EPS SEDA HUÁNUCO S.A

SUMILLA: APROBACIÓN DEL PLAN DE CONTINGENCIAS DE SEGURIDAD DE LA INFORMACIÓN DE LA EPS SEDA HUANUCO S.A.

RESOLUCIÓN DE GERENCIA GENERAL
Nº 212– 2025 - EPS SEDA HUÁNUCO S.A.

Huánuco, 15 de diciembre del 2025.

VISTO:

El Informe N° 110-2025-EPS SEDA HUANUCO S.A./GG-GAF/CI, de fecha 03.12.2025, el Informe N° 495-2025-EPS SEDA HUANUCO S.A./GG-GAF, de fecha 11.12.2025, el Informe N° 310-2025-EPS SEDA HUANUCO S.A./GG-ODP, de fecha 15.12.2025, el proveído de Gerencia General de fecha 12.12.2025, el Informe Legal 0105-2025-EPS SEDA HUÁNUCO S.A./GG-GAJ de fecha 15.12.2025 y;

CONSIDERANDO:

Que, ante la Ratificación del acuerdo del Consejo Directivo del OTASS que declara el inicio del RAT de la Empresa Prestadora de Servicios de Saneamiento Municipal de Agua Potable y Alcantarillado de Huánuco Sociedad Anónima - EPS SEDA HUÁNUCO S.A., y, estando a la emisión de la Resolución Ministerial N° 305-2020-VIVIENDA, de fecha 04 de diciembre de 2020, se RESUELVE: Artículo 1.- Ratificar el Acuerdo Nº 05 adoptado por el Consejo Directivo del Organismo Técnico de la Administración de los Servicios de Saneamiento - OTASS, en su Sesión Extraordinaria N° 004-2020 de fecha 3 de marzo de 2020, que declara el inicio del Régimen de Apoyo Transitorio de la Empresa Prestadora de Servicios de Saneamiento Municipal de Agua Potable y Alcantarillado de Huánuco Sociedad Anónima - EPS SEDA HUÁNUCO S.A.

Que, mediante Acuerdo de Consejo Directivo adoptado en Sesión Ordinaria N° 004-2025-Consejo Directivo de fecha 06 de marzo del 2024, se acordó designar al **Ing. MIRKO FELIX JURADO DUEÑAS** como Gerente General de la EPS SEDA HUANUCO S.A., a partir del 10 de marzo del 2025.

Que, en cumplimiento de las disposiciones institucionales y del Plan de Acción Anual 2025, se presentó el Plan de contingencias para seguridad de la información de SEDA HUANUCO S.A., constituyendo una herramienta estratégica para mitigar los riesgos asociados a un Ataque cibernético que podría generar pérdida de información comercial de la EPS, logrando así:

- Garantizar la continuidad de los servicios comerciales (facturación, recaudación, atención al usuario) ante fallas técnicas o emergencias.
- Reducir el impacto de interrupciones en los sistemas informáticos y operativos de la gerencia.
- Proteger la información comercial y de los usuarios (datos de clientes, consumos, pagos).
- Asegurar una respuesta rápida y coordinada del personal frente a incidentes.
- Minimizar pérdidas económicas y retrasos en la recaudación.
- Mantener la confianza de los usuarios y el cumplimiento de las obligaciones institucionales.

Que, el Plan de contingencias para seguridad de la información. tiene como finalidad proteger la información comercial y de los usuarios, asegurar la continuidad de los procesos de facturación, recaudación y atención al cliente, y establecer acciones claras para prevenir, responder y recuperar la operatividad ante incidentes de seguridad, reduciendo riesgos, pérdidas económicas y afectación a la confianza de los usuarios, en cumplimiento de la normativa vigente en la EPS SEDA HUANUCO S.A.

Que, el Plan de contingencias para seguridad de la información tiene como objetivo establecer los procedimientos que permitan asegurar la continuidad operativa de los equipos informáticos y sistemas de información de la EPS SEDA HUANUCO S.A., así como reducir el riesgo de eventos inesperados, garantizando una rápida recuperación con las menores pérdidas posibles en forma rápida y oportuna.

Que, con Informe N° 110-2025-EPS SEDA HUANUCO S.A./GG-GAF/CI, de fecha 03.12.2025, la Coordinadora de Sistemas e Informática solicita a la Gerencia Administración y Finanzas la aprobación del PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN DE LA EPS SEDA HUÁNUCO S.A.

Que, con Informe N° 495-2025-EPS SEDA HUANUCO S.A/GG-GAF, de fecha 11.12.2025, el Gerente de Administración y Finanzas solicita a la Gerencia General la aprobación mediante acto resolutivo el Plan de Contingencia de Sistemas de Información de la EPS SEDA HUANUCO S.A

Que, con Informe N° 310-2025-EPS SEDA HUANUCO S.A./GG-ODP, de fecha 15.12.2025, el Jefe de la Oficina de Desarrollo y Presupuesto, emite el informe presupuestal, señalando que no se cuenta con disponibilidad presupuestal para la ejecución del Plan de Contingencia de Sistemas de Información de la EPS SEDA HUANUCO S.A. durante el presente ejercicio fiscal y realizar gestiones que permita su implementación en el siguiente ejercicio fiscal.

Que, con proveído de fecha 12 de diciembre del 2025 la Gerencia General solicita opinión y recomendación respecto del Plan de Contingencias de Sistemas de Información de la EPS SEDA HUANUCO S.A. a la Gerencia de Asesoría Jurídica, Por consiguiente; estando en uso de las facultades conferidas por el Estatuto de la Empresa a la Gerencia General como órgano ejecutivo de más alto nivel de la sociedad y contando con el visto bueno de la Gerencia General, Gerencia de Asesoría Jurídica, Gerencia de Administración y Finanzas y Gerencia Comercial.

Que, mediante el Informe Legal 0105-2025-EPS SEDA HUÁNUCO S.A./GG-GAJ, de fecha 15.12.2025, la Gerencia de Asesoría Jurídica emite opinión favorable para aprobación mediante acto resolutivo el presente Plan de Contingencias para Seguridad de la Información, el mismo que será una herramienta estratégica planificada con una serie de procedimientos que nos faciliten u orientan a tener una solución alternativa y nos permite restituir rápidamente los servicios de la Empresa ante la eventualidad que pueda paralizar los servicios, ya sea de forma parcial o total, es decir, un plan que permite a la EPS SEDA HUANUCO SA, seguir operando, aunque sea de forma limitada.

Que, estando a las facultades conferidas en los Estatutos y Reglamento de Organización y Funciones ROF, con los V° B° de la Gerencia General, Gerencia de Administración y Finanzas, Gerencia de Asesoría Jurídica y la Coordinación del Equipo de Tecnología de la Información y comunicaciones:

SE RESUELVE:

ARTÍCULO PRIMERO. APROBAR, el **PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACIÓN DE LA EPS SEDA HUANUCO S.A.**, el mismo que consta de treinta y nueve (39) folios que forman parte integrante de la resolución.

ARTÍCULO SEGUNDO. - ESTABLECER que la Coordinación de Sistemas e Informática sea la encargada de dar cumplimiento a lo establecido en el programa aprobado en el artículo primero.

ARTÍCULO TERCERO. - **TRANSCRIBIR,** la presente resolución a quienes corresponda, para conocimiento y fines pertinentes.

ARTÍCULO CUARTO. - **ENCARGAR,** a la Coordinadora del Equipo de Tecnología de la Información y comunicaciones, publique el contenido de la presente Resolución en la Página Web de la EPS SEDA HUANUCO S.A. (www.sedahuanuco.com).

Regístrese, Comuníquese, Cúmplase y Publíquese.

GERENCIA DE ASESORÍA JURÍDICA EPS SEDA HUANUCO S.A.

COORDINADOR DE E.S.I. EPS SEDA HUANUCO S.A.

GERENCIA DE ADMINISTRACIÓN Y FINANZAS EPS SEDA HUANUCO S.A.

GERENCIA GENERAL EPS SEDA HUANUCO S.A.

Milko Jura o Dueñas
GERENTE GENERAL
EPS SEDA HUANUCO S.A.

EMPRESA PRESTADORA DE SERVICIOS DE SANEAMIENTO MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE HUANUCO SOCIEDAD ANÓNIMA

EPS SEDA HUANUCO S. A.

PLAN DE CONTINGENCIA DE LOS SISTEMAS DE INFORMACION

EQUIPO DE TECNOLOGIA DE LA INFORMACION Y COMUNICACION

CONTROLES PARA LAS TECNOLOGIAS DE LA INFORMACION Y COMUNICACIÓN - TIC

NORMA DE CONTROL INTERNO
Resolución de Contraloría No. 320-2006-CG
2 NORMA GENERAL PARA LAS EVALUACION DE RIESGOS

- 1.1 Planeamiento de la administración de riesgos
- 1.2 Identificación de los riesgos
- 1.3 La valoración de los riesgos
- 1.4 Respuesta al riesgo

Huánuco, 11 de noviembre del 2025

"AGUA Y VIDA, PARA VIVIR EN ARMONIA"

ÍNDICE

I. INTRODUCCIÓN

El Equipo de Tecnología de la Información y Comunicación, forma parte de la Oficina de Gerencia de Administración y Finanzas de la EPS SEDA HUANUCO S.A, tiene entre otras funciones las de formular, proponer y aplicar el presente Plan de Contingencias de Sistemas de Información de la Empresa.

