INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS Nº 283-2016-J/INEN.

REPUBLICA DEL PERU

RESOLUCION JEFATURAL

Surquillo, 05 de Julio del 2016.

VISTO: El Informe Nº 073-2016-OI-OGA/INEN de fecha 28 de junio de 2016, emitido por el Director Ejecutivo de la Oficina de Informática del Instituto Nacional de Enfermedades Neoplásicas; y,

CONSIDERANDO:

Que, mediante Ley Nº 28748 se creó como Organismo Público Descentralizado al Instituto Nacional de Enfermedades Neoplásicas - INEN, con personería jurídica de derecho público interno con autonomía económica, financiera, administrativa y normativa, adscrito al Sector Salud, calificado posteriormente como Organismo Público Ejecutor, en concordancia con la Ley Orgánica del Poder Ejecutivo;

Que, mediante Decreto Supremo N° 001-2007-SA, publicado en el Diario Oficial El Peruano con fecha 11 de enero del 2007, se aprobó el Reglamento de Organización y Funciones del Instituto Nacional de Enfermedades Neoplásicas (ROF-INEN), estableciendo la jurisdicción, funciones generales y estructura orgánica del Instituto, así como las funciones de sus diferentes Órganos y Unidades Orgánicas;

Que, mediante Resolución Ministerial N° 004-2016-PCM, se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2da Edición" en todas las entidades integrantes del Sistema Nacional de Informática;

Que, mediante documento de visto, el Director Ejecutivo de la Oficina de Informática ha solicitado la aprobación del documento técnico, denominado "Plan de Continuidad de la Gestión de las Tecnologías de la Información y Comunicaciones del Instituto Nacional de Enfermedades Neoplásicas – INEN", el cual tiene como objetivo el desarrollo de las medidas necesarias para minimizar la probabilidad de que los riesgos se sometan a los sistemas de información y/o infraestructura informática; y en el caso de que los riesgos se hagan una realidad, posibilitar que tanto los Sistemas de Información como la Infraestructura Informática puedan seguir respondiendo sin que ello suponga un grave impacto para su integridad;

Que, para fines de aplicación y difusión del citado Plan de Continuidad de la Gestión de las Tecnologías de la Información y Comunicaciones del Instituto Nacional de Enfermedades Neoplásicas – INEN, resulta necesario aprobar su formalización mediante la Resolución Jefatural correspondiente;

Contando con el visto bueno de la Sub Jefatura Institucional, de la Secretaría General, de la Oficina General de Planeamiento y Presupuesto, de la Oficina General de Administración, de la Oficina de Informática y de la Oficina de Asesoría Jurídica;

De conformidad con las atribuciones establecidas en la Resolución Suprema N° 008-2012-SA y el literal x) del artículo 9° del Reglamento de Organización y Funciones del INEN, aprobado mediante Decreto Supremo N° 001-2007-SA;

SE RESUELVE:

ARTÍCULO PRIMERO.- APROBAR el "Plan de Continuidad de la Gestión de las Tecnologías de la Información y Comunicaciones del Instituto Nacional de Enfermedades Neoplásicas – INEN", que como anexo forma parte integrante de la presente resolución.

ARTÍCULO SEGUNDO.- DEJAR sin efecto las disposiciones que se opongan a la presente resolución.

ARTÍCULO TERCERO.- CATALOGAR como documento confidencial el "Plan de Continuidad de la Gestión de las Tecnologías de la Información y Comunicaciones del Instituto Nacional de Enfermedades Neoplásicas – INEN", siendo el único responsable de su custodia la Oficina de Informática.

REGÍSTRESE Y COMUNÍQUESE.

Instituto Nacional de Enfermedades Neoplásicas

MC Tatiana Vidaurre Rojas
Jefe Institucional

PLAN DE CONTINUIDAD DE LA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DEL INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS – INEN

LIMA 2016

INDICE

DIRECCION DE LA OFICINA DE INFORMATICA - INEN - V°B°

Especialista en Seguridad de la Información-Oficina de Informática - INEN - V°B°

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

1. ANÁLISIS DE LA SITUACIÓN ACTUAL INFORMÁTICA

1.1. INTRODUCCIÓN

Hoy en día, los principales procesos administrativos y asistenciales del Instituto Nacional de Enfermedades Neoplásicas – INEN, se encuentran soportados por sistemas y servicios informáticos de propósito específico, asimismo contamos con una infraestructura tecnológica de primer nivel, que abarca desde la plataforma de redes y telecomunicaciones sobre la cual tenemos soluciones como la el RIS/PACS (Sistema de Información Radiológica/ Sistema de Almacenamiento y Distribución de Imágenes Médicas), la solución de telefonía IP y comunicaciones unificadas, sistema de video vigilancia, entre otros.

Todos estos recursos y servicios tecnológicos están expuestos a diversos riesgos humanos y físicos que podría causar problemas en su funcionamiento y en ciertas ocasiones esto puede afectar la continuidad de las operaciones en el INEN.

Conscientes de la importancia de adoptar medidas de seguridad que permitan mitigar riesgos y asimismo diseñar procedimientos para afrontar desastres de todo tipo, es necesario desarrollar un Plan de Continuidad del Negocio, básicamente orientado a garantizar la disponibilidad, confiabilidad e integrar de la información, desde la perspectiva de las Tecnología de la Información y Comunicaciones, contemplando actividades de prevención, actividades de acción inmediata y actividades de recuperación en casos se produzca algún siniestro.

DIRECCIÓN DE LA OFICINA DE INFORMÁTICA - INEN - VºBº

Mediante este plan, se busca gestionar procedimientos que nos permitan estar preparados ante fallas potenciales, generando de esta manera soluciones orientadas a la continuidad de las operaciones de la Institución.

1.2. OBJETIVOS E IMPORTANCIA DEL PLAN

1.2.1. OBJETIVO GENERAL

Especialista en Seguridad de la Información-Oficina de Informática - INEN - VºBº

Desarrollar las medidas necesarias para minimizar la probabilidad de que los riesgos se sometan a los sistemas de información y/o infraestructura informática; y en el caso de que los riesgos se hagan una realidad, posibilitar que tanto los sistemas de información como la infraestructura informática puedan seguir respondiendo sin que ello suponga un grave impacto para su integridad.

1.2.2. OBJETIVOS ESPECIFICOS

- Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información y/o Infraestructura Informática, en caso de una interrupción.
- Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen los Sistemas de Información y/o Infraestructura Informática.
- Iniciar un procedimiento de recuperación de los servicios informáticos ante un desastre o posibles fallas ocasionadas.
- Proteger a los Sistemas de Información y/o Infraestructura Informática de pérdidas irreparables de información procesada.
- Identificar y analizar riesgos posibles que pueden afectar las operaciones y procesos informáticos de la institución.

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

1.2.3. IMPORTANCIA

- Permite identificar los riesgos que tengan la probabilidad de ocurrir en la Institución, y posteriormente estructurar las acciones necesarias con el fin de evitar los fallos o disminuir las consecuencias que afectan considerablemente el normal proceso de la Institución.
- Permite estandarizar la forma de actuar de los responsables de la ejecución de este plan ante la ocurrencia de los desastres, considerado la seguridad lógica de la información y la seguridad física de la infraestructura informática.

2. PLAN DE GESTIÓN DE RIESGOS

Se desarrolla un análisis donde se considera a todos los riesgos a los que pueden estar expuestos los sistemas de información y/o infraestructura informática del INEN, de manera que permita reducir la posibilidad de ocurrencia y desarrollar la forma de actuar en caso de desastres.

De manera que se pueda asegurar que se están considerando todas las posibles eventualidades, se ha procedido a realizar un análisis de los posibles sucesos de forma que exista una preparación oportuna para enfrentar adecuadamente la contingencia.

2.1. ANÁLISIS DE RIESGOS

2.1.1. IDENTIFICACIÓN DE LOS ACTIVOS

DIRECCION DE LA OFICINA DE INFORMATICA - V°B° - INEN

Esta tarea es importante porque una buena identificación permitirá la siguiente clasificación:

GRUPO	ACTIVOS
Servicios	• Internet. • Telefonía IP. • Correo Electrónico. • Almacenamiento de Ficheros (FileServer). • Directorio Activo. • Video Vigilancia IP. • Red LAN. • Red WIFI.
Datos / Información	• Archivos Digitales. • Copias de respaldo. • Datos de Configuración. • Código Fuente. • Documentos Físicos.
Aplicaciones	• Sistemas informáticos Administrativos. • Sistema de Gestión hospitalaria. • Base de Datos. • Ris / Pacs. • Navegador Web. • Antivirus. • Ofimática • Sistema Operativo.
Equipos informáticos	• Servidores. • Computadoras. • Dataguard. • Firewall. • Grupo Electrógeno. • Impresoras. • Teléfonos IP.
Personal	• Usuario interno. • Usuario externo.
Redes de Comunicación	• Switches y puntos de acceso. • Cableado estructurado. • Sistema de alimentación interrumpida (UPS).
Instalaciones	• Data Center. • Central Telefónica. • Central de video vigilancia.

Especialista en Seguridad de la Información-Oficina de Informática - V°B° - INEN

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

2.1.2. VALORIZACIÓN DE LOS ACTIVOS

Los activos se valoraran utilizando la siguiente escala:

ESCALA DE VALORIZACIÓN	VALOR	DESCRIPCIÓN
Alto (A)	3	Altamente importante para el desarrollo de la organización.
Medio (M)	2	Importante para el desarrollo de la organización.
Bajo (B)	1	Importancia menor para el desarrollo de la organización.

Definida la escala de evaluación, se procede a determinar la valorización de los activos identificados de la siguiente manera:

TIPO	ACTIVOS IDENTIFICADOS	VALOR
Servicios	Internet	2
	Telefonía IP	2
	Correo Electrónico	2
	Almacenamiento de Ficheros (FileServer)	1
	Directorio Activo	2
	Video Vigilancia IP	2
	Red LAN	3
	Red Wi-Fi	1
Datos / Información	Archivos Digitales	1
	Copias de respaldo	3
	Datos de Configuración	2
	Código Fuente	3
	Documentos Físicos	1
Aplicaciones	Sistemas Informáticos Administrativos	3
	Sistema de Gestión Hospitalaria	3
	Base de Datos	3
	Ris/Pacs	3
	Navegador Web	1
	Antivirus	2
	Ofimática	1
	Sistema Operativo	1
Equipos Informáticos	Servidores	3
	Computadoras	1
	Dataguard	3
	Firewall	2
	Grupo Electrógeno	1
	Impresoras	1
	Teléfonos IP	2
Personal	Usuario Interno	3
	Usuario externo	1
Redes de Comunicación	Switches y puntos de acceso	2
	Cableado Estructurado	2
	Sistema de Alimentación Interrumpida (UPS)	1
Instalaciones	Data Center	3
	Central Telefónica	2
	Central de Video Vigilancia	1

2.1.3. IDENTIFICACIÓN DE LAS AMENAZAS

Se procede a mencionar las amenazas sobre los activos identificados.

