Municipalidad de Lince

RESOLUCIÓN DE GERENCIA N°410-2017-MDL-GM

Lince, 29 NOV 2017

EL GERENTE MUNICIPAL

VISTO: El Informe N° 112-2017-MDL-GPP/SIT, de fecha 17 de noviembre del 2017, mediante el cual la Subgerencia de Informática y Tecnología, eleva el proyectos de "Plan de Contingencia Informática" y;

CONSIDERANDO:

Que, de conformidad al artículo 39 del Reglamento de Organización y Funciones de la Municipalidad Distrital de Lince, aprobado con Ordenanza N° 393-2017-MDL, son funciones de la Subgerencia de Informática y Tecnología, entre otros, formular y actualizar los Manuales de Procedimientos y Directivas relacionadas con los procesos transversales de todas las áreas de la Municipalidad;

Que, de acuerdo a la Resolución de Contraloría N° 320-2006-CG, que aprueba las Normas de Control Interno aplicables a las Entidades del Estado, corresponde a la Institución desarrollar las actividades de control de las tecnologías de información y comunicación que garanticen el procesamiento de la información para el cumplimiento misional y de los objetivos de la organización;

Que, mediante Resolución de Contraloría N° 458-2008-CG se aprobó la "Guía para la implementación del Sistema de Control Interno de las entidades del Estado", con el objetivo de proveer, los lineamientos, herramientas y métodos para la implementación de los componentes y subcomponentes que conforman el Sistema de Control Interno – SCI establecido en la normativa de la materia;

Que, a efectos de implantar controles para el Sistema de Control Interno – SCI para las Tecnologías de la Información y Comunicaciones, el "Plan de Contingencia Informático" correspondiente a lo establecido en la normativa antes referida, en el componente "Información y Comunicación";

Que, la Resolución Ministerial N° 004-2016-PCM Norma Técnica Peruana "NTP-ISO/IEC 27001-2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información" y aprueba el uso obligatorio en todas las entidades integrantes del Sistema Nacional de Informática, de la cual forma parte la Municipalidad de Lince;

Que, la información generada en la Municipalidad de Lince constituye un activo que corresponde ser protegida bajo criterios de buenas prácticas en gestión de la seguridad establecida para este fin;

Municipalidad de Lince

Que, en ese contexto, resulta necesario aprobar el "Plan de Contingencia Informática", que tiene por objetivo de velar por la información, los equipos informáticos, así como garantizar la continuidad de las operaciones y la calidad de los servicios basados en equipos y servicios informáticos que brinda la institución;

Que, mediante el Memorándum N° 015-2017-MDL-GPP/SPIR de fecha 14 de noviembre del 2017, la Subgerencia de Planeamiento, Inversión y Racionalización emite opinión técnica favorable al "Plan de Contingencia Informática" considerando que es un documento específicamente técnico y además cuenta con la estructura mínima requerida;

Estando lo expuesto; de conformidad con lo establecido en la Ordenanza N° 393-2017-MDL que aprueba el Reglamento de Organización y Funciones de la Municipalidad Distrital de Lince; en uso de las facultades conferidas en el Numeral 6.1, Sub numeral 2, del Artículo 6° de la Directiva N° 001-2015-MDL/OAJ "Delegación de Facultades, Atribuciones y Competencias de la Municipalidad Distrital de Lince" aprobada mediante Resolución de Alcaldía N° 107-2015-ALC-MDL; y contando con el visto bueno de la Subgerencia de Planeamiento, Inversión y Racionalización, y la Subgerencia de Informática y Tecnología;

RESUELVE:

ARTÍCULO PRIMERO.- APROBAR, en el **"Plan de Contingencia Informática"** elaborado por la Subgerencia de Informática y Tecnología, el mismo que como anexo forma parte de la presente Resolución.

ARTÍCULO SEGUNDO.- DISPONER, que lo establecido en **"Plan de Contingencia Informática"**, a que se refiere el artículo precedente, es de cumplimiento obligatorio por los funcionarios y servidores de la Municipalidad Distrital de Lince.

ARTÍCULO TERCERO.- DISPONER, la publicación de la presente Resolución y su Anexo en el Portal Institucional (www.munilince.gon.pe) y en el Portal de Transparencia.

REGÍSTRESE, COMUNÍQUESE Y CÚMPLASE.

MUNICIPALIDAD DE LINCE
Eco. IVAN RODRIGUEZ JADROSICH
Gerente Municipal

PLAN DE CONTINGENCIA INFORMÁTICA

MUNICIPALIDAD DE LINCE

GERENCIA DE PRESUPUESTO Y PLANEAMIENTO

SUBGERENCIA DE INFORMÁTICA Y TECNOLOGÍA

PLANES DE ACCIÓN - 2017

ÍNDICE

1. INTRODUCCIÓN:

La Municipalidad Distrital de Lince, considera que la Información de los diferentes Sistema de Base de Datos son el patrimonio principal de toda Institución, por lo que se debe aplicar las medidas de seguridad para protegerla y estar preparados para afrontar contingencias y desastres de diversos tipos.

Esta preocupación debe ser adecuadamente comprendida y compartida por todos los trabajadores de la Institución, la Alta Dirección, Gerentes y Encargados de las diferentes áreas de la Municipalidad Distrital de Lince. Estas deben considerarse como una inversión importante puesto que se logrará mantener la operatividad y la calidad de los servicios.

Dentro de la Planeación Estratégica, se contempla la preparación de Planes Acción. Es decir, se formulan los escenarios no deseados que puedan tener un fuerte impacto en la organización, en sus objetivos o metas; todos aquellos acontecimientos que puedan afectar la producción o la calidad de productos y servicios. A partir de esta planeación, se concibe un plan para evitar o prevenir todo imprevisto o siniestro. Ese es el objetivo primordial de los Planes de Contingencia, proporcionar a la organización alternativas viables para enfrentar este tipo de situaciones.

El Plan de Contingencia, diseñado por la Subgerencia de Informática y Tecnología, nos permitirá planificar y prevenir de la manera más sencilla los futuros eventos que afecten a la entidad. Como también restaurar en el menor tiempo posible los diversos servicios brindados a favor del ciudadano.

2. GENERALIDADES:

2.1. OBJETIVOS:

El objetivo del presente documento es señalar las situaciones de riesgo de mayor impacto y alcance relacionados a los servicios informáticos críticos para la organización. Así como identificar sus causas, efectos, y plantear soluciones para brindar la correspondiente salida de contingencia, proponiendo a su vez mecanismos que garanticen la continuidad de los servicios y la operatividad de las actividades que dependen de plataformas informáticas.

Finalmente, este documento pretende indicar los pasos a seguir frente a las circunstancias de mayor riesgo para la institución.

2.2. BASE LEGAL:

- Ley N.° 30096, Ley de Delitos Informáticos.
- Decreto Supremo N.° 024-2006-PCM, que aprueba el Reglamento de la Ley N° 28612 - Ley que norma el uso, adquisición y adecuación del software en la Administración Pública.
- Resolución Jefatural N.° 076-95-INEI, que aprueba la Directiva N.° 007-95- INEI/SJI, "Recomendaciones Técnicas para la Seguridad e Integridad de la información que se procesa en la Administración Pública".

- Resolución Jefatural N.° 140-95-INEI, que aprueba la Directiva N.° 010-95- INEI/SJI, "Recomendaciones Técnicas para la Organización y Gestión de los Servicios Informáticos para la Administración Pública".
- Resolución Jefatural N.° 386-2002-INEI, que aprueba la Directiva N.° 16-2002-INEI/DTNP, "Normas Técnicas para el Almacenamiento y Respaldo de la Información procesada por las Entidades de la Administración Pública".

3. SITUACIONES DE CONTINGENCIA

Lista de Situaciones Críticas de mayor urgencia que requieren un plan de contingencia, por su posible impacto en la institución.

3.1. Falla de Servidores:
Interrupción del funcionamiento de los Servidores que contienen las bases de datos de las principales aplicaciones y servicios proveídos a la institución para la atención de los contribuyentes y la gestión y comunicación interna.

3.2. Corte de Energía:
Interrupción del fluido eléctrico del cual dependen todos equipos eléctricos, incluyendo todo el equipamiento informático y Servidores.

3.3. Falla de Red:
Interrupción de las comunicaciones por transferencia de datos, dejando inhabilitados diversos servicios, incluyendo el Portal Web Institucional y

3.4. Corte de Internet:
Interrupción del servicio de internet, el cual inhabilita la comunicación externa para la entrega y recepción de datos, tales como el funcionamiento de la Pagina Web, Correo Electrónico, Cobro mediante P.O.S.

3.5. Incendio y Sismo

- Incendio: Combustión de elementos inflamables en el área o zonas aledañas, arriesgando la integridad física de equipos y la vida de los colaboradores y demás personas que se encuentren en el recinto o zonas aledañas.
- Sismo: Movimiento telúrico por el que puede colapsar la infraestructura y provocar la caída de objetos, arriesgando la integridad física de equipos y la vida de los colaboradores y demás personas que se encuentren en el recinto o zonas aledañas.

4. RESUMEN GENERAL

Esquema de relación establecida entre las principales situaciones de riesgo con las causas, efectos y acciones de respuesta para preservar la continuidad de los servicios o minimizar las pérdidas con los recursos y alternativas que tiene actualmente la institución.

SITUACIÓN	EFECTO	CAUSA	ACCIÓN
1.- FALLA DE SERVIDORES	Corte de Internet --- Interrupción de Aplicaciones y Servicios --- Pérdida de Información	**Falla de Energía**	**6.1.1.** Reparación de fluido eléctrico en Sala
		Falla en Fuente de Poder	**6.1.2.** Cambio de Fuente de Poder
		Falla de Disco Duro	**6.1.3.** Cambio de Disco Duro
		Falla Lógica o Física	**6.1.4.** Diagnóstico y Reparación de Equipos
		Recalentamiento	**6.1.5** Regular temperatura y coordinar con Proveedor

SITUACIÓN	EFECTO	CAUSA	ACCIÓN
2.- CORTE DE ENERGÍA	Paralización de todos los servicios dependientes de Energía.	**Corte Programado o Intempestivo**	**6.2.1** Apagado de Servidores
			6.2.2. Encendido de Servidores

SITUACIÓN	EFECTO	CAUSA	ACCIÓN
3.- FALLA DE RED	Interrupción de: Internet, Portar y Correo, Sistemas de Pago, Aplicación.	**Falla de Equipos de Comunicación y Cableado.**	**6.3.1.** Verificación de Conectividad de Servidores y Switchs

SITUACIÓN	EFECTO	CAUSA	ACCIÓN
4.- CORTE DE INTERNET	- Caída del Portal - Inhabilitación de SIAF, Telebanking, POS, SIGA	**Falla del Proveedor**	**6.4.1** Coordinación con Proveedor
		Rotura de Fibra	**6.4.2** Cambio de Conexión a Internet por Radio Enlace
			6.4.3 Ubicación del Corte de Fibra Óptica

SITUACIÓN	EFECTO	CAUSA	ACCIÓN
5.- INCENDIO	Destrucción total de equipos e inmueble, y pérdida de información.	Externas al área. Recalentamiento de Equipo.	**6.6.1** Respaldo de Emergencia Llamar Bomberos 116 o 471-6442.

5. MEDICIÓN DE NIVEL DE IMPACTO Y RIESGO:

Para la medición del Nivel de Impacto se utilizan tres (03) Conceptos de Riesgo recurrentes en cada escenario que requiera Acciones de Contingencia. A su vez, se utilizan tres (03) Niveles de Riesgo para medir el grado situacional actual para cada uno de estos casos.
Estos cuadros de medición estarán incluidos en cada una de las *SITUACIONES DE RIESGO* expresadas en el punto 6 *"PLANES DE ACCIONES"*.

Conceptos y Niveles de Riesgo e Impacto:

- **Impacto en la Organización:** Indica cuánto podría impactar en la organización determinada situación de riesgo.
- **Situación de Repuestos:** Indica el nivel de riesgo frente a la necesidad de contar con repuestos para responder a una situación de riesgo.
- **Redundancia:** Indica el nivel de riesgo en el que se encuentra la institución frente a los sistemas redundantes con los que cuente actualmente.

Cuadro de Medición:

It.	Conceptos de Riesgo	Riesgo Mínimo	Riesgo Moderado	Riesgo Máximo
1	Impacto en organización	0	3	5
2	Situación de Repuestos	0	3	5
3	Redundancia	0	3	5
	TOTAL	**0**	**9**	**15**

Nivel de impacto para cada Concepto de Riesgo:
Interpretación de cada nivel para cada Concepto de Riesgo:

1

Impacto en Organización	Nivel Impacto
Mínimo	0
Servicios no críticos	3
Servicios Críticos	5

2

Situación de Repuestos	Nivel Impacto
Óptima cantidad	0
Poca cantidad	3
Insuficiente o ninguna	5

3

Redundancia implementada	Nivel Impacto
Implementada o No requiere	0
Mecanismo alternativo	3
Ninguna	5

6. PLANES DE ACCIÓN:

Pasos a seguir como *Acciones de Contingencia* frente a las diferentes **Situaciones Críticas**:

Or	Acciones	Código	Índice	SITUACIONES				
				6.1.	6.2.	6.3.	6.4.	6.5.
				A	B	C	D	E
				Falla de Servidores	Corte de Energía	Falla de Red	Corte de Internet	Incendio o Sismo
1	Reparación de Fluido Eléctrico	PCA1	6.1.1.	X				
2	Cambio de Fuente de Poder	PCA2	6.1.2.	X				
3	Cambio de Disco Duro	PCA3	6.1.3.	X				
4	Diagnóstico y Reparación de Equipos	PCA4	6.1.4.	X		X		
5	Reajuste de Temperatura en Sala de Servidores	PCA5	6.1.5.	X				X
6	Apagado de Servidores	PCB1	6.2.1.	X	X			
5	Encendido de Servidores	PCB3	6.2.2.	X	X			
6	Verificación de Conectividad de Servidores y Switchs	PCC1	6.3.1.	X		X		
7	Coordinación con Proveedor de Internet	PCD1	6.4.1				X	
8	Cambio de Conexión a Internet por Radio Enlace	PCD2	6.4.2				X	
9	Ubicación del Corte de Fibra Óptica	PCD3	6.4.3				X	
10	Respaldo de Emergencia físico y virtual	PCE1	6.5.1.	X				X

6.1 FALLA DE SERVIDORES (Código A)

Acción de Contingencia	***6.1.1.Reparación de fluido eléctrico en Sala de Servidores***		Código:	**PCA01**
SITUACIÓN	6.1. FALLA DE SERVIDORES (**A**)	**Actores**	Subgerente, Soporte Técnico	
Causa:	Falla de Energía	**Efecto:**	Servidor no enciende Paralización de Servicios.	

Detalle del Problema:

Un problema en los elementos que permiten canalizar el fluido de energía eléctrica.

Verificación:

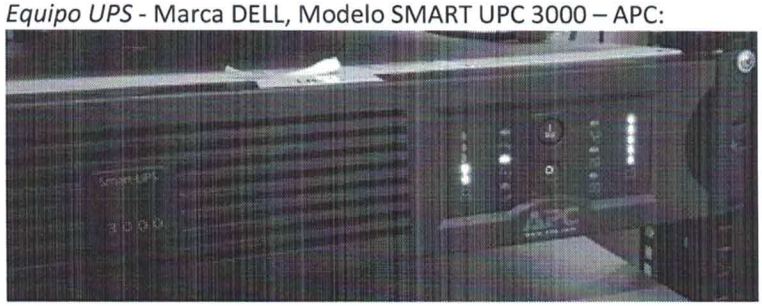
Frente a lo que podría significar un corte de energía, se requiere empezar con los elementos que podrían causar la interrupción del fluido eléctrico, verificando para ello el adecuado funcionamiento de lo siguiente:

- Conexión de cables de poder.
- Encendido de regleta eléctrica.
- Conexión de cables del equipo UPS al servidor.
- Carga del equipo UPS.

Solución:

- Corregir las posibles fallas en las conexiones eléctricas en la Sala de Servidores de los diversos equipos, extensiones y UPS.
- Encender las regletas eléctricas.
- Cargar completamente los equipos UPS antes de encender los servidores.

Equipo UPS - Marca DELL, Modelo SMART UPC 3000 – APC:



Este equipo UPS indica el nivel de carga con 5 luces verticales en su lado izquierdo, como se aprecia en la imagen.

Nivel de Impacto y Riesgo:

It	**Situación e Impacto**	**Nivel de Riesgo**	**Evaluación**
1	Impacto organización	5	Adquirir repuestos accesibles para Reducir Riesgo a un **Nivel Medio** de 10 puntos.
2	Situación de Repuestos	5	
3	Redundancia	5	
	TOTAL	**15**	**Alto**

Adquisición de Repuestos:
Es necesario contar con los repuestos para recuperar lo antes posible la operatividad de los servidores y retomar los servicios interrumpidos, lo cual sería fácilmente superable de tener estos elementos a la mano, alguno de ellos básicos y accesibles, pero que al no contar con ellos podría con facilidad interrumpir el funcionamiento de los servidores y paralizar los servicios de la institución. Por ello se requiere contar con al menos un par de cables de poder, regleta múltiple (extensión), supresor de picos y adicionalmente un equipo UPS de respaldo.

Sistema Redundante:
Para garantizar el funcionamiento continuo es necesario contar con un sistema redundante, el cual permitirá que frente a una falla similar los servicios que dependen de los servidores no se vean afectados, así como la calidad de atención a los contribuyentes.

Acción de Contingencia	*6.1.2. Cambio de Fuente de Poder*		Código	PCA02
SITUACIÓN	6.1. FALLA DE SERVIDORES (**A**)	**Actores**	Subgerente, Soporte Técnico	
Causa:	Falla de Fuente de Poder	**Efecto:**	Corte de Internet. Paralización de Servicios.	

Detalle del Problema:

La fuente de poder es un elemento indispensable para alimentar de energía eléctrica a los diversos componentes de cada servidor; su falla implica el apagado del equipo o la falla de alguno de sus componentes, lo que paralizaría los servicios que suministra el servidor.

Verificación:

Si el equipo no enciende y se debe verificar que el equipo UPS y las conexiones eléctricas funcionen adecuadamente para descartar así que se trate solo de un problema eléctrico externo. Si las conexiones eléctricas funcionan y el equipo no enciende, se tendrá que revisar la fuente de poder del servidor que se esté examinando y comprobar si es una falla de conexión o si es necesario cambiar ese elemento.

Solución:

Una vez confirmada la falla de la fuente de poder se procederá a desmontar el servidor para cambiar el mencionado componente y reemplazarlo con otro en buen estado.

Fuente de Poder estándar:

La fuente de poder es indispensable para el funcionamiento de los servidores; sin uno completamente operativo un servidor estaría totalmente inutilizable, paralizando por completo todos los servicios e información que este equipo brinde a los diversos procesos y sistemas que dependan de este equipo.

Nivel de Impacto y Riesgo:

It	Situación e Impacto	Nivel de Riesgo	Evaluación
1	Impacto organización	5	Adquirir **Fuentes de Poder** para Reducir Riesgo a un **Nivel Medio** de 10 puntos.
2	Situación de Repuestos	5	
3	Redundancia	5	
	TOTAL	**15**	**Alto**

MUNICIPALIDAD DISTRITAL DE LINCE
V°B°
Subgerencia de Informática y Tecnología

Adquisición de Repuestos:
Para reducir el tiempo de respuesta en caso se de una falla de este tipo, sería necesario y factible contar con Fuentes de Poder de repuesto, por lo menos una (01) Fuente de Poder por cada Servidor. Sin estos repuestos la paralización por este tipo de fallas podría prolongarse, afectando seriamente la atención a los contribuyentes y el cumplimiento de las tareas de las diversas áreas.

Sistema Redundante:
Para garantizar el funcionamiento continuo es necesario contar con un sistema redundante, el cual permitirá que frente a una falla similar los servicios que dependen de los servidores no se vean afectados, así como la calidad de atención a los contribuyentes.

Acción de Contingencia	***6.1.3. Reparación de Disco Duro***		Código	**PCA03**
SITUACIÓN	6.1. FALLA DE SERVIDORES (**A**)	**Actores**	Subgerente, Soporte Técnico	
Causa:	Falla del Disco Duro.	**Efecto:**	Paralización de Servicios. Pérdida de Información.	

Detalle del Problema:

Los discos duros son susceptibles a fallar y con ello podría interrumpirse o poner en riesgo el funcionamiento de los servidores y los servicios que brindan

Verificación:

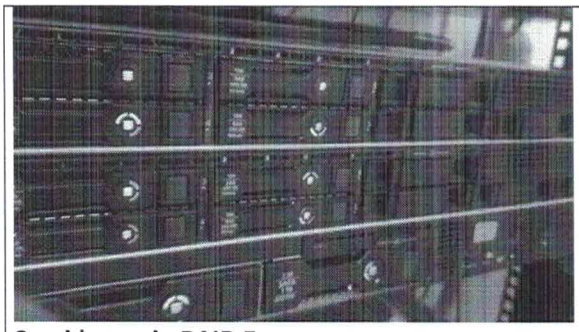
Verificar si el Servidor posee el sistema de seguridad RAID. A continuación una breve lista de los servidores físicos ubicados en la Sala de Servidores:

Item	Tipo	Modelo o Case	Servicio	RAID5	Discos
1	PC	Cool Master	Antivirus		1
2	PC	Haliar	Internet		1
3	Servidor	HP ProLiant DL 360 Gen9	Base de datos de Rentas y Catastro	X	4
4	Servidor	HP ProLiant DL 360 Gen9	Base de datos de Trámite, Información de Usuarios, Servidor Wem, SIGA info, Observatorio, Respaldo de Domicilio, Aplicaciones.	X	4
5	Servidor	HP ProLiant DL 320e Gen8 V2	Servidor de Dominio, SIAF, Máquina Virtual de Intranet y Página Web.		2
6	PC	Antryx	Correos		1
7	Servidor	HP ProLiant DL 380 G5	SIGA		2
8	Servidor	HP ProLiant DL 380 G5	Virtual, BackUp Correos		8

Servidores con sistema RAID 5:

Para el caso de los servidores con sistema RAID 5, la alerta de algún disco fallado se mostrará con un cambio en el color en la luz led de cada disco duro. Este sistema permite continuar brindado los servicios a pasar del desperfecto de alguno de los discos gracias al respaldo que provee el sistema de RAID 6.

Dos servidores HP ProLiant DL 360 Gen9 y un servidor HP ProLiant DL 320e Gen8 V2:



Servidores sin RAID 5:
El resto de servidores solo podrá evidenciar una falla en sus discos duros al no levantar el sistema a pesar de poder encender el equipo.

Solución:

Servidores con sistema RAID 5:
Una vez que se verifique que un disco duro ha fallado mediante el color de la luz led de alguno de los discos del servidor, se podrá hacer el cambio del mismo retirando el disco fallado, sin necesidad de apagar el equipo o detener los servicios.

Servidores sin RAID 5:
En caso de servidores sin RAID 5, se deberá realizar un reemplazo común del disco duro; lo que requerirá apagar el servidor, desmontarlo, verificar el disco, copiar la información respaldada en un nuevo disco o el mismo si este puede funcionar luego de un formateo u otro tratamiento.

Nivel de Impacto y Riesgo:

It	Situación e Impacto	Nivel de Riesgo	Evaluación
1	Impacto organización	5	Adquirir **Discos Duros** para Reducir Riesgo a un **Nivel Medio** de 10 puntos.
2	Situación de Repuestos	5	
3	Redundancia	5	
	TOTAL	**15**	**Alto**

Adquisición de Repuestos:
Para reducir el tiempo de respuesta en caso se de una falla de este tipo, sería necesario y factible contar Discos Duros de repuesto, por lo menos un (01) Disco Duro por cada Servidor. Sin estos repuestos la paralización por este tipo de fallas podría prolongarse afectando seriamente la atención a los contribuyentes y el cumplimiento de las tareas de las diversas áreas.

Sistema Redundante:
Para garantizar el funcionamiento continuo es necesario contar con un sistema redundante, el cual permitirá que frente a una falla similar los servicios que dependen de los servidores no se vean afectados, así como la calidad de atención a los contribuyentes.

MUNICIPALIDAD DISTRITAL DE LINCE
V°B°
Subgerencia de Informática y Tecnología

Acción de Contingencia	***6.1.4. Diagnóstico y Reparación de Equipo***		Código	**PCA04**
SITUACIÓN	6.1. FALLA DE SERVIDORES (**A**)	**Actores**	Subgerente, Soporte Técnico	
Causa:	Falla lógica o física de Servidores.	**Efecto:**	Corte de Internet. Paralización de Servicios. Pérdida de Información.	

Detalle del Problema:

Los equipos de cómputo son susceptibles a desperfectos físicos o lógicos, los cuales podrían causar la interrupción de los servicios, reinicio o apagado de los equipos.

Verificación:

En caso de una falla en los servicios basados en el funcionamiento de los Servidores, se procede a realizar un diagnóstico del equipo de cómputo en la sala de servidores basado en los siguientes síntomas del equipo de cómputo:

- No enciende.
- Se cuelga o paraliza.
- Falla en la ejecución de procesos.
- Se reinicia.

Solución:

Se evalúa si se trata de un problema lógico o físico, para realizar la configuración o formateo correspondiente o de ser físico, el reemplazo de un elemento o cambio completo del equipo, si fuese el caso.

- *Reparación de Falla Lógica*:
  Opciones de reparación para fallas Lógica.
  - Depuración de archivos corruptos
  - Liberación de espacio
  - Actualización necesaria.
  - Reinicio del equipo físico o virtual
  - Reconfiguración de Servidores
  - Formateo de Servidor y Reposición del Back

- *Reparación de Falla Física*:
  - Reemplazo de un elemento, pieza o componente, tales como tarjetas, memoras, procesadores, disco duro, entre otros.
  - Repotenciación mediante cambio de componente.
  - Cambio del equipo completo.

Nivel de Impacto y Riesgo:

It	**Situación e Impacto**	**Nivel de Riesgo**	**Evaluación**
1	Impacto organización	5	Adquirir **diversos repuestos** para Reducir Riesgo a un **Nivel Medio** de 10 puntos.
2	Situación de Repuestos	5	
3	Redundancia	5	
	TOTAL	**15**	**Alto**

Adquisición de Repuestos:
Para reducir el tiempo de respuesta en caso se de una falla de elementos diversos, se requiere contar con algunas piezas de repuesto al momento.

Sin estos repuestos la paralización por este tipo de fallas podría prolongarse afectando seriamente la atención a los contribuyentes y el cumplimiento de las tareas de las diversas áreas.

Sistema Redundante:
Para garantizar el funcionamiento continuo es necesario contar con un sistema redundante, el cual permitirá que frente a una falla similar los servicios que dependen de los servidores no se vean afectados, así como la calidad de atención a los contribuyentes.

Acción de Contingencia	**6.1.5. *Reajuste de Temperatura y Coordinación con Proveedor.***		Código	**PCA05**
SITUACIÓN	6.1. FALLA DE SERVIDORES (**A**)	**Actores**	Subgerente, Soporte Técnico	
Causa:	Recalentamiento	**Efecto:**	Daño a los equipos de Sala de Servidores.	

Detalle del Problema:

Una falla en el Sistema de Refrigeración podría ocasionar el aumento de la temperatura a niveles que provocarían lentitud en los Servidores e incluso se pondría en riesgo la integridad de los equipos de la Sala de Servidores o el desmedro de su vida útil.

Verificación:

Se realiza el monitoreo de la temperatura de la Sala de Servidores mediante el dispositivo de Control Remoto, a través del cual es posible regular la temperatura tomando en cuenta a las siguientes medidas:

- Temperatura Óptima: 18 °C
- Temperatura Máxima: 25 °C

Así mismo, verificar que el equipo de Aire Acondicionado se encuentra operativo y sea posible encenderlo y graduarlo.

Solución:

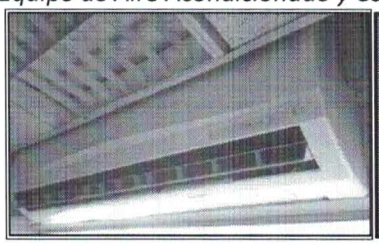
Se debe cuidar que la temperatura siempre esté en el nivel óptimo. En caso llegue a niveles cercanos al máximo, debe corregirse inmediatamente, mediante el Control Remoto.

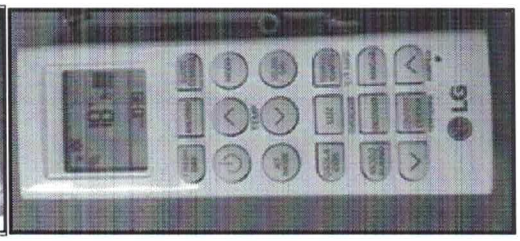
En caso de falla o desperfecto de los equipos de Aire Acondicionado, se debe coordinar con la Subgerencia de Logística y Control Patrimonial para recibir el mantenimiento correctivo correspondiente de un especialista.

Datos de los equipos de aire acondicionado:

- Cantidad: Un (01) equipo.
- Marca: LG
- Modelo: Mini Split
- Accesorio: Control remoto
- Ubicación: En el extremo superior derecho de la Sala de Servidores.

Equipo de Aire Acondicionado y Control Remoto:





Nivel de Impacto y Riesgo:

It	Situación e Impacto	Nivel de Riesgo	Evaluación
1	Impacto organización	5	Adquirir otro equipo **Aire Acondicionado** para evitar el daño de los servidores.
2	Situación de Repuestos	0	
3	Redundancia	5	
	TOTAL	**10**	**Medio**

El equipo de Aire Acondicionado requiere servicio externo especializado, por lo que no se requeriría de repuestos, pero si de un sistema de respaldo, ya que actualmente se cuenta con un (01) solo equipo de aire acondicionado operativo y lo adecuado sería contar con otro más, ya que reparar o incuso conseguir otro podría demorar un tiempo sumamente prolongado, arriesgando la integridad de los equipos y los servicios que de ellos dependen. Se requiere contar con dos (02) equipos de Aire Acondicionado en la Sala de Servidores.

6.2 CORTE DE ENERGÍA (Código B)

Acción de Contingencia	***6.2.1. Apagado de Servidores***		Código	**PCB01**
SITUACIÓN	6.2. CORTE DE ENERGÍA (B)	**Actores**	Subgerente, TI, Soporte Técnico, SLCP	
Acción de Contingencia	***6.2.1. Apagado de Servidores***			
Causa:	Falla del proveedor o incidente eléctrico local.	**Efecto:**	Paralización de todos los equipos electrónicos.	

Detalle del Problema:

Un corte de energía no atendido previamente de manera adecuada, podría dañar los servidores; por ende es necesario realizar el apagado de los equipos antes de que el corte de energía apague los servidores.

Equipos UPS: Estos equipos proveen de energía a los servidores por **10 minutos** aproximadamente, una vez suscitado el corte de energía. En ese corto tiempo deberá realizarse el apagado de los servidores.

Tipos de Corte de Energía:

- Corte Programado: El proveedor de energía anuncia con anticipación la fecha, hora y duración del corte de energía.
- Corte intempestivo: Se debe a falla sin aviso del proveedor o incidencia eléctrica local.

Verificación:

La Subgerencia de Logística y Control Patrimonial es la responsable de comunicar a las diversas áreas de algún corte de corriente eléctrica programado, advertido por el proveedor de energía.

En caso de un corte intempestivo es también dicha subgerencia la encargada de comunicarse con el proveedor de energía para saber sobre el motivo y hora de reposición del fluido eléctrico, así como absolver la incidencia si se debe a un desperfecto en eléctrico local.

A su vez, la mencionada subgerencia es la responsable coordinar la adquisición de los servicios de Grupo Electrógeno que provea por el tiempo requerido de un suministro alternativo de energía eléctrica.

Solución:

Frente al anuncio de un corte de energía, se debe proceder a realizar el apagado de los servidores, tanto virtuales como los físicos de Windows y Linux, empezando con los virtuales.

- Relación de servidores:

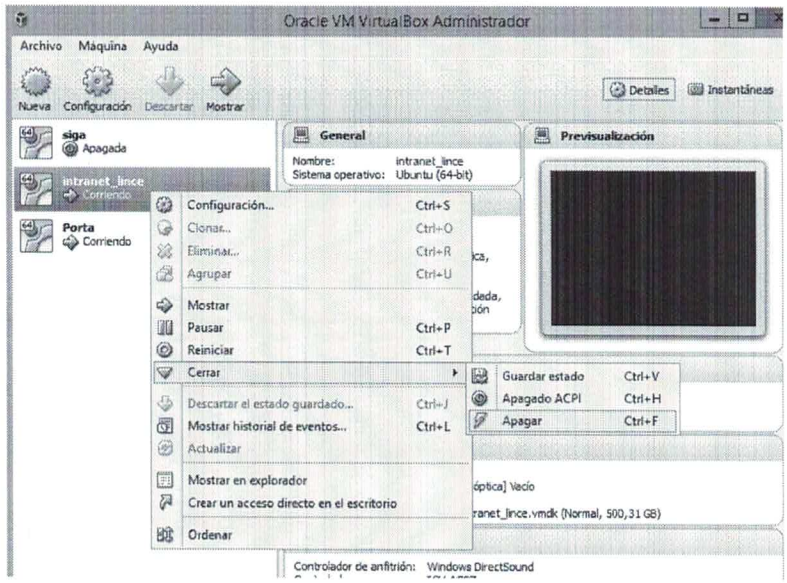
Item	Sistema Operativo	Item	Nombre de Virtual	Servicio
1	Windows Server	1	intranet_lince	Intranet
		2	Porta	Portal Web
2	Windows Server	3	usuarios.mdl.gob.pe	
		4	icinga2	
		5	observium_red	
		6	chamilion_muni	Aula Virtual
		7	gps.mdl.gob.pe	GPS Radios
		8	usuarios3920.mdl.gob.pe	
		9	windows7-adm	
		10	central.mdl.gob.pe	
3	Linux Ubuntu	11		Zimbra - Correo Electrónico
4	Linux Ubuntu	12		

6.2.1.1. Servidores Virtuales: Se debe iniciar con el apagado de los servidores virtuales, luego el apagado de Servidores Físicos.

- **Ingreso a los Servidores por Escritorio Remoto indicando IP y clave:**

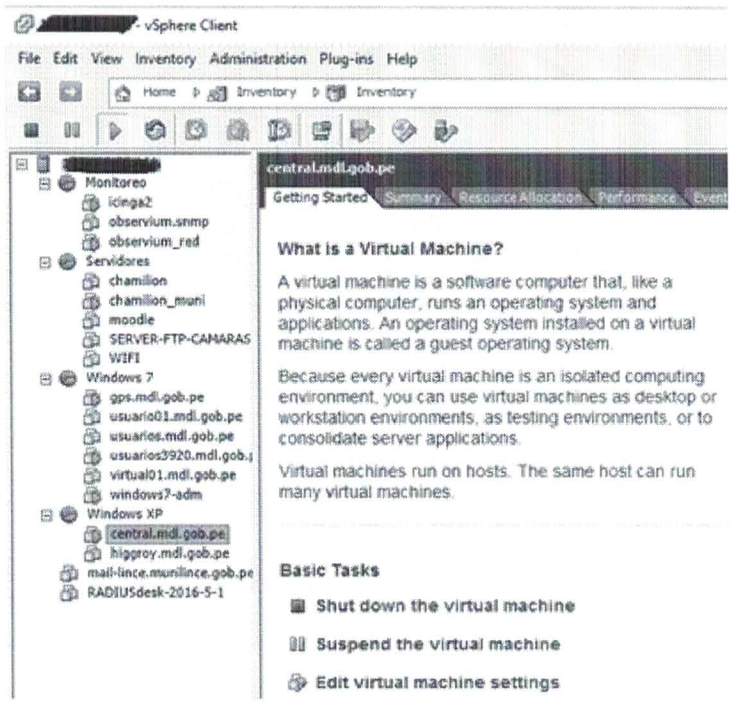
- **Para Servidor del ítem 1 con Windows - Ingreso al Oracle VM Virtual Box:**

  Ingresar al ícono de Oracle VM Virtual, donde observará los Servidores encendidos o "Corriendo", clic derecho sobre ellos, ir a la opción "Cerrar" y luego presionar el apagado.



- **Para servidor del Item 2 con Windows - Ingreso mediante vSphere:**

  Seleccionar las ventanas activas del programa vSphere, luego marque uno de los servidores activos y presione el botón para detener (cuadrado rojo) de cada uno de los servidores virtuales.



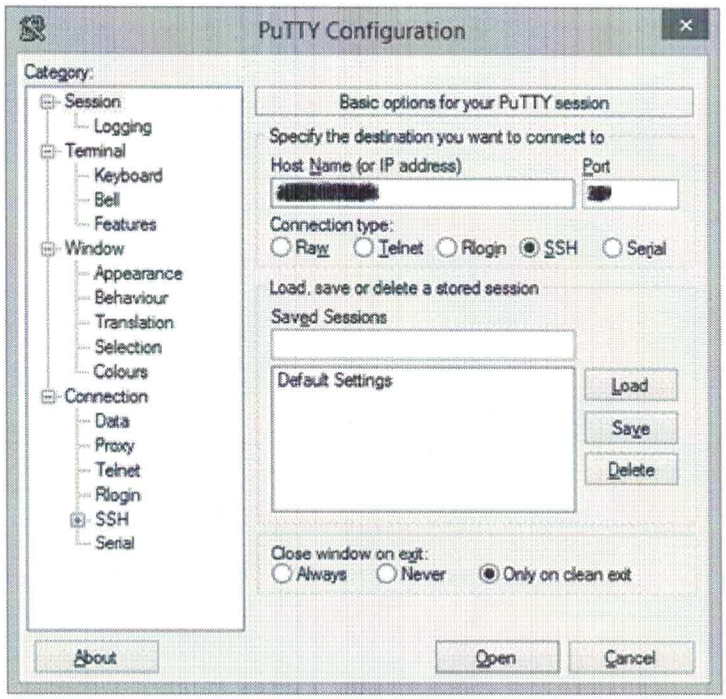
6.2.1.2. Servidores Físicos Windows:

Una vez apagado todos los servidores virtuales, proceder con el apagado físico.

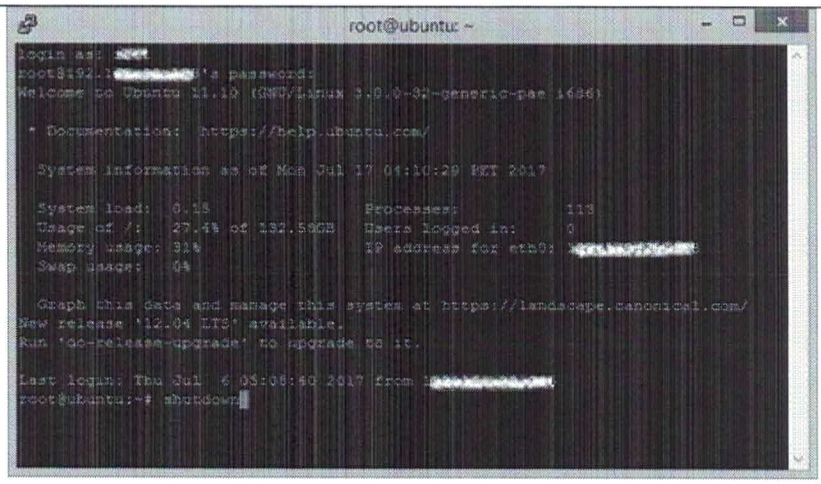
- Ingreso al servidor por Escritorio Remoto.
- Apagado del Sistema Operativo

6.2.1.3. Servidor Físico Linux – ítem 3: Zimbra – Correo Electrónico

Ingreso remoto mediante programa PUTTY, indicando IP y Puerto (Port) correspondiente.



En la pantalla de la consola ingresar la clave y luego el comando shutdown:



6.2.1.4. Coordinación con Grupo Electrógeno

Se debe mantener una comunicación oportuna con el área de Logística, responsables de la coordinación para la adquisición del servicio de un Grupo Electrógeno que provea, por el tiempo requerido, del fluido eléctrico necesario para mantener la continuidad de los servicios básicos de la Institución, incluyendo a todos los equipos de la Sala de Servidores.

Nivel de Impacto y Riesgo:

It	Situación e Impacto	Nivel de Riesgo	Evaluación
1	Impacto organización	5	Adquirir otro **equipo UPS** para Reducir Riesgo a un **Nivel Medio** de 10 puntos.
2	Situación de Repuestos	5	
3	Redundancia	5	
	TOTAL	**15**	**Alto**

Un corte de luz significa una paralización total de todos los equipos que dependen de energía eléctrica. Actualmente no se cuenta con alguna alternativa para dar una acción inmediata.

Adquisición de Repuestos:
Se requiere contar con un equipo UPS de respaldo para realizar el cambio de este equipo del cual dependen los servidores para garantizar un correcto apagado de los equipos.

Sistema Redundante:
La Institución requiere acceso inmediato a un grupo electrógeno que permita continuar con las operaciones y atención, en caso se presente algún tipo de corte.

Acción de Contingencia	6.2.2. ***Encendido de Servidores.***		Código	PCB02
SITUACIÓN	6.2. CORTE DE ENERGÍA (**B**)	**Actores**	Subgerente, TI, Soporte Técnico, SLCP	
Causa:	Falla del proveedor o incidente eléctrico local.	**Efecto:**	Paralización de todos los equipos electrónicos.	

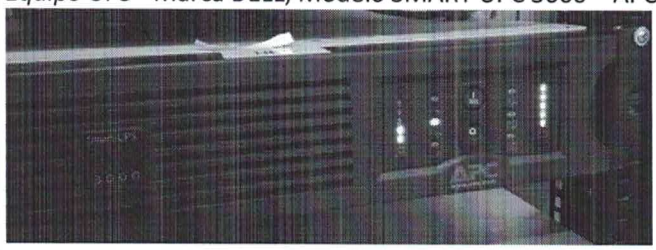
Detalle del Problema:

Al regresar el fluido eléctrico ya sea por restablecimiento del servicio del proveedor o puesta en marcha del Grupo Electrógeno, se debe reiniciar el funcionamiento de los Servidores para retomar los servicios básicos que brinda la institución.

Verificación:

Se verifica el restablecimiento del fluido eléctrico estable en las instalaciones, verificando que los equipos reciben energía y pueden encenderse.
Se verifica también que el equipo UPS ubicado en la Sala de Servidores se encuentra completamente cargado, para lo cual es necesario visualizar todas las luces encendidas en el lado izquierdo del equipo (a nuestra mano derecha).

Equipo UPS - Marca DELL, Modelo SMART UPC 3000 – APC:



Solución:

Una vez restablecido el fluido eléctrico y confirmado que los equipos UPS se encuentran completamente cargados, se procederá al encendido de los servidores. Empezando con los Servidores Físicos y luego la activación de los Servidores Virtuales mediante el acceso remoto:

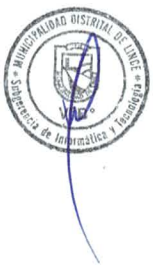
- Se realiza el encendido manual de cada servidor físico.
- Se realiza el encendido remoto de cada servidor virtual.
- Se ejecutan mediante red algunos Script para refrescar las rutas y servicios para determinados servidores:
  - Comando *sh ruta.sh* y Comando *sudo shorewall restart*.
- Se evalúa la respuesta de los servicios: Lanzador, SATMunXP, Portal Web, Intranet, Correo

Nivel de Impacto y Riesgo:

It	Situación e Impacto	Nivel de Riesgo	Evaluación
1	Impacto organización	5	Adquirir otro **equipo UPS** para Reducir Riesgo a un **Nivel Medio** de 10 puntos.
2	Situación de Repuestos	5	
3	Redundancia	5	
	TOTAL	**15**	**Alto**

Adquisición de Repuestos:
Se requiere contar con un equipo UPS de respaldo para realizar el reemplazo inmediato de este equipo del cual dependen los servidores para garantizar un correcto apagado de los mismos y evitar cualquier daño a las bases de datos e información resguardada.

Sistema Redundante:
La Institución requiere acceso inmediato a un grupo electrógeno que permita continuar con las operaciones y atención, en caso se presente algún tipo de corte.



6.3. FALLA DE RED (Código C):

Acción de Contingencia	6.3.1. *Verificación de conectividad de Servidores y Switchs*		Código	PCC01
SITUACIÓN	6.3. FALLA DE RED (C)	Actores	Subgerente, Soporte Técnico	
Causa:	Falla de Servidores o Switch	Efecto:	Corte de Internet y Aplicaciones Interrupción de Atención y Cobros a contribuyentes.	

Detalle del Problema:

Una falla en la red provoca la pérdida de conectividad, impidiendo a las aplicaciones y otros sistemas que requieren conexión a los servidores y a Internet continuar operando.

Verificación:

Se verifica si la falla presentada es local, es decir, si se circunscribe a una sección, ambiente o piso a fin de identificar el equipo que requeriría intervención, revisando los siguientes elementos:

- Servidores: Equipos en Salas de Servidores.
- Switchs Administrable: Permiten su configuración y conexiones de cables de red.
- Switchs con función Hub: Solo es factible realizar conexiones de cables de red.

Relación de Servidores: Ver punto 6.1.2 "Reparación de Disco Duro de Servidores".

Relación de Swichs: A continuación la lista de los diversos Switch:

Nro	Edificio	Piso	Ambiente	Marca	Modelo	Port
1	Casa Adulto	1	Salón de Cómputo	Falta	Falta	24
2	Castilla	1	GSC	D-LINK	DES-1016D	16
3	Colegio	2	Dirección	D-LINK		16
4	Colegio	2	Psicología	HP	1920 (confirmar)	8
5	Colegio	2	Salón de Cómputo	HP		16
6	Palacio	1	Banco	TP-LINK	GL-SG3424	24
7	Palacio	1	Rentas	3 COM	3C16471B	24
8	Palacio	1	Rentas	3 COM	3C16475CS	24
9	Palacio	1	SEC	CISCO	SF300	24
10	Palacio	1	SFTC	3 COM	3C16475CS	24
11	Palacio	1	SFTC	D-LINK	DES-1016A	16
12	Palacio	1	SRAC	3 COM	3C16475CS	28
13	Palacio	3	GPP	D-LINK	DES-10160	16
14	Palacio	3	SIT - Data Center	HP	JG924A	24
15	Palacio	3	SIT - Data Center	HP	J9727A	24
16	Palacio	3	SIT - Data Center	HP	JE006A	28
17	Palacio	3	SIT - Data Center	Allied Telesis	AT-8000GS	24
18	Palacio	3	SIT - Data Center	HP	HNGZA-HA0008	8

19	Palacio	3	SIT - Data Center	HP	HNGZA-HA0008	8
20	Palacio	3	SIT - Soporte	HUAWEI	S1700-28GFR-4P-AC	24
21	Palacio	4	SLCP	BASELINE	3C1647CS	24
22	Palacio	4	SRH	3 COM	3C16471B	24
23	Palacio	4	ST	CISCO	CATALYS EXPRESS 500	24
24	Palacio	5	PPM	3 COM	3C16475	26
25	Palacio	Sot	SFCU	CISCO	CATALYST EXPRESS 500	26
26	Palacio	Sot	SIU	3COM	3C16471B	28
27	Palacio	Sot	SLCP - Almacén	CNET		8
28	Casa Adulto	1	Salón de Cómputo	Falta		24
29	Castilla	1	GSC	D-LINK	DES-1016D	16
30	Colegio	2	Dirección	D-LINK		16
31	Colegio	2	Psicología	HP	1920 (confirmar)	8
32	Colegio	2	Salón de Cómputo	HP		16
33	Sanidad	2	EFSP	ENCORE	ENH916P-NWY	16
34	Vecino	2	GDH	HP	Office Connect 1920	24
35	Vecino	2	GGA	3COM	SuperStack II Dual Speed Hub 500	24
36	Vecino	2	OCI	TP-LINK	TL-SF1016	16

Solución:

Servidores:
Si se trata de una falla desde los servidores, proseguir con las pautas indicadas en los planes de acción 6.1 para *"Fallas de Servidores"* y *"6.2.1. Apagado de Servidores"* de este mismo documento.

Switch:

- Realizar las configuraciones correspondientes.
- Corregir la conexión de cables de red y puertos correspondientes.
- Cambiar el equipo Switch si fuese el caso.

Nivel de Impacto y Riesgo:

It	Situación e Impacto	Nivel de Riesgo	Evaluación
1	Impacto organización	5	Adquirir **2 Switch** de respaldo para Reducir Riesgo a un **Nivel Medio** de 10 puntos.
2	Situación de Repuestos	5	
3	Redundancia	5	
	TOTAL	**15**	**Alto**

Los servicios relacionados a la conexión por red serían vulnerables a este tipo de fallas.

Adquisición de Repuestos:
Para dar una respuesta oportuna frente a la falla de algún equipo, sería necesario contar con al menos dos (02) equipos Switch administrables de respaldo.

6.4. CORTE DE INTERNET:

Acción de Contingencia	**6.4.1. *Coordinación con proveedor de Internet***		Código	**PCD1**
SITUACIÓN	6.4. CORTE DE INTERNET (**D**)	**Actores**	Subgerente, Soporte Técnico, SGC y SFCU.	
Acción de Contingencia	**6.4.1. *Coordinación con proveedor de Internet***			
Causa:	Falla de Proveedor	**Efecto:**	Corte de Internet. Caída del Portal Interrupción de Atención y Cobros a contribuyentes.	

Detalle del Problema:

Por una falla de origen del proveedor del servicio de Internet la institución queda incomunicada, impidiendo su normal operatividad, como el cobro por POS, uso del TeleBanking, caída del Portal Web, entre otros.

Verificación:

Se verifica que los equipos no pueden conectarse a Internet, descartando previamente fallas de otro tipo, como "6.1. Falla de Servidores" y "6.3 Falla de Red".
Realiza verificación del Ping con el servidor del proveedor de Internet.

Solución:

Frente a un corte del servicio de Internet por falla del proveedor se procede a contactar al proveedor, el cual debe dar respuesta a los 10 minutos; caso contrario insistir. Datos del proveedor:

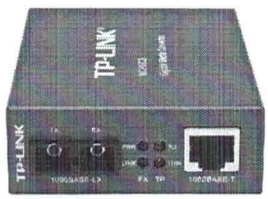
- Nombre: MG Trading SAC
- Teléfono: 6175757 / 940205363
- Dirección: Av. César Vallejo 578, Lince.

Nivel de Impacto y Riesgo:

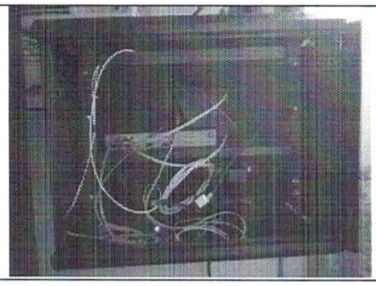
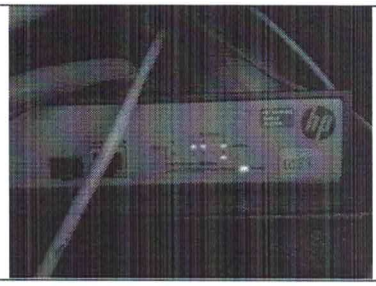
It	Situación e Impacto	Nivel de Riesgo	Evaluación
1	Impacto organización	5	Contar con **Sistema Redundante** para evitar interrupción de Internet y los Servicios de Atención y **Cobros**.
2	Situación de Repuestos	0	
3	Redundancia	5	
	TOTAL	**10**	**Medio**

Adquisición de Repuestos:
El servicio de conexión a Internet es proveído por un tercero, el cual se encarga de todo el mantenimiento relacionado a su servicio y no se requieren repuestos a fallas relacionadas directamente con el proveedor.

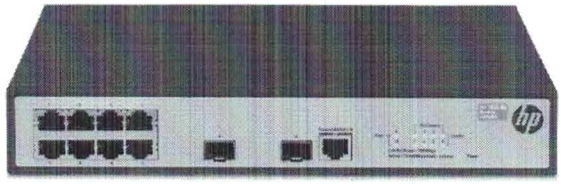
Sistema Redundante: No se cuenta con un sistema redundante que permita saltar a otro proveedor alternativo, lo cual expone a la institución a quedar desconectada por el tiempo que el proveedor demore en retomar el servicio.

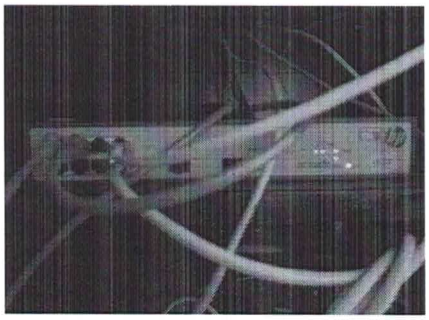
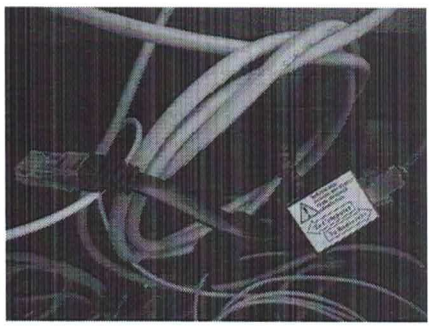
Acción de Contingencia	**6.4.2. *Cambio de Conexión a Internet por Radio Enlace***		Código	**PCD2**
SITUACIÓN	6.4. CORTE DE INTERNET	**Actores**	Subgerente, Soporte Técnico	
Causa:	Corte de Fibra Óptica	**Efecto:**	Corte de Internet. Caída de Portal, Correo y Cobros por POS.	
Detalle del Problema:				
Un corte de la fibra óptica a través del cual se proporciona el servicio de conexión a Internet deja incomunicada a la institución y provoca la caída de varios servicios, operaciones críticas, incluyendo los servicios de cobro por POS.				
Verificación:				
Descartar falla del proveedor en el servicio de Internet: • Realiza verificación del Ping con el servidor del proveedor de Internet para descartar falla del proveedor. Ver Plan de Acción *"6.4.1. Coordinación con proveedor de Internet"*. • Se comunica con proveedor para consultar sobre el servicio, confirmando que ellos siguen brindándolo adecuadamente. • Verifica en el equipo Convertidor de medios (**Media Converter**) si las luces de los enlaces están encendidas, indicando que hay conexión, si las dos (02) luces de "LINK" están apagadas, dejando solo dos (02) encendidas, se evidenciará que no hay conexión y se debe proceder a ubicar el lugar de la ocurrencia. *Equipo Convertidor de Medios marcaTP-LINK, modelo MC210CS:* 				
Solución:				

Para realizar el cambio de la conexión a Internet vía Radio enlace se deberá modificar conexiones el Switch HP 1920-8G/JG920A identificado con número 1089 colocado en la cabina ubicada en el extremo derecho de la Sala de Servidores:

Gabinete de equipos de conexión a Internet.	*Switch número 1089.*
	

En el Switch del Data Center, se realiza el cambio de conexión del cable, pasando de la conexión por fibra al punto de conexión del Radio Enlace.



Quitar el cable de red del <u>puerto 1</u>, que procede del Media Converter.	Conectar el Cable de Radio enlace en el <u>puerto 1</u> liberado.
	

Revisar la conexión a Internet mediante en la navegación Web y el uso de los diversos servicios para dar por restablecido el servicio de modo alternativo.

Volver a conectar a servicio de Internet por Fibra:

Una vez reparado el corte de fibra, se debe regresar a la conexión por este medio, dejando la conexión por Radio Enlace:

- Abrir el gabinete ubicada en el extremo derecho de la sala de servidores
- Desconectar el cable de Radio Enlace del puerto 1 del Switch número 1089.
- Conectar el cable de red libre que sale del Media Converter ubicado en la parte

baja del gabinete al puerto 1.

Comprobar los servicios de Internet mediante la navegación Web el uso de las diferentes aplicaciones y servicios que requieren conexión a Internet, finalizando así el proceso de reconexión.

Nivel de Impacto y Riesgo:

It	Situación e Impacto	Nivel de Riesgo	Evaluación
1	Impacto organización	5	Contar con **Topología de Red** para evitar, por corte de fibra, la interrupción de Internet y los Servicios de Atención y **Cobros**.
2	Situación de Repuestos	0	
3	Redundancia	5	
	TOTAL	**10**	**Medio**

Frente a un corte de fibra óptica toda la institución quedaría incomunicada y varios servicios críticos se verían afectados.
Ante casos como este, el responsable serían terceros y recaería en ellos la reparación del incidente.

Sistema Redundante:
La red de fibra óptica actual no garantiza otras alternativas y requiere un cambio de topología (esquema o disposición de la fibra óptica) mediante al cual se garanticen otras vías de conexión en caso algún tramo de la fibra se rompa.
Se tiene de manera provisional la opción de cambio a radio enlace; pero esta es una salida alternativa no adecuada para preservar la calidad de servicio.

Acción de Contingencia	**6.4.3. *Ubicación del Corte de Fibra e Identificación de Responsabilidades***		Código	**PCD3**
SITUACIÓN	6.4. CORTE DE INTERNET	**Actores**	Subgerente, Soporte Técnico, SGC y SFCU.	
Causa:	Corte de Fibra Óptica	**Efecto:**	Corte de Internet. Caída de Portal, Correo y Cobros por POS.	

Detalle del Problema:

El corte de fibra óptica suele darse en los exteriores de los ambientes de la institución y requieren una atención técnica oportuna, que significa un gasto sobre el que no tiene responsabilidad la institución, por lo que es urgente identificar, además de la ubicación de la incidencia, a los causantes del hecho para asumir responsabilidades.

Verificación:

Habiendo descartado otras causas, como se verifica en el Plan de Acción "6.4.1 Cambio de Conexión por Radio Enlace", se procede a ubicar el lugar de la incidencia y a identificar al causante para que se haga cargo de las reparaciones correspondientes y restablecimiento del servicio.

Solución:

Al realizarse un corte de la fibra, frente a la interrupción de las comunicaciones se realizan pruebas para localizar el lugar donde podría haber ocurrido el corte de la fibra:

- Se coordina con la Gerencia de Seguridad Ciudadana.
- Motorizados patrullan la zona para identificar actividades de construcción u otras similares donde haya podido ocurrir el hecho.
- Se ubica y comprueba el lugar donde ocurrió el corte.
- Se identifica a las personas u organizaciones responsables.
- Se comunica a la Subgerencia de Fiscalización y Control Urbano para que tome acciones y exija la reparación de la fibra cortada.

6.5. INCENDIO O SISMO (Código E)

Acción de Contingencia	**6.5.1. *Respaldo de Información de emergencia***		Código	**PCE1**
SITUACIÓN	6.5. INCENDIO Y SISMO (E)	**Actores**	Subgerente, Soporte Técnico, SGC	
Causa:	Combustión de elementos inflamables o Movimiento telúrico	**Efecto:**	Destrucción de bienes, infraestructura y riesgo para la vida.	

Detalle del Problema:

Un **Incendio** en las instalaciones de la institución, dentro o fuera del área, así como un **Sismo** significaría un riesgo mayor no solo para los bienes, sino también para la vida de los colaboradores y personas presentes al momento del siniestro.

Verificación:

Se alerta de un incendio por advertencia del personal o percepción de humo o fuego. En caso de incendio, llamar a los bomberos al 116 o al 471-6442, teléfono de la Brigada B-4, ubicada en Jr. Manuel Candamo No. 455, Lince.

Solución:

Las acciones a tomar en caso de **incendio o sismo** son los mismos procedimientos establecidos para cualquier ambiente de la institución referente a extinción de amago de fuego y evacuación, según la situación de desastre que se presente. De manera conjunta se realiza de manera preventiva el respaldo de la información en otro ambiente y en un espacio virtual en Internet.

- **Respaldo en Disco Duro Físico:**

  De manera preventiva, a fin de resguardar la información, bases de dato y programas críticos, se mantiene un respaldo en discos físicos de back up en otro local para su resguardo; en este caso, en las instalaciones de la Gerencia de Seguridad Ciudadana, lugar ubicado en el Parque Mariscal Castilla.

- **Respaldo en la nube o Internet:**

  Así mismo. Para reafirmar los cuidados de la mencionada información, se realiza también un respaldo en un disco duro virtual en la nube o Internet.

Nivel de Impacto y Riesgo:

It	Situación e Impacto	Nivel de Riesgo	Evaluación
1	Impacto organización	5	Adquirir Alarmas y Detectores de Humo para de reducir los riesgos a un **Nivel Medio** de 10 puntos.
2	Situación de Repuestos	5	
3	Redundancia	5	
	TOTAL	**10**	**Medio**