EPS ILO S.A.

Agua Ilo

RESOLUCION DE GERENCIA GENERAL Nº039-2024-GG-EPS ILO S.A.

Ilo, 16 de Febrero del 2024.

VISTOS: El Informe Nº059-2024-GAF-EPS ILO S.A. e Informe N° 015-2024-OTIC-GAF-EPS ILO S.A. con proveído de la Gerencia General hace llegar el Plan de Contingencias Informático de la EPS ILO S.A.; y,

CONSIDERANDO:

La EPS ILO S.A. es una empresa prestadora de servicios de saneamiento, cuya misión es proveer servicios de saneamiento, con altos estándares de calidad para satisfacer las necesidades de la población atendida por EPS ILO S.A. Es propiedad de la Municipalidad Provincial de Ilo y está sujeta a la Ley Marco de la Gestión y Prestación de los Servicios de Saneamiento, su reglamento y modificatorias, así como a la Ley General de Sociedades.

Tiene como Finalidad el Plan de contingencia que es una herramienta que le ayudara a que los procesos críticos de su empresa u organización continúen funcionando a pesar de una posible falla en los sistemas computarizados, es decir un plan que le permite a su negocio u organización seguir operando aunque sea el mínimo.

Los objetivos que persigue el plan son los siguientes: Definir las actividades de planeación, preparación, capacitación y ejecución de tareas destinadas a proteger la información contra los daños y perjuicios producidos por corte de servicios, fenómenos naturales o humanos, Establecer un plan de recuperación, formación de equipos y entrenamiento para restablecer la operatividad del sistema en el menor tiempo posible, Establecer actividades que permitan evaluar los resultados y retroalimentación del plan general, Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información, Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen un Sistema de Información; por lo que una vez revisado, es pertinente emitir Resolución;

En uso de las facultades conferidas en el Estatuto Social de la EPS ILO S.A.;

SE RESUELVE:

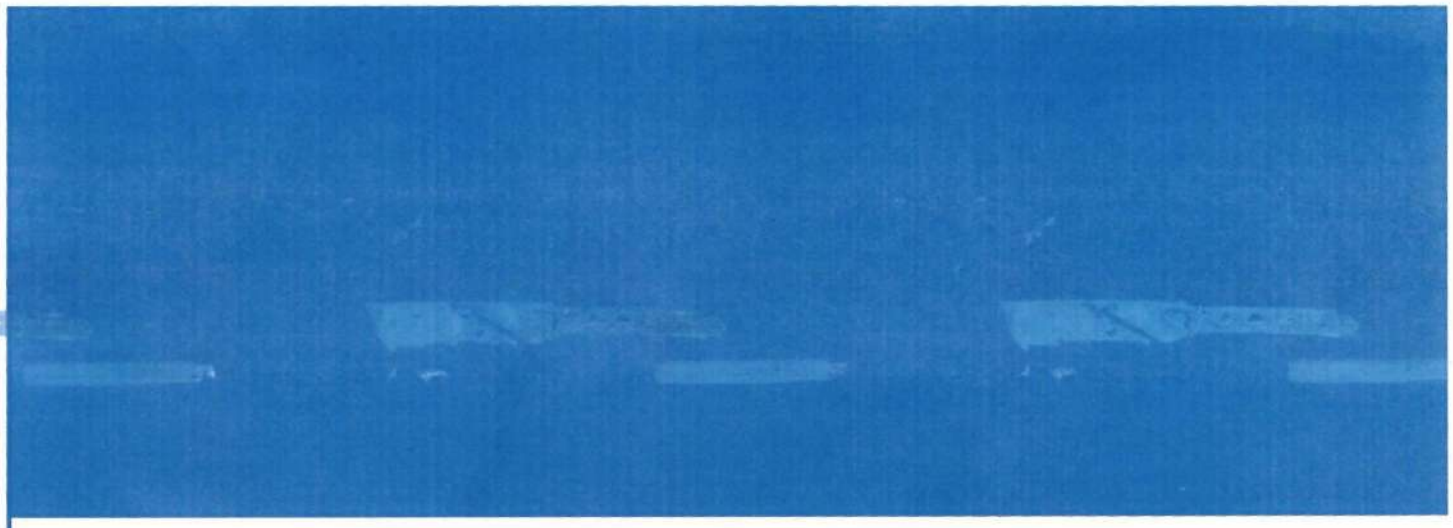
ARTICULO PRIMERO.- APROBAR el Plan de Contingencias Informático de la EPS ILO S.A., que a fojas 51 forma parte integrante de la presente Resolución.

ARTICULO SEGUNDO.- NOTIFICAR, con esta Resolución a la Oficina de Tecnología de la Información y Comunicaciones, Gerencia de Administración y Finanzas, Gerencia de Operaciones, Gerencia Comercial, Gerencia de Asesoría Jurídica, para conocimiento y fines.

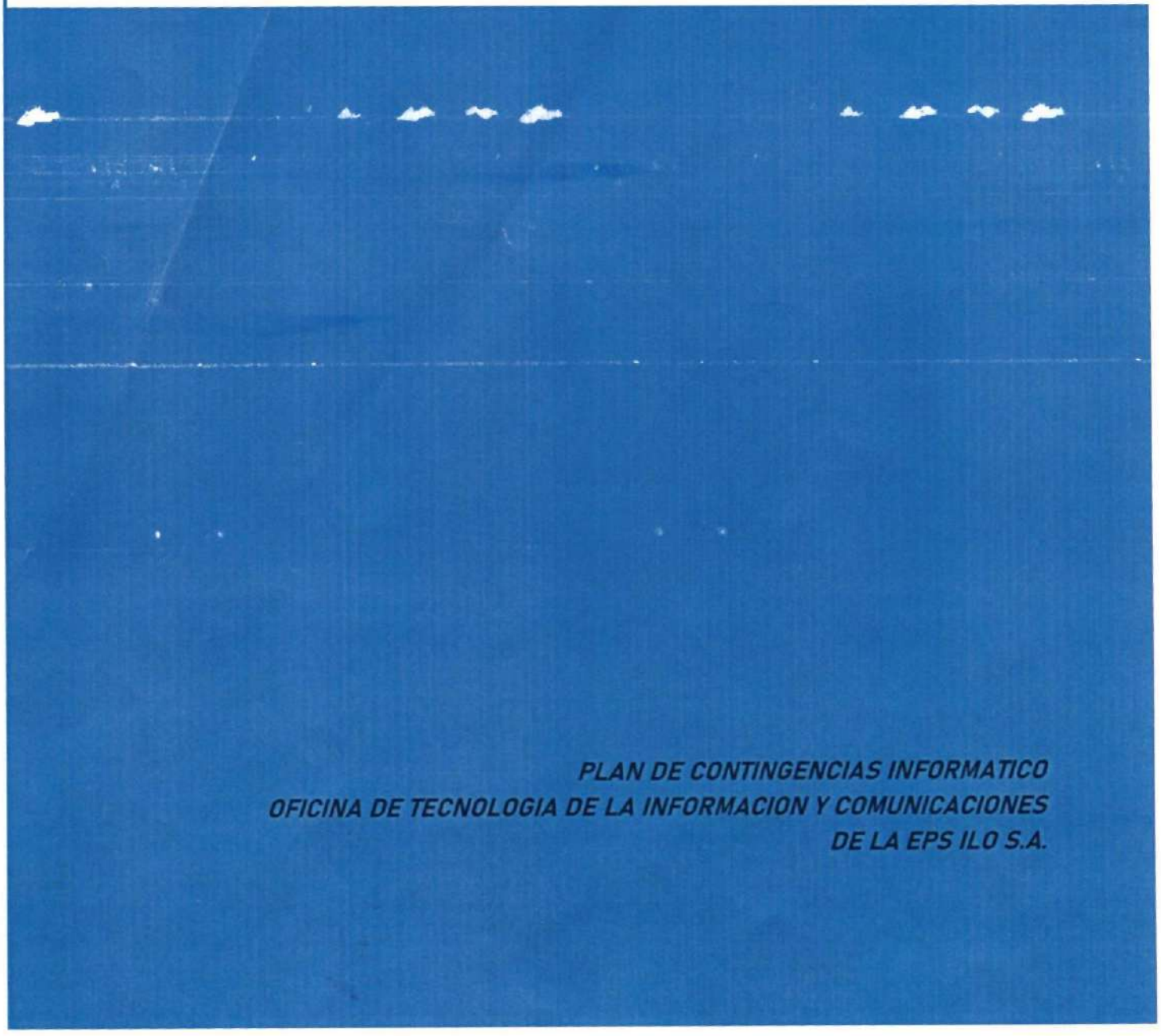
REGÍSTRESE, COMUNIQUESE Y CÚMPLASE

E.P.S. ILO S.A.

CPC. SOLANGE AGRAMONTE FLORES
GERENTE GENERAL
COD. MATRICULA 20-186



PLAN DE CONTIGENCIAS INFORMATICO



PLAN DE CONTINGENCIAS INFORMATICO
OFICINA DE TECNOLOGIA DE LA INFORMACION Y COMUNICACIONES
DE LA EPS ILO S.A.

CONTENIDO

E.P.S. ILO S.A. GERENCIA ADMINISTRACIÓN Y FINANZAS -ILO-

E.P.S. ILO S.A. OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES -ILO-

E.P.S. ILO S.A. GERENTE ASESORÍA JURÍDICA -ILO-

PLAN DE CONTINGENCIAS INFORMATICO

1. FINALIDAD

Podríamos definir a un plan de contingencias como una estrategia planificada con una serie de procedimientos que nos faciliten o nos orienten a tener una solución alternativa que nos permita restituir rápidamente los servicios de la organización ante la eventualidad de todo lo que lo pueda paralizar, ya sea de forma parcial o total.

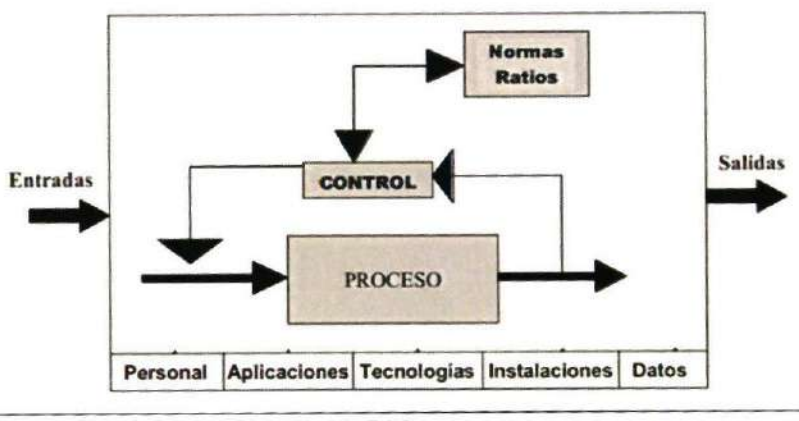
El plan de contingencia es una herramienta que le ayudará a que los procesos críticos de su empresa u organización continúen funcionando a pesar de una posible falla en los sistemas computarizados. Es decir, un plan que le permite a su negocio u organización, seguir operando, aunque sea al mínimo.

La Gestión de la Continuidad del Servicio se preocupa de impedir que una imprevista y grave interrupción de los servicios TI, debido a desastres naturales u otras fuerzas de causa mayor, tenga consecuencias catastróficas para el negocio.

La estrategia de la Gestión de la Continuidad del Servicio debe combinar equilibradamente procedimientos Proactivos y Reactivos:

- **Proactivos**: que buscan impedir o minimizar las consecuencias de una grave interrupción del servicio.
- **Reactivos**: cuyo propósito es reanudar el servicio tan pronto como sea posible (y recomendable) tras el desastre.

Este trabajo ha sido elaborado tomando como base la metodología ITIL (INFORMATION TECNOLOGY INFRASTRUTURE LIBRARY), formado por personas, equipos y procedimientos. Al conjugar una serie de elementos como hombres y servidores se hace imprescindible tomar medidas que nos permitan una continuidad en la operatividad de los sistemas para no ver afectados los objetivos de las mismas y no perder la inversión de costos y tiempo.