El Plan de Contingencia de Sistemas de Información implica un análisis de los posibles riesgos a los cuales pueden estar expuestos nuestros equipos de cómputo y la información contenida en los diversos medios de almacenamiento, por lo que se desarrollado un análisis detallado de los principales riesgos a los que se enfrenta la institución, reducir la probabilidad de ocurrencia, como estar preparados antes del desastre o contingencia a fin de minimizar los daños y los procedimientos a seguir en caso que se presentara el suceso negativo.

Un plan de contingencia Sistemas de Información como documento de gestión es un conjunto de procedimientos y estrategias que detalla cómo la EPS SEDA HUANUCO S.A. responderá a incidentes inesperados, fallas o desastres para garantizar la continuidad de sus operaciones de tecnología de la información (TI), así como también minimizar el impacto de las interrupciones, asegurar la protección de datos críticos y permitir una recuperación rápida de los sistemas y servicios.

Así también consideramos que no sólo es responsabilidad del Área de Sistemas e Informática, sino de todas las unidades orgánicas el proteger la información y los equipos que la contienen.

II DEFINICION

Un Plan de Contingencias de Sistemas de Información es una herramienta estratégica planificada con una serie de procedimientos que nos facilitan u orientan a tener una solución alternativa y nos permite restituir rápidamente los servicios de la organización ante la eventualidad que pueda paralizar los servicios, ya sea de forma parcial o total, es decir, un plan que le permite a su negocio u organización, seguir operando, aunque sea de forma limitada

III OBJETIVO

3.1 OBJETIVO GENERAL

El objetivo general del presente Plan de Contingencias de Sistemas de Información es establecer los procedimientos que permitan asegurar la continuidad operativa de los equipos informáticos y sistemas de información de la EPS SEDA HUANUCO S.A., así como reducir el riesgo de eventos inesperados, garantizando una rápida recuperación con las menores pérdidas posibles en forma rápida y oportuna.

3.2 OBJETIVOS ESPECIFICOS

- Identificar los riesgos que pueden afectar el logro de los objetivos de la EPS debido a factores externos o internos. Los factores externos incluyen factores económicos, medioambientales, políticos, sociales y tecnológicos.

- Los factores internos son los que realiza la empresa como infraestructura, personal, procesos y tecnología.

- Valorar los riesgos potenciales que pueden afectar los equipos informáticos y sistemas de información de la EPS.

- Establecer procedimientos de recuperación y reducir las consecuencias en una posible pérdida de sistema de información relacionada con el evento inesperado en un nivel aceptable.

IV ALCANCE

La implementación del presente Plan de Contingencia de Sistemas de Información, tiene un alcance para todas las Unidades Orgánicas y áreas de la EPS SEDA HUANUCO S.A., así como al personal que cuenta y hace uso de los 0equipos informáticos para el procesamiento de los sistemas de información.

También incluye referente a la infraestructura, personal, y servicios, orientado a minimizar eventuales riesgos ante situaciones adversas que afecten contra el normal funcionamiento de los servicios de EPS SEDA HUANUCO S.A.

4.1 COMPROMISO DE LA EMPRESA

a. Participar en forma activa y directa en el cumplimiento del presente Plan de Contingencia de Sistemas de Información.
b. Asegurar que exista el personal idóneo para implementar los requerimientos del Plan de Contingencia Informático.
c. Organizar, definir la responsabilidad y funciones del personal de la EPS para actuar ante contingencias; así como, aprobar la adquisición y proporcionar los equipos de emergencia necesarios.
d. Capacitar e informar adecuadamente a todo el personal, sobre las disposiciones del presente Plan de Contingencia, con la finalidad que puedan estar preparados para actuar en casos de contingencia.
e. Evaluar en forma continua el Plan de Contingencia y definir responsabilidades y funciones para el manejo de emergencias. Poner en conocimiento de todo el personal cualquier modificación efectuada.
f. Aplicar medidas correctivas de prevención, limpieza y restauración en el medio ambiente.

4.2 COMPROMISO DE LOS TRABAJADORES

a. Participación activa en el cumplimiento del Plan de Contingencia.
b. Mantenerse capacitado e informado permanentemente acerca de las disposiciones de este Plan en lo referente a responsabilidades y procedimientos.
c. Cumplimiento de los Reglamentos, Estándares y Procedimientos de Trabajo Seguro Establecidos.
d. La acción primaria e inmediata será asistir al accidentado ante una contingencia, haciendo uso de los equipos, implementos de seguridad y dándole los primeros auxilios necesarios según las disposiciones de este Plan.

4.3 ORGANIGRAMA INSTITUCIONAL

ORGANIGRAMA

Aprobado mediante **RESOLUCIÓN Nº 250-2024-GG-EPS SEDA HUANUCO S.A.**

V REFERENCIAS NORMATIVAS Y LEGALES

- Ley No. 26338 - Ley General de Servicios de Saneamiento y su Reglamento.
- Resolución de Superintendencia N°08-95-PRES/VMI/SSS. (Reconocen como Entidad Prestadora de Servicios de Saneamiento)
- Estructura Orgánica aprobada mediante resolución N° 011-2018-PD-EPS SEDA HUANUCO S.A.
- R. J. N° 090-95-INEI, Recomendaciones Técnicas para la protección física de los equipos y medios de procesamiento de la información en la administración pública.
- Reglamento Interno de Trabajo aprobado mediante resolución N° 077-2017-GG-SEDA HUANUCO S.A.
- Norma de Control Interno:

  Resolución de Contraloría No. 320-2006-CG

  2 NORMA GENERAL PARA LA EVALUACION DE RIESGOS

  1.1. Planeamiento de la administración de riesgos

  1.2. Identificación de los riesgos

  1.3. La valoración de los riesgos

  1.4. Respuesta al riesgo

- Norma general para las actividades de control gerencial

  3.10. Controles para las Tecnologías de la Información y Comunicaciones –TIC
- Ley No. 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD). Establece el marco general para la gestión del riesgo de desastres, incluyendo la necesidad de planes de contingencia en diferentes sectores
- Resolución Ministerial N° 004-2016-PCM - Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

VI DEFINICIONES

Acceso

Es la autorización para ingresar y recuperar o grabar datos que han sido almacenados en un sistema de información. Cuando se consulta a una base de datos, los datos son primeramente recuperados hacia la computadora y luego transmitidos a la pantalla del terminal.

Acceso no autorizado a la información

Si no existen medidas de seguridad se pueden producir accesos no autorizados a los sistemas de información, computadoras personales, terminales de red e información confidencial.

Amenaza

Cualquier factor que pueda interferir el funcionamiento adecuado de una computadora personal o Servidor de Bases de Datos, o causar la difusión no autorizada de información confiada a una computadora, Ejemplo, fallas del suministro eléctrico, virus, saboteadores o usuarios descuidados.

Análisis de riesgos

El análisis de riesgos es el proceso de identificar y evaluar las amenazas potenciales como ciberataques, desastres naturales o errores humanos y las vulnerabilidades de los sistemas de TI de una organización.

Aplicación

Es aquel programa informático que permite a un usuario utilizar una computadora con un fin específico. Las aplicaciones son parte del software de una computadora y se ejecutan bajo un sistema operativo. Una aplicación de software suele tener un objetivo único: navegar en la web, revisar correo, explorar el disco duro, etc.

Ataque

Termino General usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora.

Backup

Copia de seguridad o respaldo puede ser parcial o total que se realiza a un tipo de información importante en un periodo determinado.

La copia de seguridad puede ser realizada en forma manual o automática.

Bases de Datos

Es un conjunto de información almacenado, organizado y relacionados entre sí los cuales son producidos por los sistemas de información.

En las Bases de Datos del tipo Referencial la información que contiene es muy estructurada principalmente a través de tablas.

Con estas tablas se pueden establecer relaciones que pueden dar lugar a nuevas tablas o bases de datos.

Cifrado

El cifrado es un proceso que utiliza algoritmos matemáticos para ocultar el significado de un mensaje, los algoritmos de cifrado es el método utilizado para ocultar el contenido de un mensaje

Contingencia

Cualidades o características necesarias de lo contingente, es decir de lo que puede suceder o no suceder.

Confidencialidad

Propiedad de la información que hace que será protegida para que no sea divulgada sin consentimiento de la persona. Dicha garantía se lleva a cabo por medio de un grupo de reglas que limitan el acceso a esta información.

Desastre

Es la interrupción prolongada de los recursos informáticos y de comunicación de una organización, que no puede remediarse dentro de un periodo predeterminado aceptable y que necesita el uso de un sitio o equipo alterno para su recuperación.

Hardware

Es el componente o parte física de una computadora, (periféricos de entrada/salida).

Incidente

Cuando se produce un ataque o se materializa una amenaza, ejemplo, intento de borrar archivos o fallas del fluido eléctrico

Integridad

Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos.

El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.

Integridad de la Información

Consiste en mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

LAN

Local Area Network – Red de Area Local.

Es un grupo de ordenadores y periféricos que pertenecen a la misma organización y están interconectados dentro de un área geográfica pequeña a través de una red y de este modo pueden compartir recursos

Probabilidad

La posibilidad de que un evento dado ocurra.

Riesgo

Es la probabilidad de ocurrencia de eventos negativos que perjudiquen el Hardware, Software, e información en los equipos informáticos.

Sistema de información

Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, que se genera para cubrir una necesidad o un objetivo.

Seguridad

Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

En el caso de los datos de una organización, la privacidad y la seguridad guardan estrecha relación, aunque la diferencia entre ambas radica en que la primera se refiere a la distribución autorizada de información, mientras que la segunda, al acceso no autorizado de los datos.

El acceso a los datos queda restringido mediante el uso de palabras claves, de forma que los usuarios no autorizados no puedan ver o actualizar la información de una base de datos o a subconjuntos de ellos.

