.

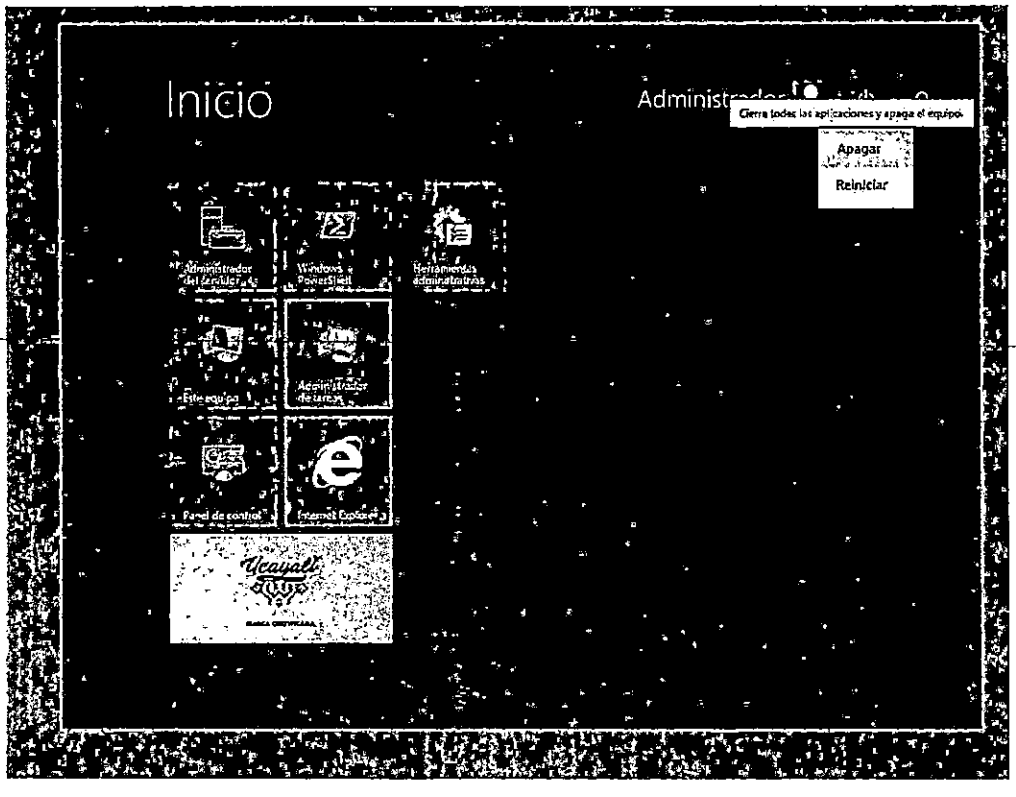
OFICINA REGIONAL DE ASESORÍA JURÍDICA
V°B°
G.R.U.