TIPO DE ACTIVOS	AMENAZAS
Servicios	• Corte de fluido eléctrico. • Fallas por tensión. • Incendio. • Inundación. • Sismo. • Ataque de hackers. • Falla o caída de la Red de comunicaciones. • Falla o caída de la telefonía IP. • Falla o caída del sistema de video vigilancia. • Falla o caída del sistema de virtualización de los servidores.

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

Datos / Información	• Infección de virus. • Acceso lógico no autorizado.
Aplicaciones	• Acceso lógico no autorizado. • Corte de fluido eléctrico. • Falla o caída de la red de comunicaciones.
Equipos informáticos	• Incendio. • Inundación. • Sismo. • Corte de fluido eléctrico. • Fallas por tensión.
Personal	• Acceso lógico no autorizado. • Acceso físico no autorizado.
Redes de Comunicación	• Acceso lógico no autorizado. • Acceso físico no autorizado. • Falla o caída de la Red de Comunicaciones. • Falla o caída de la Telefonía IP. • Falla o caída del Sistema de Videovigilancia.
Instalaciones	• Acceso físico no autorizado. • Inundación. • Incendio. • Sismo.

2.1.4. VALORIZACIÓN DEL RIESGO

NIVELES DE IMPACTO	VALOR	DESCRIPCIÓN
Crítico	10	El evento provoca una interrupción completa de la tecnología en informática y de todas sus operaciones. Los procesos críticos del negocio no tienen acceso a las instalaciones y tampoco a los recursos de información.
Significativo	7	El evento provoca una interrupción entre parcial y completa de la tecnología en informática y afecta a todos sus procesos.
Moderado	5	El evento provoca una interrupción en los servicios de TI y esto afecta los procesos, pero las actividades críticas no son interrumpidas.
Menor	3	El evento genera un leve impacto en los procesos, pero no ocasiona una interrupción importante en las operaciones. La interrupción de los servicios de TI afecta a menos de un 30% de los usuarios y dura lo suficiente para afectar levemente sus operaciones.
Insignificante	1	El evento no provoca un impacto en los procesos. La interrupción de los servicios de TI afecta a uno o algunos usuarios, pero no dura lo suficiente para provocar un impacto en sus procesos.

DIRECCION DE LA OFICINA DE INFORMATICA - INEN - VºBº

NIVELES DE PROBABILIDAD	VALOR	DESCRIPCIÓN
Casi Cierta	10	Es muy probable que ocurra un evento de esta naturaleza en un periodo de 3 meses.
Probable	7	Es probable que ocurra un evento de esta naturaleza en periodo de 3 a 6 meses.
Moderada	5	El evento ocurrirá en algún momento en un periodo de 6 meses a un año.
Poco Probable	3	Es poco probable que el evento suceda pero podría ocurrir en algún momento de un periodo de un año o dos.
Muy Poco Probable	1	Es muy poco probable que el evento se presente en un periodo más de 2 años y no se detectaron vulnerabilidades que aumenten su probabilidad de ocurrencia.

Especialista en Seguridad de la Información-Oficina de Informática - INEN - VºBº

NIVELES DE RIESGO	RANGO MENOR	RANGO SUPERIOR
Crítico	70	100
Alto	35	69
Moderado	16	34
Bajo	6	15
Muy bajo	1	5

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

	RIESGO	DESCRIPCIÓN DE FALLAS	DESCRIPCIÓN DEL IMPACTO	NIVEL DE IMPACTO	NIVEL DE PROBABILIDAD	NIVEL DE RIESGO
1	Corte de fluido eléctrico	La falla de los servidores del Data Center, puede ser ocasionada por el corte intempestivo del suministro de la energía eléctrica, ocasionado por algún factor externo.	El Data Center no cuenta con el Grupo electrógeno del INEN, esto ocasionaría la paralización de los sistemas del INEN.	Crítico (10)	Probable (7)	**Crítico (70)**
2	Fallas por Tensión	Son fallas que se presentan como fluctuaciones constantes, de la energía, causando problemas en las instalaciones internas.	Puede llegar a malograr los equipos de las estaciones de trabajo y/o equipos médicos.	Crítico (10)	Muy Poco Probable (1)	Bajo (10)
3	Acceso físico no autorizado	Son ingresos a áreas restringidas por procesar información vital de la institución.	Equipos o información de servidores expuestos a personas no autorizadas, las cuales pueden hacer el uso indebido de dichos equipos o información.	Crítico (10)	Muy Poco Probable (1)	Bajo (10)
4	Acceso lógico no autorizado	Son accesos indebidos a los sistemas que cuentan la institución, y que personas no autorizadas obtienen el acceso de manera indebida.	Puede ocasionar cambios, sustracción, eliminación y hasta pérdida de información.	Crítico (10)	Probable (5)	Alto (50)
5	Inundaciones	Un aniego es una abundancia excesiva de agua. Desbordamiento de agua en zonas que habitualmente están libres de esta.	Inutiliza las estaciones de trabajo, servidores, switches, etc. Puede ocasionar perdida de información relevante para el usuario o para la institución misma.	Crítico (10)	Poco Probable (3)	Moderada (30)
6	Incendio	Un incendio es una ocurrencia de fuego no controlada que puede abrasar algo que no está destinado a quemarse.	Perdida de información relevante para la Institución (Informes impresos, Discos duros etc.). Perdida de equipos (PCs, Impresoras, Muebles, etc.)	Crítico (10)	Probable (7)	**Crítico (70)**
7	Sismo	Es un desastre natural que provoca gran destrucción y que puede ocurrir en cualquier momento.	Puede ocasionar corte de energía eléctrica. Deterioro de la infraestructura de la Institución.	Crítico (10)	Probable (7)	**Crítico (70)**
8	Falla o Caída de la Red de comunicaciones	Fallo en la Red de comunicaciones, No conexión con servidores.	Inoperatividad de sistemas de información.	Crítico (10)	Muy Poco Probable (1)	Moderada (10)
9	Falla o caída de la telefonía IP.	Cuando se interrumpen las comunicaciones telefónicas	No habría comunicaciones por medio de teléfonos dentro de la institución.	Significativo (7)	Muy poco Probable (1)	Bajo (7)
10	Falla o caída del sistema de Video Vigilancia.	Cuando el sistema no responde.	Inoperatividad de las cámaras IPs o del Nvr.	Moderado (5)	Poco Probable (3)	Bajo (15)
11	Falla o caída del sistema de virtualización de los servidores.	No se tiene acceso al equipo de administración de servidores.	No se puede acceder a los sistemas informáticos.	Moderado (5)	Poco Probable (3)	Bajo (15)

DIRECCION DE LA OFICINA DE INFORMATICA - INEN - VºBº

Especialista en Seguridad de la Información-Oficina de Informática - INEN - VºBº

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

12	Ataque de hackers	Es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control de las maquinas internas o servidores.	Estos ataques pueden desestabilizar o dañar sistemas operativos de nuestros servidores u otro sistema informático.	Moderado (5)	Probable (7)	Alto (35)
13	Infección de virus	Infecta al SO, base de datos, sistemas o aplicativos.	Podría ocasionar fallas técnicas del equipo como lentitud, o inconvenientes al realizar trabajos en el equipo de tal manera que la información pueda perderse o dañarse.	Significativo (7)	Probable (7)	Alto (49)

Posterior a la evaluación, se ha definido que los siguientes riesgos tienen alto impacto en el desarrollo de las operaciones del INEN:

- Corte de fluido eléctrico.
- Incendio.
- Sismo.

3. PLAN DE PREVENCIÓN DE DESASTRES

Se busca definir las actividades que se realizarán periódicamente, de manera que permitan analizar y minimizar la probabilidad de ocurrencia de algunos de los riesgos que se han detallado anteriormente. Asimismo permitirá validar si las tareas de respaldo tanto en hardware como en software que se han establecido, se están ejecutando, de manera que permita estar preparados cuando surja una eventualidad.

DIRECCIÓN DE LA OFICINA DE INFORMÁTICA - INEN - V°B°

❖ Riesgo: Corte de Fluido Eléctrico

La Oficina de Informática realiza la coordinación respectiva con el Taller de Electricidad, a través de la Oficina de Ingeniería, Mantenimiento y Servicios, para que se desarrolle un plan de mantenimiento preventivo semestral con supervisiones mensuales de las conexiones que suministran energía eléctrica al Data Center Principal como al Secundario; así como también a los gabinetes de redes que están ubicados dentro la Institución.

Especialista en Seguridad de la Información-Oficina de Informática - INEN - V°B°

Adicionalmente se viene ejecutando un plan de mantenimiento preventivo a los pozos de tierra, juntamente con el Taller de Electricidad, de manera que se pueda asegurar el adecuado funcionamiento de las conexiones que suministran fluido eléctrico a todos los equipos informáticos.

Actualmente en el INEN, se viene suministrando corriente estabilizada mediante las diversas conexiones que se encuentran instaladas en la Institución.

Adicionalmente se menciona que existen problemas en cuanto a la continuidad de los servicios informáticos del INEN; debido a que nuestro Data Center Principal no cuenta con un Grupo Electrógeno puesto a punto que le permita abastecerse del servicio eléctrico cuando se presentan fallas o caídas de dicho servicio, ya sea por mantenimiento interno o externo. Por lo tanto se viene coordinando con la Oficina de Ingeniería, Mantenimiento y Servicios para la pronta implementación de este Grupo Electrógeno, de manera que permita garantizar la continuidad de los servicios informáticos.

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

❖ **Riesgo: Fallas por tensión.**

La Oficina de Informática del INEN en coordinación con el Taller de Electricidad, realiza supervisiones constantes de manera que se pueda asegurar que el suministro de energía que se les brinda a los equipos informáticos, sea corriente estabilizada, esto como medida para prevenir que los equipos informáticos puedan sufrir fluctuaciones de corriente eléctrica, ya que esto se presentan en el servicio que brinda el proveedor externo y lo que conlleva a que se originen problemas en el funcionamiento de los equipos informáticos.

❖ **Riesgo: Acceso físico no autorizado.**

Se cuenta con diversas medidas que nos permiten llevar un adecuado control sobre los accesos físicos que se dan en los diversos ambientes que conforman a la Oficina de Informática del INEN.

- **Oficina de Informática**

  La primera persona en llegar a la oficina, deberá acercarse a la Oficina de Vigilancia y recoger la llave y al mismo tiempo registrar en el cuaderno de cargo los siguientes datos: Nombre Completo, fecha, hora, firma y oficina. De igual forma la última persona en retirarse de la oficina deberá poner seguro a la puerta de acceso; y posteriormente, entregar las llaves al área de vigilancia del INEN, dejando como constancia el registro en el cuaderno de cargo.

- **Soporte Técnico**

  Para el control de acceso físico se llevara a cabo el mismo proceso que se ha implementado en la Oficina de Informática.