Software

Es el componente o parte lógica de una computadora, (sistemas operativos, aplicaciones, programas).

Software Antivirus

Son programas que buscan prevenir, detectar y eliminar virus.

VII. PLAN DE SEGURIDAD

7.1 EVALUACION DE RIESGOS

La evaluación de riesgos es el proceso de identificar, analizar y priorizar las amenazas y vulnerabilidades que podrían afectar a los sistemas de información en la EPS. El objetivo es comprender la probabilidad de que ocurran y el impacto que tendrían, para así definir las medidas de seguridad y planes de acción necesarios para prevenir o mitigar esos riesgos y asegurar la continuidad de las operaciones.

Es fundamental en este proceso de evaluación de riesgos que se ha de llevar a cabo, tener en cuenta las siguientes preguntas:

- ¿Qué se intenta proteger?
- ¿Cuál es su valor para uno o para la organización?
- ¿Frente a qué se intenta proteger?
- ¿Cuál es la probabilidad de un ataque?

7.1.1. PLANEAMIENTO DE LA GESTION DE RIESGO

7.1.2. IDENTIFICACION DE LOS RIESGOS

a) IDENTIFICACIÓN DE LOS SISTEMAS DE INFORMACIÓN Y ACTIVOS CRÍTICOS

b) INVENTARIO DE LOS SISTEMAS DE INFORMACIÓN Y ACTIVOS DIGITALES

La EPS SEDA HUANUCO S.A. comprende la importancia de realizar el inventario de los aplicativos y sistemas de información así como de los equipos que forman parte del Data Center - Centro de Datos, lo que le permite hacer un seguimiento de estos, así como tener identificados a aquellos que son de que siempre hacen uso en las actividades diarias y aplicarles los controles que

reduzcan el riesgo de impacto sobre los procesos a los que están directamente asociados, manteniendo así el control sobre dichos activos.

c) CLASIFICACIÓN DE SISTEMAS Y ACTIVOS SEGÚN SU ESTADO CRÍTICO E IMPORTANCIA.

Como parte de su plan de prevención, la EPS SEDA HUANUCO S.A. ha realizado la identificación de los procesos, aplicaciones críticas y los recursos de TI con los que cuenta. Se ha considerado todos los elementos susceptibles a incidentes que activen alguna contingencia. Los procesos y recursos identificados son los siguientes:

TABLA No. 01 - PROCESOS Y RECURSOS CRÍTICOS DE TIC

PROCESO CRITICO	RECURSOS
Gestión de Redes e Infraestructura de Tecnología de la Información - TI	Equipo de Grupo Electrógeno
	Gabinete del Data Center (Centro de Datos).
	Equipos de comunicaciones (Switch, Router, Access Point)
	Enlaces de fibra óptica para el servicio de Internet
	Equipo de seguridad perimetral (Firewall)
	Cableado estructurado de red datos (LAN)
	Sistema de almacenamiento en red LAN (storage NAS
	Servidores en Torre, Rack y Blade.
	Servidores físicos.
	Servidor virtual.
	Servidor remoto.
Gestión de Sistemas de Información Gestión Comercial - WEB Gestión Administrativa Sistemas Integrados - ERP y Bases de Datos	SIINCO WEB
	ERP AVALON v. 2025.2
	SICAP v. 2.1
	INTRANET - Sistema de Trámite Documentario
	SIAF - Sistema Informático de Administración Financiera
	Base de datos y biblioteca digital utilizados por los sistemas y aplicativos informáticos.
Soporte Técnico	Equipo de estaciones de trabajo del personal crítico (computadoras de escritorio y PC's portátiles)
Operación y mantenimiento de TIC	Personal crítico responsable de los procesos de TIC.

7.1.3 VALORACION DE LOS RIESGOS

El análisis o valoración del riesgo le permite a la EPS SEDA HUANUCO S.A. considerar cómo los riesgos potenciales pueden afectar el logro de sus objetivos. Se inicia con un estudio detallado de los temas puntuales sobre riesgos que se hayan decidido evaluar. El propósito es obtener la suficiente información acerca de las situaciones de riesgo para estimar su probabilidad de ocurrencia, tiempo, respuesta y consecuencias.

7.1.4 RESPUESTA AL RIESGO

Consiste en identificar las alternativas de respuesta al riesgo considerando la probabilidad y el impacto en relación con la tolerancia al riesgo y su relación costo beneficio. La consideración del manejo del riesgo y la selección e implementación de una respuesta son parte integral de la administración de los riesgos.

7.2 ANÁLISIS DE RIESGOS

El análisis de riesgos es el proceso de identificar y evaluar las amenazas potenciales como ciberataques, desastres naturales o errores humanos y las vulnerabilidades de los sistemas de TI en la EPS, Su objetivo es determinar la probabilidad de que ocurra un evento y el impacto negativo que tendría en la EPS para poder priorizar riesgos y diseñar medidas de seguridad adecuadas.

7.2.1 METODOLOGÍA DE ANÁLISIS DE RIESGOS

Para determinar el nivel de riesgo de un recurso de TIC crítico de la EPS SEDA HUANUCO S.A. se consideraron los controles existentes que reducen la afectación de la amenaza, de acuerdo con la aplicación de la metodología de riesgos.

Para la evaluación y análisis de riesgos se va utilizar en el presente plan una matriz de riesgos; que viene hacer una herramienta visual que nos va permitir identificar, evaluar y priorizar los riesgos.

7.2.2 IDENTIFICACIÓN DE RIESGOS

Se identifican aquellas amenazas que pueden vulnerar los servicios TIC de la EPS SEDA HUANUCO S.A., considerando la ubicación geográfica, el contexto actual del Data Center - Centro de Datos. Las amenazas identificadas se describen en la siguiente tabla:

TABLA No. 02 – RIESGOS A LOS SERVICIOS DE TIC

No.	RIESGOS (EVENTO)	TIPO
1	Sismo	Naturales
2	Inundación y aniego en el Data Center	
3	Incendio en el Data Center	
4	Falla en las telecomunicaciones	Tecnológico
5	Delito informático	
6	Falla en el Hardware y Software	
7	Falla en el suministro eléctrico en el Data Center	Físico y Ambiental
8	Ausencia del personal critico de TIC	Humanos

RIESGOS EN LA SEGURIDAD INFORMÁTICA A QUE SE ENFRENTA LA INSTITUCIÓN.

1 Fuego, que pueden destruir los equipos y archivos.
2 Robo común, pérdida de los equipos.
3 Fallas en los equipos informáticos que dañen los archivos.
4 Errores del usuario, que dañen los archivos.
5 Acción de virus, que dañen los equipos y archivos.
6 Factores geológicos como sismos y terremotos, que destruyen los equipos y archivos.
7 Robo de Datos: difusión de datos

1. FUEGO QUE DESTRUYEN LOS EQUIPOS Y LOS ARCHIVOS	
¿La EPS cuenta con protección contra incendios?	No
¿Se cuenta con sistema de aspersión automática?	No
¿Se cuenta con diversos tipos de Extintores?	Si
¿Detectores de Humo?	Si
¿Los empleados están preparados para un posible incendio?	No

2. ROBO COMÚN, PERDIDA DE LOS EQUIPOS Y ARCHIVOS	
¿Hay personal de seguridad en la institución?	Si
¿Cuántos vigilantes hay?	4 por turno
¿Los vigilantes están ubicados en zonas estratégicas?	Si

¿Hay personal de seguridad en la institución?	Si
¿Existe un sistema de seguridad para prevenir el ingreso no autorizado?	Si
¿Existe un sistema de video vigilancia para para prevenir el ingreso de personas no autorizadas?	SI

3. FALLAS EN LOS EQUIPOS QUE DAÑEN LOS ARCHIVOS	
¿Los equipos tienen mantenimiento continuo por parte de personal calificado?	Si
¿Cuáles son las condiciones actuales de Hardware?	Bueno
¿Es posible predecir las fallas a que están expuestos los equipos?	Sí, es posible saberlo

4. ERRORES DE LOS USUARIOS QUE DAÑEN LOS ARCHIVOS	
¿Cuánto saben los empleados de computadoras o redes?	Un nivel medio
Los que no conocen de manejo de computadoras, ¿Saben a quien pedir ayuda?	Si
Durante el tiempo de vacaciones de los empleados, ¿Qué tipo de personal los sustituye y qué tanto saben del manejo de computadoras?	Poco

5. CON RELACION A LA ACCION DE VIRUS	
¿Se prueba software sin hacer un examen previo?	No
¿Está permitido el uso de USB, DVD y CD en la empresa?	Si
¿Todas las máquinas tienen unidades de USB's?	Si
¿Se cuenta con procedimientos contra virus?	Si

6. TERREMOTOS QUE DESTRUYAN LOS EQUIPOS Y ARCHIVOS	
¿La empresa se encuentra en zona sísmica?	No
¿El local cumple con las normas antisísmicas?	No
Un terremoto, ¿Cuánto daño podría causar?	50%

7. ROBO DE DATOS Y LA POSIBLE DIFUSION DE DATOS	
¿Cuánto valor tiene actualmente la Base de Datos?	Muy importante
¿Cuánta pérdida podría causar en caso de que se hicieran públicas?	90%
¿Se ha elaborado una lista de los posibles sospechosos que pudieran efectuar el robo?	No

PROBABILIDAD DE FACTOR RIESGO.