2. OBJETIVO

Disponer de un plan que permita atender de manera ordenada y prevista situaciones que pongan en riesgo la operatividad de los Sistemas Informáticos y de Redes en la EPS ILO S.A.; estableciendo procedimientos que eviten interrupciones en su operación.

Los objetivos que se persigue en el presente plan son los siguientes:

- Definir las actividades de planeación, preparación, capacitación y ejecución de tareas destinadas a proteger la información contra los daños y perjuicios producidos por corte de servicios, fenómenos naturales o humanos.
- Establecer un plan de recuperación, formación de equipos y entrenamiento para restablecer la operatividad del sistema en el menor tiempo posible.
- Establecer actividades que permitan evaluar los resultados y retroalimentación del plan general.
- Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información.
- Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen un Sistema de Información.

E.P.S. ILO S.A. GERENCIA GENERAL ILO

3. EPS ILO S.A.

El presente acápite describe de manera general y ejecutiva las principales características organizativas de EPS ILO S.A. con el objetivo de sentar las bases para el Plan de Contingencias Informático para la EPS ILO S.A.

E.P.S. ILO S.A. GERENCIA ADMINISTRACIÓN Y FINANZAS ILO

3.1. Naturaleza

E.P.S. ILO S.A. OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES ILO

EPS ILO S.A. es una empresa prestadora de servicios de saneamiento, cuya misión es proveer servicios de saneamiento, con altos estándares de calidad para satisfacer las necesidades de la población atendida por EPS ILO S.A. Es propiedad de la municipalidad provincial de ILO y está sujeta a la Ley Marco de la Gestión y Prestación de los Servicios de Saneamiento, su reglamento y modificatorias, así como a la Ley General de Sociedades.

Se ciñe, en lo sectorial a las políticas emanadas del Ministerio de Vivienda, Construcción y Saneamiento, como ente rector, asimismo, se sujeta al control de calidad de servicios y de regulación de precios dispuestos por la Superintendencia Nacional de Servicios de Saneamiento (SUNASS), como ente regulador. En el aspecto de gestión empresarial y de presupuesto se sujeta a las disposiciones de la Dirección General de Presupuesto Público, lo que respecta al control de legalidad esto corresponde a la Contraloría General de la República.

ILO S.A. ENTE SECTORIAL JURÍDICA ILO

3.2. Misión y visión

La misión y visión de la EPS ILO S.A. son las siguientes:

MISION	VISION
Brindar servicios de agua potable y de alcantarillado, preservando el medio ambiente, para mejorar la calidad de vida de la población de Ilo.	Ser una empresa líder a nivel nacional en servicios de saneamiento, comprometida con el desarrollo sustentable de la provincia de Ilo.

3.3. Valores empresariales

- Honestidad.
- Responsabilidad.
- Respeto
- Trabajo en equipo.
- Liderazgo.
- Identificación y compromiso empresarial.

3.4. Objetivos

- Mejorar la calidad de los servicios de agua potable en la ciudad de Ilo.
- Ampliar y asegurar sostenibilidad de la infraestructura de agua potable, alcantarillado y tratamiento y disposición de aguas residuales.
- Mejorar la eficiencia de los procesos comerciales, operacionales y administrativos de la EPS.
- Mejorar la situación económica financiera de la EPS hasta alcanzar la autonomía empresarial.
- Contribuir a la gestión sostenible de los recursos hídricos y el ambiente.

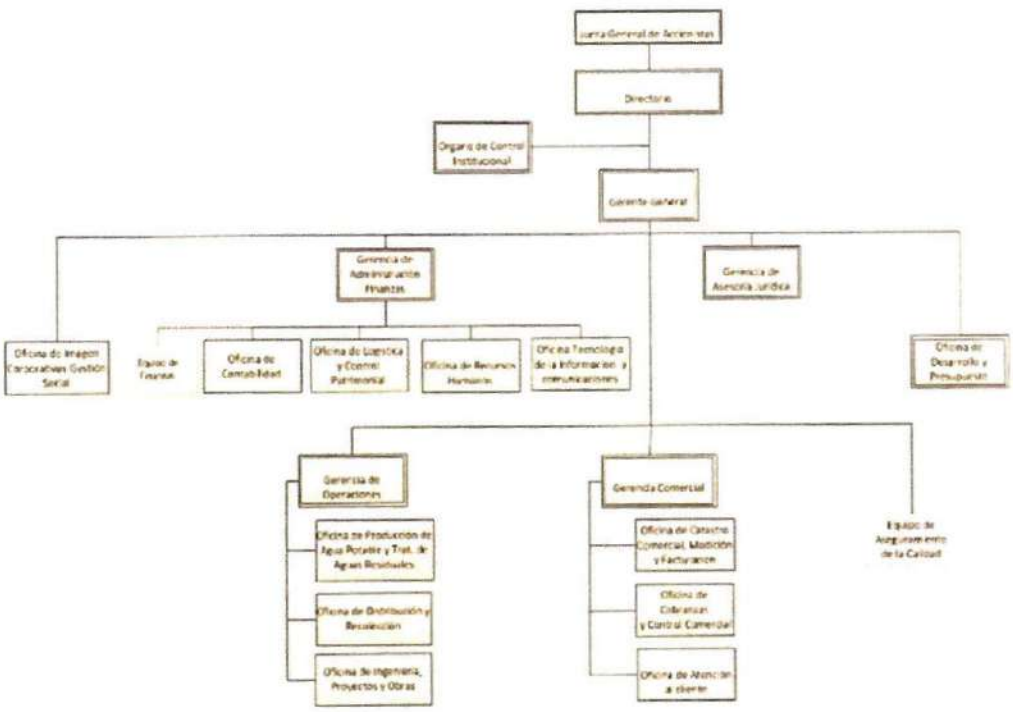
3.5. Estructura orgánica

La estructura orgánica de EPS ILO S.A. se encuentra configurada por tres niveles orgánicos:

NIVELES ORGANICOS DE LA EPS ILO S.A.		
NIVEL	**DESCRIPCIÓN**	**REPRESENTANTE**
Primer Nivel	Gerencia General	Gerente General
Segundo Nivel	Gerencia	Gerente
Tercer Nivel	Oficinas	Jefe

A continuación, se muestra a continuación la estructura orgánica de EPS ILO S.A.:

ORGANIGRAMA – EPS ILO S.A.



Organigrama de la EPS ILO S.A:

4. ALCANCE

La presente Directiva es de aplicación y cumplimiento obligatorio para todos los órganos y unidades orgánicas de la EPS ILO S.A.

5. BASE LEGAL

- Ley N° 27658 - Ley Marco de Modernización de la Gestión del Estado.
- Ley N" 23716 - Ley de Control Interno de las Entidades del Estado.
- Ley N° 27309, Ley que incorpora los Delitos Informáticos al Código Penal.
- Ley N° 27815, Ley del Código de Ética de la Función Pública y sus modificatorias.
- Ley N° 29733, Ley de Protección de Datos Personales y sus modificatorias.
- Decreto Supremo N° 033-2018-PCM, que crea la Plataforma Digital Única del Estado Peruano y establecen disposiciones adicionales para el desarrollo del Gobierno Digital y sus modificatorias.
- Decreto Supremo N° 004-2019- JUS, que aprueba el Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General.
- Resolución de Gerencia General No. 116-202-GG-EPS ILO S.A., que aprueba la modificación del Reglamento de Organización y Funciones de la EPS ILO S.A.

6. DEFINICIÓN DE TÉRMINOS

Para efectos de la presente directiva, se entenderá por:

- **Copias de Seguridad (Backup)**: una copia de seguridad o backup (su nombre en inglés) en tecnología de la información o informática es una copia de seguridad - o el proceso de copia de seguridad - con el fin de que estas copias adicionales puedan utilizarse para restaurar el original después de una eventual pérdida de datos.
- **Disco Duro:** en informática, un disco duro o disco rígido (en inglés Hard Disk Drive, HDD) es un dispositivo de almacenamiento de datos no volátil que emplea un sistema de grabación magnética para almacenar datos digitales. Se compone de uno o más platos o discos rígidos, unidos por un mismo eje que gira a gran velocidad dentro de una caja metálica sellada. Sobre cada plato se sitúa un cabezal de lectura/escritura que flota sobre una delgada lámina de aire generada por la rotación de los discos.
- **Enrutador (Rourter)**: el enrutador (calco del inglés Router), direccionador, ruteador o encaminador es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red). Un enrutador es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la mejor ruta que debe tomar el paquete de datos.
- **Hardware**: corresponde a todas las partes físicas y tangibles de una computadora: sus componentes eléctricos, electrónicos, electromecánicos y mecánicos; sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.
- **LAN: (Local Área Network - Red de Área Local).** Interconexión de computadoras y periféricos para formar una red dentro de una empresa u hogar, limitada generalmente a un edificio.
- **Plan de Contingencia**: Conjunto de estrategias, acciones, procedimientos planificados y responsabilidades definidas para minimizar el impacto de una interrupción imprevista de las funciones críticas y conseguir la restauración de las mismas, dentro de unos límites de tiempo

establecidos. Sin que sea una regla general, se suele aplicar al plan circunscrito a las actividades de los departamentos de Sistemas de Información.

- **Red:** Una red de computadoras, también llamada red de ordenadores o red informática, es un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos para compartir información y recursos. Este término también engloba aquellos medios técnicos que permiten compartir la información.
- **Software**: se conoce como software al equipamiento lógico o soporte lógico de una computadora digital; comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos del sistema, llamados hardware.
- **Servidores**: una aplicación informática o programa que realiza algunas tareas en beneficio de otras aplicaciones llamadas clientes. Algunos servicios habituales son los servicios de archivos, que permiten a los usuarios almacenar y acceder a los archivos de una computadora y los servicios de aplicaciones, que realizan tareas en beneficio directo del usuario final. Este es el significado original del término. Es posible que un ordenador cumpla simultáneamente las funciones de cliente y de servidor.
- **Sistema Operativo**: un Sistema operativo (SO) es un software que actúa de interfaz entre los dispositivos de hardware y los programas de usuario o el usuario mismo para utilizar un computador. Es responsable de gestionar, coordinar las actividades y llevar a cabo el intercambio de los recursos y actúa como intermediario para las aplicaciones que se ejecutan.

7. INFRAESTRUCTURA TECNOLÓGICA

7.1. Hardware

- Equipos de EPS ILO S.A.

A continuación, se muestra el inventario de hardware en todas las sedes y el inventario de hardware por sede:

SEDE	EQUIPO	CANTIDAD
R4	Computadora personal	128
	Laptop	6
	Access Point	6
	Escáner	2
	Impresora	25

	Switch	10
R5	Computadora personal	3
	Laptop	0
	Impresora	3
	Switch	1
PTAP 1	Computadora personal	1
	Laptop	1
	Servidor	0
	Impresora	1
	Switch	1
PTAP 2	Computadora personal	1
	Laptop	2
	Servidor	0
	Impresora	2
	Switch	1

En resumen, se tiene:

EQUIPO	CANTIDAD
Computadora personal	134
Laptop	10
Access Point	12
Escáner	10
Impresora	2
Switch	25

El parque de computadoras personales y laptops es moderno y va acorde a las funciones de los usuarios que demandan potencia en rendimiento para el procesamiento de los sistemas de información y aplicaciones de uso interno. Asimismo, el parque de servidores es

moderno.

- Esquema de red de EPS ILO S.A.

EPS ILO S.A. cuenta con sedes descentralizadas en la ciudad de ILO, integradas en una topología Estrella hacia el DATA CENTER, brindando a sus usuarios los siguientes servicios:

- Aplicaciones administrativas y sistema comercial.
- Intranet.
- Correo institucional.
- Telefonía IP.
- Video vigilancia.
- Repositorios de archivos.

Para el acceso a la Red WAN, EPS ILO S.A. cuenta con una (1) enlaces de internet configurando una arquitectura de alta disponibilidad y con contingencia de operadores ISP.