- **Data Center**

  El acceso en el Data Center es más restringido debido a que cuenta con un sistema biométrico y que solo las personas autorizadas por la Jefatura de TIC y la Dirección de Informática, podrán ingresar ya sea por el reconocimiento de la huella digital o por la tarjeta que le brinda la encargada de TIC. Asimismo las personas que accedan a dicho ambiente deberán registrar en el cuaderno de vistas que se encuentra dentro del Data Center; sus datos, hora de ingreso y hora de salida.

- **Central Telefónica (Data Center Secundario)**

  El acceso a la Central Telefónica (Data Center Secundario) deberá ser solicitado a la Jefatura de TIC, debido a que es la unidad responsable de la llave que da acceso a dicho ambiente. Del mismo modo que Data Center, cuenta con un cuaderno de visitas donde el personal que accede al ambiente deberá registrar sus datos, hora de ingreso y hora de salida.

❖ **Riesgo: Acceso lógico no autorizado.**

En la institución ha implementado diversas medidas que apoyan en la mitigación del riesgo de acceso lógico no autorizado tanto a los sistemas operativos, a los sistemas de información como al servicio de correo institucional. Estas medidas implementadas son las siguientes:

- A los trabajadores que ingresan a laborar por primera vez al INEN, se les hará entrega de manera personal su usuario y contraseña tanto del sistema operativo, sistema de información y cuenta de correo electrónico, previa solicitud del Director Ejecutivo o Jefe del Departamento al que ha ingresado el nuevo trabajador remitida al Director Ejecutivo de la Oficina de Informática, donde se detalle los accesos que se le debe asignar.

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

- Los trabajadores que accedan por primera vez con su cuenta de usuario y contraseña a los servicios informáticos, el sistema les solicitará que modifiquen su contraseña de acceso de manera que solo puede ser conocida por ellos mismos.

- Se ha programado para que todos los usuarios de la institución modifiquen periódicamente (cada 30 días) sus claves de acceso tanto al Sistema Operativo como al Sistema Hospitalario.

- El administrador de los servidores modifica periódicamente las claves de accesos de los equipos que están bajo su cargo.

- La Oficina de Informática ha solicitado a la Oficina de Recursos Humanos, la implementación del procedimiento de Altas, Reasignaciones y Bajas de los trabajadores del INEN de manera que permita mantener un control actualizado de los accesos a los sistemas informáticos que se le les brinda a los usuarios de la Institución.

❖ **Riesgo: Inundaciones.**

En el caso de las inundaciones, el Data Center cuenta con un sistema de drenaje óptimo que evita la presencia de agua en dicho ambiente lo cual evita el peligro de que los equipos informáticos puedan dañarse; asimismo se cuenta con políticas de protección de los equipos informáticos, que prohíben tener equipos en los suelos.

DIRECCIÓN DE LA OFICINA DE INFORMÁTICA - INEN - V°B°

❖ **Riesgo: Incendio.**

A manera de prevención de que se pueda originar un incendio dentro de los ambientes que conforman la Oficina de Informática, se ha implementado dentro del Data Center un sistema antiincendios que incluye cuatro (04) alarmas que alertarán a los encargados ante la presencia de humo, de manera que dichas personas procedan a activar el agente limpio F200 mediante el sistema de disparo y aborto. Este sistema recibe constantemente su mantenimiento preventivo de manera que se pueda asegurar su correcto funcionamiento.

Especialista en Seguridad de la Información-Oficina de Informática - INEN - V°B°

Para el ambiente de Central telefónica (Data Center Secundario), la Oficina de Informática ha solicitado mediante pedido de servicio a la Oficina de Logística del INEN, el acondicionamiento del Data Center Secundario de manera que pueda albergar equipos informáticos de los cuales depende mucho el funcionamiento de los servicios informáticos que se utilizan para el desarrollo de los procesos de la Institución.

Existen extintores tanto en la Oficina de Informática, Oficina de Soporte técnico y Central Telefónica (Data Center Secundario) a manera de estar prevenidos ante una eventualidad de incendio que se pueda presentar. Asimismo es claro precisar que se está coordinando con la Oficina de Ingeniería, Mantenimiento y Servicios del INEN para que el personal pueda ser capacitado en el uso de los extintores de manera que se pueda dar solución inmediata al desastre.
De igual manera se ha recomendado que cada trabajador debe eliminar todo tipo de material inflamable que se encuentren en los ambientes que conforman la Oficina de Informática; y asimismo que deben apagar todos los equipos informáticos que se encuentren a su cargo evitando así que se pueda originar una sobrecarga de energía.

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

❖ **Riesgo: Sismo.**

En caso de sismos, en estos últimos años no se ha presentado un gran número de este tipo de siniestros que tengan gran intensidad; sin embargo se cuenta con medidas de prevención para el personal que labora en la Institución; por ejemplo se vienen realizando constantemente capacitaciones y simulacros, en coordinación con el Instituto Nacional de Defensa Civil, con el fin de mantener preparado al personal en caso se presente este tipo de siniestro y de esta manera poder evitar la pérdida de vidas humanas o daños que se puedan producir a la integridad física; de igual forma se realiza comúnmente supervisiones a los ambientes informáticos de manera que se pueda asegurar de que los equipos que están alojados en dichos ambientes mantengan una correcta ubicación; sin embargo en caso de que el siniestro se dé con una intensidad fuerte, podría ocasionar la caída y/o destrucción de estos equipos, sin embargo como medida preventiva se cuenta con los backups correspondientes de la información del INEN, los cuales se generan mensualmente para luego poder ser llevados a un ambiente fuera de las instalaciones del INEN.

❖ **Riesgo: Falla o caída de la red de comunicaciones.**

En el año 2014 se implementó en el INEN, la nueva red de comunicaciones que consistía en la instalación de nuevos y modernos equipos de comunicaciones que iban a estar enlazados entre sí mediante fibra óptica, lo que conlleva a mejorar considerablemente la velocidad de las transacciones que se realizan en los sistemas informáticos.

Los equipos que conforman la nueva red de comunicaciones del INEN son los siguientes:

- 35 switch cisco 2960-X.
- 02 switch de Distribución en Data Center Cisco N6k-C6001-64P.
- 02 switch de Core WS-C6513-E.
- 23 UPS Emerson liebert de 3 kva.
- 55 Access Point (AP).
- 01 Wirelles Controller cisco 5500.
- 01 Plataforma de autenticación y acceso a la red.

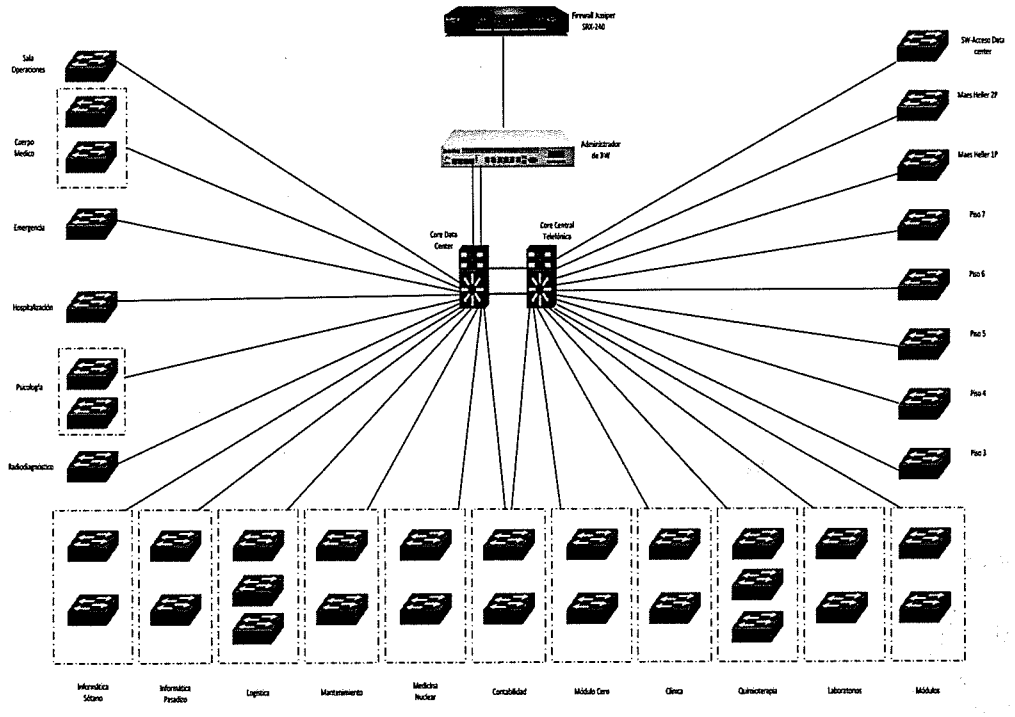
La nueva red de comunicaciones cuenta con alta disponibilidad en vista que cuenta con dos (02) switches de core WS-C6513-E (Un switch core en Data Center Principal y un switch core en Central Telefónica), lo que permite garantizar la disponibilidad en caso de suceder algún inconveniente en cada uno de ellos.

Estos switches de core tienen redundancia consigo mismo ya que están enlazados entre sí mediante fibra monomodo; y asimismo están respaldados con equipos UPS ante alguna eventualidad de corte de fluido eléctrico tanto en el Data Center Principal como en Central Telefónica (Data Center Secundario).

Asimismo se menciona que los switches de acceso se conectan a los switches de core a través de dos (02) enlaces de fibra multimodo (uno a cada switch de core) permitiendo así la redundancia y la alta disponibilidad del servicio. Esto se complementa con el uso de los equipos UPS en cada uno de los Gabinetes de Comunicaciones, ya que de esta forma se puede asegurar corriente eléctrica por un tiempo prudente ante la eventualidad de que suceda un corte de fluido eléctrico.

A continuación se muestra el diagrama de cómo está estructurada la nueva red de comunicaciones del INEN:

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe



Es claro precisar que existe un contrato vigente con el proveedor de la nueva red de comunicaciones, que está orientado principalmente al servicio de soporte técnico que se le da a esta nueva infraestructura; ya que en caso de presentarse algún problema tanto en hardware como en software debe ser solucionado por el proveedor a través de un mantenimiento correctivo a la brevedad posible; asimismo en dicho contrato se ha incluido que el proveedor realizará el mantenimiento preventivo de los equipos de la nueva red de comunicaciones; por lo tanto cada año se realizan dos (02) mantenimientos preventivos a todos los switches y tres (03) mantenimientos preventivos a todos los equipos UPS, esto se realiza previa coordinación con el proveedor para que liego pueda ser programado en el Plan de Mantenimiento Preventivo de Servicios y Recursos Informáticos del INEN que es elaborado por la Oficina de Informática cada año.

❖ **Riesgo: Falla o caída de la telefonía IP.**

En el año 2014, se renovó el servicio de telefonía en el INEN mediante la implementación de un nuevo servicio de telefonía IP que permite la utilización de la red de datos para la realización de llamadas telefónicas.