RIESGOS	ALTO	MEDIO	BAJO
1. AL FUEGO, QUE PUEDE DESTRUIR LOS EQUIPOS Y ARCHIVOS			X
2. AL ROBO COMÚN, LLEVÁNDOSE LOS EQUIPOS Y ARCHIVOS			X
3. A FALLAS EN LOS EQUIPOS QUE DAÑEN LOS ARCHIVOS			X
4. A ERRORES DEL USUARIO QUE DAÑEN LOS ARCHIVOS	X		
5. CON RELACION A ACCIÓN DE VIRUS QUE DAÑEN LOS ARCHIVOS		X	
6. A TERREMOTOS QUE DESTRUYEN EL EQUIPO Y LOS ARCHIVOS			X
7. AL ROBO DE DATOS Y LA DIFUSION DE ESTOS			X

7.3 EVALUACION DE RIESGOS POTENCIALES Y NO POTENCIALES

Todos los sistemas integrados y aplicativos informáticos con que cuenta la EPS SEDA HUANUCO S.A, están expuestos a grandes riesgos como la pérdida de información, así como también al robo de las computadoras (extracción de accesorios), virus informático, así como el cableado de energía eléctrica, cable de telefonía y cableado estructurado de redes de transmisión de datos y comunicación.

A continuación, se presenta una lista detallada, previa evaluación de los posibles riesgos potenciales y no potenciales que podrían presentarse en el área del Equipo de Tecnología de la Información y Comunicación y otras áreas de nuestra EPS SEDA HUANUCO S.A,

7.3.1. RIESGOS POTENCIALES

Destrucción total o parcial área del Equipo de Tecnología de la Información y Comunicación, por desastres naturales o causados por la negligencia del hombre: inundaciones, terremotos, incendios, etc.

Solución:

Contar con el stock de material técnico para todo el año, (CDs, DVDs, Discos Duros externos de gran capacidad, memorias USB.

Realizar copias de seguridad de los diversos sistemas informático en forma diaria, debiendo preservar una copia en caja fuerte y otra en alguna entidad de almacenamiento de la localidad.

Actualizar las copias de seguridad de la información fuente de los sistemas informáticos en forma semanal o quincenal y de las bases de datos en forma diaria.

Se realizará las copias de seguridad en forma periódica de los datos y sistemas de información críticos para poder recuperarlos en caso de pérdida o daño de acuerdo a la Directiva vigente:

DIRECTIVA No. 001-2025 - EQUIPO DE TECNOLOGIA DE LA INFORMACION Y COMUNICACIÓN - EPS SEDA HUANUCO S.A.
PROCEDIMIENTOS PARA LA GENERACION Y RESTAURACION DE COPIAS DE SEGURIDAD – BACKUPS - SISTEMA INTEGRADO [ERP AVALON v.PRO 2025.1.7] [APLICATIVOS INFORMATICOS] – [ARCHIVOS].

Restaurar la información a partir del último Backup existente en los archivos, de la caja fuerte o entidades de almacenamiento

Apagones del fluido eléctrico en la sede central y desde la misma planta de servicios eléctricos u otras averías externas.

Solución:

Contar con un generador de energía eléctrica y un sistema de UPS en óptimas condiciones, para poder continuar brindando el servicio informático a los usuarios, en caso de pérdida de información se recuperará a partir de los backups.

DIRECTIVA No. 001-2025 - EQUIPO DE TECNOLOGIA DE LA INFORMACION Y COMUNICACIÓN - EPS SEDA HUANUCO S.A.
PROCEDIMIENTOS PARA LA GENERACION Y RESTAURACION DE COPIAS DE SEGURIDAD – BACKUPS - SISTEMA INTEGRADO [ERP AVALON v.PRO 2025.1.7] [APLICATIVOS INFORMATICOS] – [ARCHIVOS]

Cableado de sistema eléctrico tendido a la intemperie por los techos y paredes de este local, lo cual genera interferencias en la transmisión de datos al cableado estructurado.

Solución:

Revisión y evaluación total del actual sistema eléctrico de la EPS SEDA HUANUCO S.A, por parte del personal electricista especializado donde pueda proponer una inmediata solución, recomendándose que el nuevo tendido de cable se implemente en el interior de las estructuras del edificio o en su defecto mediante canaletas para protegerlo y evitar las interferencias eléctricas.

Robo de Información en forma automatizada por personas mal intencionadas.

Solución:

Se procederá a recuperar la información a partir de la última copia de seguridad, backups.

Iniciar una investigación interna exhaustiva a los administradores de los servidores y/o operadores de PC.

Formular la denuncia correspondiente ante el órgano policial.

Infección de la Información por virus informático, transmitido por una mala práctica en el uso de Internet y otros medios magnéticos de transporte de información.

Solución:

Restaurar la información a partir del último Backup existente en los archivos, de la caja fuerte o entidades de almacenamiento.

DIRECTIVA No. 001-2025 - EQUIPO DE TECNOLOGIA DE LA INFORMACION Y COMUNICACIÓN - EPS SEDA HUANUCO S.A.
PROCEDIMIENTOS PARA LA GENERACION Y RESTAURACION DE COPIAS DE SEGURIDAD – BACKUPS - SISTEMA INTEGRADO [ERP AVALON v.PRO 2025.1.7] [APLICATIVOS INFORMATICOS] – [ARCHIVOS]

Identificar a los usuarios que generan este daño innecesario a sus equipos informáticos, para capacitarlos en el uso de programas antivirus.

7.3.2 RIESGOS NO POTENCIALES

Cableado estructurado de redes para transmisión de datos instaladas a la intemperie, expuestas a los problemas del medio ambiente y otros.

Solución:

Revisión y evaluación del actual sistema de cableado estructurado de redes, por parte del personal técnico profesional de redes y comunicaciones quien deberá proponer una solución que permita brindar seguridad en la transmisión de datos, recomendándose que el tendido de cable se haga con canaleta o empotrado en la pared para protegerlo y evitar las interferencias, trabajo que debe estar supervisado por el Equipo de Tecnología de la Información y Comunicación de la EPS.

Ambiente inadecuado para realizar las funciones asignadas al personal del área del Equipo de Tecnología de la Información y Comunicación de la EPS.

Solución:

Gestionar ante la Oficina de Gerencia de Administración y Finanzas de la EPS SEDA HUANUCO S.A, un ambiente adecuado para reparación y mantenimiento de equipos informáticos.

Contratar un técnico electrónico, así como realizar un convenio con una empresa de soporte informático para la reparación de equipos servidores de datos, impresoras, monitores, plotters, etc.

Comunicar a todos los usuarios de EPS SEDA HUANUCO S.A. que presenten inconvenientes con el normal funcionamiento de su computadora que se comuniquen y remitan sus equipos para el soporte informático correspondiente por el Equipo de Tecnología de la Información y Comunicación de la EPS, los cuales serán atendidos dando prioridad y en función al stock de repuestos.

Sistemas Integrados y aplicativos informáticos de la EPS sin un inventario detallado que permita una rápida recuperación ante un desastre.

Solución:

El personal asignado a desarrollo de sistemas deberá realizar un inventario detallado de los Sistemas Integrados y aplicativos informáticos de la EPS.
Mantener actualizado el inventario de software en forma digital.

Equipos informáticos sin seguro, poniendo en riesgo ante desastres imprevistos.

Solución:
Realizar un convenio con alguna una empresa de seguros con la finalidad asegurar los equipos de cómputo (Servidores de Bases de Datos, Servidores Web), sistemas integrados y aplicativos informáticos.

Distribución y asignación de equipos informáticos sin asignación de perfiles de usuario.

Solución:
Crear los perfiles de usuario estándar para los trabajadores que tienen asignados equipos informáticos, de esta manera se podrá distribuir y asignar equipos teniendo en cuenta las funciones y tareas de cada trabajador.

Caída del servicio o de conexión del servicio de Internet sin respaldos.

Solución:
Tener contratado el servicio de Internet con un operador que garantice una rápida velocidad y continuidad ya que este servicio se ha convertido en un activo esencial para la productividad empresarial y la continuidad de los negocios, en cualquier lugar, especialmente si tenemos en cuenta que la mayoría de personas han pasado a trabajar de forma remota.

Pozos de conexión a tierra con falta de mantenimiento

Solución:
Ejecutar el mantenimiento de los pozos a tierra con el apoyo del servicio técnico personal externo según cronograma de mantenimiento establecido por la Equipo de Tecnología de la Información y Comunicación de la EPS.

Sistemas integrados y aplicativos Informáticos no documentados apropiadamente el cual va imposibilitar su mantenimiento.

Solución:
Toda la documentación fuente de los diversos sistemas informáticos debe encontrarse

debidamente actualizados en formato digital en una biblioteca virtual.

Todas las modificaciones realizadas al software deben ser registradas en una bitácora y control de versiones detallando las funciones actualizadas o cambios realizados.

Sistemas Informáticos sin autorización normativa de aplicación de la EPS.

Solución:
Todo sistema integrado o aplicativo informático desarrollado por el Equipo de Tecnología de la Información y Comunicación de la EPS, adquirido por terceros o cedido en uso debe ser debidamente autorizado por Resolución de Gerencia General, y debidamente operado por las áreas usuarias y bajo la supervisión de la Equipo de Tecnología de la Información y Comunicación de la EPS.

Cabina de servidores de bases de datos y servidor Web sin control de cámaras de video, poniendo en riesgo a la información almacenada física y digitalmente.

Solución:
Instalación de cámaras de video, además el acceso físico en la cabina de servidores debe ser limitado, el uso de llaves debe ser controlado y dado solo al personal que asumirá las responsabilidades de todos los implementos y recursos que esta oficina tiene a disposición cuando sea necesario.