GOBIERNO REGIONAL DE UCAYALI
V°B°
SECRETARÍA GENERAL

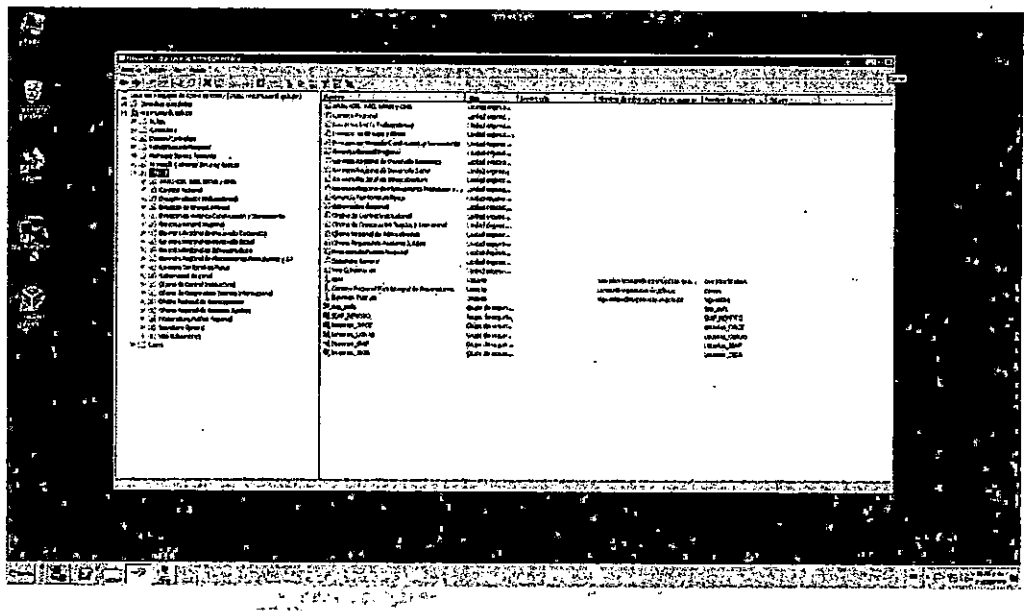
GERENCIA DE DESARROLLO INSTITUCIONAL
V°B°
G.R.U. - GRPP

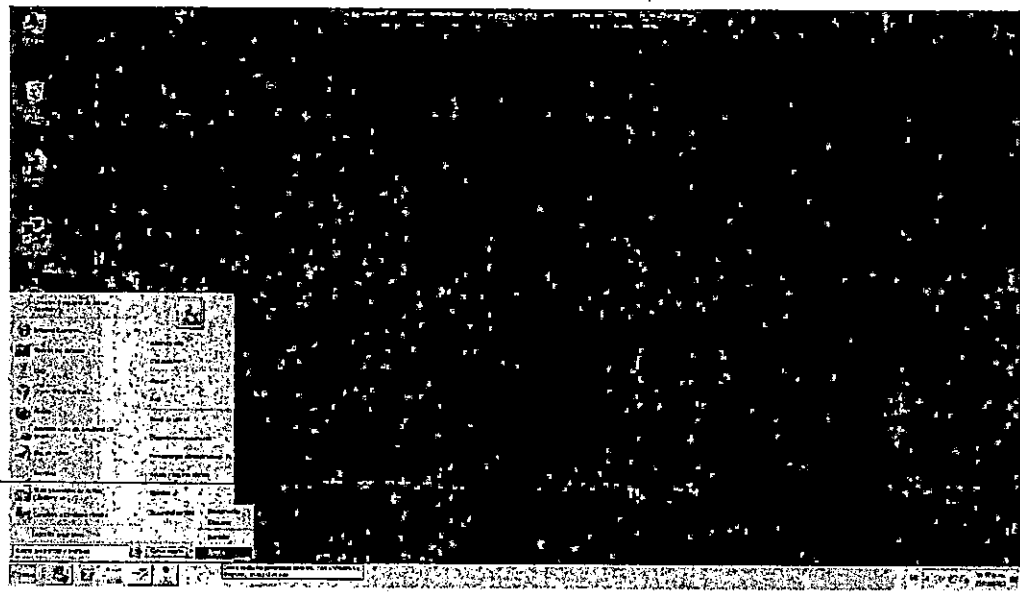
3. LUEGO DE APAGAR LOS SERVIDORES VIRTUALES, PROCEDEMOS CON EL **CORRECTO APAGADO** DE LOS **SERVIDORES FISICOS:**
   a. SIAF_ARCHIVOS(172.16.3.166)
   b. SVR IDE(172.16.3.167)





4. FINALMENTE INGRESAR POR ACCESO REMOTO AL SERVIDOR FISICO **172.16.3.170 (DC02)** CERRAMOS LA **VENTANA DE USUARIOS Y EQUIPOS DE ACTIVE DIRECTORY** Y APAGAMOS DE MANERA CORRECTA.





GOBIERNO REGIONAL DE UCAYALI - GOBERNACIÓN - V°B°

GOBIERNO REGIONAL DE UCAYALI - GERENCIA GENERAL - V°B°

OFICINA REGIONAL DE ADMINISTRACIÓN - G.R.U. - V°B°

Gerencia Regional de Planeamiento y Pres. - G.R.U. - V°B°

OFICINA REGIONAL DE ASESORÍA JURÍDICA - G.R.U. - V°B°

GOBIERNO REGIONAL DE UCAYALI - SECRETARÍA GENERAL - V°B°

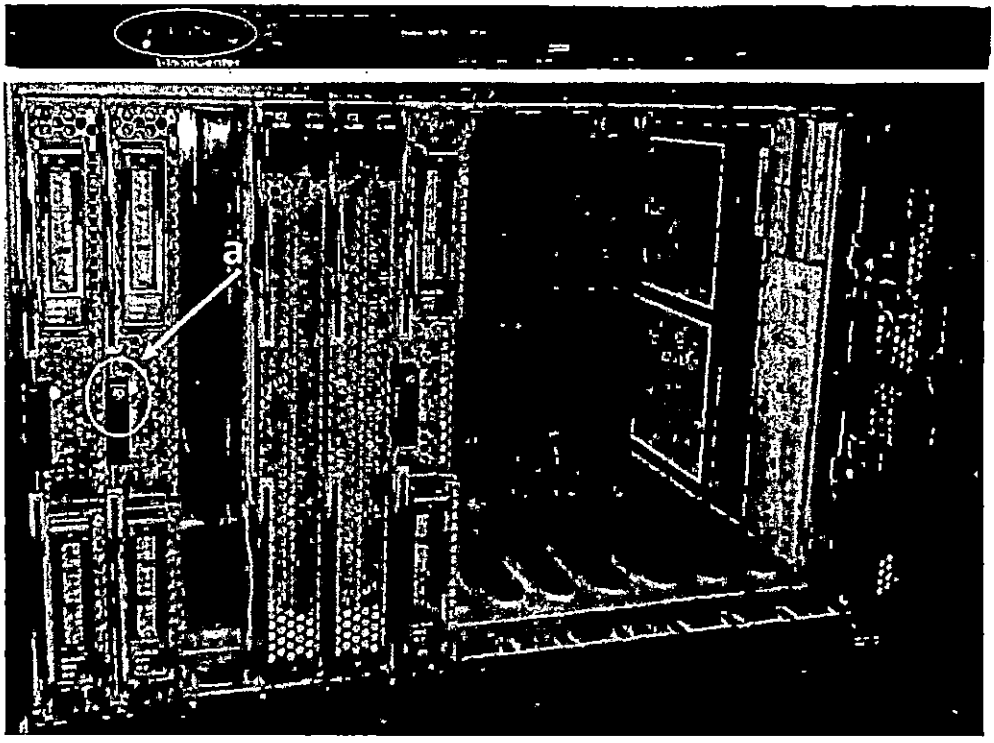
SUB GERENCIA DE DESARROLLO INSTITUCIONAL - GRPP - V°B°

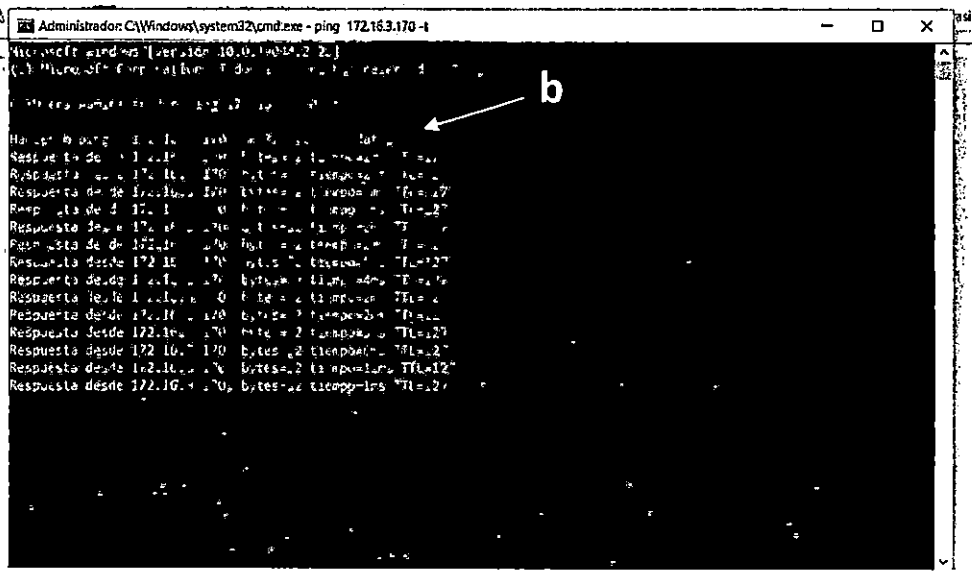
SECUENCIA DEL CORRECTO ENCENDIDO DEL CENTRO DE DATOS ANTE CUALQUIER EVENTUALIDAD DE ELECTRICIDAD EN EL GOBIERNO REGIONAL DE UCAYALI

Luego de presentarse alguna interrupción o corte total de la energía eléctrica en la sede central del Gobierno Regional de Ucayali, lugar en donde se encuentra ubicado el **CENTRO DE DATOS,** esperar que la energía se mantenga estable para proceder al correcto encendido de los equipos de servidores y de comunicación.

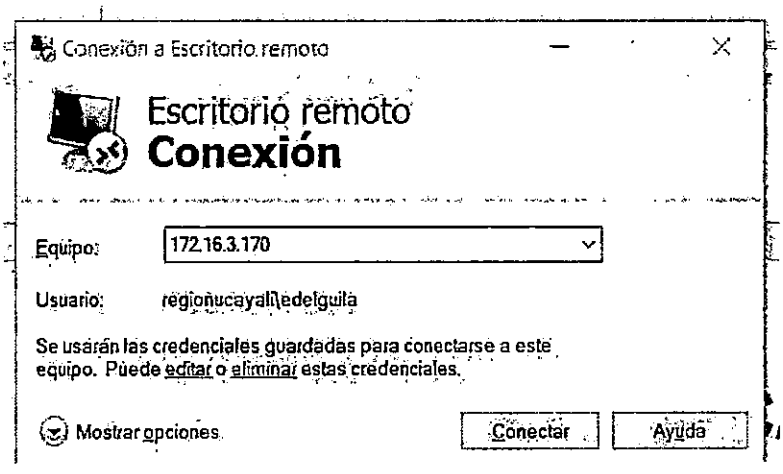
1. PRIMERO VERIFICAMOS QUE ESTE ENCENDIDO EL **BLADE CENTER:**
   a. PRESIONAMOS EL BOTON DE ENCENDER EN EL **BLADE O CUCHILLA DEL DC2**(SE UBICA EN LA SEGUNDA RANURA CONTANDO DE IZQUIERDA A DERECHA).

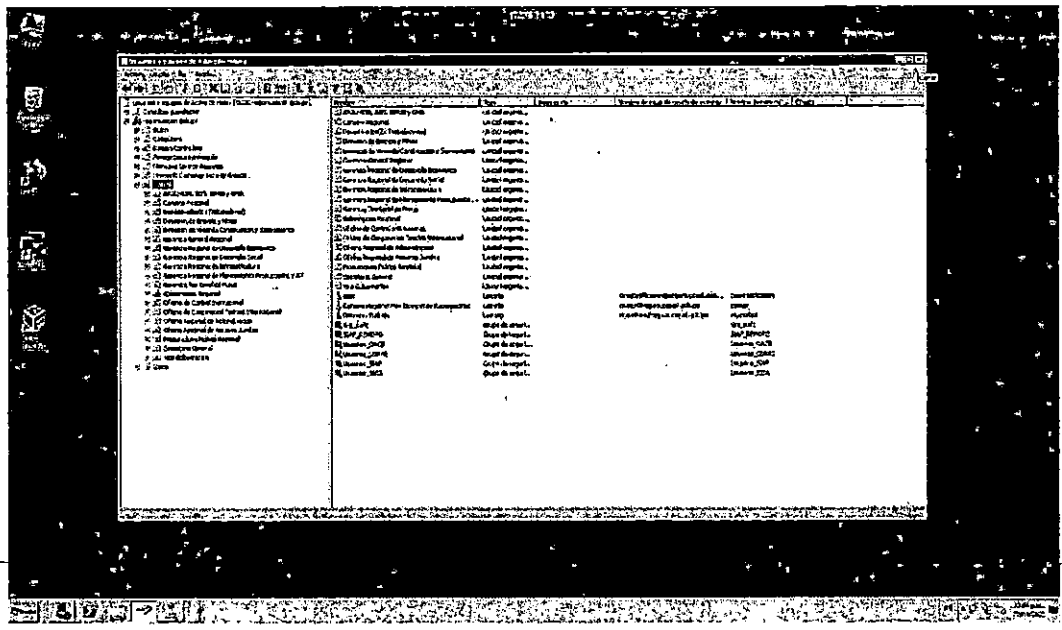
   b. DESDE UNA PC EJECUTAMOS EL CMD Y HACEMOS PING DE CONEXIÓN A LA IP 172.16.3.170 Y VERIFICAMOS QUE HAYA RESPUESTA DE CONEXIÓN.





2. UNA VEZ VERIFICADO EL PUNTO "b" DESDE UNA PC INGRESAMOS DE MANERA REMOTA AL 172.16.3.170 (DC2) PARA ABRIR LA **VENTANA DE USUARIOS Y EQUIPOS DE ACTIVE DIRECTORY**





GOBIERNO REGIONAL DE UCAYALI V°B° GOBERNACIÓN

GOBIERNO REGIONAL DE UCAYALI V°B° GERENCIA GENERAL

OFICINA REGIONAL DE ADMINISTRACIÓN V°B° G.R.U.

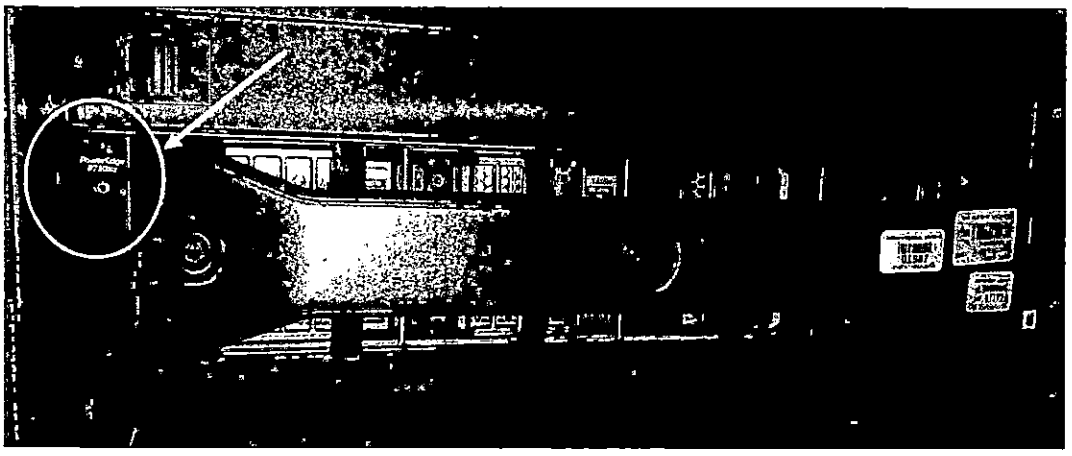
Gerencia Regional de Planeamiento y Pres. V°B° G.R.U.

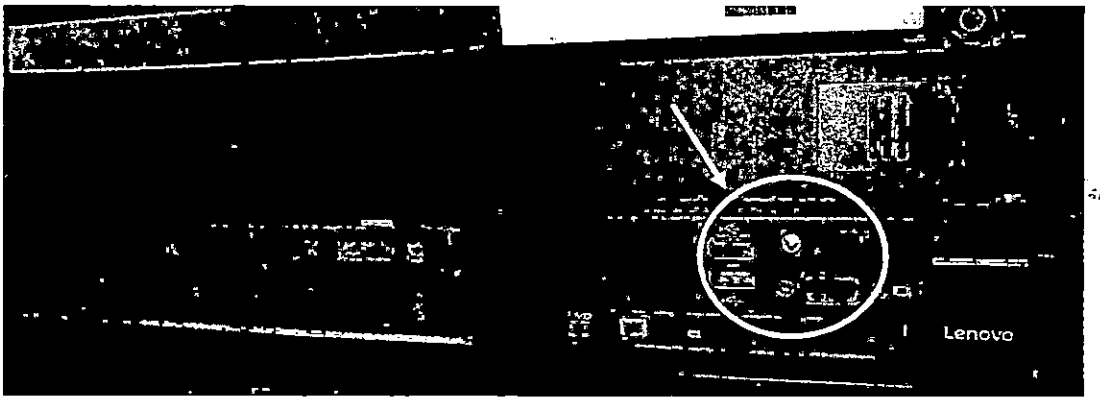
OFICINA REGIONAL DE ASESORÍA JURÍDICA V°B° G.R.U.

GOBIERNO REGIONAL DE UCAYALI V°B° SECRETARÍA GENERAL

SUB GERENCIA DE DESARROLLO INSTITUCIONAL V°B° GRPP

3. LUEGO **ENCENDEMOS DE FORMA MANUAL** EL SERVIDOR FISICO **DELL Y LENOVO.**





GOBIERNO REGIONAL DE UCAYALI V°B° GOBERNACIÓN

GOBIERNO REGIONAL DE UCAYALI V°B° GERENCIA GENERAL

OFICINA REGIONAL DE ADMINISTRACIÓN V°B° G.R.U.

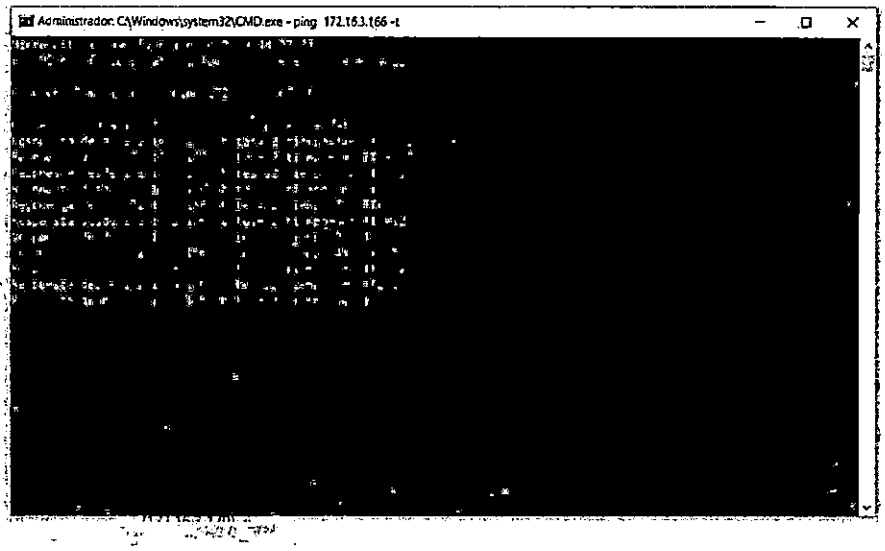
Gerencia Regional de Planeamiento y Presupuesto V°B° G.R.U.

OFICINA REGIONAL DE ASESORÍA JURÍDICA V°B° G.R.U.

GOBIERNO REGIONAL DE UCAYALI V°B° SECRETARÍA GENERAL

GERENCIA DE DESARROLLO INSTITUCIONAL V°B° SUB GRPP

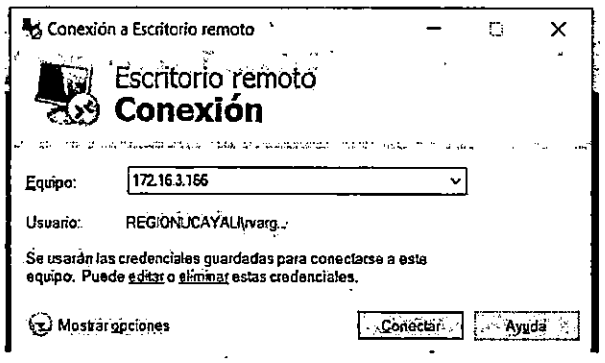
4. DESPUES DE ENCENDER DE FORMA MANUAL AMBOS SERVIDORES FISICOS, DESDE UNA PC EJECUTAMOS EL CMD Y HACEMOS PING PARA VERIFICAR LA CONEXIÓN A LAS SIGUIENTES IP'S:
    a. 172.16.3.166 (SIAF_ARCHIVOS)
    b. 172.16.3.167(SVR IDE)

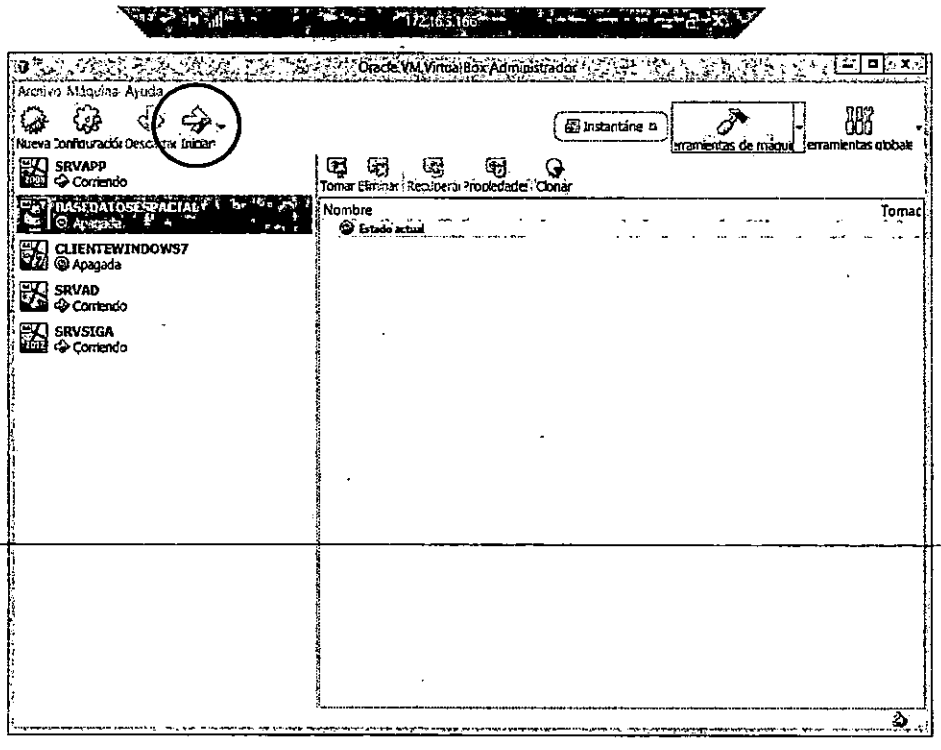


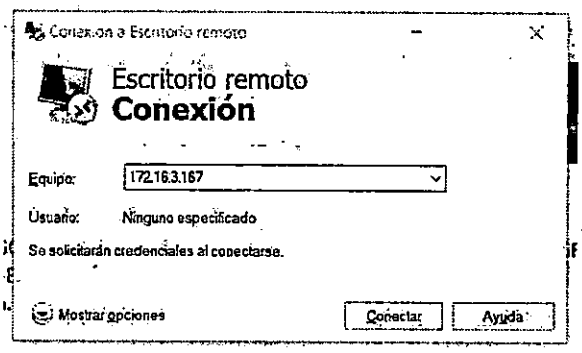
5. LUEGO DE VERIFICAR LA CONEXIÓN A LAS IP'S DEL PUNTO "a" y "b" DEL NUMERAL 4, INGRESAMOS DE MANERA REMOTA A LO SIGUIENTE:

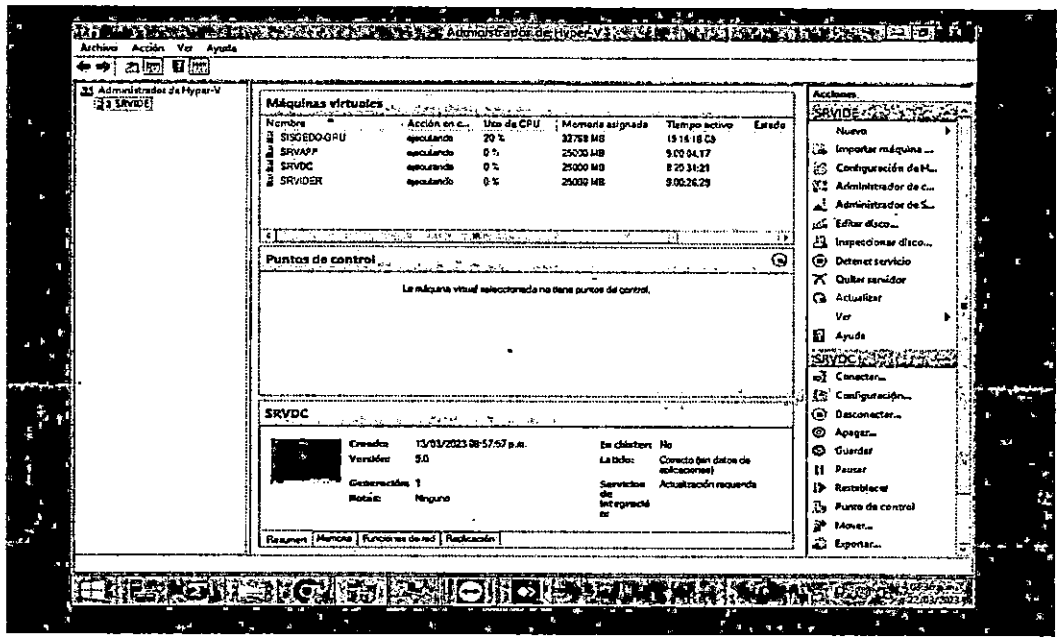
   a. 172.16.3.166 (SIAF_ARCHIVOS), ABRIMOS EL PROGRAMA **ORACLE VM VIRTUALBOX ADMINISTRADOR** Y ENCENDEMOS LOS **SERVIDORES VIRTUALES (SRVAPP, SRVAD Y SRVSIGA)** HACIENDO CLICK EN INICIAR.

   b. 172.16.3.167 (SVR IDE), ABRIMOS EL ADMINISTRADOR DE HYPER-V Y ENCENDEMOS CADA SERVIDOR VIRTUAL









GOBIERNO REGIONAL DE UCAYALI · GOBERNACIÓN · V°B°

GOBIERNO REGIONAL DE UCAYALI · GERENCIA GENERAL · V°B°

OFICINA REGIONAL DE ADMINISTRACIÓN · G.R.U. · V°B°

Gerencia Regional de Planeamiento y Pres. · G.R.U · V°B°

OFICINA REGIONAL DE ASESORÍA JURÍDICA · G.R.U. · V°B°

GOBIERNO REGIONAL DE UCAYALI · SECRETARÍA GENERAL · V°B°

SUB GERENCIA DE DESARROLLO INSTITUCIONAL · GRPP · V°B°