El nuevo servicio de telefonía cuenta con el siguiente equipamiento:

- 01 Licea Lyric.
- 01 Cisco ISR Generación 2 2901.
- 02 UCS C220 M3.
- 01 UCS C22 M3
- 586 anexos telefónicos:

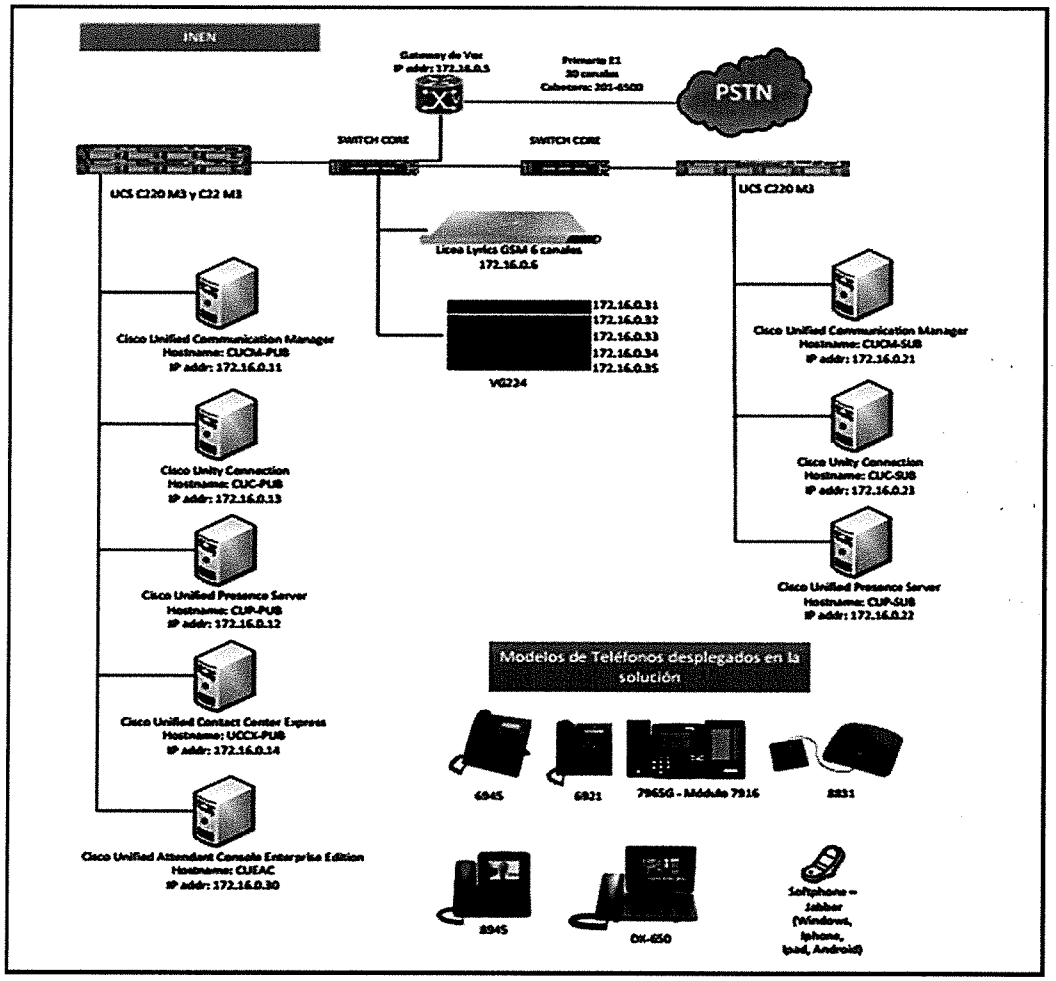
  ✓ 11 dispositivos configurados del modelo DX-650.
  ✓ 85 dispositivos configurados del modelo CP-6921.
  ✓ 435 dispositivos configurados del modelo CP-6965.
  ✓ 3 dispositivos configurados del modelo CP-8831.

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

- ✓ 50 dispositivos configurados del modelo CP-8945.
- ✓ 2 dispositivos configurados del modelo 7916 que contiene 12 botones.

- 04 equipos de videoconferencia:

  - ✓ 02 dispositivos configurados del modelo SX-20.
  - ✓ 02 dispositivos configurados del modelo MX-300.



Este servicio tiene redundancia y alta disponibilidad ya que las dos (02) centrales telefónicas se encuentran en los ambientes donde están ubicados los switches de core (Data Center Principal y Central Telefónica)

Este servicio cuenta con redundancia ya que los servidores trabajan en modo activo – pasivo; es decir ante la caída del servidor principal de telefonía, inmediatamente se activa el servidor secundario de backup

Este servicio tiene alta disponibilidad ya que los dos (02) servidores de central telefónica se encuentran en los ambientes donde están ubicados los switches de core (Data Center Principal y Central Telefónica) es decir, ante la caída de un switch core, sigue activo el servicio de telefonía por lo que la red de datos se encuentra también en redundancia.

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

Asimismo se menciona que los equipos que componen el servicio de telefonía IP (excepto los anexos telefónicos y los equipos de videoconferencia), cuentan con conexión a los equipos UPS de acuerdo a su ubicación, lo que asegura la continuidad del servicio ante una eventualidad o en todo caso brinda el tiempo necesario para buscar una pronta solución.

Según el contrato realizado entre el proveedor y el INEN, los equipos de esta solución deben recibir dos (02) veces por año el mantenimiento preventivo correspondiente de manera que pueda asegurar su correcto funcionamiento, esto se encuentra programado en el Plan de Mantenimiento Preventivo de Servicios y Recursos Informáticos del INEN que es elaborado por la Oficina de Informática cada año.

❖ **Riesgo: Falla o caída del Sistema de Video Vigilancia.**

En el año 2014 el INEN adquirió una solución de Sistema de video vigilancia IP de última tecnología que permite tener un mejor control de la seguridad de cada uno de los ambientes de la institución; ya que las imágenes que transmite son en tiempo real mediante la red de comunicaciones

Esta nueva plataforma de video vigilancia IP, está compuesta por el siguiente equipamiento tecnológico de la marca SAMSUNG:

- 04 NVR Samsung SRN-1000 de 24 TB.
- 50 cámaras fijas modelo SNO-6084R.
- 07 cámaras Domo PTZ modelo SNP-6200RH.

DIRECCIÓN DE LA OFICINA DE INFORMÁTICA V°B° - INEN -

Se estableció como medida de prevención que ante la caída o falla en el sistema de vigilancia, es necesario que todos los equipos que conforman esta solución deban estar conectados a la corriente estabilizada y además, que deban estar instalados en los lugares con las condiciones ambientales adecuadas para asegurar su funcionamiento.

Cada equipo NVR de acuerdo a su ubicación (02 NVR en Data Center Principal y 02 en Central Telefónica) se encuentra conectado al equipo UPS, de manera que pueda continuar con su funcionamiento ante la eventualidad de un corte de fluido eléctrico suceda.

Especialista en Seguridad de la Información-Oficina de Informática V°B° - INEN -

Se precisa además que estos equipos reciben dos (02) veces por año el mantenimiento respectivo correspondiente para asegurar su óptimo funcionamiento, por lo tanto esta actividad se ha de coordina con anterioridad con el proveedor de la solución contratada; y posteriormente se programa en el Plan de Mantenimiento Preventivo de Servicios y Recursos Informáticos del INEN que es elaborado por la Oficina de Informática cada año.

❖ **Riesgo: Falla o caída del Sistema de virtualización de los servidores.**

Desde el año 2014, el INEN cuenta con una solución de Sistema de Virtualización de sus servidores de manera que les permite trabajar bajo un entorno de alta tecnología lo que promueve la reducción de costos en equipamiento así como también liberación de espacio en los ambientes de trabajo.

Esta solución cuenta con una administración centralizada y un monitoreo de todos los servidores configurados, brindándonos la facilidad de incorporar de manera inmediata hardware como procesador, memoria, disco de almacenamiento, entre otros; los cuales permitirá incrementar la performance de los servidores.

Esta solución cuenta con alta disponibilidad entorno a red ya que presenta cuatro conexiones tipo fibra que se conectan a los equipos de Nexus (dos conexiones por equipo); adicionalmente esta solución cuenta con la funcionalidad de migración de servidores virtuales ante una caída de alguno

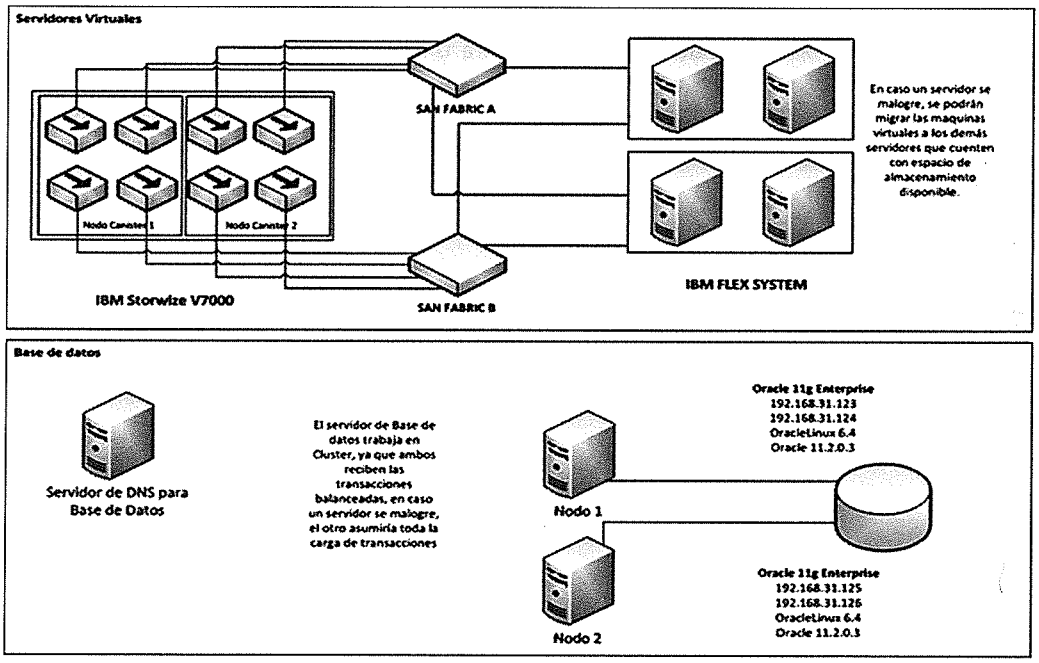
INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

de los cuatro (04) servidores físicos que comprende la solución; teniendo en consideración que se cuente con el almacenamiento disponible para poder llevar acabo la ejecución de la migración.