El ingreso y salida de equipos informáticos, accesorios y otros materiales debe ser controlado estrictamente por el personal de soporte informático,

Es importante definir los procedimientos y planes de acción antes, durante y después de la ocurrencia del siniestro o desastre dentro en la EPS SEDA HUANUCO. S.A. con la finalidad de recuperar la total o mayor parte de la información, archivos y equipos informáticos.

7.4 PLAN DE RECUPERACION DE DESASTRES

7.4.1. ACTIVIDADES PREVIAS AL DESASTRE

Son las actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de información y equipos informáticos que nos aseguren el proceso de recuperación de los mismos.

7.4.1.1 Establecer el Plan de Acción

El establecimiento del plan de acción comprende una planificación estructurada de actividades que deben cumplirse durante un desastre, y que a continuación se detalla.

SISTEMAS DE INFORMACIÓN

La EPS SEDA HUANUCO S.A deberá tener una relación de todos los sistemas de información tanto los realizados por el Equipo de Tecnología de la Información y Comunicación como los realizados por terceros. Debiendo identificar toda información sistematizada, que sea necesaria para la buena marcha Institucional.

La relación de Sistemas de Información deberá detallar los siguientes datos:

Nombre del Sistema.

Lenguaje de programación con el que fue creado el sistema, programas que lo conforman (tanto programas fuentes como programas objetos, rutinas, macros).

Las unidades que usan la información del Sistema.

El volumen de los archivos que trabaja el Sistema.

El volumen de transacciones diarias, semanales y mensuales que maneja el sistema.

El equipamiento necesario para un manejo óptimo del Sistema.

Las fechas en las que la información es necesitada con carácter de urgencia.

COORDINADOR DE E.S.I. EPS SEDA HUANUCO S.A

GERENCIA DE ADMINISTRACIÓN Y FINANZAS EPS SEDA HUÁNUCO S.A

GERENCIA COMERCIAL EPS SEDA HUÁNUCO S.A

RELACION DE SOFTWARE Y APLICATIVOS INFORMATICOS

No.	SIGLAS	NOMBRE	MÓDULOS	AREA RESPONSABLE
01	SIINCO WEB	Sistema Integrado de Información Comercial - WEB	Facturación Comercialización Cobranza Recaudación Reclamos Operacional	Gerencia Comercial (todas las áreas)
02	ERP AVALON v. 2025.2 AMD Consultores	Sistema Integrado de Gestión Administrativa	Contabilidad y Costos Finanzas Logística Nomina Patrimonio Planeamiento	Administración, Logística Contabilidad Tesorería Presupuesto
03	SICAP v. 2.1	Sistema de Captura y Transferencia de Datos SUNASS	Administrativo Comercial Operacional Control de Calidad	Gerencia Comercial, Gerencia Operacional
04	INTRANET	Sistema de Trámite Documentario	Es un sistema informático que permite registrar y administrar el flujo de documentos de todo tipo en la EPS, además nos facilita la búsqueda o seguimiento del estado y ubicaciones recorridas por un documento como parte del trámite administrativo.	Todas las Unidades Orgánicas
05	SIAF	Sistema Informático de Administración Financiera	Es un sistema informático que permite administrar, mejorar y supervisar las operaciones de ingresos y gastos de las Entidades del Estado, además de permitir la integración de los procesos presupuestarios, contables y de tesorería de cada entidad. Todos estos datos se registran en el SIAF y son Transferidos al MEF.	Administración Logística Contabilidad Tesorería Presupuesto

EQUIPOS INFORMÁTICOS

Señalización o etiquetado de las computadoras de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación. Por ejemplo, etiquetar de color rojo a los servidores, color amarillo a las PC's con información importante estratégica y color verde a las PC's de contenidos normales.

7.4.1.2 Formación de Equipos Operativos

Formar equipos con todas las áreas y oficinas de la EPS SEDA HUANUCO S.A, donde generan y almacenen información y sirva para la operatividad institucional, deberán designar un responsable de la seguridad de dicha información. Puede ser el Jefe del Área o el trabajador que maneje directamente la información.

Entre las acciones a tomar por la Coordinación de Organización, Métodos y Sistema conjuntamente con las demás oficinas serán:

Ponerse en contacto con los propietarios de las aplicaciones y trabajar con ellos el Plan de Contingencia.

GENERACION Y RESTAURACION DE COPIAS DE SEGURIDAD – BACKUPS

Se realizará las copias de seguridad en forma periódica de los datos y sistemas de información críticos para poder recuperarlos en caso de pérdida o daño de acuerdo a la Directiva vigente:

DIRECTIVA No. 001-2025 - EQUIPO DE TECNOLOGIA DE LA INFORMACION Y COMUNICACIÓN - EPS SEDA HUANUCO S.A.

PROCEDIMIENTOS PARA LA GENERACION Y RESTAURACION DE COPIAS DE SEGURIDAD – BACKUPS - SISTEMA INTEGRADO [ERP AVALON v.PRO 2025.1.7] [APLICATIVOS INFORMATICOS] – [ARCHIVOS].

POLÍTICAS NORMAS Y PROCEDIMIENTOS DE BACKUPS.

Se establecerán los procedimientos, normas, y determinación de responsabilidades en la generación de los Backups de los sistemas de información.

DIRECTIVA No. 001-2025 - EQUIPO DE TECNOLOGIA DE LA INFORMACION Y COMUNICACIÓN - EPS SEDA HUANUCO S.A.

PROCEDIMIENTOS PARA LA GENERACION Y RESTAURACION DE COPIAS DE SEGURIDAD – BACKUPS - SISTEMA INTEGRADO [ERP AVALON v.PRO 2025.1.7] [APLICATIVOS INFORMATICOS] – [ARCHIVOS].

7.4.1.3 Formación de Equipos de Evaluación

Esta función debe ser realizada de preferencia por con el apoyo de una empresa consultora externa con experiencia en seguridad de la información, de no ser posible, la realizará el personal de La Oficina de Informática, debiendo establecerse claramente sus funciones, responsabilidades y objetivos:

a) Revisar el cumplimiento de las normas y procedimientos con respecto a Backups y seguridad de equipos y data.

b) Supervisar la realización periódica de los Backups, por parte de los equipos operativos, comprobando físicamente su realización, adecuado registro y almacenamiento.

c) Revisar la correlación entre la relación de sistemas e informaciones necesarios para la buena marcha de la EPS, y los backups realizados.

Informar de los cumplimientos e incumplimientos de las normas, para las acciones de corrección respectivas.

7.4.2. ACTIVIDADES DURANTE EL DESASTRE

7.4.2.1 Plan de Emergencias

En este plan se establecen las acciones que se deben realizar cuando se presente un siniestro; así como la difusión de las mismas. Es conveniente prever los posibles escenarios de ocurrencia del siniestro.

Este plan 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 la contingencia se recomienda adoptar las siguientes medidas con el fin de asegurar la información:

- Apagar los equipos inmediatamente después de haber detectado el siniestro.
- Desconexión del equipo para su retiro del lugar del siniestro.
- Salir rápidamente a través de las vías de escape.
- Proteger y cubrir los equipos.
- Enseñanza del manejo de extintores.

En caso de contingencias como fallas en equipos de cómputo, fallas humanas,

acción de virus, etc.; lo más recomendable es solicitar la ayuda del personal informático, si es que en el área no existe una persona capacitada para resolver el problema.

7.4.2.1 Formación de Equipos

Establecer claramente cada equipo (nombres, puestos, ubicación, etc.) con funciones definidas a ejecutar durante el siniestro. Si bien la prioridad básica es la protección de la Integridad del personal, en caso de que el siniestro lo permita (por estar en un inicio o estar en un área cercana, etc.), deberá de existir dos equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y otro para el salvar los recursos informáticos, de acuerdo a los lineamientos o clasificación de prioridades.

7.4.2.3 Entrenamiento

Se deberá establecer un programa de prácticas periódicas de todo el personal en la lucha contra los diferentes tipos de siniestros, de acuerdo a las funciones que se le hayan asignado en los planes de evacuación del personal y equipos, para minimizar costos se puede aprovechar fechas de recarga de extinguidores, charlas de los proveedores.

El personal de la EPS SEDA HUANUCO.S.A. Deberá tomar 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 el personal directivo.

7.4.3. ACTIVIDADES DESPUÉS DEL DESASTRE

7.4.3.1 Evaluación de Daños

Inmediatamente después que la contingencia ha concluido, se deberá evaluar la magnitud del daño que se ha producido, que sistemas se están afectando, que equipos han quedado no operativos, cuales se pueden recuperar, y en cuanto tiempo, etc.

7.4.3.2 Priorización de Actividades del Plan de Acción.

La evaluación de daños reales y su comparación contra el Plan, nos dará la lista de las actividades que debemos realizar, siempre priorizándola en vista a las actividades estratégicas y urgentes de nuestra Institución.

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

7.4.3.3 Ejecución de Actividades.

La ejecución de actividades implica la creación de equipos de trabajo para realizar las actividades previamente planificadas en el Plan de acción.

Cada uno de estos equipos deberá contar con un coordinador que deberá reportar diariamente el avance de los trabajos de recuperación y, en caso de producirse algún problema, reportarlo de inmediato al personal a cargo del Plan de Contingencias de Sistemas de Información.

7.4.3.4 Evaluación de Resultados

Una vez concluidas las labores de recuperación de los sistemas que fueron afectados por la contingencia, debemos de evaluar objetivamente, todas las actividades realizadas, que tan bien se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades del plan de acción, como se comportaron los equipos de trabajo, etc.

7.4.3.5 Retroalimentación del Plan de Acción.

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

VIII. MEDIDAS PREVENTIVAS

Las medidas preventivas en un Plan de Contingencia Informático se centran en evitar o minimizar la ocurrencia de incidentes, como actualizaciones de software, mantenimiento regular de los equipos informáticos, capacitaciones al personal y el uso de sistemas de seguridad.

HARDWARE

Mantenimiento Preventivo y Correctivo a nivel de Hardware y Software:

Se realizará revisiones y mantenimiento preventivo y correctivo a los equipos informáticos y software.

Tener un servidor nuevo en stock como servidor alterno de contingencia.

Tener instalado un sistema de aspersión automática en todas las oficinas de la EPS

Tener instalado extinguidores manuales operativos y con vigencia

PLAN DE MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE EQUIPOS INFORMÁTICOS - 2025

El Plan de Mantenimiento de Equipos Informáticos, constituye un instrumento de gestión de corto plazo, este plan tiene como objetivos principales prevenir fallas y averías inesperadas, alargar la vida útil de los equipos y optimizar su rendimiento.

Instalación de estabilizadores, UPS y Generadores:

Tener instalados en buen estado: supresores de picos, estabilizadores, Sistemas de Alimentación Ininterrumpida (UPS) para asegurar el suministro de energía durante fallas eléctricas prolongadas.

SOFTWARE

Tener instalado los sistemas operativos de MS Windows original y vigente y con licencia.

Tener instalado un buen software antivirus actualizado y con licencia vigente.

Generación de las Copias de Seguridad (Backups):

Se realizará las copias de seguridad en forma periódica de los datos y sistemas de información críticos para poder recuperarlos en caso de pérdida o daño de acuerdo a la Directiva vigente:

DIRECTIVA No. 001-2025 - EQUIPO DE TECNOLOGIA DE LA INFORMACION Y COMUNICACIÓN - EPS SEDA HUANUCO S.A.

PROCEDIMIENTOS PARA LA GENERACION Y RESTAURACION DE COPIAS DE SEGURIDAD – BACKUPS - SISTEMA INTEGRADO [ERP AVALON v.PRO 2025.1.7] [APLICATIVOS INFORMATICOS] – [ARCHIVOS]

Seguridad Perimetral:

Implementar y mantener un sistema de seguridad para proteger la red, como firewalls y software de detección de intrusos.

Seguridad de la Red y Control de Accesos:
Implementar políticas de contraseñas seguras, así como restringir el acceso a los sistemas y datos solo al personal autorizado para prevenir accesos no deseados.

Capacitación del Personal:
Capacitar al personal en temas de seguridad informática y buenas prácticas para que puedan identificar y reportar posibles riesgos, como uso de dispositivos de almacenamiento externo (USB).

IX. MEDIDAS CORRECTIVAS

Las acciones correctivas de un Plan de Contingencia Informático son las que se aplican después de que ocurre un incidente, incluyendo la recuperación de datos con las copias de seguridad Backups la restauración de sistemas y la implementación de medidas para solucionar la falla específica.

Son las medidas que se toman después de que ocurre un incidente para restaurar la normalidad

Evaluación del Incidente:
Analizar y comprender la naturaleza del incidente si es con relación al Hardware, Software, equipos de comunicación, infraestructura, (por ejemplo, una infección de virus en una PC) para determinar los pasos de recuperación necesarios.

Comunicación y coordinación:
Notificar a los usuarios y jefes de área sobre la situación y coordinar las acciones con el personal correspondiente para la recuperación de los servicios.

HARDWARE

Reparación o sustitución del Hardware:
Reemplazar componentes de hardware que hayan fallado y requieran sustitución.

Si hay fallos en el hardware, se debe proceder al reemplazo inmediato de las piezas o equipos dañados, contando con proveedores y repuestos disponibles.

SOFTWARE

Aislamiento del incidente en caso de infección de virus:

Desconectar los equipos afectados de la red para evitar que el problema se propague, y dar aviso a los usuarios para que salgan del sistema de manera controlada.

Restauración de la Copia de Seguridad:

El proceso de restauración consistirá en recuperar la integridad de la información desde el archivo del último respaldo generado de acuerdo a la Directiva vigente:

DIRECTIVA No. 001-2025 - EQUIPO DE TECNOLOGIA DE LA INFORMACION Y COMUNICACIÓN - EPS SEDA HUANUCO S.A.

PROCEDIMIENTOS PARA LA GENERACION Y RESTAURACION DE COPIAS DE SEGURIDAD – BACKUPS - SISTEMA INTEGRADO [ERP AVALON v.PRO 2025.1.7] [APLICATIVOS INFORMATICOS] – [ARCHIVOS]

Reconstrucción de sistemas:

En caso de daño severo, puede ser necesario reinstalar sistemas operativos y aplicaciones.

Análisis forense:

Investigar la causa raíz del incidente para prevenir futuras ocurrencias y tomar las medidas de seguridad adecuadas.

Desinfección de los equipos informáticos:

Utilizar software antivirus para eliminar virus o malware de los sistemas infectados.

X. PRESUPUESTO PARA LA IMPLMENTACION DEL PLAN

RIESGOS	NIVEL	ACCION	Sede Central		Planta		Taller de medidores		Sede Tingo Maria		Sede Aucayacu		TOTAL POR RIESGO
			Cant.	Monto	Cant.	Monto	Cant.	Monto	Cant.	Monto	Cant.	Monto	
1. AL FUEGO, QUE PUEDE DESTRUIR LOS EQUIPOS Y ARCHIVOS	Bajo	Compra de equipos tecnologicos	15	S/.60,000.00	6	S/.24,000.00	3	S/.12,000.00	4	S/.16,000.00	3	S/.12,000.00	S/.124,000.00
		Restauracion y/o implementacion de Infraestructura de red	Global	S/.15,000.00	Global	S/.6,000.00	Global	S/.4,000.00	Global	S/.4,000.00	Global	S/.3,000.00	S/.32,000.00
		Compra de servidor	2	S/.42,000.00	0	S/.0.00	0	S/.0.00	0	S/.0.00	0	S/.0.00	S/.42,000.00
2. AL ROBO COMUN, LLEVANDOSE LOS EQUIPOS Y ARCHIVOS	Bajo	Compra de equipos tecnologicos	7	S/.28,000.00	3	S/.12,000.00	1	S/.4,000.00	2	S/.8,000.00	2	S/.8,000.00	S/.60,000.00
3. A FALLAS EN LOS EQUIPOS QUE DAÑEN LOS ARCHIVOS	Bajo	Compra de equipos tecnologicos	4	S/.16,000.00	2	S/.8,000.00	1	S/.4,000.00	1	S/.4,000.00	1	S/.4,000.00	S/.36,000.00
4. A ERRORES DEL USUARIO QUE DAÑEN LOS ARCHIVOS	Alto	Capacitacion en manejo de archivos	0	S/.0.00	0	S/.0.00	0	S/.0.00	0	S/.0.00	0	S/.0.00	S/.0.00
5. CON RELACION A ACCIÓN DE VIRUS QUE DAÑEN LOS ARCHIVOS	Medio	Software de recuperacion de archivos	1	S/.1,250.00	1	S/.1,250.00	1	S/.1,250.00	1	S/.1,250.00	1	S/.1,250.00	S/.6,250.00
6. A TERREMOTOS QUE DESTRUYEN EL EQUIPO Y LOS ARCHIVOS	Bajo	Compra de equipos tecnologicos	15	S/.60,000.00	6	S/.24,000.00	3	S/.12,000.00	4	S/.16,000.00	3	S/.12,000.00	S/.124,000.00
		Restauracion y/o implementacion de Infraestructura de red	Global	S/.15,000.00	Global	S/.6,000.00	Global	S/.4,000.00	Global	S/.4,000.00	Global	S/.3,000.00	S/.32,000.00
		Compra de servidor	2	S/.42,000.00	0	S/.0.00	0	S/.0.00	0	S/.0.00	0	S/.0.00	S/.42,000.00
7. AL ROBO DE DATOS Y LA DIFUSION DE ESTOS	Bajo	Software de proteccion de datos	1	S/.950.00	1	S/.950.00	1	S/.950.00	1	S/.950.00	1	S/.950.00	S/.4,750.00
TOTAL POR SEDE			S/.280,200.00		S/.82,200.00		S/.42,200.00		S/.54,200.00		S/.44,200.00		S/.503,000.00

COORDINADOR DE E.S.I. SEDA HUÁNUCO S.A.

XI. CONCLUSIONES

La EPS SEDA HUANUCO S.A, como Empresa Prestadora de Servicio de Saneamiento es muy importante y necesario que cuente con un Plan de Contingencias de Sistemas de Información bien estructurado.

La conclusión de un plan de contingencia de TIC resume la efectividad del plan y los resultados de las pruebas, mientras que la recomendación debe detallar los próximos pasos para mantener el plan actualizado, mejorar su eficacia y asegurar que la organización esté preparada para eventos futuros.

El Plan de Contingencias de Sistemas de Información es un documento de gestión y debe ser considerado en los Plan Operativo Institucional, Plan Operativo Informático y desde luego en los Cuadros de Necesidad en cada periodo.

Se deberá evaluar el éxito y la viabilidad del plan comparando los resultados con los esperados, identificando las fortalezas y debilidades del mismo. Las recomendaciones deben centrarse en la mejora continua, como la actualización periódica del plan, la realización de simulacros regulares, la implementación de mejores prácticas de seguridad y la capacitación del personal para asegurar la continuidad operativa ante desastres.

XII. RECOMENDACIONES

Realizar la actualización continúa del presente Plan de Contingencia Informático, especialmente ante cambios tecnológicos, de equipamiento y de personal.

Realizar las pruebas periódicas para asegurar que el plan sigue siendo viable y que el personal está capacitado.

Mejorar los procesos ante los cambios y mejoras continuas basada en las lecciones aprendidas durante las pruebas o la implementación real.

Realizar capacitaciones continuas al personal clave y de todos los empleados sobre los procedimientos a seguir en caso de una contingencia.

El presente Plan de Contingencias como documento de gestión debe ser aprobado con Resolución de Gerencia General.

Se recomienda designar al supervisor del plan de contingencias con el responsable de cada área para conformar el comité para que participe activamente en el Plan de Contingencias Informático.

ANEXOS:

DIAGRAMA DE FLUJO Y MAPAS CONCEPTUALES

12.1.1 Mapa Conceptual - [Plan de Contingencia - TIC]

12.1.2 Diagrama de Flujo - Análisis de Riesgos [1 - 4]

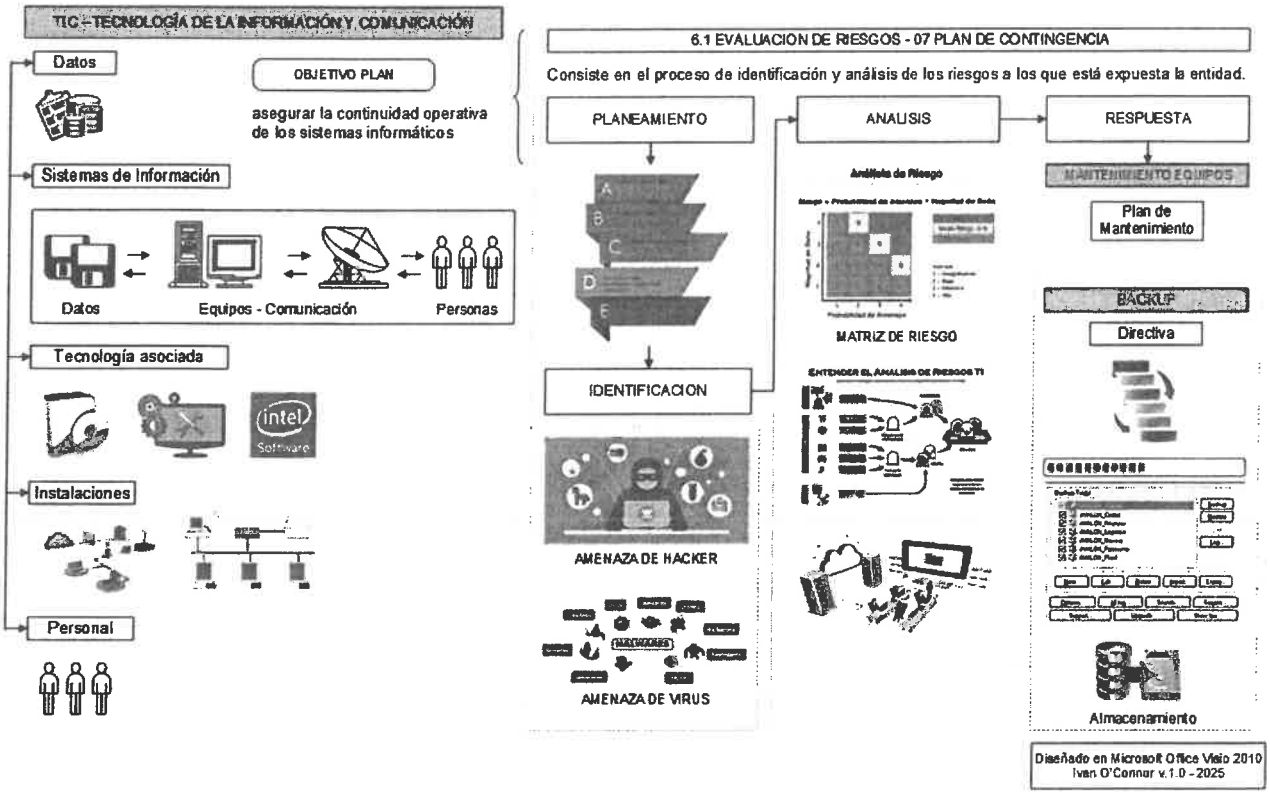
12.1.3 Diagrama de Flujo - Análisis de Riesgos [5 - 7]

12.1.4 Mapa Conceptual - Análisis de Riesgos [1 - 3]

12.1.5 Mapa Conceptual - Análisis de Riesgos [4 - 6]

COORDINADOR DE E.S.I. EPS SEDA HUÁNUCO S.A.

MAPA CONCEPTUAL | CONTROLES PARA LAS TECNOLOGIAS DE LA INFORMACION Y COMUNICACIÓN - TIC | Norma de Control Interno: Resolución de Contraloría No. 320-2006-CG NORMA GENERAL PARA LA EVALUACION DE RIESGOS



COORDINADORA DE E.S.I. EPS SEDA HUANUCO S.A

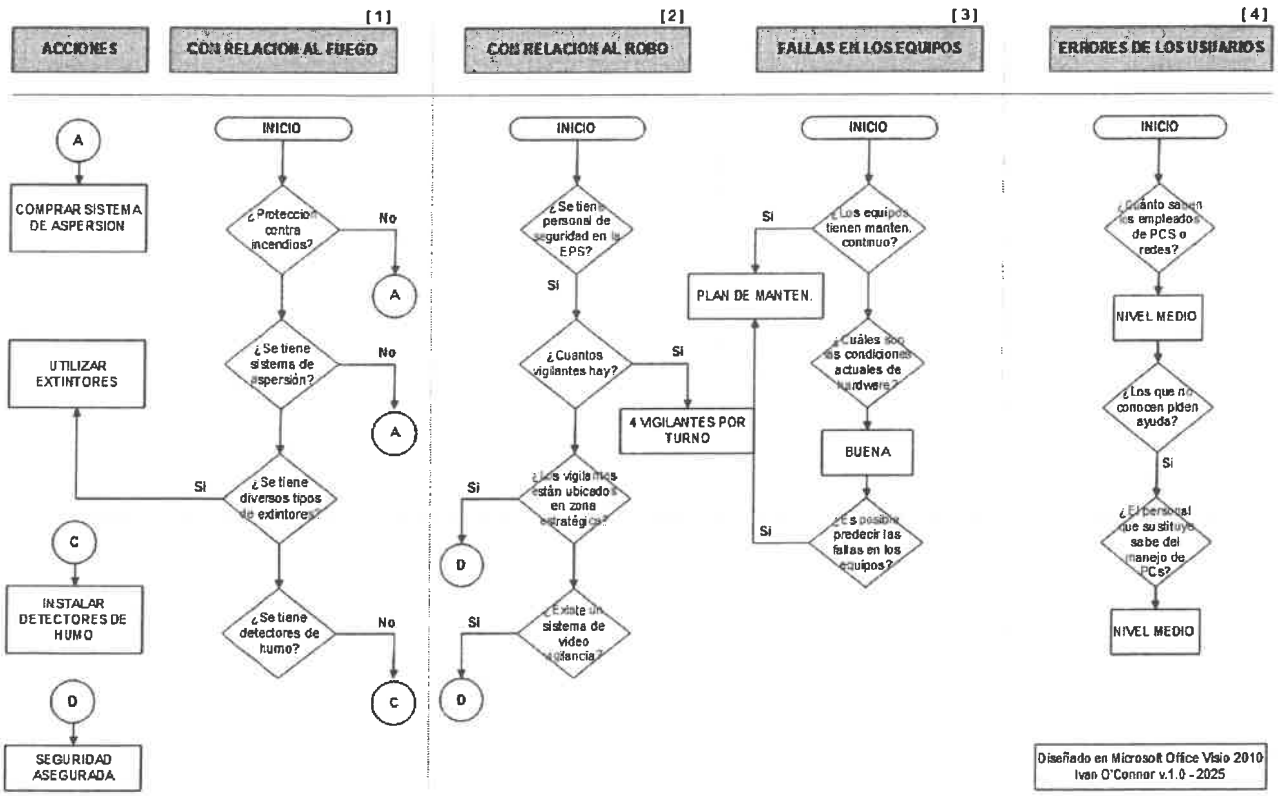
GERENCIA COMERCIAL EPS SEDA HUANUCO S.A.

GERENCIA DE ADMINISTRACION Y FINANZAS EPS SEDA HUANUCO S.A.

DIAGRAMA DE FLUJO

PLAN DE SEGURIDAD - EVALUACION - ANALISIS DE RIESGOS

Norma de Control Interno: Resolución de Contraloría No. 320-2006-CG
NORMA GENERAL PARA LA EVALUACION DE RIESGOS
2.2. Identificación de los Riesgos



Diseñado en Microsoft Office Visio 2010
Ivan O'Connor v.1.0 - 2025

COORDINADOR DE E.S.I. EPS SEDA HUÁNUCO S.A.

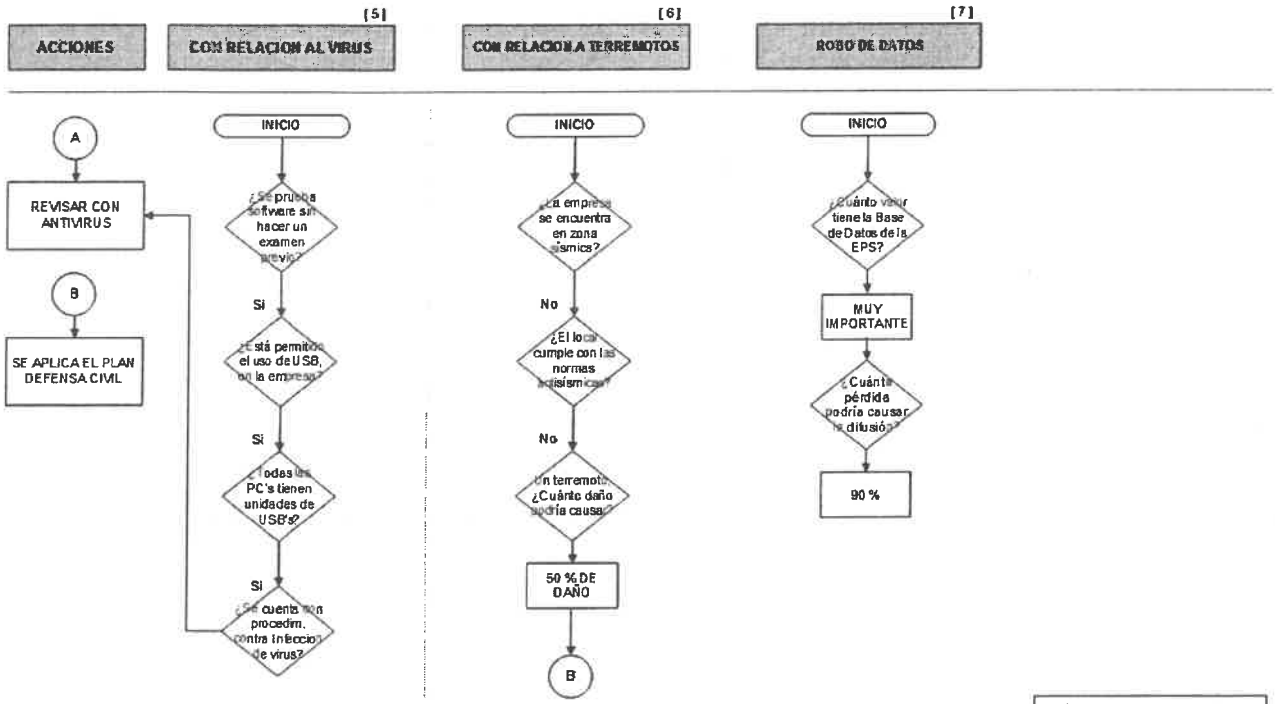
GERENCIA COMERCIAL EPS SEDA HUÁNUCO S.A.

GERENCIA DE ADMINISTRACION Y FINANZAS EPS SEDA HUÁNUCO

DIAGRAMA DE FLUJO

PLAN DE SEGURIDAD - EVALUACION - ANALISIS DE RIESGOS

Norma de Control Interno: Resolución de Contraloría No. 320-2006-CG
NORMA GENERAL PARA LA EVALUACION DE RIESGOS
2.2. Identificación de los Riesgos



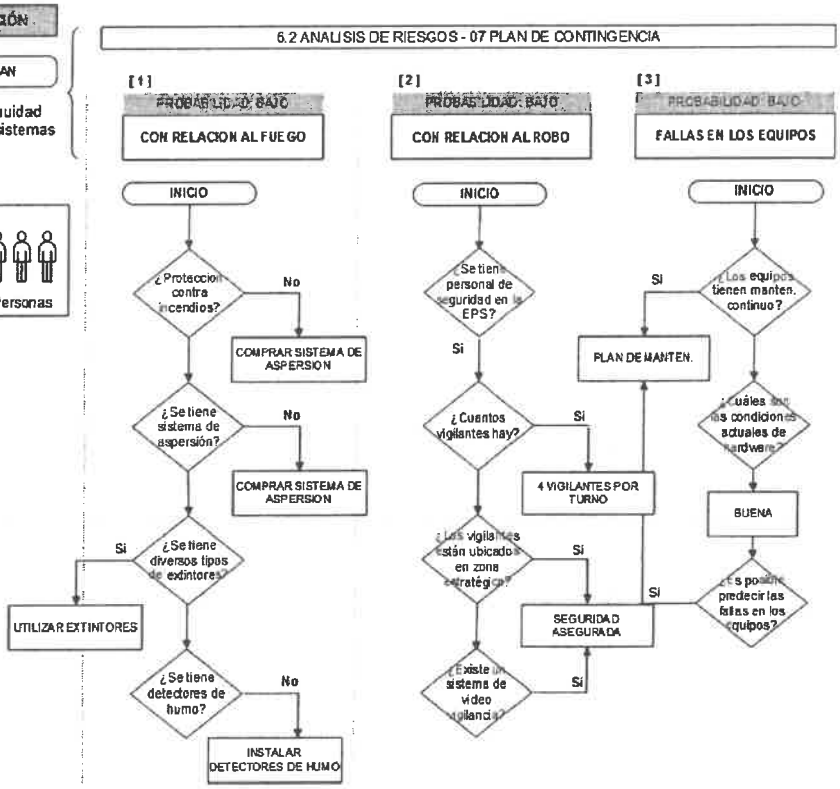
Diseñado en Microsoft Office Visio 2010
Ivan O'Connor v.1.0 - 2025

COORDINADOR DE S.I.
EPS SEDA HUÁNUCO S.A

GERENCIA COMERCIAL
EPS SEDA HUÁNUCO S.A.

GERENCIA DE ADMINISTRACION Y FINANZAS
EPS SEDA HUÁNUCO S.A

MAPA CONCEPTUAL | **CONTROLES PARA LAS TECNOLOGIAS DE LA INFORMACION Y COMUNICACIÓN - TIC** | Norma de Control Interno: Resolución de Contraloría No. 320-2006-CG
NORMA GENERAL PARA LA EVALUACION DE RIESGOS
2.2 Identificación de los Riesgos

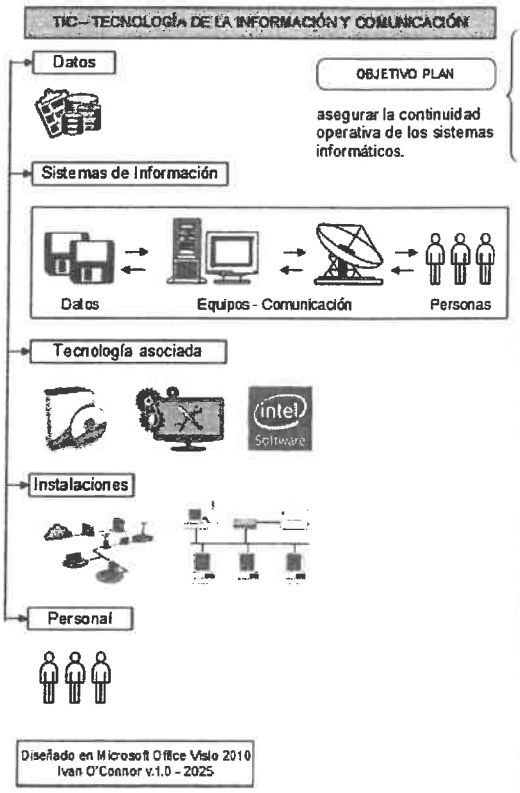


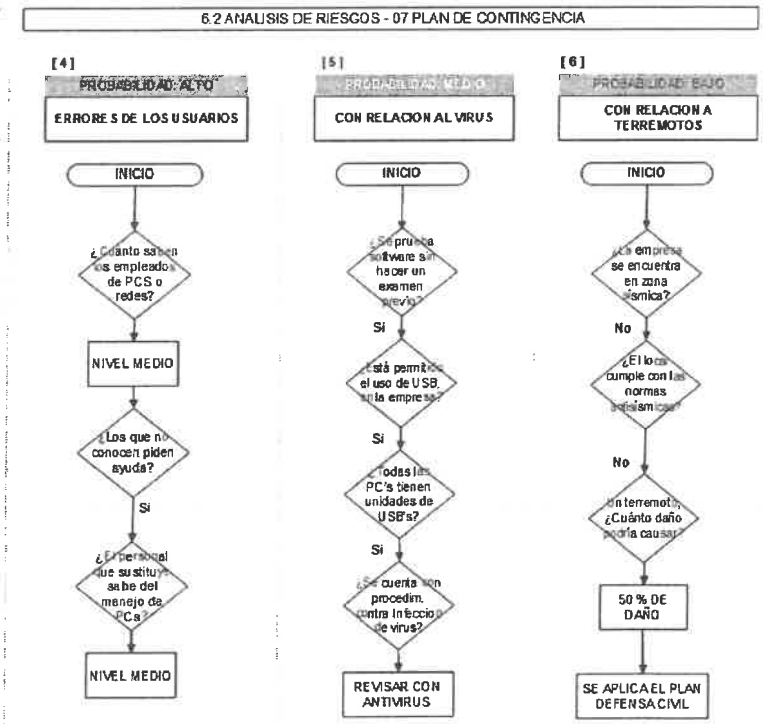
COORDINADOR DE E.S.I. EPS SEDA HUANUCO S.A.

GERENCIA COMERCIAL EPS SEDA HUANUCO S.A.

GERENCIA DE ADMINISTRACION Y FINANZAS EPS SEDA HUANUCO S.A.

MAPA CONCEPTUAL | **CONTROLES PARA LAS TECNOLOGIAS DE LA INFORMACION Y COMUNICACIÓN - TIC** | Norma de Control Interno: Resolución de Contraloría No. 320-2006-CG
NORMA GENERAL PARA LA EVALUACION DE RIESGOS
2.2 Identificación de los Riesgos





COORDINADOR DE E.S.I. EPS SEDA HUANUCO S.A.

GERENCIA COMERCIAL EPS SEDA HUANUCO S.A.

GERENCIA DE ADMINISTRACION Y FINANZAS EPS SEDA HUANUCO S.A.