Las redes internas, servidores de aplicaciones internas, de bases de datos y de almacenamiento se encuentran protegidos y aislados de las conexiones hacia internet por una configuración de cascada-doble de firewalls.

A continuación, se muestra el diagrama general de red y la topología de red de EPS ILO S.A.:

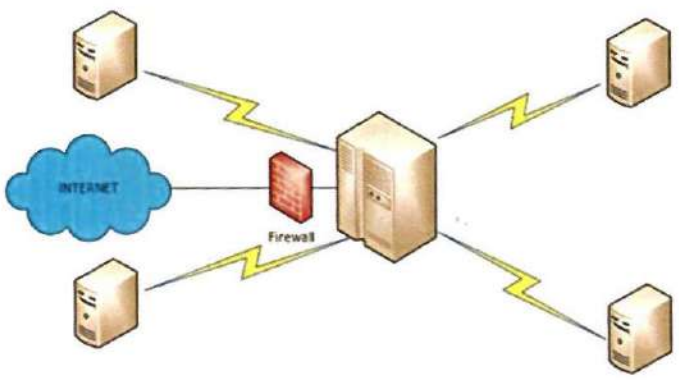


Diagrama de red LAN

- Esquema de red LAN de la sede central
- Switches de SIINCO

Los switches de SIINCO están encargados de administrar y gestionar todo el tráfico de la red

LAN y para garantizar la disponibilidad y continuidad de los servicios informáticos se realizó la configuración del protocolo VRRP (este protocolo garantiza la alta disponibilidad de la puerta de enlace de cada segmento de red).

Ambos switches de SIINCO administran las siguientes VLANs y segmentos de red definidas de la siguiente manera:

VLAN	ID	Descripción
DATOS 1	10	Segmento de red OTIC
DATOS 2	20	Segmento de red RRHH
DATOS 3	30	Segmento de red SUM
VOZ	40	Segmento de red de Telefonía
VIDEO	50	Segmento de red de CCTV
ADMINISTRACION	60	Segmento de red de la administración de switches
GESTION_AP	70	Segmento de red de la administración de los AP
WIFI CORPORATIVO	80	Segmento de red del Wifi Corporativo

- Switch de distribución

El switch de distribución se ha configurado en la modalidad de STACK, es decir ambos switches operan lógicamente como un único equipo. En esta configuración, se declara físicamente un Switch Primario como Slot1/Master y un Switch secundario como Slot 2/Backup. En caso de que el Switch primario se detectara inoperativo, no existirá ningún impacto ya que la comunicación seguiría por los enlaces redundantes del Switch secundario. Este switch conecta todos los switches de bordes con los switches de TP LINK.

La configuración aplicada en el switch de distribución está basada con la configuración de las VLANs que administra el switch TP LINK.

- Switches de acceso

Los switches de acceso se han configurado en la modalidad de STACK, es decir que switches que se encuentran apilados operan lógicamente como un único equipo. En esta configuración, se declara físicamente un Switch Primario como Slot1/Master y un Switch secundario como Slot 2/Backup y los switches que cuentan con 3 switches apilados tienen al Slot3 como rol de StandBy. En caso de que el Switch primario se detectara inoperativo, no existirá ningún impacto ya que la comunicación seguiría por los enlaces redundantes del Switch secundario. Los mencionados switches son de la marca Extreme Networks.

La configuración aplicada en todos los switches de acceso extiende las VLANs administradas por los switches de TP LINK

La alta disponibilidad de los switches de acceso consta en tener un enlace activo de 10 Gb y un enlace redundante de 1 Gb hacia el switch de distribución.

- Switches de sedes remotas

Los switches en sedes remotas se han configurado y utilizan el Servicio DHCP de los Firewall en cada sede.

  - 1 switch en la sede PTAP Pampa Inalámbrica
  - 1 switch en la sede R5 Pampa Inalámbrica

- Esquema de red inalámbrica de la sede central

Se cuenta con una red inalámbrica para visitantes y una red inalámbrica para clientes que permite el acceso a internet a los usuarios visitantes (usuarios) y a los usuarios clientes (clientes de EPS ILO S.A.) por medio de un portal cautivo donde los usuarios se ingresan manualmente a la base interna del ClearPass. Para el despliegue se configuró el SSID (red inalámbrica) con autenticación abierta y portal cautivo en los Access Point. Estas redes tienen políticas de Firewall.

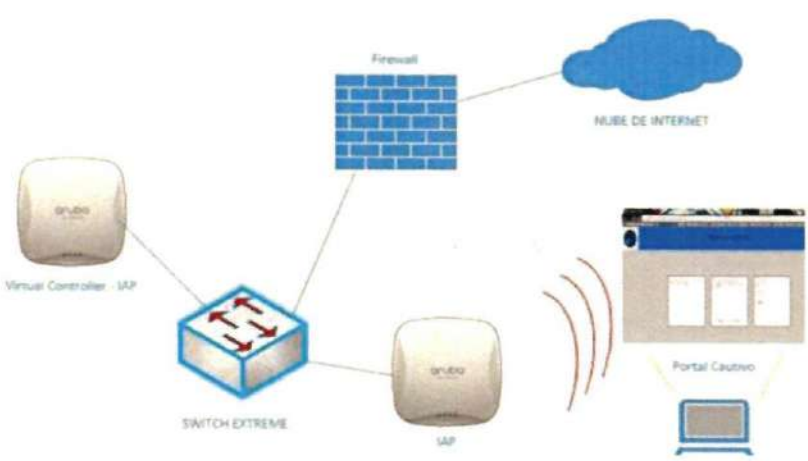


Diagrama de red inalámbrica para visitantes o clientes

Asimismo, se cuenta con una red inalámbrica para usuarios corporativos (Directorio Activo), la cual permite el acceso a los usuarios registrados en el Directorio Activo. Estos usuarios se registran con el mismo nombre de Dominio (Directorio Activo) que cada usuario tiene asignado para tener acceso a la navegación WEB. Para este despliegue se configuró el SSID (Red Inalámbrica) con autenticación WPA2-Empresa y se utiliza la base de datos del Directorio Activo. Los usuarios al conectarse a la red inalámbrica se le solicitara credenciales (usuarios y

contraseña) de dominio.

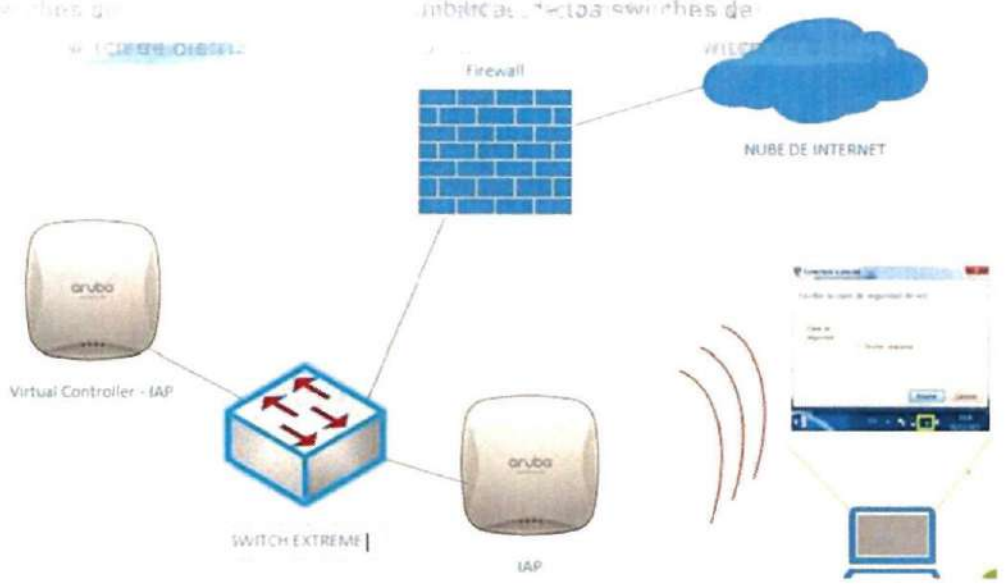


Diagrama de red inalámbrica para usuarios

- Alimentación eléctrica de equipos

EPS ILO S.A. cuenta con dos tipos de servicio de energía eléctrica, una es la tensión estabilizada (equipos electrónicos: computadoras personales, servidores, impresoras, fotocopiadoras, etc.) y la segunda de servicio común (equipos eléctricos y mecánicos: calentador, taladro, lustradora, etc.).

EPS ILO S.A. contrata el servicio de energía eléctrica a ELECTROSUR para la sede principal de ILO, y las Oficinas de R5, PTAP1 y PTAP2.

- Mantenimiento de equipos

No se cuenta con un contrato de mantenimiento preventivo y correctivo de las computadoras personales, laptops e impresoras hasta el año 2023, asimismo, se ha implementado una Mesa de Servicios TIC que permite gestionar en forma virtual el mantenimiento y control de los equipos, con el fin de reducir los tiempos de respuesta y automatizar el proceso de toma de inventarios de HW y SW base, instalación remota de software, soporte técnico de usuarios (gestión de licencias), gestión de incidentes, entre otros.

- Central telefónica

La central telefónica que se ha implementado desde el 2017 es un software open source, los

anexos telefónicos están compuestos por equipos de marca Yealink. Para la extensión de los anexos.

7.2. DATA CENTER

- Las zonas exteriores con constantemente vigiladas por personal de seguridad (24x7).
- Se cuenta con un sistema de videovigilancia mediante cámaras de videovigilancia y detección de intrusiones ubicadas en el edificio de la Sede Central, el Oficina de Tecnología de la Información y Comunicaciones y en el interior del DATA CENTER.
- Se cuenta con equipos que realizan la monitorización periódica de la temperatura y climatización del DATA CENTER para el correcto funcionamiento de los equipos de cómputo instalados en el mismo: a) un equipo de aire acondicionado York, que proporciona una temperatura adecuada al gabinete de comunicaciones y UPS
- Se cuenta con sistemas de protección contra incendios en el DATA CENTER: a) un sistema de control para supresión de incendios (extinguidor PQS), b) un sistema detector de humos por aspiración que emite avisos de forma temprana (inoperativo)
- Se cuenta con UPS (inoperativo).

7.3. Seguridad lógica

- Se cuenta con segmentación de redes, protegiendo equipos críticos. La red de EPS ILO S.A. se encuentra segmentada mediante VLANs: datos, voz y video.
- Se cuenta con firewalls para control de tráfico de las aplicaciones en todo momento, integración de usuarios y dispositivos en las políticas previniendo las amenazas conocidas y desconocidas.
- Se cuenta con un Sistema de Prevención de Intrusiones (IPS por sus siglas en inglés), software que ejerce control de acceso a la red protegiendo los sistemas de EPS ILO S.A. de intrusiones, ataques y abusos, asimismo, detecta actividad maliciosa e intenta detenerla.
- Se realiza la revisión de permisos de las cuentas de los usuarios proporcionando acceso adecuado para cubrir sus necesidades operativas.
- Se cuenta con un conjunto de políticas, directivas y grupos que protegen, gestionan y supervisan el acceso, los usuarios y las credenciales con privilegios.
- Se cuenta con el sistema de control granular Endpoint (marca BITDEFENDER) que asegura el cumplimiento de las políticas, en las cuales se especifica a qué recursos y aplicaciones en línea pueden acceder los usuarios y en qué momento hacerlo.
- Se cuenta con la solución corporativa de antivirus BITDEFENDER.
- Se cuenta con un sistema de control para la creación de respaldos periódicos de los datos.

7.4. Software

- Licencias de software

En cuanto a las licencias de software según el último inventario de la entidad se cuenta con la cantidad necesaria para los equipos informáticos que están operativos en la entidad usando en la totalidad software propietario. A continuación, se muestra el inventario de licencias de software

Software	Detalle adicional	Licencias
Windows 2016 Professional	Sistema operativo	
Windows 10 Professional	Sistema operativo	
Bitdefender Endpoint	Antivirus	118
Microsoft Visio	Office	
Microsoft Project	Office	
Autodesk Autocad	Software Diseño CAD	4
ZWCAD	Software Diseño CAD	8
ArcGIS	Software Diseño GIS	2
Windows Server 2012	Sistema operativo	10
Autodesk Autocad Civil 3D 2017	-	4
PROXMOX	Software de máquinas virtuales para servidores	1
SQL Server Enterprise SIINCO 2016	Gestor de base de datos	4
Microsoft Windows Server Standard 2016	Sistema operativo de red	4

Según las distribuciones de los sistemas operativos para los equipos de cómputo (computadoras personales y laptops) se puede apreciar que el 11.69% (49 de 419 licencias) cuentan con Windows 8 Professional, el 73.99% (310 de 419 licencias) cuentan con Windows 8.1 y el 14.32% (60 de 419 licencias) cuentan con Windows 10 Professional. Asimismo, según las distribuciones para los servidores se puede apreciar que el 10% (10 de 100 licencias) cuentan con Windows Server 8, el 10% (10 de 100 licencias) cuentan con Windows Server 2012 y el 80% (80 de 100 licencias) cuentan con Windows Server Standard 2016.

En lo concerniente al software de gestión de base de datos, la entidad tiene licencias la solución SQL Server Enterprise SIINCO 2016 (4 licencias). Todo lo descrito permite cumplir con la

normatividad en materia de licenciamiento de software en la entidad.

- Software público

Se está usando el software público "Sistema de Registro de Visitas", el cual pertenece a la Presidencia del Consejo de Ministros - Secretaría de Gobierno Digital y está publicado en el Portal de Software Público Peruano (PSPP). Actualmente no se cuenta con software para publicar en el PSPP de manera que pueda ser reutilizado por otras entidades.

7.5. Sistemas de información y aplicaciones

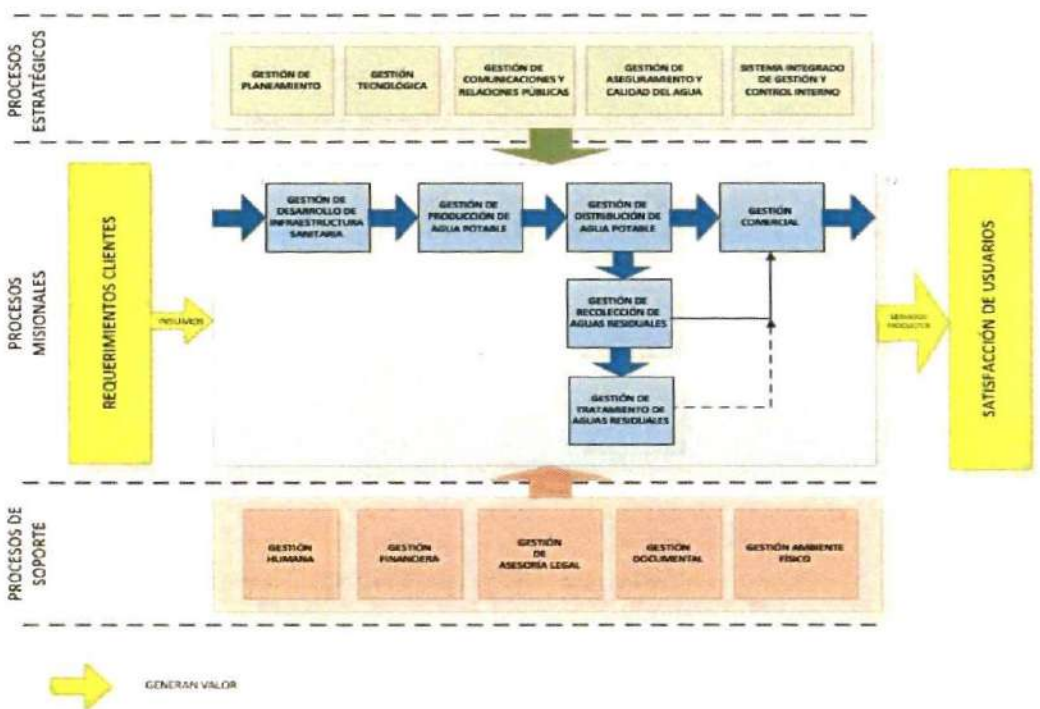
Los sistemas de información y aplicaciones que soportan los procesos y servicios de la entidad son los siguientes:

Sistema de información / Aplicación	Descripción		Situación	Puesta en producción	Áreas donde se utiliza
SIINCO	Soportar las operaciones comerciales: Reclamos Reconsideraciones Apelaciones Solicitud de servicio Cambio de categoría Cambio de titularidad Saldos Histórico de consumos Consulta de agentes de cobranza Pagos en línea	Leng. Programación: sybase	Producción	2016 - 2023	Gerencia Comercial: Todas las oficinas. Gerencia de Administración y Finanzas Oficina de Contabilidad Equipo de Finanzas
AVALON	Soporta las operaciones del área administrativa	Leng. Programación: Foxpro Visual	Producción	2010 - 2023	Gerencia de Administración y Finanzas Todas las oficinas. Todas las Oficinas para requerimiento.
Sistema de Gestión Documenta INTRANET	Registro y seguimiento de documentación interna y externa	Leng. Programación: Perl, Angular Base de Datos: PostgresSQL	Producción	2023	A nivel institucional
SIAF	Gestión de presupuesto institucional	Ejecutable	Producción	2016	Gerencia de Administración Equipo de Finanzas

					Gerencia General Planes y Presupuesto
Sistema de gestión documental INTRANET - E-TRAMI	Registro y seguimiento del trámite documentario	Leng. Programación: PHP Base de Datos: PostgreSQL	Producción	2023	A nivel institucional
Sistema de gestión documental INTRANET - E-DANA	Registro de incidencias operacionales	Leng. Programación: PHP Base de Datos: PostgreSQL	Producción	2023	A nivel institucional
Sistema de registro de visitas	Registro de visitas a la entidad	Leng. Programación: PHP Base de Datos: MySQL	Producción	2019	Gerencia de Administración y Finanzas

7.6. Procesos digitalizados

Dentro del marco de la política de modernización de la gestión pública vigente, la institución ha desarrollado la gestión por procesos, habiéndose identificado el mapa de procesos, el cual permite identificar la secuencia e interacción de los diferentes macroprocesos de la entidad:



De acuerdo con el mapa de procesos se desglosan los procesos hasta el nivel 1 y se han correlacionado con los sistemas de información de EPS ILO S.A., los que se muestran en el siguiente cuadro:

Procesos estratégicos				
Proceso Nivel 0 (Macroproceso)		Proceso Nivel 1		Sistema de información / Aplicación
Cód.	Descripción	Cód.	Descripción	
GPL	Gestión de planeamiento	GPL-P-100	Planeamiento Institucional	AVALON SIAF
GTE	Gobierno y gestión digital	GTE-P-100	Gestión de activos TIC	active directory
GCR	Gestión de comunicaciones y relaciones públicas	GCR-P-100	Imagen Institucional	
		GCR-P-200	Educación Sanitaria	
GAC	Gestión de aseguramiento y calidad del agua	GAC-P-100	Control de Calidad del Agua	
SIG	Sistema integrado de gestión y control interno	SIG-P-100	Gestión de Seguridad y Salud en el Trabajo	
		SIG-P-200	Gestión Ambiental	
		SIG-P-300	Satisfacción del Cliente Interno y Externo	
		SIG-P-400	Gestión de Control Interno	
GDI	Gestión de desarrollo de infraestructura sanitaria	GDI-P-100	Gestión de Estudios de Pre-Inversión	
		GDI-P-200	Gestión de Inversiones	
		GDI-P-300	Gestión de Servicios Colaterales	
GPA	Gestión de producción de agua potable	GPA-P-100	Potabilización del Agua Natural	
GDA	Gestión de distribución de agua potable	GDA-P-100	Almacenamiento y Distribución de Agua Potable	
GRA	Gestión de recolección de aguas residuales	GRA-P-100	Recolección de agua residual	
GTA	Gestión de tratamiento de aguas residuales	GTA-P-100	Tratamiento de agua residual	

GCO	Gestión comercial	GCO-P-100	Contratación de Nuevos Servicios	SIINCO
		GCO-P-200	Lectura y Facturación	SIINCO
		GCO-P-300	Recaudación y Cobranza	SIINCO
		GCO-P-400	Servicio de atención al cliente	SIINCO
GHU	Gestión humana	GHU-P-100	Reclutamiento, Evaluación y Selección de Personal	
		GHU-P-200	Control de Personal y Remuneraciones	AVALON
		GHU-P-300	Desarrollo del Talento Humano	
		GHU-P-400	Gestión Social y de Salud	
GFI	Gestión financiera	GFI-P-100	Gestión Contable	AVALON
		GFI-P-200	Gestión de Tesorería	AVALON SIAF
GAL	Gestión de asesoría legal	GAL-P-100	Defensa Legal	
		GAL-P-200	Asesoría Legal	
GDO	Gestión documental	GDO-P-100	Planeamiento y Control Documental	Sistema de gestión documental
		GDO-P-200	Conservación Archivística	
GAF	Gestión ambiente físico	GAF-P-100	Formulación y seguimiento del Plan Anual de Contrataciones	AVALON
		GAF-P-200	Adquisición de Bienes y Servicios	AVALON
		GAF-P-300	Mantenimiento infraestructura, parque automotor, maquinaria y equipos	
		GAF-P-400	Control Patrimonial	AVALON
		GAF-P-500	Administración de Catastro Técnico	ARC GIS

Podemos observar que los procesos de soporte y el proceso comercial cuentan con una o más soluciones tecnológicas que soportan de manera parcial o total las actividades de cada uno de los procesos, siendo los sistemas de información denominados SIINCO y AVALON los que tienen mayor presencia en estos procesos.

Se han identificado las siguientes brechas tecnológicas:

- Los procesos misionales, exceptuando el proceso comercial no tienen soluciones tecnológicas que los soporten.
- Para la generación de reportes e indicadores se utiliza más de una fuente de datos o en su defecto se trabaja de manera manual.
- Existencia de soluciones que requieren de innovación tecnológica.

Toda esta información será importante para un posterior análisis, la definición de los objetivos de Gobierno Digital y del portafolio de proyectos del Plan de Gobierno Digital.

7.7. Servicios digitales

La entidad cuenta con servicios digitales que pone a disposición a sus grupos de interés a través de diversos canales (aplicaciones móviles, páginas web y mensajes de texto) y cumplen con los principios: automático, no presencial y uso intensivo de las tecnologías digitales. La lista de servicios digitales es la siguiente:

Servicio digital	Descripción	Canal
Sistema de gestión documental	Servicio para el registro y seguimiento del trámite documentario.	Web
Reclamos	Servicio para la gestión de reclamos dentro de la Oficina Virtual	Web / Móvil
Solicitud de servicio	Servicio para la gestión de solicitud de servicio dentro de la Oficina Virtual	Web / Móvil
Saldos	Servicio para la consulta de saldos dentro de la Oficina Virtual	Web / Móvil
Histórico de consumos	Servicio para la consulta del histórico de consumos dentro de la Oficina Virtual	Web / Móvil
Consulta de agentes de cobranza	Servicio para la consulta de agentes de cobranza dentro de la Oficina Virtual	Web / Móvil
Pagos en línea	Servicio para la gestión de pagos en línea dentro de la Oficina Virtual	Web / Móvil
Interconexión para pagos en línea (BCP, SCOTIABANK y Caja AREQUIPA)	Servicio para la gestión de pagos en línea. Para BCP, SCOTIABANK,y Caja Arequipa se conecta a través de un acceso directo y una red privada virtual realizando transacciones a través de servicios web API REST. Para BCP se conecta a través de una red privada virtual por internet realizando transacciones a través de servicios web API REST.	Web / Móvil

Actualmente se encuentra por pasar a producción los siguientes servicios digitales:

Servicio digital	Descripción	Canal
Interconexión para pagos en línea (BCP, SCOTIABANK, Caja Arequipa)	Servicio para la gestión de pagos en línea	Web / Móvil

Los ciudadanos y personas en general desean poder obtener respuesta inmediata a su necesidad de información o de trámite / servicio. La coyuntura actual está llevando a EPS ILO S.A. a configurar sus servicios de esta manera.

8. RESPONSABILIDADES

- La Oficina de Tecnología de Información y Comunicaciones es la unidad encargada de desarrollar, implementar y gestionar los sistemas información, la infraestructura tecnológica y las telecomunicaciones que brindan soporte a las unidades orgánicas de la EPS ILO S.A.
- La Oficina de Distribución y Recolección de la Gerencia de Operaciones, es la unidad encargada de desarrollar, implementar y gestionar los sistemas eléctricos y la infraestructura correspondiente que brindan soporte a las unidades orgánicas de la EPS ILO S.A.

9. MARCO METODOLÓGICO

El presente Plan de Contingencia ha sido elaborado tomando como base las fases definidas en "Guía Práctica para el Desarrollo de Planes de Contingencia de Sistemas de información" publicada por el INEI. Es a partir de esta guía que son adoptadas las siguientes fases y son detalladas a continuación:

- Identificación de riesgos
- Estrategias para la recuperación de desastre, incidencia o evento.
- Realización de pruebas (implementación).

9.1. Las escalas a utilizar

- Escala cualitativa de probabilidades.

Constituye la representación de escalas descriptivas para demostrar la magnitud de consecuencias potenciales y su posibilidad de ocurrencia. Para cada riesgo identificado se evalúan los niveles de probabilidad e impacto.

CATEGORIA	DEFINICIÓN
ALTO	Es muy probable la materialización del riesgo o se presume que llegará a materializarse.
MEDIO	Es probable la materialización del riesgo o se presume que posiblemente se podrá materializar
BAJO	Es poco probable la materialización del riesgo o se presume que no llegará a materializarse.

- Escala cuantitativa de impacto.

El mismo diseño definido para la escala cualitativa es empleado para la escala cuantitativa, la cual es detallada a continuación:

CATEGORIA	DEFINICIÓN
ALTO	Si el hecho llegara a presentarse, se tendría alto impacto o efecto sobre la entidad.
MEDIO	Si el hecho llegara a presentarse, se tendría media impacto o efecto sobre la entidad
BAJO	Si el hecho llegara a presentarse, se tendría bajo impacto o efecto sobre la entidad.

- Escalas cuantitativas de probabilidad e impacto.

A continuación, son descritas las escalas cuantitativas de probabilidad e impacto:

NIVEL	PROBABILIDAD DE OCURRENCIA
BAJO	1
MEDIO	2
ALTO	3

NIVEL	IMPACTO
BAJO	1
MEDIO	2
ALTO	3

9.2. Evaluación y clasificación de riesgo

Se describe la Evaluación y Clasificación de riesgos.

		PROBABILIDAD		
		1 BAJO	2 MEDIO	3 ALTO
IMPACTO	1 BAJO	(1) Riesgo Aceptable	(2) Riesgo Tolerante	(3) Riesgo Moderado
	2 MEDIO	(2) Riesgo Tolerante	(4) Riesgo Moderado	(6) Riesgo Importante
	3 ALTO	(3) Riesgo Moderado	(6) Riesgo Importante	(9) Riesgo Inaceptable

9.3. Niveles de Riesgo

Nivel de Riesgo (Cualitativo)	Nivel de Riesgo (Cuantitativo)	Prioridad	Descripción
Riesgo Aceptable	1	Muy Baja	Riesgo insignificante. No se requiere ninguna acción.
Riesgo Tolerante	2	Baja	Menores efectos que pueden ser fácilmente remediados, se administran con procedimientos rutinarios.
Riesgo Moderado	3 y 4	Medio	Debe ser administrado con procedimientos normales de control.
Riesgo Importante	6	Alta	Se requieren planes de tratamiento requeridos, implementados y reportados a los jefes de las oficinas, direcciones entre otros.
Riesgo Inaceptable	9	Muy Alta	Se requiere acción inmediata, planes de tratamiento requeridos, implementados y reportados a la alta dirección.

Cuantificación de Riesgos

Los riesgos serán cuantificados de acuerdo a dos factores:

Probabilidad, que representa la posibilidad de que se presente el desastre, incidencia o evento.

Impacto, representa la envergadura del riesgo, es decir cuánto puede afectar

RIESGO = PROBABILIDAD X IMPACTO

10. IDENTIFICACIÓN DE RIESGOS

10.1. Análisis de riesgo.

La empresa está expuesta a riesgos que pueden ser causados por eventos fortuitos o por el mal uso de los recursos, pudiendo afectar los objetivos o las metas trazadas por la empresa. En ese sentido, la identificación de los riesgos se encuentra referidos a aquellos que afectan la seguridad del centro de datos, el cual trae como consecuencia la indisponibilidad, y afecta la operación y continuidad de los servicios.

10.2. Relación de riesgos que pueden afectar al DATA CENTER

A continuación, son detallados riesgos identificados at Data Center de la EPS ILO S.A. y se describen a continuación:

#	Riesgo Identificado	Descripción del riesgo	Consecuencia
1	Terremoto	Fenómeno natural manifestado por una sacudida brusca de la corteza terrestre producida por la liberación de energía acumulada en forma de ondas sísmicas.	Destrucción del ambiente destinado para el centro de datos, generando la interrupción de todos los servicios que brinda.
2	Vandalismo.	Se refiere a atentados que podrían afectar o destruir las instalaciones, equipos, programas informáticos, datos, documentación y el ministerio, por su función está expuesto a ser afectado.	Interrupción parcial o total de los servicios que brinda el centro de datos.
3	Fraude.	Evento referido a la alteración o sustracción de datos para uso en contra de la institución o en beneficio del autor del acto.	Uso ilícito de los recursos de la Empresa en contra de la institución.
4	Intrusión de la red.	Ataques que provienen localmente o de Internet, originados por hackers, virus con la finalidad de alterar el normal funcionamiento de los recursos informáticos.	Interrupción parcial o total de los servicios que brinda el centro de datos.

5	Inundación / aniego.	Ocupación de agua en zonas que habitualmente están libres debido al desbordamiento de ríos, torrentes, lluvias torrenciales, deshielo, por subida de las mareas por encima del nivel habitual, por maremotos entre otros.	Equipos inservibles por el ingreso de agua al ambiente destinado para el centro de datos, generando la interrupción de todos los servicios que brinda.
6	Incendio.	Ocurrencia de fuego no controlado que puede afectar los bienes.	Destrucción del ambiente destinado para el centro de datos, generando la interrupción de todos los servicios que brinda.
7	Falta de fluido Eléctrico.	Pérdida del suministro eléctrico en el centro de datos.	Perdida del suministro de energía eléctrica en el centro de datos, pudiendo originar daño en los equipos sensibles, perdida de información originando una interrupción en los servicios que brinda el centro de datos

10.3. Cuantificación de los riesgos identificados

En el siguiente cuadro se detallan la clasificación de los riesgos identificados en atención a lo señalado en la metodología definida.

#	Riesgo Identificado	Probabilidad (P)	Impacto (I)	(P)x(I)	Nivel de Riesgo
1	Terremoto	3	3	9	Riesgo Inaceptable
2	Falta de fluido Eléctrico	2	3	6	Riesgo Importante
3	Intrusión de la red	2	2	4	Riesgo Moderado
4	Inundación / aniego	1	3	3	Riesgo Moderado
5	Incendio	1	3	3	Riesgo Moderado
6	Vandalismo	1	2	2	Baja
7	Fraude	1	2	2	Baja

De la valoración realizada en la matriz probabilidad por impacto, se ha identificado que existen riesgos cuyo nivel han sido valorados como importante y moderado según la probabilidad y el impacto que estos podrán generar en el centro de datos de producirse.

En ese sentido, concluimos que el análisis evidencia las posibles contingencias que pudieran presentarse y afectar a los sistemas de información y la plataforma que permite su operación, para lo cual el presente "PLAN DE CONTINGENCIA" desarrollara las estrategias a fin de poder mitigar los

RIESGOS IMPORTANTES y RIESGOS MODERADOS identificados

11. ESTRATEGIA PARA LA RECUPERACIÓN DE DESASTRES

La generalización del uso de los medios electrónicos, informáticos y telemáticos supone beneficios, pero también riesgos asociados ante la ocurrencia de un desastre, incidente o evento por lo que se debe mitigar su impacto non acciones que permitan dar continuidad de los servicios de TI, por lo que son definidas acciones antes (preventivas), durante y después (reactivas)

11.1. Actividades previas al desastre (Preventiva)

Son aquellas actividades de planeamiento, preparación, entrenamiento y ejecución de las acciones de resguardo de información que nos permita un proceso de recuperación viable de los servicios de TI proporcionados por el Data Center de la EPS ILO S.A., En ese sentido, se hace necesario el contar con la siguiente información:

- Sistemas de Información

  La Oficina de Tecnología de la Información y Comunicaciones de la EPS ILO S.A., deberá contar con una relación de los Sistemas de Información (anexo 1); dicha relación debe considerar la siguiente información:

  - Nombre de la aplicación o Sistema.
  - Lenguaje con el que fue creado el Sistema, incluyendo la relación de librarías que lo conforman.
  - Área usuaria, esto es el área usuaria dueña del proceso sistematizado.
  - Las unidades orgánicas y entidades (internos/ externos) que usan la información del Sistema.
  - El volumen de los archivos (en MB) que trabaja el Sistema, si fuera el caso.
  - El Tamaño de la base de datos (en MB).
  - La(s) fecha(s) criticas, en las que la información es necesaria y debe estar disponible.

- Hardware del centro de datos

  - La Oficina de Tecnología de la Información y Comunicaciones de la EPS ILO S.A. deberá inventariar los servidores y PCs de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación.
  - Alta disponibilidad de hardware del centro de datos; El centro de datos principal ubicado en la Sede administrativa, deberá contar con un centro de datos alterno a nivel de hardware y software en otra Sede Comercial permitiendo la continuidad de negocio, en

este caso se probará y asegurará que los procesos de restauración de información posibiliten el funcionamiento adecuado de los sistemas

- Respaldo de la información (Backups)

Establecer los procedimientos (políticas o procedimientos de backup determinando responsabilidades en la obtención de los Backups críticos identificados) para la obtención de copias de seguridad necesarios para asegurar la disponibilidad de la información para la correcta ejecución de los sistemas o aplicativos ante la ocurrencia de un desastre, incidente o evento tales como:

- Archivos de configuración de aplicativos
- Código fuente de aplicativos
- Documentos adjuntos de aplicativos
- Archivos de unidades compartidas
- Motor de Base de datos
- Software base de PCs y Servidores

- Entrenamiento

Establecer un programa de Prácticas periódicas de todo el personal en la lucha contra los diferentes tipos de siniestros, de acuerdo a los roles que se le hayan asignado en los planes de evacuación del personal o equipos.

Un aspecto importante es que el personal tome conciencia de que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) pueden realmente ocurrir, y tomen con seriedad y responsabilidad estos entrenamientos, para estos efectos es conveniente que participen los elementos directivos, dando el ejemplo de la importancia que la alta dirección otorga a la Seguridad Institucional.

- Formación de equipos de evaluación

Esta función debe ser realizada de preferencia por personal externo con experiencia en Seguridad de la Información, de no ser posible, la realizará el personal de la Oficina de Tecnología de la Información y Comunicaciones, debiendo establecerse claramente sus funciones, responsabilidades y objetivos:

- Revisar el cumplimiento de las normas y/o procedimientos con respecto a Backups y seguridad de equipos y data.
- Supervisar la realización periódica de los backups, por parte de los equipos operativos, comprobando físicamente su realización, adecuado registro y almacenamiento.
- Revisar la correlación entre la relación de sistemas e informaciones necesarios para la buena marcha de la Empresa, y los backups realizados.
- Informar de los cumplimientos e incumplimientos de las normas y/o procedimientos, para las acciones de corrección respectivas.

11.2. Actividades durante el desastre.

Una vez presentada la contingencia, es necesaria la participación de todas las personas del área donde ocurre la contingencia para lo cual se debe:

- Plan de emergencias.

  En este plan se establecen las acciones se deben realizar cuando se presente un Siniestro, además deberá incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre el siniestro, debiendo detallar:

  - Vías de salida o escape.
  - Plan de Evacuación del Personal.
  - Plan de puesta a buen recaudo de los activos (incluyendo los activos de Información) de la Institución (si las circunstancias del siniestro lo posibilitan).
  - Ubicación y señalización de los elementos contra el siniestro (extinguidores, cobertores contra agua, etc.).
  - Secuencia de llamadas en caso de siniestro, tener a la mano: elementos de iluminación (linternas), lista de teléfonos de Bomberos / Ambulancia, Policía Nacional del Perú y de su personal (equipos de seguridad) asignados para estos casos.
  - Se debe seguir lo señalado en las fichas de contingencia para los casos identificados en el presente plan de contingencia (anexo 3)

- Formación de equipos

  El personal de la Oficina de Tecnología de la Información y Comunicaciones, es el responsable del salvamento de equipos informáticos, de acuerdo a la clasificación de prioridades.

11.3. Actividades después del desastre

Después de ocurrido el Siniestro o Desastre es necesario realizar las actividades que se detallan, para restaurar todos los servicios de TI y la operación de la empresa:

- Evaluación de Daños

  Inmediatamente después que el desastre, incidente o evento ha concluido, se evaluará la magnitud de los daños producidos, estableciendo que sistemas están afectados, que equipos han quedado inoperativos, cuales se pueden recuperar y en cuanto tiempo de acuerdo a la matriz de probabilidad por impacto. Luego de la evaluación, se identificarán las actividades a ser desarrolladas a fin de restaurar los servicios de TI afectados para lo cual se deberá tomar

como referencia las actividades descritas en las fichas de contingencia identificadas (anexo 3).

- Priorización de Actividades

Si el siniestro es general y contempla una pérdida total; la evaluación de daños reales y su comparación contra el plan, proporcionará la lista de las actividades a realizar en función de la prioridad.

Es importante evaluar la dedicación del personal a actividades que puedan no haberse afectado, a fin de asignarlos en forma temporal a las actividades afectadas, en apoyo al personal de los sistemas afectados y soporte técnico.

- Ejecución de Actividades

Las actividades identificadas y priorizadas para la recuperación de ocurrido el desastre, incidente o evento, deberán ser realizadas por los equipos de trabajo y se contará con un coordinador que reportará el avance de los trabajos de recuperación al encargado del Plan de Contingencias. Las actividades de recuperación serán en dos etapas:

  - La primera, la restauración de los servicios priorizados de TI del centro de datos.
  - La segunda, es volver a contar con todos los servicios y los recursos informáticos, debiendo ser esta última etapa lo suficientemente rápida y eficiente en la medida de lo posible.

- Evaluación de Resultados

Una vez concluidas las labores de Recuperación de los servicios de TI que fueron afectados por el siniestro, debemos de evaluar objetivamente, todas las actividades realizadas, que tan bien se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades de recuperación de los servicios, como se comportaron los equipos de trabajo, etc.

De la Evaluación de resultados y del siniestro en si, deberían de salir dos tipos de recomendaciones, una la retroalimentación del plan de Contingencias y otra una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionaron el siniestro

- Retroalimentación

Con la evaluación de resultados, debemos de optimizar el Plan de Contingencia original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente

11.4. Realizar pruebas de implementación

El equipo operativo será conformado por los colaboradores que designe el Área de TI y el oficial de

seguridad de la información, esto con la finalidad de realizar las pruebas antes de ocurrir un desastre, incidente o evento ocurra. Las actividades que serán realizadas corresponden a:

- Supervisar los procedimientos de respaldo y restauración de los sistemas de información.
- Participar en las pruebas y simulacros de desastres.
- Contar con un listado de personas que serán contactadas de ocurrir un desastre (anexo 2).

12. DISPOSICIONES FINALES

- El Plan de Contingencias de TI deberá contar con el apoyo correspondiente por parte de la Alta Dirección, para suministrar de recursos financieros y humanos a fin de su implementación y ejecución.
- Realizar la conformación de un Comité el encargado de planificar, implementar y supervisar la ejecución del Plan de Contingencia, que asegure la legalidad, consistencia, adecuado uso, seguridad, inviolabilidad y sostenibilidad de los Sistemas de Información, hardware y software.
- La actualización del presente plan de contingencia debe ser realizado una vez al año.
- Todos los colaboradores que laboren en el Área de TI, deben formar parte de las actividades y están obligados a participar en la implementación y ejecución del Plan de Contingencias de TI.
- Definir políticas de seguridad, como una herramienta para el control permanente del cumplimiento del Plan de Contingencia.
- Las medidas que debemos adoptar para protegernos son tantas como amenazas existen, es por ello que se debe difundir a todas las unidades operativas de EPS ILO S.A. el presente plan de contingencia.
- Realizar las acciones necesarias para cumplir y hacer cumplir los objetivos y funciones determinadas en el presente Plan de Contingencia.
- Contar con un centro de datos alterno a fin de minimizar el tiempo de recuperación de los servicios de TI.
- Se debe prever contar con un sistema de respaldo eléctrico (UPS más banco de baterías) exclusivo para ambos centros de datos; y que la trasferencia de energía sea de manera automática.

La **Oficina de Tecnología de Información y Comunicaciones**, coordinará, evaluará y propondrá las medidas pertinentes para solucionar todo aquello relacionado al uso Adecuado de los Equipos de Cómputo y Servicios Informáticos, que no estén contemplados en la presente directiva.

ANEXO 1: RELACIÓN DE LOS SISTEMAS DE INFORMACIÓN

Sistema de información / Aplicación	Descripción		Situación	Puesta en producción	Áreas donde se utiliza
SIINCO	Soportar las operaciones comerciales: Reclamos Reconsideraciones Apelaciones Solicitud de servicio Cambio de categoría Cambio de titularidad Saldos Histórico de consumos Consulta de agentes de cobranza Pagos en línea	Leng. Programación: sybase	Producción	2016 – 2023	Gerencia Comercial: Gerencia de Administración y Finanzas Oficina de Contabilidad Equipo de Finanzas
AVALON	Soporta las operaciones del área administrativa	Leng. Programación: Foxpro Visual	Producción	2010 – 2023	Gerencia de Administración y Finanzas Todas las Oficinas para requerimiento.
Sistema de Gestión Documenta INTRANET	Registro y seguimiento de documentación interna y externa	Leng. Programación: Perl, Angular Base de Datos: PostgresSQL	Producción	2023	A nivel institucional
SIAF	Gestión de presupuesto institucional	Ejecutable	Producción	2016	Gerencia de Administración Equipo de Finanzas Gerencia General Planes y Presupuesto
Sistema de gestión documental INTRANET - E-TRAMI	Registro y seguimiento del trámite documentario	Leng. Programación: PHP Base de Datos: PostgreSQL	Producción	2023	A nivel institucional
Sistema de gestión documental INTRANET - E-DANA	Registro de incidencias operacionales	Leng. Programación: PHP Base de Datos: PostgreSQL	Producción	2023	A nivel institucional
Sistema de registro de visitas	Registro de visitas a la entidad	Leng. Programación: PHP Base de Datos: MySQL	Producción	2019	Gerencia de Administración y Finanzas

ANEXO 2: DESCRIPCIÓN DE EQUIPOS DE TRABAJOS

EQUIPO DE RESPUESTA A EMERGENCIA EN EL CENTRO DE DATOS			
Nro.	**Nombre de Personal**	**Cargo**	**Celular/Teléfono**
01	Milagros Karin Caytano Aguilar	Gerente de Administración y Finanzas	954 665 880
02	Jose Luis Portugal Astoquilca	Jefe de Oficina de Tecnología de Información y Comunicaciones	997 352 230
03	Wilbert Jose Torrico Quispe	Analista en Tecnología de la información y comunicaciones	997 353 430

EQUIPO DE RESPUESTA DE EMERGENCIA DE SEGURIDAD PERIMETRAL			
Nro.	**Nombre de Personal**	**Cargo**	**Celular/Teléfono**
01	Milagros Karin Caytano Aguilar	Gerente de Administración y Finanzas	954 665 880
02	Jose Luis Portugal Astoquilca	Jefe de Oficina de Tecnología de Información y Comunicaciones	997 352 230
03	Wilbert Jose Torrico Quispe	Analista en Tecnología de la información y comunicaciones	997 353 430

EQUIPO DE RESPUESTA DE EMERGENCIA DEL CENTRO DE DATOS			
Nro.	**Nombre de Personal**	**Cargo**	**Celular/Teléfono**
01	Milagros Karin Caytano Aguilar	Gerente de Administración y Finanzas	954 665 880
02	Jose Luis Portugal Astoquilca	Jefe de Oficina de Tecnología de Información y Comunicaciones	997 352 230
03	Wilbert Jose Torrico Quispe	Analista en Tecnología de la información y comunicaciones	997 353 430

E.P.S. ILO S.A. GERENCIA GENERAL - ILO -

E.P.S. ILO S.A. GERENCIA ADMINISTRACIÓN Y FINANZAS - ILO -

E.P.S. ILO S.A. - ILO -

E.P.S. ILO S.A. GERENTE ASESORÍA JURÍDICA - ILO -

ANEXO 3: DESCRIPCIÓN DE ACTIVIDADES POR TIPO DE RIESGO

ANEXO 3:1 Riesgo: TERREMOTO

a) DESCRIPCIÓN DEL EVENTO

Un terremoto es un movimiento de la corteza terrestre que se percibe como una vibración brusca y que es producido por la liberación de energía en forma de ondas sísmicas desde el interior del planeta. Las principales partes de un terremoto son el hipocentro y el epicentro. Además, podemos decir que hay diferentes tipos de terremotos según si su origen es natural o antrópicas.

b) CUANTIFICACIÓN DE LOS RIESGOS

#	Riesgo Identificado	Probabilidad (P)	Impacto (I)	(P)x(I)	Nivel de Riesgo
1	Terremoto	3	3	9	Riesgo Inaceptable

c) ACTIVIDADES DE PREVENCIÓN (ANTES)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES				
RESPONSABILIDAD				
ACTIVIDADES	GG	GAF	JOTIC	ATIC
Actividades preventivas (antes)	I	I	RC	E
I: Informado R: Responsable C: Consultado E: Encargado				

JEFE DE OFICINA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES (JOTIC)

- Verificar que se realicen respaldos de la información de manera periódica por la ATIC, debiendo generar la respectiva acta de evidencia.

ANALISTA EN TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES (ATIC)

- Contar con respaldos actualizados de los datos electrónicos de la Empresa, almacenados fuera del inmueble y/o en el centro de datos alterno.
- Asegurar que los elementos que se encuentran en el centro de datos sean ubicados de manera tal que permanezcan estables durante la contingencia y cumplan con el estándar para centro de datos

- Se mantendrán cerradas las puertas de los gabinetes a fin de minimizar la caída de equipos u otros.

d) **ACTIVIDADES DE EJECUCIÓN (DURANTE).**

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES				
	RESPONSABILIDAD			
ACTIVIDADES	GG	GAF	JOTIC	ATIC
Actividades preventivas (antes)	I	I	RC	E
I: Informado R: Responsable C: Consultado E: Encargado				

JEFE DE OFICINA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES (JOTIC)

- Realizar el monitoreo del incidente

ANALISTA EN TECNOLOGIA DE LA INFORMACION Y COMUNICACIONES (ATIC)

- Evacuar el área si es necesario, utilizando las rutas de emergencia buscando un lugar seguro y evitando ventanas, así como el uso de escaleras

e) **ACTIVIDADES DE RECUPERACIÓN (DESPUES).**

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES				
	RESPONSABILIDAD			
ACTIVIDADES	GG	GAF	JOTIC	ATIC
Actividades preventivas (antes)	I	I	RC	E
I: Informado R: Responsable C: Consultado E: Encargado				

JEFE DE OFICINA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES (JOTIC)

- Registrar lo sucedido; así como las actividades que fueron realizadas para su solución debiendo llevar un control del mismo en un registro de evidencia de riesgo.
- Analizar lo ocurrido a fin de retroalimentar el Plan de contingencia (mejora continua) y actualizar las fichas de contingencia.

ANALISTA EN TECNOLOGIA DE LA INFORMACION Y COMUNICACIONES (ATIC)

- Levantar los servicios replicados en el centro de datos alterno, si fuera el caso. No ingresar al área afectada hasta que las respectivas brigadas y/o autoridades
- indiquen que es seguro. Al ingresar hacerlo con cuidado y únicamente si cuenta con la

protección necesaria.

- Realizar un diagnóstico preliminar al ingresar al centro de datos afectado por la
- contingencia, para detectar el nivel de daño y así solicitar el equipo, material y personal necesarios para su recuperación y/o reemplazo.

ANEXO 3:2 Riesgo: FALTA DE FLUIDO ELÉCTRICO

a) DESCRIPCIÓN DEL EVENTO

Pérdida de electricidad a corto o largo plazo en una zona, y puede tener muchas causas, como fallos en una estación eléctrica, daños en las líneas de transmisión, subestaciones u otras partes del sistema de distribución, un cortocircuito o una sobrecarga de la alimentación eléctrica.

b) CUANTIFICACIÓN DE LOS RIESGOS

#	Riesgo Identificado	Probabilidad (P)	Impacto (I)	(P)x(I)	Nivel de Riesgo
2	Falta de fluido Eléctrico	2	3	6	Riesgo Importante

c) ACTIVIDADES DE PREVENCIÓN (ANTES)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES				
RESPONSABILIDAD				
ACTIVIDADES	GG	GAF	JOTIC	ATIC
Actividades preventivas (antes)	I	I	RC	E
I: Informado R: Responsable C: Consultado E: Encargado				

JEFE DE OFICINA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES (JOTIC)

- Proveer sistema eléctrico de abastecimiento (UPS + banco de baterías), independiente en el centro de datos con un tiempo de autonomía suficiente para que se pueda activar el centro de datos alterno
- Realizar las coordinaciones del caso con el área de Logística para llevar a cabo el mantenimiento periódico del UPS

ANALISTA EN TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES (ATIC)

- Realizar pruebas periódicas del sistema de abastecimiento eléctrico.
- Realizar las configuraciones respectivas de fallas, caídas o problemas del UPS.

d) ACTIVIDADES DE EJECUCIÓN (DURANTE).

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES				
RESPONSABILIDAD				
ACTIVIDADES	GG	GAF	JOTIC	ATIC
Actividades preventivas (antes)	I	I	RC	E
I: Informado R: Responsable C: Consultado E: Encargado				

JEFE DE OFICINA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES (JOTIC)

- Realizar el monitoreo del incidente

ANALISTA EN TECNOLOGIA DE LA INFORMACION Y COMUNICACIONES (ATIC)

- Validar que el UPS este activo y en operación durante el corte de fluido eléctrico.
- Realizar el apagado de los equipos y/o dispositivos cuyo uso no sea prioritario.
- Levantar los servicios replicados en el centro de datos alterno, si fuera el caso.

e) **ACTIVIDADES DE RECUPERACIÓN (DESPUES).**

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES				
RESPONSABILIDAD				
ACTIVIDADES	GG	GAF	JOTIC	ATIC
Actividades preventivas (antes)	I	I	RC	E
I: Informado R: Responsable C: Consultado E: Encargado				

JEFE DE OFICINA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES (JOTIC)

- Registrar lo sucedido; así como las actividades que fueron realizadas para su solución debiendo llevar un control del mismo en un registro de evidencia de riesgo.
- Analizar lo ocurrido a fin de retroalimentar el Plan de contingencia (mejora continua) y actualizar las fichas de contingencia.

ANALISTA EN TECNOLOGIA DE LA INFORMACION Y COMUNICACIONES (ATIC)

- Constatar el buen funcionamiento de todos los equipos y dispositivos de computo.

ANEXO 3:3 Riesgo: INTRUSIÓN DE LA RED

a) DESCRIPCIÓN DEL EVENTO

Una intrusión en la red denota cualquier actividad no autorizada o agresiva en una red digital. Las actividades no autorizadas pueden poner en riesgo la seguridad de las redes y los datos. En el mundo digital actual, las pequeñas y grandes empresas están sujetas a estos ataques

Ataques que provienen desde Internet, originales por hackers, virus con la finalidad de alterar el normal funcionamiento de los recursos

b) CUANTIFICACIÓN DE LOS RIESGOS

#	Riesgo Identificado	Probabilidad (P)	Impacto (I)	(P)x(I)	Nivel de Riesgo
3	Intrusión de la red	2	2	4	Riesgo Moderado

c) ACTIVIDADES DE PREVENCIÓN (ANTES)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES				
RESPONSABILIDAD				
ACTIVIDADES	GG	GAF	JOTIC	ATIC
Actividades preventivas (antes)	I	I	RC	E
I: Informado R: Responsable C: Consultado E: Encargado				

JEFE DE OFICINA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES (JOTIC)

- Verificar que se realicen respaldos de la información de manera periódica, debiendo generar la respectiva acta de evidencia.
- Verificar se cuente con la actualización y el soporte vigente del IPS y el antivirus, debiendo generar la respectiva acta de evidencia.

ANALISTA EN TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES (ATIC)

- Contar con respaldos actualizados de los datos electrónicos de la Empresa, almacenados fuera del inmueble y/o en el centro de datos alterno.
- Contar con los equipos de seguridad perimetral actualizados y con soporte vigente.
- Contar con antivirus instalados en las PC y servidores, actualizados y con soporte vigente.

d) ACTIVIDADES DE EJECUCIÓN (DURANTE).

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES				
	RESPONSABILIDAD			
ACTIVIDADES	GG	GAF	JOTIC	ATIC
Actividades preventivas (antes)	I	I	RC	E
I: Informado R: Responsable C: Consultado E: Encargado				

JEFE DE OFICINA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES (JOTIC)

- Realizar el monitoreo del incidente

ANALISTA EN TECNOLOGIA DE LA INFORMACION Y COMUNICACIONES (ATIC)

- Confirmada la presencia de una intrusión en la red, se deberá investigar su origen para lo cual se debe comprobar cuáles son los equipos y servicios que se están siendo comprometidos a fin de identificar los causantes del ataque.
- Desconectar el o los equipos infectados de la red.
- Visualizar los procesos activos en los servidores a fin de identificar comportamiento inusual en estos, debiendo considerar:
  - Procesos que llevan activos un largo periodo de tiempo
  - Procesos que consumen un nivel elevado de CPU
  - Procesos que no están ejecutados desde una PC perteneciente a la red del EPS ILO S.A.
- Revisar los archivos de registro (log) a fin de obtener información sobre
- conexiones a lugares poco frecuentes, utilización de aplicaciones inusuales y otras actividades sospechosas de intrusión.
- Chequeo de los archivos del sistema a fin de detectar si han sido modificados.
- Comprobar los puertos de conexión abiertos; a fin de detectar si hay alguno en especial que no lo debería ser.
- Comprobar la existencia de sniffers en la red de EPS ILO S.A.

e) ACTIVIDADES DE RECUPERACIÓN (DESPUES).

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES				
	RESPONSABILIDAD			
ACTIVIDADES	GG	GAF	JOTIC	ATIC
Actividades preventivas (antes)	I	I	RC	E

I: Informado R: Responsable C: Consultado E: Encargado

JEFE DE OFICINA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES (JOTIC)

- Registrar lo sucedido; así como las actividades que fueron realizadas para su solución debiendo llevar un control del mismo.
- Identificar las oportunidades de mejora a fin de retroalimentar el plan de contingencia.
- Analizar lo ocurrido a fin de retroalimentar el Plan de contingencia (mejora ·continua) y actualizar las fichas de contingencia.

ANALISTA EN TECNOLOGIA DE LA INFORMACION Y COMUNICACIONES (ATIC)

- De detectarse que la incidencia ha afectado a algún componente de software o hardware del servidor, se debe comunicar al dueño de la información a fin de que verifique su impacto.
- Si se comprueba que los equipos de seguridad han fallado en la detección de intrusos, debe recurrirse al proveedor a fin de comunicar el hecho.

ANEXO 3:4 Riesgo: INUNDACIÓN / ANIEGO

a) DESCRIPCIÓN DEL EVENTO

Un fenómeno natural es un evento de cambio que ocurre en la naturaleza, en cuyo origen el ser humano tiene poco o nada que ver. Esto puede abarcar desde un evento recurrente y cotidiano, hasta uno fortuito, sorprendente o catastrófico. En el último caso, puede usarse también el término desastre natural.

b) CUANTIFICACIÓN DE LOS RIESGOS

#	Riesgo Identificado	Probabilidad (P)	Impacto (I)	(P)x(I)	Nivel de Riesgo
4	Inundación / aniego	1	3	3	Riesgo Moderado

c) ACTIVIDADES DE PREVENCIÓN (ANTES)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES				
RESPONSABILIDAD				
ACTIVIDADES	GG	GAF	JOTIC	ATIC
Actividades preventivas (antes)	I	I	RC	E
I: Informado R: Responsable C: Consultado E: Encargado				

JEFE DE OFICINA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES (JOTIC)

- Verificar se realicen respaldos de la información de manera periódica, debiendo generar la respectiva acta de evidencia

ANALISTA EN TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES (ATIC)

- Contar con respaldos actualizados de los datos electrónicos de la Empresa, almacenados fuera del inmueble y/o en el centro de datos alterno

d) ACTIVIDADES DE EJECUCIÓN (DURANTE).

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES
RESPONSABILIDAD

ACTIVIDADES	GG	GAF	JOTIC	ATIC
Actividades preventivas (antes)	I	I	RC	E
I: Informado R: Responsable C: Consultado E: Encargado				

(antes)

JEFE DE OFICINA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES (JOTIC)

- Realizar el monitoreo del incidente

ANALISTA EN TECNOLOGIA DE LA INFORMACION Y COMUNICACIONES (ATIC)

- Evacuar el área, utilizando las rutas de emergencia de ser el caso
- Únicamente si las brigadas y/o autoridades indiquen que es seguro, desconectar los equipos de comunicaciones y servidores del centro de cómputo considerando su correcto apagado, de ser factible.

e) ACTIVIDADES DE RECUPERACIÓN (DESPUES).

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES				
RESPONSABILIDAD				
ACTIVIDADES	GG	GAF	JOTIC	ATIC
Actividades preventivas (antes)	I	I	RC	E
I: Informado R: Responsable C: Consultado E: Encargado				

JEFE DE OFICINA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES (JOTIC)

- Registrar lo sucedido; así como las actividades que fueron realizadas para su solución debiendo llevar un control del mismo en un registro de evidencia de riesgo.
- Analizar lo ocurrido a fin de retroalimentar el Plan de contingencia (mejora continua) y actualizar las fichas de contingencia.

ANALISTA EN TECNOLOGIA DE LA INFORMACION Y COMUNICACIONES (ATIC)

- Levantar los servicios replicados en el centro de datos alterno, si fuera el caso.
- No ingresar al área afectada hasta que las respectivas brigadas y/o autoridades
- indiquen que es seguro. Al ingresar hacerlo con cuidado y únicamente si cuenta con la protección necesaria.
- Realizar un diagnóstico preliminar al ingresar al centro de datos afectado por la contingencia, para detectar el nivel de daño y así solicitar el equipo, material y personal necesarios para su recuperación y/o reemplazo.

ANEXO 3:5 Riesgo: INCENDIO

a) DESCRIPCIÓN DEL EVENTO

Ocurrencia de fuego no controlado que puede afectar los bienes

b) CUANTIFICACIÓN DE LOS RIESGOS

#	Riesgo Identificado	Probabilidad (P)	Impacto (I)	(P)x(I)	Nivel de Riesgo
5	Incendio	1	3	3	Riesgo Moderado

c) ACTIVIDADES DE PREVENCIÓN (ANTES)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES				
RESPONSABILIDAD				
ACTIVIDADES	GG	GAF	JOTIC	ATIC
Actividades preventivas (antes)	I	I	RC	E
I: Informado R: Responsable C: Consultado E: Encargado				

JEFE DE OFICINA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES (JOTIC)

- Distribuir el área de Informática de tal forma que los equipos y dispositivos de mayor cuidado y valor sean colocados en lugares con menor riesgo y fácil evacuación.
- Implementar extintores de hielo seco y recibir el entrenamiento necesario para su utilización.
- Verificar las instalaciones eléctricas y reemplazar todas las tomas corrientes defectuosos.
- Verificar se realicen respaldos de la información de manera periódica, debiendo generar la respectiva acta de evidencia.

ANALISTA EN TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES (ATIC)

- Contar con respaldos actualizados de los datos electrónicos de la Empresa, almacenados fuera del inmueble y/o en el centro de datos alterno.

d) ACTIVIDADES DE EJECUCIÓN (DURANTE).

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES				
RESPONSABILIDAD				
ACTIVIDADES	GG	GAF	JOTIC	ATIC
Actividades preventivas (antes)	I	I	RC	E
I: Informado R: Responsable C: Consultado E: Encargado				

JEFE DE OFICINA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES (JOTIC)

- Realizar el monitoreo del incidente

ANALISTA EN TECNOLOGIA DE LA INFORMACION Y COMUNICACIONES (ATIC)

- Evacuar el área, utilizando las rutas de emergencia de ser el caso.
- Uso de extintores para tratar de apagar el incendio
- Alertar a los Bomberos, para ello se recurrirá a los números telefónicos de emergencia, a efectos de obtener una pronta respuesta al acontecimiento.
- Evacuación de los equipos mas importantes, de mayor costo y de fácil movilidad.
- Únicamente si existen las condiciones de seguridad, desconectar los equipos de comunicaciones y servidores del centro de cómputo considerando su correcto apagado de ser factible.

e) **ACTIVIDADES DE RECUPERACIÓN (DESPUES).**

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES				
RESPONSABILIDAD				
ACTIVIDADES	GG	GAF	JOTIC	ATIC
Actividades preventivas (antes)	I	I	RC	E
I: Informado R: Responsable C: Consultado E: Encargado				

JEFE DE OFICINA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES (JOTIC)

- Registrar lo sucedido; así como las actividades que fueron realizadas para su solución debiendo llevar un control del mismo en un registro de evidencia de riesgo.
- Analizar lo ocurrido a fin de retroalimentar el Plan de contingencia (mejora continua) y actualizar las fichas de contingencia.

ANALISTA EN TECNOLOGIA DE LA INFORMACION Y COMUNICACIONES (ATIC)

- Levantar los servicios replicados en el centro de datos alterno, si fuera el caso.
- No ingresar al área afectada hasta que las respectivas brigadas y/o autoridades indiquen que es seguro. Al ingresar hacerlo con cuidado y únicamente si cuenta con la protección necesaria.
- Realizar un diagnóstico preliminar al ingresar al centro de datos afectado por la contingencia, para detectar el nivel de daño y así solicitar el equipo, material y personal necesarios para su recuperación y/o reemplazo.

ANEXO 3:6 Riesgo: VANDALISMO

a) DESCRIPCIÓN DEL EVENTO

El vandalismo es la hostilidad aparentemente injustificada hacia las posesiones de los demás. Suele manifestarse en el espacio público con ataques a monumentos, bancos, paredes, etc., ya sea con la intención de transmitir un mensaje o por el simple hecho de destruir lo ajeno.

El vandalismo también puede llevarse a cabo de forma virtual a través de la alteración de las páginas de Internet. Una muestra del vandalismo digital ocurre cuando se interviene un sitio para la publicación de un mensaje contrario al verdadero espíritu de la página en cuestión.

b) CUANTIFICACIÓN DE LOS RIESGOS

#	Riesgo Identificado	Probabilidad (P)	Impacto (I)	(P)x(I)	Nivel de Riesgo
6	Vandalismo	1	2	2	Baja

c) ACTIVIDADES DE PREVENCIÓN (ANTES)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES				
RESPONSABILIDAD				
ACTIVIDADES	GG	GAF	JOTIC	ATIC
Actividades preventivas (antes)	I	I	RC	E
I: Informado R: Responsable C: Consultado E: Encargado				

JEFE DE OFICINA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES (JOTIC)

- Verificar que se realicen respaldos de la información de manera periódica, debiendo generar la respectiva acta de evidencia.
- Verificar se cuente con la actualización y el soporte vigente del IPS y el antivirus, debiendo generar la respectiva acta de evidencia.

ANALISTA EN TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES (ATIC)

- Contar con respaldos actualizados de los datos electrónicos de la Empresa, almacenados fuera del inmueble y/o en el centro de datos alterno.
- Contar con los equipos de seguridad perimetral actualizados y con soporte vigente.
- Contar con antivirus instalados en las PC y servidores, actualizados y con soporte vigente.

d) ACTIVIDADES DE EJECUCIÓN (DURANTE).

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES				
	RESPONSABILIDAD			
ACTIVIDADES	GG	GAF	JOTIC	ATIC
Actividades preventivas (antes)	I	I	RC	E
I: Informado R: Responsable C: Consultado E: Encargado				

JEFE DE OFICINA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES (JOTIC)

- Realizar el monitoreo del incidente

ANALISTA EN TECNOLOGIA DE LA INFORMACION Y COMUNICACIONES (ATIC)

- Confirmada la presencia de una intrusión en la red, se deberá investigar su origen para lo cual se debe comprobar cuáles son los equipos y servicios que se están siendo comprometidos a fin de identificar los causantes del ataque.
- Desconectar el o los equipos infectados de la red.
- Visualizar los procesos activos en los servidores a fin de identificar comportamiento inusual en estos, debiendo considerar:
  - Procesos que llevan activos un largo periodo de tiempo
  - Procesos que consumen un nivel elevado de CPU
  - Procesos que no están ejecutados desde una PC perteneciente a la red del EPS ILO S.A.
- Revisar los archivos de registro (log) a fin de obtener información sobre
- conexiones a lugares poco frecuentes, utilización de aplicaciones inusuales y otras actividades sospechosas de intrusión.
- Chequeo de los archivos del sistema a fin de detectar si han sido modificados.
- Comprobar los puertos de conexión abiertos; a fin de detectar si hay alguno en especial que no lo debería ser.
- Comprobar la existencia de sniffers en la red de EPS ILO S.A.

e) ACTIVIDADES DE RECUPERACIÓN (DESPUES).

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES				
	RESPONSABILIDAD			
ACTIVIDADES	GG	GAF	JOTIC	ATIC
Actividades preventivas (antes)	I	I	RC	E

I: Informado R: Responsable C: Consultado E: Encargado

JEFE DE OFICINA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES (JOTIC)

- Registrar lo sucedido; así como las actividades que fueron realizadas para su solución debiendo llevar un control del mismo.
- Identificar las oportunidades de mejora a fin de retroalimentar el plan de contingencia.
- Analizar lo ocurrido a fin de retroalimentar el Plan de contingencia (mejora continua) y actualizar las fichas de contingencia.

ANALISTA EN TECNOLOGIA DE LA INFORMACION Y COMUNICACIONES (ATIC)

- De detectarse que la incidencia ha afectado a algún componente de software o hardware del servidor, se debe comunicar al dueño de la información a fin de que verifique su impacto.
- Si se comprueba que los equipos de seguridad han fallado en la detección de intrusos, debe recurrirse al proveedor a fin de comunicar el hecho.

ANEXO 3:7 Riesgo: FRAUDE

a) DESCRIPCIÓN DEL EVENTO

El fraude es cualquier acción de engaño o manipulación que se realiza con el propósito de obtener beneficio de manera ilícita. Por consiguiente, estas acciones son consideradas un delito, el cual genera consecuencias legales

Bajo esta perspectiva, un acto fraudulento tiene como finalidad perjudicar o dañar a un tercero para lograr algún beneficio propio. Considerando como mecanismos de acción la mentira, el engaño y la manipulación.

b) CUANTIFICACIÓN DE LOS RIESGOS

#	Riesgo Identificado	Probabilidad (P)	Impacto (I)	(P)x(I)	Nivel de Riesgo
7	Fraude	1	2	2	Baja

c) ACTIVIDADES DE PREVENCIÓN (ANTES)

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES				
RESPONSABILIDAD				
ACTIVIDADES	GG	GAF	JOTIC	ATIC
Actividades preventivas (antes)	I	I	RC	E
I: Informado R: Responsable C: Consultado E: Encargado				

JEFE DE OFICINA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES (JOTIC)

- Verificar que se realicen respaldos de la información de manera periódica, debiendo generar la respectiva acta de evidencia.
- Verificar se cuente con la actualización y el soporte vigente del IPS y el antivirus, debiendo generar la respectiva acta de evidencia.

ANALISTA EN TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES (ATIC)

- Contar con respaldos actualizados de los datos electrónicos de la Empresa, almacenados fuera del inmueble y/o en el centro de datos alterno.
- Contar con los equipos de seguridad perimetral actualizados y con soporte vigente.
- Contar con antivirus instalados en las PC y servidores, actualizados y con soporte vigente.

d) ACTIVIDADES DE EJECUCIÓN (DURANTE).

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES				
	RESPONSABILIDAD			
ACTIVIDADES	GG	GAF	JOTIC	ATIC
Actividades preventivas (antes)	I	I	RC	E
I: Informado R: Responsable C: Consultado E: Encargado				

JEFE DE OFICINA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES (JOTIC)

- Realizar el monitoreo del incidente

ANALISTA EN TECNOLOGIA DE LA INFORMACION Y COMUNICACIONES (ATIC)

- Confirmada la presencia de una intrusión en la red, se deberá investigar su origen para lo cual se debe comprobar cuáles son los equipos y servicios que se están siendo comprometidos a fin de identificar los causantes del ataque.
- Desconectar el o los equipos infectados de la red.
- Visualizar los procesos activos en los servidores a fin de identificar comportamiento inusual en estos, debiendo considerar:
  - Procesos que llevan activos un largo periodo de tiempo
  - Procesos que consumen un nivel elevado de CPU
  - Procesos que no están ejecutados desde una PC perteneciente a la red del EPS ILO S.A.
- Revisar los archivos de registro (log) a fin de obtener información sobre
- conexiones a lugares poco frecuentes, utilización de aplicaciones inusuales y otras actividades sospechosas de intrusión.
- Chequeo de los archivos del sistema a fin de detectar si han sido modificados.
- Comprobar los puertos de conexión abiertos; a fin de detectar si hay alguno en especial que no lo debería ser.
- Comprobar la existencia de sniffers en la red de EPS ILO S.A.

e) ACTIVIDADES DE RECUPERACIÓN (DESPUES).

MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES				
	RESPONSABILIDAD			
ACTIVIDADES	GG	GAF	JOTIC	ATIC
Actividades preventivas (antes)	I	I	RC	E

I: Informado R: Responsable C: Consultado E: Encargado

JEFE DE OFICINA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES (JOTIC)

- Registrar lo sucedido; así como las actividades que fueron realizadas para su solución debiendo llevar un control del mismo.
- Identificar las oportunidades de mejora a fin de retroalimentar el plan de contingencia.
- Analizar lo ocurrido a fin de retroalimentar el Plan de contingencia (mejora continua) y actualizar las fichas de contingencia.

ANALISTA EN TECNOLOGIA DE LA INFORMACION Y COMUNICACIONES (ATIC)

- De detectarse que la incidencia ha afectado a algún componente de software o hardware del servidor, se debe comunicar al dueño de la información a fin de que verifique su impacto.
- Si se comprueba que los equipos de seguridad han fallado en la detección de intrusos, debe recurrirse al proveedor a fin de comunicar el hecho.