En el caso de los servidores de Base de Datos que trabajan bajo la tecnología Clúster, se cuenta actualmente con dos servidores físicos que reciben las transacciones balanceadas de todas las consultas que se realizan a nivel institucional por medio del sistema de información SISINEN.

Estos servidores como están dentro de la misma chasis de la solución de servidores virtuales, trabajan bajo la misma plataforma de alta disponibilidad de red (cuatro conexiones de fibra a los equipos Nexus) y adicionalmente como trabaja bajo la tecnología Clúster; en caso un servidor deje de funcionar; inmediatamente todas las transacciones se direccionarán al servidor activo hasta que se la solución respectiva al servidor en problemas.

A la solución de virtualización de servidores se le realiza mantenimiento preventivo dos (02) veces por año, según lo programado en el Plan de Mantenimiento Preventivo de Servicios y Recursos Informáticos del INEN que se realiza cada año. A continuación se muestra el diagrama de cómo está estructurada la solución de virtualización de servidores:



❖ **Riesgo: Ataque de hackers.**

Hoy en día existen muchos ataques de hackers a diversas organizaciones tanto privadas como estatales que conlleva a que su información sea vulnerada; lo que se puede considerar como un riesgo que puede causar alto impacto en el desarrollo de las funciones de la organización atacada.

Por este motivo es que se ha visto necesario, como medida preventiva, que en el INEN se implemente un IPS e IDS de manera que nos permita estar protegidos ante futuros ataques de hackers que se puedan afectar el desarrollo de los procesos en el INEN.

El IPS es un software que permite el control del acceso a la red informática de manera que se pueda proteger a los sistemas computacionales frente ataques y abusos. Asimismo se precisa que este software ofrece mejoras importantes con respecto a las tecnologías cortafuegos tradicionales, ya

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

que toma decisiones de control de acceso basándose en los contenidos del tráfico, en lugar de direcciones IP o puertos.

El IDS es un programa usado para detectar accesos no autorizados tanto a un computador como a la red, por lo que se basa principalmente en el análisis detallado del tráfico de la red, ya que al ingresar al analizador de la red es comparado con firmas de ataques conocidos o comportamientos sospechosos, como puede ser el escaneo de puertos, paquetes mal formados, etc. Por ende se determina que el IDS no solo analiza que tipo de tráfico es, sino que también revisa el contenido y su comportamiento.

- **Riesgo: Infección de virus.**

Los servidores informáticos cuentan con licencia de antivirus de un año contabilizado a partir del 24 de Junio del 2015, lo que permite asegurar la protección de la información que se manejan en dichos equipos, así como también sus configuraciones establecidas. Asimismo es necesario mencionar que mientras se realiza el proceso de licitación para la contratación del servicio de adquisición de licencias del software Antivirus para que sean distribuidas en todo el parque informático del INEN, se ha instalado actualmente en todo el parque informático un software antivirus de libre distribución que se mantiene actualizado mensualmente gracias a las coordinaciones realizadas entre Unidad de Soporte Técnico del INEN y la Jefatura de la Unidad Funcional de Servicios de Tecnologías de la Información y Comunicaciones; con la finalidad de resguardar la información que se encuentra alojada en cada una de la PCs de los usuarios y al mismo tiempo prevenir fallas durante su funcionamiento.

DIRECCIÓN DE LA OFICINA DE INFORMÁTICA - INEN - V°B°

Especialista en Seguridad de la Información-Oficina de Informática - INEN - V°B°

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

4. PLAN DE RECUPERACIÓN DE DESASTRES

En el caso de que ocurra una contingencia, es necesario que se conozca la razón de cómo se originó y cuál es el daño producido, de manera que permita establecer o definir los procedimientos y planes de acción para el caso en que se presenten a futuro posibles fallas, siniestros y desastres en los ambientes que están bajo la responsabilidad de la Oficina de Informática.

Los procedimientos que se estructuren deben permitir afrontar de una manera adecuada los casos de emergencia que se pudiesen presentar; para esto es recomendable que dichos procedimientos deben ser previamente planeados y probados fehacientemente.

Los procedimientos deben ser ejecutados obligatoriamente, bajo la responsabilidad de los encargados designados por la Institución y la Oficina de Informática, por lo tanto consideraran procesos de verificación que les permita asegurar el correcto cumplimiento de dichos procedimientos.

Los reportes o informes que se obtengan en relación a la ejecución de los procedimientos definidos, deberán ser dirigidos en primera instancia a los responsables del de la ejecución del Plan de Continuidad; los cuales posteriormente, lo elevarán a instancias superiores.

4.1. ACTIVIDADES PREVIAS AL DESASTRE

Se definen las actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de la información.

DIRECCIÓN DE LA OFICINA DE INFORMÁTICA - INEN - V°B°

4.1.1. ESTABLECIMIENTO DEL PLAN DE ACCIÓN

Se establecen los procedimientos relativos a:

4.1.1.1. SISTEMAS DE INFORMACIÓN

Actualmente el INEN, cuenta con Sistemas de Información con desarrollo propio y desarrollo por entidades externas. A continuación se detallan los sistemas:

Especialista en Seguridad de la Información-Oficina de Informática - INEN - V°B°

Sistemas Propios:

- Sistema Integrado Hospitalario del INEN (SISINEN).
- Sistema de Generación de Citas Online (Generación de Cita).
- Sistema de Queja y Sugerencia (Buzón de Queja y Sugerencia).
- Sistema de Aplicativo Web (INTRANET).

Sistemas Externos:

- Sistema Integrado de Administración Financiera (SIAF): Sistema de información asociado a la ejecución del presupuesto anual, de registro único de las operaciones de gastos e ingresos públicos. Lo opera la Oficina Central de Ejecución Presupuestaria.
- Sistema Integrado de Gestión Administrativa del Ministerio de Economía y Finanzas. (SIGA MEF): El sistema de información SIGA MEF es un proyecto desarrollado por el Ministerio de Economía y finanzas a través de un convenio con el Ministerio de Salud y financiado por el Banco Interamericano de Desarrollo -BID.

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

4.1.1.2. EQUIPOS DE CÓMPUTO

El INEN cuenta con un buen número de hardware como: impresoras, teléfono, computadoras entre otros, a continuación se detallan:

EQUIPOS	CANTIDAD
CPU (MONITOR+TECLADO+MOUSE)	1200
IMPRESORAS MONOCROMATICAS	461
IMPRESORAS MULTIFUNCIONALES	146
IMPRESORAS FOTOCOPIADORAS	25
LAPTOP	130
EQ. MEDICOS EN RED	90
PROYECTORES	30
TELEFONOS IP	600

Para los temas de identificación y protección de equipo se cuenta con los siguientes criterios:

- A cada equipo informático se le asigna un número llamado "Código Patrimonial", el cual es determinado por la Unidad de Patrimonio al ingresar a la Institución.
- Anualmente se realiza el inventario de los equipos informáticos, de manera que se tengan una información actualizada con respecto a los recursos con los que cuenta la Oficina de Informática.
- Anualmente se realizan dos (02) mantenimientos preventivos a los equipos informáticos. Previa coordinación con la Jefatura de Informática y las jefaturas de las demás direcciones.

DIRECCIÓN DE LA OFICINA DE INFORMÁTICA - INEN - V°B°

4.1.1.3. Obtención y almacenamiento de Copias de Seguridad

Actualmente se tiene implementada la Directiva Administrativa N° 001-INEN/OGA-OI-V.01 "Procedimiento Operativo de Generación, Resguardo y Custodia de las Copias de Seguridad de la Información del Instituto Nacional de Enfermedades Neoplásicas – INEN". A continuación se detallan los servicios informáticos, de los cuales su información generada ha sido considerada en la directiva administrativa mencionada anteriormente:

Especialista en Seguridad de la Información-Oficina de Informática - INEN - V°B°

N°	SERVICIOS INFORMÁTICOS
1	Base de Datos
2	Apl. Siga Mef
3	Apl. Siaf
4	Correo Electrónico
5	Portal Web
6	Apl. Web
7	Servidor Fileserver
8	Servidor Dominio 25
9	Servidor Dominio 26
10	Servidor Siga Mef
11	Servidor Moodle
12	Servidor FTP

Es importante mencionar que para el proceso de restauración de información, se realizan pruebas mensuales en un entorno de pruebas.

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

4.1.2. FORMACIÓN DE EQUIPOS OPERATIVOS

Cada unidad operativa del Instituto Nacional de Enfermedades Neoplásicas – INEN que almacene información de vital importancia para la operatividad institucional, deberá designar a un responsable, de creerlo conveniente podría ser el Jefe de cada unidad, el cual se encargará de solicitar y validar el cumplimiento de los procesos relacionados a la seguridad de la información; los cuales serán implementados por la Oficina de Informática, a través de los siguientes responsables:

- **Unidad Funcional de Desarrollo de Sistema de Información** - Jefe de la Unidad Funcional de Desarrollo y Sistemas

  Ing. Peter Rojas Durand - Celular: 975513480

- **Unidad Funcional de Tecnología de la Información y Comunicaciones** – Jefe (e) de la Unidad Funcional de Tecnología de la Información y Comunicaciones.

  Ing. Benjamín Anyaypoma Ocon - Celular: 989129151

- **Unidad de Servidores y Base de Datos** - Administrador de Servidores y Base de Datos

  Ing. María Ramón Velásquez - Celular: 993506500

- **Unidad de Soporte Técnico** - Coordinadora del Área de Soporte Técnico

  Tec. Guadalupe Aguirre Rojas - Celular: 993506525

El equipo operativo deberá cumplir las siguientes funciones:

- ✓ Establecer el proceso de copias de respaldo de las aplicaciones, junto a los propietarios de dichos software.
- ✓ Supervisar el desarrollo de los procedimientos de respaldo y restauración.
- ✓ Ejecutar trabajos de recuperación y comprobación de datos.
- ✓ Supervisar la carga de los archivos de datos de las aplicaciones, y la creación de los respaldos.
- ✓ Establecer procedimientos de seguridad en los sitios de recuperación.
- ✓ Organizar la prueba de hardware y software.
- ✓ Cargar y probar archivos del sistema operativo y otros sistemas almacenados en el local alternante.
- ✓ Realizar procedimientos de control de inventario y seguridad del almacenamiento en el local alternante.
- ✓ Establecer y llevar a cabo procedimientos para restaurar el lugar de recuperación.
- ✓ Participar en las pruebas y simulacros de desastres.

4.1.3. FORMACIÓN DE EQUIPOS DE EVALUACIÓN

Actualmente la Oficina de Informática cuenta con un Especialista de Seguridad de Información que supervisa y estructura procesos de seguridad bajo los estándares nacionales e internacionales, por lo tanto se encargará del equipo de evaluación que tendrá que cumplir las siguientes funciones:

- ✓ Revisar que las Normas y procedimientos con respecto a Backups y seguridad de equipos y data se cumpla.

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

- ✓ Supervisar la realización periódica de los backups, por parte del equipo operativo, comprobando físicamente su realización, adecuado registro y almacenamiento.
- ✓ Revisar la relación entre los sistemas de información necesarios para la buena marcha de la Institución y los backups realizados.

	RIESGO	ACTIVIDADES PREVIAS AL DESASTRE
1	Corte de fluido eléctrico	• Contar con un grupo electrógeno que suministre energía regulada al DataCenter Central y Secundario. • Solicitar que se desarrolle un plan de mantenimiento preventivo semestral con supervisiones mensuales, de las conexiones eléctricas que alimentan a nuestro DataCenter Principal y Secundario; así como también a los gabinetes de redes. • Contar con equipos UPS necesarios para asegurar el suministro eléctrico en todos los gabinetes de redes así como los switches que están ubicados dentro del DataCenter Principal como del Secundario. • Asegurar que los equipos UPS cuenten con su debido mantenimiento preventivo cada tres (03) meses; así como también con la suficiente energía para soportar una operación continua de 20 minutos (Gabinetes de Redes) y 15 minutos (Switch de Core tanto del DataCenter Central como del Secundario). • Realizar pruebas periódicas de los equipos UPS para asegurar su correcto funcionamiento. • Contar con equipos de luces de emergencia con tolerancia de 15 minutos, accionados automáticamente al producirse un corte de fluido eléctrico, los cuales deben estar instalados en los ambientes críticos. • Contar con el procedimiento operativo alterno para el caso en que faltase el sistema, de tal forma que no afecte considerablemente a la atención de los pacientes **(Anexo N° 1)**.
2	Incendio	• Contar con extintores en buenas condiciones y en lugares estratégicos. • Promover charlas sobre el uso y manejo de extintores. • Contar con salidas de emergencia. • Contar con los números telefónicos donde se pueda reportar cualquier emergencia, incluir Bomberos, ambulancia y personal del INEN responsable de la prevención y ejecución de la contingencia. • Los servidores deben encontrase debidamente protegidos y ubicados en los lugares estratégicos para que no resulten muy afectados cuando se presente un incendio. • Evitar sobrecargar las líneas eléctricas, no conectando más de un aparato en cada toma de corriente. • Apagar y desconectar todos los aparatos y equipos electrónicos al término de la jornada laboral. • El personal de limpieza no deberá utilizar productos inflamables en los lugares donde se encuentren funcionando equipos informáticos. • Está prohibido que el personal fume dentro de las áreas que acogen equipos informáticos, y en áreas totalmente restringidas. • Contar con elementos para la detección y extinción de un posible incendio: ✓ Implementar detectores de humo. ✓ Mantener actualizado los extintores.
3	Sismo	• El Director Ejecutivo de la Oficina de Informática debe solicitar a la Oficina de Ingeniería, Mantenimiento y Servicios, la identificación de las partes más vulnerables de la Oficina y DataCenter (Principal y Secundario) ante un sismo e identificar los lugares más seguros e los que el personal pueda protegerse. • Revisar periódicamente y reparar, si es el caso, las instalaciones de electricidad para que siempre se encuentren en buen estado. • Realizar periódicamente simulacros con todos los miembros de la oficina, para luego realizar lo aprendido en caso se presente un sismo. • El Director de la Oficina conjuntamente con una persona especialista en electricidad debe delegar a un número de empleados acerca de cómo y dónde se desconectan los suministros de electricidad dentro de la Oficina y el DataCenter. • La Oficina de Informática debe contar con un botiquín de primeros auxilios, así como también con los números telefónicos de emergencia, Defensa Civil, Hospitales, Bomberos, Policía, etc. • Se debe tener identificado los lugares peligrosos de la oficina y de los pasillos para alejarse de ellos. • Señalizar todas las salidas y las zonas seguras. • Identificar las rutas de evacuación y mantenerlas libres.

DIRECCION DE LA OFICINA DE INFORMATICA - V°B° - INEN

Especialista en Seguridad de la Información-Oficina de Informática - V°B° - INEN

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

4.2. ACTIVIDADES DURANTE EL DESASTRE

En caso se presente el siniestro o desastre, se debe ejecutar las siguientes actividades planificadas previamente:

4.2.1. PLAN DE EMERGENCIAS

La presente etapa incluye las actividades a realizar durante el desastre o siniestros, se debe tener en cuenta la probabilidad de su ocurrencia durante: el día, noche o madrugada. Este plan incluirá 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.

La integridad de las personas es primordial; por ende, se deben adoptar medidas con el fin de asegurar la información detallando:

- Localización de vías de escape o salida: las vías de escape o salida para solicitar apoyo o enviar mensajes de alerta, a cada oficina debe señalizar las vías de escape.
- Plan de Evaluación Personal: el personal ha recibido periódicamente instrucciones para evacuación entre sismos, a través de simulacros, esto se realiza acorde a los programas de seguridad organizadas por Defensa Civil a nivel local. Esta actividad se realizara utilizando las vías de escape mencionadas en el punto anterior.
- Ubicación y señalización de los elementos contra el siniestro: tales como extintores, las zonas de seguridad que se encuentran señalizadas (ubicadas normalmente en las columnas), donde el símbolo se muestra en color blanco con fondo verde. De existir un repintado de paredes deberá contemplarse la reposición de estas señales.
- Secuencia de llamadas en caso de siniestros: tener a la mano elementos de iluminación, lista de teléfonos de instituciones como: Compañía de Bomberos, Hospitales, Centros de Salud, Ambulancias, Seguridad.

4.2.2. FORMACIÓN DE EQUIPOS

Se debe establecer los equipos de trabajo (nombres, puestos, ubicación, etc.) con funciones claramente definidas que deberá realizar en caso de desastre. Si bien en la premisa básica es la protección de la integridad del personal, en caso de que el siniestro lo permita (al estar en un inicio o estar en un área cercana, etc.), deberá existir dos (02) equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y el otro para salvamento de los equipos informáticos, de acuerdo a los lineamientos o clasificación de prioridades.

4.2.3. ENTRENAMIENTO

Se debe desarrollar un programa de prácticas periódicas que permitan al personal afrontar su lucha contra los diferentes tipos de siniestro, de acuerdo a las funciones que se les haya asignado en los planes de evacuación del personal o equipos.

Estas prácticas deben de ser asumidas por el personal con la seriedad y responsabilidad adecuada, debido a que los siniestros pueden ocurrir en cualquier momento. Asimismo se debe hacer partícipe a los directores, como muestra de que la alta dirección otorga la importancia debida a la seguridad institucional.

Para ayudar al entrenamiento y capacitación de los equipos, el responsable de la implementación del Plan de Continuidad deberá solicitar la ayuda y colaboración de ciertas instituciones o áreas:

- Cuerpo de Bomberos Voluntarios del Perú.
- Comandante de la Comisaria de Surquillo.

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

- Serenazgo de la Municipalidad de Surquillo.
- Gerente de Administración de la Municipalidad de Surquillo.
- Jefe de Defensa Civil de la Municipalidad de Surquillo.
- Sub Gerente del Sistema Metropolitano de Solidaridad – SISOL - Surquillo

	RIESGOS	ACTIVIDADES DURANTE EL DESASTRE
1	Corte de fluido eléctrico	• Dar aviso del corte de energía eléctrica en forma oportuna a todas las áreas del INEN y coordinar las acciones necesarias. • La Unidad Funcional de Desarrollo de Sistemas de Información ejecutará su procedimiento operativo alterno que se tomara como contingencia a fin de no afectar a la atención de los pacientes **(Anexo N°1)**. • En el caso de los equipos que entren en funcionamiento automático con UPS's, se deberá monitorear el tiempo de autonomía del equipo y no exceder el tiempo establecido. • En caso la interrupción de energía sea mayor a treinta minutos, se deberán apagar todos los servidores así como también todos los equipos que conforman los servicios informáticos, hasta que regrese el fluido eléctrico.
2	Incendio	• El director o cualquier miembro de la oficina deben llamar a los bomberos. • Mantener la calma sin gritar ni provocar el pánico entre los empleados. • Abandonar inmediatamente la oficina. • No perder el tiempo buscando objetos o pertenencias. • Recordar que el fuego, el humo y los gases tóxicos tienden a subir, por lo cual si el personal tuviera que pasar forzosamente a través del humo no lo deben intentar de pie, deben hacerlo cerca del suelo ya que habrá aire menos contaminado y con menos temperatura. • Arrastrase por el suelo con la cabeza a unos 30 centímetros del piso y taparse la boca y nariz con pañuelo que le permita respirar inhalando la menos cantidad de gases y humo. • No utilizar las escaleras si el humo las ha invadido. • Para poder subir y dirigirse a la salida del INEN, transitar pegados a las paredes. • No abrir ninguna puerta de las oficinas cuya superficie esté caliente, es casi seguro que tras la puerta haya fuego y si usted la abre alimentará con más aire las llamas que tenderán a salir fuera de la oficina propagándose por todas partes; además de que los trabajadores que se encuentren cerca pueden recibir quemaduras graves. • Una vez que los trabajadores hayan salido, no volver a ingresar sin autorización de los bomberos y del director de la oficina de informática. • Informar a los bomberos la situación que los empleados vieron en el interior antes de salir. • Si se quedan atrapados en alguna oficina mientras tratan de escapar: Separar todo material combustible de la puerta y mojarlo si les es posible. • Si el fuego alcanza a alguno de sus compañeros: No permitir que corra. Haga que se detenga, se tire al piso y ruede, cubriéndose la cara con las manos. Una vez apagadas las llamas no intente quitarle las ropas quemadas, le arrancaría la piel pegada a ellas. Sacar todo elemento metálico que la víctima tenga, ejemplo: reloj, cadenas, anillos etc.
3	Sismo	• El Director, los Jefes de Unidad y los demás empleados deben mantener la calma y si no se tiene tiempo para salir, deben ubicarse en las zonas de seguridad de la oficina, bajo los marcos de las puertas, escritorios, o mesas observando las reglas de posición. • Mantenerse retirado de muebles pesados que podrían caerse o dejar caer su contenido. • En caso el personal escucha una alarma preventiva procederán de inmediato a desalojar las instalaciones y ubicarse en un área abierta que previamente se haya definido (retirándose del edificio, barandas y cables de energía). • De ser posible, asegurar el DataCenter Principal y Secundario, y cerrar las sesiones de su centro de trabajo; sería recomendable apagar las máquinas para que no pueda presentarse ningún problema eléctrico. • Una vez que haya finalizado el movimiento sísmico, los trabajadores, sin esperar que se les ordene, iniciarán la evacuación ordenada de las instalaciones.

DIRECCION DE LA OFICINA DE INFORMATICA - INEN - V°B°

Especialista en Seguridad de la Información-Oficina de Informática - INEN - V°B°

4.3. ACTIVIDADES DESPUÉS DEL DESASTRE

Las actividades que se deben realizar inmediatamente después de ocurrido el siniestro, son las siguientes:

4.3.1. EVALUACIÓN DE DAÑOS

Luego de que el siniestro haya concluido, se deberá realizar en primer caso, una evaluación de los bienes materiales, equipos y sistemas de información que se hayan visto afectados por el siniestro, indicando cuales pueden ser recuperados y en cuanto tiempo.

En el caso del INEN se deberá dar prioridad a los procesos de contabilidad, tesorería, documentación clínica y demás sistemas de información que son considerados fundamentales por

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

su importancia estratégica en el desarrollo de las funciones de la Entidad. Asimismo se dará prioridad a la recuperación y puesta en marcha de los servidores que alojan a los sistemas de información con los que trabaja la entidad.

4.3.2. PRIORIZAR ACTIVIDADES DEL PLAN DE ACCIÓN

Las oficinas involucradas en el Plan de Continuidad de la Gestión de las TIC de acuerdo al ámbito de su competencia, previa evaluación de los daños ocasionados por los siniestros, priorizan las actividades correspondientes, a fin de habilitar los ambientes y poner en funcionamiento a los equipos, sistemas operativos y sistemas de información con los que trabaja la institución. En lo relacionado a informática se dará prioridad a las actividades estratégicas y urgentes, las cuales pueden ser:

- Restablecimiento de los servicios informáticos mediante la habilitación de los servidores, si en caso hubiesen sido dañados por los siniestros.
- Restauración del último backup de datos de los sistemas en producción.
- Reinstalación de los sistemas de información de acuerdo al cuadro de prioridades en las PCs de los usuarios.
- Reinstalación de los sistemas operativos y software de base en los terminales que se encuentren operativos en dicho momento, si es que presentasen problemas.
- Restablecimiento de la Central de Telefonía IP y de los anexos telefónicos que se encuentran distribuidos en las diversas áreas del Instituto.

4.3.3. EJECUCIÓN DE ACTIVIDADES

La ejecución de las actividades implica la colaboración de todos los funcionarios de la Entidad, creando equipos de trabajo a los que se les asignara diversas tareas. Cada uno de estos equipos deberá contar con un líder que tendrá la obligación de reportar el avance de los trabajos de recuperación y en caso de producirse un inconveniente, reportarlo de inmediato al Directivo, indicándole las posibles soluciones.

Los trabajos de recuperación se iniciarán con la restauración del servicio usando los recursos de la Entidad, teniendo en cuenta que en la evaluación de daños se contempló y gestiono la adquisición de accesorios dañados. La segunda etapa es volver a contar con los recursos en las cantidades y lugares propios del Sistema de Información, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar la operatividad de la institución y el buen servicio de nuestro sistema e imagen institucional.

4.3.4. EVALUACIÓN DE RESULTADOS

Una vez concluidas las labores de recuperación de los sistemas que fueron afectados por el siniestro, se deberá evaluar objetivamente, todas las actividades realizadas; con que eficacia se hicieron, que tiempo tomaron, que circunstancias tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades, como se comportaron los equipos de trabajo, etc. Finalizado la evaluación de los resultados, se deberían obtener dos tipos de recomendaciones:

- La retroalimentación del plan de continuidad de la gestión de las TIC.
- La lista de recomendaciones para minimizar los riesgos y pérdida que ocasionó el siniestro.

4.3.5. RETROALIMENTACIÓN DE ACTIVIDADES

El Plan de Continuidad es un documento de gestión de la Oficina de Informática, teniendo como característica particular que cambia en el tiempo, es decir, debe adaptarse de acuerdo a las

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

emergencias que pudiesen suscitar, y con los cambios tecnológicos de los equipos informáticos; esta información tendrá que incorporarse al documento en el marco de la retroalimentación constante, garantizando la vigencia y utilidad de este Plan.

En pos de mantener actualizado este importante documento, se define como política de la Oficina de Informática la revisión y actualización del Plan de Continuidad de la Gestión de las Tecnologías de la Información y Comunicaciones dos veces al año, mediante la siguiente programación:

- Primera actualización en el mes de Agosto del año en curso.
- Segunda actualización en el mes de Diciembre del año en curso.

	RIESGOS	ACTIVIDADES DESPUES DEL DESASTRE
1	Corte de fluido eléctrico	• Brindar un tiempo de gracia, de acuerdo a la magnitud de la contingencia, para que pueda ser restablecido los equipos y servicios informáticos. • El personal de informática debe validar que los equipos y servicios informáticos deben estar funcionando correctamente. • En caso de que presenten problemas en el funcionamiento los equipos informáticos, el personal de Soporte Técnico debe realizar una revisión al equipo para que pueda corregir el daño presentado. • Se notificará a cada una de las áreas de la institución, sobre el restablecimiento de todos los servicios informáticos, previa validación de su correcto funcionamiento por parte de las personas encargadas pertenecientes a la Oficina de Informática del INEN.
2	Incendio	• Verificar los daños que se originaron a causa del incendio. • Verificar el buen funcionamiento y las pérdidas que hubieron de los equipos de cómputo que se encuentran distribuidas en la Oficina de Informática, DataCenter Principal y Secundario, y en las distintas áreas del Instituto. • Todo aquel trabajador que tenga información relacionada con el origen del incendio debe hacerlo del conocimiento • Cuando sea necesario, los encargados de la Oficina (Director y Jefes de Unidad), participarán en la investigación de las causas que originaron el siniestro • De ser necesario, los encargados de la Ofician de Informática colaborarán con especialistas, participando en la investigación del origen del problema para emitir el dictamen correspondiente • Elaborar un reporte por escrito a sus superiores, que contengan: descripción cronológica de los hechos, gravedad de los daños humanos y materiales, las posibles causas, lugar de la emergencia, forma en que se recibió el reporte, medios utilizados para el combate al fuego y eficiencia respecto al funcionamiento de los medios utilizados fallas de organización, humanos o de equipos que se observaron durante la emergencia, así como recomendaciones o sugerencias para atenuar y eliminar en su caso esas anomalías. • Rendir a sus superiores un informe detallado del comportamiento de los sistemas y equipos a su cargo, incluyendo sugerencias para corregir anomalías observadas • Ejecutar y Gestionar ante quien sea necesario las recomendaciones o emplazamientos derivados de la investigación del siniestro, llevando un control de avance.
3	Sismo	• Los trabajadores no deben utilizar los ascensores, ser cautelosos con las escaleras; ya que podrían haberse debilitado con el sismo. • Evitar pisar o tocar cualquier cable caído o suelto. • No encender las computadoras, impresoras y servidores hasta asegurarse que no haya problemas en las instalaciones eléctricas. • Si hay incendios, el personal encargado de la oficina debe llamar a los bomberos o a las brigadas de auxilio. • Usar los teléfonos y anexos sólo para reportar una emergencia. • Atender las indicaciones de las autoridades o de las brigadas de auxilio. • Efectuar con cuidado una revisión completa de la Oficina y del Data Center tanto el principal como el secundario. • En caso de que un trabajador haya quedado atrapado, deberá conservar la calma y tratar de comunicarse al exterior golpeando con algún objeto.

DIRECCION DE LA OFICINA DE INFORMATICA - V°B° - INEN

Especialista en Seguridad de la Información-Oficina de Informática - V°B° - INEN

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

5. CONCLUSIONES

1. El Plan de Continuidad de la Gestión de las Tecnologías de la Información y Comunicaciones, permitirá salvaguardar la infraestructura de la red y sistemas de información del INEN, asimismo contendrá medidas de seguridad extremas de manera que permita protegerlos, al mismo tiempo mantenerlos preparados a una contingencia de cualquier tipo.

2. El Plan de Continuidad de la Gestión de las Tecnologías de la Información y Comunicaciones fue estructurado en base a la infraestructura y servicios tecnológicos considerados críticos o de alto impacto para el desarrollo de las funciones de la Institución; los cuales son gestionados por la Oficina de Informática, bajo la supervisión de la Alta Dirección.

3. El presente documento da a conocer los antecedentes del Plan de Continuidad de las Tecnologías de la Información y Comunicaciones, de manera que permita comprender y concientizar sobre los beneficios que tiene su ejecución; y asimismo reflejar la razón de como la continuidad aporta valor a los servicios que se brindan en la Institución.

4. Se ha conformado el grupo de trabajo que ayudara a gestionar los procedimientos definidos en el plan de recuperación de desastres, asimismo determinar sus responsabilidades durante el desarrollo de las actividades descritas en este plan.

5. En el presente plan se ha incluido la gestión de los riesgos que, de acuerdo a la vulnerabilidades existentes, se pueden presentar en la Institución, ante esto se elaboró el plan de recuperación de los riesgos que tienen mayor nivel de impacto y ocurrencia dentro de los procesos que se desarrollan en la Institución.

6. RECOMENDACIONES

1. Hacer de conocimiento a nivel Institucional sobre el contenido del presente Plan de Continuidad de la Gestión de las Tecnologías de la Información y Comunicaciones, con la finalidad de instruir adecuadamente al personal que labora en el INEN.

2. El Plan de Continuidad de la Gestión de las Tecnologías de las Información y Comunicaciones debe probarse por lo menos dos (02) veces al año, empleando los recursos humanos y tecnológicos necesarios para llevar acabo adecuadamente la ejecución de dicho plan. Los resultados que se obtengan de estas pruebas deben ser documentadas y conservarse hasta la próxima prueba programada.

3. Es necesario contar con el apoyo de la alta gerencia, en el desarrollo y ejecución del presente plan de Continuidad de la Gestión de las Tecnologías de la Información, ya que su implementación no se enfoca particularmente al aspecto técnico; sino que implica que sea ejecutado integralmente en toda la Institución, incluyendo aspectos humanos y técnicos.

4. Si bien es cierto que existe un personal que se encarga de velar por la continuidad de las operaciones, no se debe permitir que toda la responsabilidad recaiga únicamente sobre dicho personal, ya que se bien es cierto que dicho grupo tiene a cargo dicho plan, hay que tener presente que esto involucra a todo el personal de la Institución.

5. Se debe programar continuamente la revisión del presente Plan, de manera que se pueda verificar que esté ajustado a la realidad de la institución; ya que en el caso de se haya presentado una modificación, se deberá modificar, inmediatamente, el plan para que este sea, en todo momento útil.

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

ANEXOS

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

ANEXO N°1

"PROCEDIMIENTO DE CONTINGENCIA ANTE LA AUSENCIA DEL SISTEMA HOSPITALARIO SISINEN"

La Unidad Funcional de Desarrollo de Sistemas de Información ha elaborado un procedimiento de contingencia que le permitirá dar respuesta inmediata a eventos que provoquen la interrupción del sistema Hospitalario SISINEN, con la finalidad de no afectar la atención de los pacientes.

El procedimiento de contingencia consiste en lo siguiente:

7. SE IDENTIFICAN LOS PROCESOS CRÍTICOS EN LA INSTITUCIÓN EN FUNCIÓN DE LOS SISTEMAS DE INFORMACIÓN DE MANERA GENÉRICA Y EVALUANDO SU GRADO DE IMPORTANCIA. SE UTILIZADA LOS SIGUIENTES NIVELES: H (ALTA), R (REGULAR), L (BAJO).

MODULO	OPERACIONES PRINCIPAL	CONTENIDO DE LA OPERACIÓN	PRIORIDAD
FARMACIA FACTURACION	VENTAS (A)	Venta de medicamentos a los clientes con seguro	H
		Venta de medicamentos directa	H
FARMACIA LOGISTICA	INGRESO Y SALIDA MEDICAMENTO (B)	Ingreso de Medicamentos	R
		Salida de Medicamentos	R
		Administración de Kárdex de farmacias	R
CONTABILIDAD	ELABORACION DE INFORMES DE RECAUDACION (C)	Elaboración de reportes de recaudación diaria	H
FACTURACION SERVICIO	EMISION DE COMPROBANTES DE PAGO (D)	Emisión de documentos contables (Boletas, Factura, Recibo , Notas de Créditos, Nota de Rebaja)	H
LABORATORIO	GESTION DE MUESTRAS (E)	Generación de acto médico	H
		Generación de Etiquetas	H
		Transmisión de resultados validados	H
BANCO DE SANGRE	ADMINISTRACION DE DONANTES (F)	Gestión Donación	R
PATOLOGIA	EMISION DE ORDENES y ENTREGA DE RESULTADOS (G)	Generación de acto médico	R
		Registro de Resultados	R
HOSPITALIZACION	ADMISION Y ADMINISTRACION DE CUENTA (H)	Admisión hospitalaria y administración de cuenta	H
EMERGENCIA	ADMISION Y ADMINISTRACION DE CUENTA (I)	Admisión hospitalaria y administración de cuenta	H
HISTORIA CLINICA	GESTION DE HISTORIAS CLINICAS (K)	Registrar movimiento de las historias clínicas	R
CIRUGIA	GESTION DE OPERACIONES Y PROCEDIMIENTOS (L)	Registrar las intervenciones realizadas	R
CONSULTA EXTERNA	ATENCION DE CONSULTA Y GENERACION DE ORDEN MEDICA (M)	Registro de la consulta y ordenes medicas del paciente	R
RAYOS X	ADMINISTRACION DE CITAS Y PROCEDIMIENTOS REALIZADOS (N)	Registro del procedimiento y programación de citas	R

DIRECCION DE LA OFICINA DE INFORMATICA - INEN - VºBº

Especialista en Seguridad de la Información-Oficina de Informática - INEN - VºBº

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

8. SE PROCEDE A EJECUTAR LAS CONSULTAS (QUERYS) QUE SE VAN A UTILIZAR DURANTE EL DESARROLLO DE LA CONTINGENCIA, CONSIDERANDO LAS QUE ESTÁN RELACIONADAS A LAS OPERACIONES CRÍTICAS DETALLADAS EN EL PUNTO ANTERIOR.

LISTA DE QUERYS	
Código	A
Nombre	Lista de Saldos y Precio de Medicamento por Farmacia
Descripción	Script que permite obtener información respecto a los saldos de medicamentos y precio de venta.
Código	B
Nombre	Listado de Medicamentos no cubierto por la compañía
Descripción	Script que permite obtener el listado de medicamentos bloqueados
Código	C
Nombre	Listado de pacientes de SIS
Descripción	Script que permite obtener el listado de pacientes con condición SIS al corte
Código	D
Nombre	Listado de pacientes de CLINICA
Descripción	Script que permite obtener el listado de pacientes con condición Clínica con Fondo en Efectivo al corte
Código	E
Nombre	Listado de pacientes con ultima condición
Descripción	Script que permite obtener el listado de pacientes con la condición actual al corte
Código	F
Nombre	Listado de tarifario por precio y tarifa
Descripción	Script que permite obtener el tarifario actualizado sus precios correspondiente a las tarifas
Código	G
Nombre	Listado de tarifario no cubierto por la compañía por servicio
Descripción	Script que permite obtener el listado de tarifarios bloqueados
Código	H
Nombre	Listado de pacientes con cuenta activa Ambulatorios (Pacientes atendidos en forma ambulatoria en clínica y Pacientes atendidos en forma ambulatoria)
Descripción	Script que permite obtener el listado de paciente con cuenta activa al corte.
Código	I
Nombre	Listado de pacientes Hospitalizados en Clínica – Hospitalización - Emergencia
Descripción	Script que permite obtener el listado de pacientes Hospitalizados
Código	J
Nombre	Listado de pacientes Citados por departamento
Descripción	Script que permite obtener el listado de paciente citados por departamento.

DIRECCION DE LA OFICINA DE INFORMATICA - INEN - V°B°

Especialista en Seguridad de la Información-Oficina de Informática - INEN - V°B°

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

En el siguiente cuadro se detalla que consultas o querys se van a utilizar para cada operación crítica, tener en cuenta que cada consulta maneja una letra como código de identificación.

MODULO	OPERACIONES PRINCIPAL	COD. CONSULTA
FARMACIA FACTURACION	VENTAS (A)	A,B,C,D
FARMACIA LOGISTICA	INGRESO Y SALIDA MEDICAMENTO (B)	A
FACTURACION SERVICIO	EMISION DE COMPROBANTES DE PAGO (D)	E,F,G
LABORATORIO	GESTION DE MUESTRAS (E)	E,C,D
BANCO DE SANGRE	ADMINISTRACION DE DONANTES (F)	E,C,D
PATOLOGIA	EMISION DE ORDENES y ENTREGA DE RESULTADOS (G)	E,C,D
HOSPITALIZACION	ADMISION Y ADMINISTRACION DE CUENTA (H)	H,E,C
EMERGENCIA	ADMISION Y ADMINISTRACION DE CUENTA (I)	H,E,C
HISTORIA CLINICA	GESTION DE HISTORIAS CLINICAS (K)	I
CIRUGIA	GESTION DE OPERACIONES Y PROCEDIMIENTOS (L)	H,J
CONSULTA EXTERNA	ATENCION DE CONSULTA Y GENERACION DE ORDEN MEDICA (M)	H
RAYOS X	ADMINISTRACION DE CITAS Y PROCEDIMIENTOS REALIZADOS (N)	E,C,D

DIRECCION DE LA OFICINA DE INFORMATICA - INEN - V°B°

Especialista en Seguridad de la Información-Oficina de Informática - INEN - V°B°

9. **EL ENCARGADO DE LA UNIDAD DE DESARROLLO DE SISTEMAS DE INFORMACIÓN JUNTO CON SU EQUIPO DE TRABAJO; COORDINARA CON LOS USUARIOS QUE FORMEN PARTE DE LOS PROCESOS CRÍTICOS DE LA INSTITUCIÓN, PARA INDICARLES LA UBICACIÓN DE LA ESTACIÓN DE TRABAJO DONDE SE ALMACENARÁ LOS ARCHIVOS DE EXCEL CON LA INFORMACIÓN ACTUALIZADA, QUE SE OBTUVO MEDIANTE LA EJECUCIÓN DE LAS CONSULTAS O QUERYS, PARA QUE SEA IMPRESA Y DE ESTA MANERA PODER DAR INICIO AL PROCEDIMIENTO MANUAL. POR LO GENERAL LA UBICACIÓN DE ESTOS ARCHIVOS ESTÁN EN LA SIGUIENTE RUTA: C:\ARCHIVO CONTINGENCIA**

10. **LUEGO DE QUE SE HAYA DESACTIVADO EL PLAN DE CONTINGENCIA, SE PROCEDERÁ A REALIZAR EL SIGUIENTE PROCEDIMIENTO DE RECUPERACIÓN:**

- **Farmacia Facturación (A):** Dar indicaciones lo que debe contener los documentos escritos y calculados de forma manual, considerando la Historia Clínica, Nombres y apellidos, código SIGAMEF, Lote, cantidad, precio y monto total de facturación. Esta información permitirá la regularización posterior al sistema.

- **Farmacia Servicio (D):** Dar indicaciones lo que debe contener los documentos escritos y calculados de forma manual, considerando la Historia Clínica, Nombres y apellidos, código tarifario, cantidad,

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

precio y monto total de facturación. Esta información permitirá la regularización posterior al sistema siguiendo el correlativo pre impreso facturado.

- **Laboratorio (E), Banco Sangre (F), Patología (G), Rayos X (N):** Dar indicaciones a los usuarios que deberán consultar estos documentos impresos dado por informática para generar solicitudes de los procedimientos. Esto significa que la orden médica de los procedimientos será escrita a mano y firmada por el médico tratante.

  Dar indicaciones lo que debe contener los documentos escritos como: Historia Clínica, Nombres y apellidos, código tarifario, cantidad. Esta información permitirá la regularización posterior al sistema de información.

  Para el procesamiento de resultado de las muestras para aquellas áreas que cuentan con el equipos médicos (Laboratorio, Banco de Sangre), se programara de manera manual el procesamiento de los análisis, reportando vía telefónica los resultados a los usuarios para aquellos pacientes hospitalizados o emergencia; para pacientes de consulta externa esperaran sus resultados sea regularizado en el sistema.

- **Hospitalización (H), Emergencia (I):** Dar indicaciones lo que debe contener los documentos escritos considerando la Historia Clínica, Nombres, apellidos y condición. Esta información permitirá la regularización posterior al sistema del módulo afectado.

- **Historia Clínica (K):** Los datos que forman la Historia Clínica deben llenarse de manera obligatoria. Esta información permitirá la regularización posterior al sistema del módulo afectado.

DIRECCION DE LA OFICINA DE INFORMATICA - INEN - V°B°

- **Cirugía (L):** Dar indicaciones a los usuarios de sala de Operaciones, que el registro del informe de operatorio se realizará manualmente.

  Dar indicaciones lo que debe contener los documentos escritos considerando la Historia Clínica, Nombres, apellidos, condición, operación y sala. Esta información permitirá la regularización posterior al sistema del módulo afectado.

Especialista en Seguridad de la Información-Oficina de Informática - INEN - V°B°

- **Cirugía (L):** Dar indicaciones a los usuarios de sala de Operaciones, que el registro del informe de operatorio se realizará manualmente.

- **Consulta Externa (M):** Dar indicaciones lo que debe contener los documentos escritos en la consulta Historia Clínica, Nombres, apellidos, Departamento. Esta información permitirá la regularización posterior al sistema del módulo afectado.

  Respecto a los procedimientos y receta de medicamentos descritos por el medico se realizaran con sus respectivo formatos impresos generados por el área de Imprenta.

- **Farmacia Logística (L):** Dar indicaciones a los usuarios de Almacén especializados, que los registros de ingreso y salidas de medicamentos se registraran manualmente en la tarjeta visible , donde deben especificar el Código del Medicamento (SIGA MEF), Nombre del Lote, Fecha de Vencimiento, Registro Sanitario y cantidad

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 . Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe