ESCUELA POLITÉCNICA DEL EJÉRCITO EXTENSIÓN LATACUNGA

TECNOLOGÍA EN COMPUTACIÓN

PLAN DE CONTINGENCIAS PARA LOS LABORATORIOS DE REDES E INFORMÁTICA

ROBINSON GONZALO PEÑALOZA OÑATE

TESIS PRESENTADA COMO REQUISITO PREVIO A LA OBTENCIÓN DEL GRADO DE TECNÓLOGO EN COMPUTACIÓN

AÑO 2011

CERTIFICACIÓN

Los suscritos Ing. Santiago Jácome e Ing. Mayra Salazar, certifican que el presente trabajo titulado: “PLAN DE CONTINGENCIAS PARA LOS LABORATORIOS DE REDES E INFORMÁTICA” fue desarrollado íntegramente por el Sr. Peñaloza Oñate Robinson Gonzalo, bajo nuestra supervisión.

_____

Ing. Santiago Jácome

DIRECTOR DE TESIS

_____

Ing. Mayra Salazar

CODIRECTOR DE TESIS

ESCUELA POLITÉCNICA DEL EJÉRCITO EXTENSIÓN LATACUNGA
CARRERA DE TECNOLOGÍA EN COMPUTACIÓN

DECLARACIÓN DE RESPONSABILIDAD

Yo, PEÑALOZA OÑATE ROBINSON GONZALO, declaro que:

El proyecto de grado denominado “PLAN DE CONTINGENCIAS PARA LOS LABORATORIOS DE REDES E INFORMÁTICA”, ha sido desarrollado en base a una investigación exhaustiva, respetando derechos intelectuales de terceros, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este trabajo es de mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Latacunga, marzo del 2011.

_____

Peñaloza O. Robinson G.
C. C. 1803416344

ESCUELA POLITÉCNICA DEL EJÉRCITO EXTENSIÓN LATACUNGA
CARRERA DE TECNOLOGÍA EN COMPUTACIÓN

AUTORIZACIÓN

Yo, PEÑALOZA OÑATE ROBINSON GONZALO, declaro que:

Autorizó a la Escuela Politécnica del Ejército Extensión Latacunga, la publicación en la biblioteca virtual de la institución el trabajo "PLAN DE CONTINGENCIAS PARA LOS LABORATORIOS DE REDES E INFORMÁTICA", cuyo contenido, ideas y criterios es de mi exclusiva responsabilidad y autoría.

Latacunga, marzo del 2011.

_____

Peñaloza O. Robinson G.
C. C. 1803416344

DEDICATORIA

Este proyecto se lo ofrendo muy infinitamente a Dios, mi querida esposa por todo su amor incondicional, mi inocente hijo a quien amo y protegeré siempre, a mi madre por guiarme, creer y confiar en mí, a mi querido padre que DIOS lo tenga en su gloria, a mis hermanos y familiares quienes han sido mi soporte a lo largo de mi vida. Además quiero dedicarlo a todas las personas que siempre han estado a mi lado apoyándome y alentándome a conseguir mis metas.

Robinson

AGRADECIMIENTO

Mi principal agradecimiento a Dios, A mi Director, Codirector y a la Fuerza Terrestre por la oportunidad que me brindaron de fomentar mis conocimientos por medio de la Educación Superior, también quiero extender el agradecimiento a todas las personas que me ayudaron a desarrollar este proyecto.

Robinson

ÍNDICE

ÍNDICE DE TABLAS

RESUMEN

El Plan de Contingencias para los Laboratorios de Redes e Informática es un instrumento necesario para la continuidad de las actividades académicas sigue el ciclo de vida iterativo (renovado), es decir que se puede planificar, hacer, comprobar y actuar además este debe ser revisado periódicamente.

El Plan de Contingencias para los Laboratorios de Redes e Informática comprende tres subplanes (Prevención Contención y Recuperación), permitiendo que el personal que labora en los Laboratorios de Redes e Informática pueda actuar ante cualquier desastre este sea natural o accidental reduciendo el costo y tiempo.

En el tiempo actual es un requisito primordial para las empresas e instituciones educativas tener a la mano un plan de contingencias, estas se han visto obligadas a salvaguardar los equipos de computo donde posa la información que es de carácter importante e irreparable.

En el Plan de Contingencias se hace constar un inventario real de los equipos informáticos existentes en los laboratorios y la Jefatura Laboratorista así como el Software adquirido para el funcionamiento y desarrollo de actividades académicas.

CAPÍTULO I PLAN DE CONTINGENCIAS PARA LOS LABORATORIOS DE REDES E INFORMÁTICA

1.1 ANTECEDENTES.

El Plan de Contingencias es un conjunto de procedimientos alternativos a la operación normal, que permitirá que los laboratorios sigan operando, aún cuando falle algún sistema que soporta.

El Plan de Contingencias es un documento que le permite al personal que administra los Laboratorios de Redes e Informática prever, reaccionar y recuperarse en caso de un desastre y reducir el impacto.

1.2 OBJETIVOS.

1.2.1 OBJETIVO GENERAL

Desarrollar el “PLAN DE CONTINGENCIAS PARA LOS LABORATORIOS DE REDES E INFORMÁTICA” con sus respectivas etapas (Prevención, Contención y Recuperación), con el propósito de enfrentar en el menor tiempo y costo, los posibles desastres de tipo natural o accidental que impacten el proceso operativo, reduciendo el tiempo de indisponibilidad.

1.2.2 OBJETIVOS ESPECÍFICOS

Obtener un diagnóstico real de los equipos informáticos y flujo de información

Efectuar el análisis de riesgos realizando una evaluación de: Identificación del hardware y software critico a ser protegido, Análisis de vulnerabilidades y riegos que afecten a la información.

Desarrollar una lista con las posibles medidas de seguridad la cual permita reducir los riegos para los laboratorios de Redes e Informática.

Desarrollar e implementar estrategias.

Elaborar los planes de Prevención, Contención y Recuperación

Capacitar al personal para enfrentar todo tipo de desastres naturales o accidentales.

Definir acciones y procedimientos a ejecutar en caso de fallas originadas por desastres.

Establecer procedimientos para evitar las interrupciones prolongadas del servicio de datos, debido a contingencias como incendio e inundaciones hasta que sea restaurado el servicio completo y se retorne el normal funcionamiento los laboratorios de Redes e Informática.

1.3 ALCANCE.

Desarrollo del “PLAN DE CONTINGENCIAS PARA LOS LABORATORIOS DE REDES E INFORMÁTICA” el mismo que abarcará elementos tales como: Hardware, Software, Infraestructura Física y Eléctrica.

1.4 ANÁLISIS DE LA SITUACIÓN ACTUAL

Los Laboratorios de Redes e Informática en la actualidad cuentan con el 80% de equipos y tecnología nueva mientras que el 20% son equipos de tecnología anterior, estos equipos son utilizados por docentes y alumnos de las diferentes carreras de la Escuela y la MED (Modalidad de educación a Distancia), para las prácticas y toma de pruebas.

1.4.1. ORGANISMOS DE DIRECCIÓN

Los Laboratorios de Redes e Informática pertenecen al Departamento de Eléctrica y Electrónica de la Escuela Politécnica del Ejército extensión Latacunga, este es un departamento Estratégico de la Escuela Politécnica además es responsable de la gestión de la docencia, investigación y extensión en las siguientes áreas del conocimiento: Eléctrica, Electrónica, Comunicaciones, Sistemas Digitales, Instrumentación, Control, Sistemas Eléctricos de Potencia,

Software. Es por consiguiente la unidad organizacional clave para el cumplimiento de la misión de la ESPE y el logro de los objetivos del plan estratégico institucional.

El departamento tiene como objetivos:

- Gestionar la docencia, investigación extensión en las áreas del conocimiento técnico de Eléctrica, Electrónica y de la Computación.
- Gestionar, formular y ejecutar proyectos de investigación y extensión
- Transferir, difundir y aplicar los resultados de la investigación

1.4.2. INFRAESTRUCTURA FÍSICA Y ELÉCTRICA

La infraestructura física y eléctrica de los laboratorios de Redes e Informática se encuentra en buenas condiciones

TABLA 1.4.2.1 DESCRIPCIÓN DE LOS ELEMENTOS DE LA INFRAESTRUCTURA FÍSICA Y ELÉCTRICA

No	ELEMENTO	SITUACIÓN ACTUAL
1	Infraestructura física y ubicación de los Laboratorios de Redes e Informática de la ESPE-Extensión Latacunga.	Los Laboratorios de Redes e Informática de la Escuela Politécnica del Ejército extensión Latacunga se encuentran ubicados en el cuarto piso de los bloques de aulas A y B. en el Campus Politécnico. La infraestructura es de tipo mixto ladrillo y bloque, columnas de hormigón, piso falso y cielo raso.

No	ELEMENTO	SITUACIÓN ACTUAL
2	Instalaciones eléctricas de los L.R.I. de la ESPE-EL.	Las tomas eléctricas cumplen con los estándares de seguridad, es decir fase, neutro y tierra
3	Detectores y alarmas de los Laboratorios de Redes e Informática de la ESPE-EL.	Los Laboratorios de Redes e Informática de la ESPE-Extensión Latacunga. no cuenta con detectores de humo y alarmas contra incendios
4	Planos estructurales de los Laboratorios de Redes e Informática de la ESPE-EL.	Los Laboratorios de Redes e Informática de la ESPE-Extensión Latacunga, no cuenta con planos arquitectónicos estructurales.
5	Extintores de los Laboratorios de Redes e Informática de la ESPE-Extensión Latacunga.	Los Laboratorios de Redes e Informática de la ESPE- Extensión Latacunga, disponen de un sistema contra incendios a base de extintores.
6	Acceso y control de ingreso físico a los Laboratorios de Redes e Informática de la ESPE-Extensión Latacunga.	Los Laboratorios de Redes e Informática de la ESPE- Extensión Latacunga, posee una entrada general desde la planta baja. La misma que se divide en 2 alas, derecha e izquierda en el cuarto piso se controla el ingreso a los laboratorios desde la Jefatura de Laboratorios de Redes e Informática. El ingreso es controlado por los Laboratorista.
7	Salida de emergencia de los Laboratorios de Redes e Informática de la ESPE- Extensión Latacunga.	Los Laboratorios de Redes e Informática de la ESPE-Extensión Latacunga, no cuenta con ninguna salida emergente.

1.4.3 INVENTARIO DE HARDWARE

Se denomina hardware o soporte físico al conjunto de elementos y materiales que componen un ordenador. Hardware son los componentes físicos de una computadora tales como el disco duro, CD-Rom, disquetera (floppy), etc.. En dicho conjunto se incluyen los dispositivos electrónicos y electromecánicos, circuitos, cables, tarjetas, armarios o cajas, periféricos de todo tipo y otros elementos físicos.

Para el inventario del Hardware existente en los Laboratorios de Redes e Informática se realizó una entrevista directa y personal con las personas encargadas del mismo.

TABLA 1.4.3.1 EQUIPOS INFORMÁTICOS DE LOS LABORATORIOS DE REDES E INFORMÁTICA

LABORATORIOS	EQUIPOS	FUERA
Jefatura Laboratorios	3	0
Servidores	4	0
Lenguajes de Programación	16	0
Redes de Datos	20	0
Computación I	20	0
Computación II	16	0
Ingeniería de Software	16	1 Reparación
Sistemas Operativos	15	0
Inteligencia Artificial	16	0
Computación III	16	0
Herramientas Administrativas	16	0

TABLA 1.4.3.2 FRECUENCIA DE OBTENCIÓN DE BACKUPS (RESPALDOS)

Tipo Respaldo	Frecuencia	Medio	Horario de Obtención	Destino	Responsable
Datos del sistema	Semestral (Viernes)	CD o DVD	16h:00 a 18h:00	Archivador de Software	Administrador de Base de Datos

1.4.4 SOFTWARE BASE / APLICACIÓN

Software Base.- Corresponde aquellos programas como (Linux, Ubuntu, Unix, Windows XP, etc.) adquiridos para el funcionamiento de los Laboratorios de Redes e Informática de la ESPE- Extensión Latacunga.

Software Aplicación.- Considerados aquellos programas que han sido desarrollados y adquiridos para cubrir las necesidades de los Laboratorios de Redes e Informática.
A continuación se detallan los subsistemas.

TABLA 1.4.4.1 SUBSISTEMAS

No	Subsistema	Área de Gestión
1	Sistema de Control de Inventarios	Jefatura Laboratorios

SOFTWARE PARA EL DESARROLLO DE ACTIVIDADES ACADÉMICAS

En la siguiente tabla se encuentra la descripción del software existente en los diferentes laboratorios y que son utilizados por todas las carreras existentes en la escuela para poner en prácticas los conocimientos adquiridos por los alumnos.

TABLA 1.4.4.2 SOFTWARE BASE PARA EL DESARROLLO

NOMBRE SOFTWARE	TIPO SOFTWARE	CUENTA CON LICENCIA	RESPALDO UBICACIÓN
Visual Basic 6.0	Lenguaje de Programación	Si	CD's Jefatura Laboratorios, Servidor de archivos
Java	Lenguaje de Programación	Si	CD's Jefatura Laboratorios, Servidor de archivos
DreamWeaver	Lenguaje de Programación	Si	CD's Jefatura Laboratorios, Servidor de archivos
Borland c++	Lenguaje de Programación	No	CD's Jefatura Laboratorios, Servidor de archivos
Winzip, Winrar	Compresores de archivos	No	CD's Jefatura Laboratorios, Servidor de archivos
Adobe	Utilitario	No	CD's Jefatura Laboratorios, Servidor

			de archivos
NOMBRE SOFTWARE	**TIPO SOFTWARE**	**CUENTA CON LICENCIA**	**RESPALDO UBICACIÓN**
Ubuntu	Sistema Operativo	FREE	CD's Jefatura Laboratorios, Servidor de archivos
Firefox	Navegador web libre	No	CD's Jefatura Laboratorios, Servidor de archivos
Matlab	Lenguaje de programación Software matemático	No	CD's Jefatura Laboratorios, Servidor de archivos
Oracle	Administrador de la Base de Datos	Si	CD's Jefatura Laboratorios, Servidor de archivos
Simulador de Red	Software y Herramienta para redes	No	CD's Jefatura Laboratorios, Servidor de archivos
Solidwork	Software modelado mecánico	No	CD's Jefatura Laboratorios, Servidor de archivos
Fenix	Software de contabilidad	Si	CD's Jefatura Laboratorios, Servidor de archivos
Geogebra	Software matemático libre	No	CD's Jefatura Laboratorios, Servidor de archivos
Windows XP	Sistema Operativo	Si	CD's Jefatura

con parches			Laboratorios, Servidor de archivos
NOMBRE SOFTWARE	**TIPO SOFTWARE**	**CUENTA CON LICENCIA**	**RESPALDO UBICACIÓN**
Antivirus Avira	Programa protección de equipos	Si	CD's Jefatura Laboratorios, Servidor de archivos
Microsoft Office 2000	Programas Aplicaciones Office 97	Si	CD's Jefatura Laboratorios, Servidor de archivos

1.4.5 RECURSO HUMANO DE LOS LABORATORIOS

Los Laboratorios de Redes e Informática cuentan con el siguiente personal laborando en los laboratorios.

Nomina del personal de los Laboratorios de Redes e Informática

Ord.	Grado	Apellidos y Nombres	Observación
1	S.P.	Jácome Guerrero Santiago Patricio	Responsable Laboratorios
2	S.P.	Salazar Grandes Mayra Cecilia	Laboratorista
3	S.P.	Estrella Vaca Tatiana Cecilia	Laboratorista

1.4.6 DETERMINACIÓN DE RECURSOS CRÍTICOS

Para determinar el recurso crítico en los sistemas de información es esencial conocer la amenaza o la condición del entorno (persona, maquina, suceso o idea) que podría dar lugar a que se produjese una violación de la seguridad.

Todos los recursos son críticos y necesarios la información está expuesta a perdida por no contar con estrategias de respaldo y políticas de contraseñas, el software (propietario o adquirido) puede ser fácilmente copiado, el hardware está expuesto a una serie de problemas como daños, perdidas etc.

Para la disminución de los recursos críticos es necesario conocer las distintas amenazas que ponen en peligro los sistemas de Información, las técnicas correspondientes que se pueden utilizar, los controles de seguridad y los puntos vulnerables que existen en las directivas de seguridad.

TABLA 1.4.6.1 NIVEL DEL RECURSO CRÍTICO

Nivel	Significado
(C) Criticas	No admiten interrupción por un periodo de 24 horas
(N) Necesarias	Admiten interrupción de mediana magnitud y pueden aceptar reemplazos parciales por procedimientos manuales
(O) Opcionales	Admiten una interrupción prolongada no siendo indispensables la recuperación de la información durante el tiempo de interrupción

CLASIFICACIÓN DE LOS LABORATORIOS DE REDES E INFORMÁTICA CONSIDERADOS CRÍTICOS.

Para la clasificación de los Laboratorios de Redes e Informática considerados críticos hemos tomado en cuenta su importancia tanto funcional como aplicativa.

TABLA 1.4.6.2 CLASIFICACIÓN DE LOS LABORATORIOS DE ACUERDO AL RECURSO CRÍTICO

Jefatura y Laboratorios	Modulo / subsistema	Función	Clasificación
Jefatura Laboratorios	• Controlador de Dominios. • Servidor Antivirus • Servidor de Archivos • Web Access	Software útil para la administración de los laboratorios y control de accesos	Criticas
Laboratorios de Redes e Informática	Visual studio 6.0, Temax, Fenix, Avira, java, Dreamweaver,	Software disponible para el aprendizaje de los alumnos de las diferentes carreras existentes en la escuela	Necesarias

1.4.7 HARDWARE

Considerando el inventario de hardware se ha tomado en cuenta los equipos principales que operan en los Laboratorios de Redes e Informática de la ESPE-Extensión Latacunga.

TABLA 1.4.7.1 CLASIFICACIÓN DEL HARDWARE DE ACUERDO A SU FUNCIÓN

Clasificación	Significado
Indispensable	Funcionamiento no se puede obviar por su funcionamiento.
Necesario	Funcionamiento que no representa tan prioritario y puede ser suplido por otros mecanismos inclusive manuales.
Opcional	Funcionamiento adicional que puede estar en servicio y cuya labor no es trascendental.

LABORATORIOS	EQUIPOS	CLASIFICACIÓN
Jefatura laboratorios	3	Necesario
Servidores	4	Indispensable
Lenguajes de Programación	16	Necesario
Redes de Datos	20	Necesario
Computación I	20	Necesario
Computación II	16	Necesario
Ingeniería de Software	16	Necesario
Sistemas Operativos	15	Necesario
Inteligencia Artificial	16	Necesario
Computación III	16	Necesario
Herramientas Administrativas	16	Necesario

1.4.7.2 SOFTWARE BASE Y DE APLICACIÓN

Para determinar el software base y de aplicación considerados críticos en los laboratorios de Redes e Informática se realizo un análisis de su importancia.

TABLA 1.4.7.2.1 CLASIFICACIÓN DE SOFTWARE DE ACUERDO A SU FUNCIÓN.

Departamento	Recurso Informático	Clasificación	Software Aplicación	Software Base
Jefatura Laboratorios	Controlador de Dominios. Servidor Antivirus Servidor de Archivos Web Access	Indispensable		
Laboratorios de Redes e Informática	Visual Basic 6.0 Antivirus Avira Winzip, Winrar Adobe, Firefox Matlab, Oracle, Ubuntu Simulador de Red Solidwork, Java DreamWeaver	Necesario		**X**

Jefatura Laboratorios	Sistema de Control de Inventarios	Necesario	**X**	
Software Operativo y Aplicativo	Windows XP service Pack 3	Indispensable		**X**

1.4.7.3 RECURSO HUMANO CRÍTICO

- Los laboratorios de Redes e Informática no cuentan con el suficiente personal por el momento solo existen dos Ingenieras Laboratorista trabajando de 7:00 am hasta las 21:30 pm de lunes a viernes sin interrupciones.
- La falta de personal para cumplir estas funciones ha llevado a la carga de trabajo para las dos Ingenieras Laboratorista.
- Para cumplir las diferentes funciones en los laboratorios por lo menos debe existir 2 personas encargadas por la mañana y 2 personas por la tarde y noche

1.4.8 ANÁLISIS DE RIESGO E IMPACTO

Se entiende por riesgo cualquier circunstancia u ocurrencia que pudiera producir algún tipo de efecto negativo, el cual acarrearía un retraso temporal en su planificación o modificaría el planteamiento del mismo

1.4.8.1 NIVELES DE RIESGO

Se tomará en cuenta el nivel de riesgo que puede tener la información realizando un adecuado estudio así previniendo la pérdida de información y el costo de un sistema de seguridad, para lo cual se debe considerar lo siguiente:

- Se clasifican las instalaciones en términos de riesgo (Catastrófico, Crítico, Marginal y Despreciable).
- Se identifican aquellas aplicaciones que tengan un alto riesgo.
- Se formularán medidas de seguridad necesarias dependiendo del nivel de seguridad que se requiera.
- Clasificar los datos, información y programas que contienen información confidencial la cual será difícil de recuperarla.
- Identificar a la información que tenga gran costo financiero en caso de pérdida o bien puede provocar un gran impacto en la toma de decisiones.

Se realizará una identificación de los distintos tipos de riesgos que podrían surgir en los Laboratorios de Redes e Informática. El efecto de estos riesgos deberá ser analizado y estudiado, puesto que su trascendencia puede causar imprevistos que dificulten el normal funcionamiento de los laboratorios de Redes e Informática en la ESPE-Extensión Latacunga.

A continuación se detallan los posibles riesgos que se pueden presentar y que serían los causantes de la interrupción de la continuidad de las operaciones.

- Fallas equipos informáticos
- Acción de virus
- Fallas humanas
- Desastres naturales
- Accesos no autorizados
- Inundaciones
- Fallas eléctricas
- Incendios

1.4.8.2. CRITERIOS PARA EVALUAR LOS NIVELES DE IMPACTO

De acuerdo con las posibles causas que interrumpirían el funcionamiento de los Laboratorios de Redes e Informática se realizó un análisis dando como resultado la tabla de impactos.

TABLA 1.4.8.2.1 DEFINICIÓN DE NIVELES DE IMPACTO

Nivel	Impacto	Descripción
1	Catastrófica	Sus consecuencias afectan en forma total a los laboratorios, sus pérdidas son sumamente altas.
2	Crítica	Las consecuencias afectan parcialmente a los laboratorios, en forma grave, existen pérdidas considerables.

3	Marginal	Las consecuencias afectan en forma superficial a los laboratorios, es decir se cuenta con pérdidas menores.
4	Despreciable	Las consecuencias no afectan el funcionamiento de las actividades de los laboratorios y no existen pérdidas.

TABLA 1.4.8.3 DEFINICIÓN DE NIVELES DE IMPACTO DE ACUERDO A SU CATEGORÍA.

Categoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Fallas equipos informáticos	-	X	-	-
Acción de virus	X	-	-	-
Fallas humanas	-	X	-	-
Desastres naturales	X	-	-	-
Accesos no autorizados	-	X	-	-
Inundaciones	X	-	-	-
Fallas eléctricas	-	X	-	-
Incendios	X	-	-	-

1.4.8.4. INFRAESTRUCTURA FÍSICA

En la infraestructura física se ha tomado en cuenta los errores en su construcción.

TABLA 1.4.8.4.1 DEFINICIÓN DE RIESGOS POTENCIALES CON RESPECTO A LAS INSTALACIONES FÍSICAS

No	ELEMENTO	RIESGO
1	Infraestructura física y ubicación de los laboratorios de Redes e Informática.	Los laboratorios de Redes e Informática cuenta con una infraestructura moderna, se ubican en el cuarto piso del Campus Politécnico, su ubicación fue planificada pero no se tomo en cuenta los potenciales riesgos que podrían ocasionarse por algún desastre natural.
2	Instalaciones eléctricas de los laboratorios de Redes e Informática.	No dispone de un plan emergente en el caso de existir una falla en la energía No existe diagramas de red estabilizada No existe una red estabilizada para todo el edificio
3	Detectores y alarmas de los laboratorios de Redes e Informática.	Los laboratorios de Redes e Informática no cuentan con detectores de humo y alarmas contra incendios.
4	Planos estructurales de los laboratorios de Redes e Informática.	No cuentan con planos estructurales y eléctricos actualizados debido a que se han realizado modificaciones.
5	Esquema de cableado estructurado de los laboratorios de Redes e Informática.	No cuentan con diagramas de red actualizados
6	Acceso y Control de Ingreso Físico a los laboratorios de Redes e Informática.	No existe un control riguroso de acceso a los laboratorios de Redes e Informática. No se cuenta con el uso de tarjetas magnéticas u otras medidas que controlen el

		ingreso a los laboratorios de Redes e Informática.
7	Salida de Emergencia de los laboratorios de Redes e Informática.	Los laboratorios de Redes e Informática no cuentan con una salida de emergencia.

1.4.8.5 SOFTWARE BASE Y DE APLICACIÓN DE ACUERDO AL RIESGO

El software base y de aplicación considerado en riesgo potencial en los Laboratorios de Redes e Informática es todo, porque todo el software que se utiliza para la administración de los laboratorios es de vital importancia así como en el software para el desarrollo de actividades académicas.

TABLA 1.4.8.5.1 DEFINICIÓN DE RIESGOS POTENCIALES CON RESPECTO AL SOFTWARE BASE/APLICACIÓN

laboratorios de Redes e Informática	Equipo	clasificación	descripción del riesgo	tiempo caída permisible	tiempo recuperación
Jefatura Laboratorios	Super Power Pentium D de 3.20 GHz, 2 GB RAM	Controlador de Dominio	- Error de conexión - Error en los componentes internos - Errores en los componentes externos. - Errores lógicos	30 min	Depende del riesgo.

			- Acción de virus - Desastres naturales - Fallas eléctricas - Incendios		
Jefatura Laboratorios	Servidor Premio Pentium III 933 MHz, 256 MB RAM	Servidor de Archivos	- Error de conexión - Error en los componentes internos - Errores en los componentes externos. - Errores lógicos - Acción de virus - Desastres naturales - Fallas eléctricas - Incendios	30 min	Depende del riesgo.
Jefatura Laboratorios	Servidor IBM modelo	Firewall	- Error de conexión	30 min	Depende del

	Netfinity 3000 Procesador Pentium II de 300 MHz 128 Mb RAM		- Error en los componentes internos - Errores en los componentes externos. - Errores lógicos - Acción de virus - Desastres naturales - Fallas eléctricas - Incendios		riesgo
Jefatura Laboratorios	Pentium IV de 3.2 GHz, 1GB RAM	Antivirus	- Error de conexión - Error en los componentes internos - Errores en los componentes externos.	30 min	Depende del riesgo

			- Errores lógicos - Acción de virus - Desastres naturales - Fallas eléctricas - Incendios		
Lenguajes de Programación	CORE 2 QUAD 2.8 GHZ HD 300 GB M 3GB	Office 2000 Office 97 Windows XP con parches Visual Basic 6.0 Antivirus Avira Borland c++ Winzip, Winrar Adobe Firefox Matlab Oracle Ubuntu	- Error de conexión - Error en los componentes internos - Errores en los componentes externos. - Errores lógicos - Acción de virus - Desastres naturales - Fallas eléctricas - Incendios	2 horas	Depende del riesgo

		Simulador de Red Solidwork Java DreamWeaver Office			
Redes de Datos	Pentium IV 3.2 GHz HD 120 GB M 1GB	Windows XP con parches Visual Basic 6.0 Antivirus Avira Borland c++ Winzip, Winrar Adobe Firefox Matlab Oracle Ubuntu Simulador de Red		2 horas	Depende del riesgo

		Solidwork Office Fenix Geogebra			
Computación I	CORE 2 QUAD 2.4 GHz HD 200GB M 4GB	Windows XP con parches Visual Basic 6.0 Antivirus Avira Borland c++ Winzip, Winrar Adobe Firefox Matlab Oracle Ubuntu Simulador de Red Solidwork Office	- Error de conexión - Error en los componentes internos - Errores en los componentes externos. - Errores lógicos - Acción de virus - Desastres naturales - Fallas eléctricas - Incendios	2 horas	Depende del riesgo

Computación II	Pentium IV 2.8 GHz HD 120 GB M 1GB	Windows XP con parches Visual Basic 6.0 Antivirus Avira Borland c++ Winzip, Winrar Adobe Firefox Matlab Oracle Ubuntu Simulador de Red Solidwork Office	- Error de conexión - Error en los componentes internos - Errores en los componentes externos. - Errores lógicos - Acción de virus - Desastres naturales - Fallas eléctricas - Incendios	2 horas	Depende del riesgo
Ingeniería de Software	CORE 2 QUAD 2.8 GHz HD 300 GB M 3 GB	Windows XP con parches Visual Basic 6.0 Antivirus Avira	- Error de conexión - Error en los componentes internos	2 horas	Depende del riesgo

		Borland c++ Winzip, Winrar Adobe Firefox Matlab Oracle Ubuntu Simulador de Red Solidwork Office	- Errores en los componentes externos. - Errores lógicos - Acción de virus - Desastres naturales - Fallas eléctricas - Incendios		
Sistemas Operativos	Pentium IV 3.0 GHz HD 80 GB M 1 GB	Windows XP con parches Visual Basic 6.0 Antivirus Avira Borland c++ Winzip, Winrar Adobe Firefox	- Error de conexión - Error en los componentes internos - Errores en los componentes externos. - Errores lógicos	2 horas	Depende del riesgo

		Matlab Oracle Ubuntu Simulador de Red Solidwork Office	- Acción de virus - Desastres naturales - Fallas eléctricas - Incendios		
Inteligencia Artificial	CORE 2 DUO 3.0 GHz HD 250 GB M 4GB	Windows XP con parches Visual Basic 6.0 Antivirus Avira Borland c++ Winzip, Winrar Adobe Firefox Matlab Oracle Ubuntu Simulador de	- Error de conexión - Error en los componentes internos - Errores en los componentes externos. - Errores lógicos - Acción de virus - Desastres naturales - Fallas eléctricas	2 horas	Depende del riesgo

		Red Solidwork Office	- Incendios		
Computación III	CORE 2 QUAD 2.8 GHz HD 300GB M 3GB	Windows XP con parches Visual Basic 6.0 Antivirus Avira Borland c++ Winzip, Winrar Adobe Firefox Matlab Oracle Ubuntu Simulador de Red Solidwork Office	- Error de conexión - Error en los componentes internos - Errores en los componentes externos. - Errores lógicos - Acción de virus - Desastres naturales - Fallas eléctricas - Incendios	2 horas	Depende del riesgo
Herramientas	Pentium D 3.4 GHz	Windows XP con	- Error de conexión	2 horas	

Administrativas	HD 120GB M 1GB	parches Visual Basic 6.0 Antivirus Avira Borland c++ Winzip, Winrar Adobe Firefox Matlab Oracle Ubuntu Simulador de Red Solidwork Office	- Error en los componentes internos - Errores en los componentes externos. - Errores lógicos - Acción de virus - Desastres naturales - Fallas eléctricas - Incendios		

CAPÍTULO II PLAN DE PREVENCIÓN

PLAN DE PREVENCIÓN

En este plan se reflejan todas las actividades de planeación, preparación entrenamiento y ejecución de las actividades para prevenir siniestros o catástrofes en los laboratorios de Redes e Informática, asegurando de esta manera un proceso de recuperación con el menor costo posible.

2.1 MEDIDAS DE PREVENCIÓN PARA LA INFRAESTRUCTURA FÍSICA

Mediante el Análisis de Riesgos efectuados en los Laboratorios de Redes e Informática se han tomado en consideración los siguientes puntos para la elaboración de Medidas Preventivas.

- **INFRAESTRUCTURA FÍSICA Y UBICACIÓN DE LOS LABORATORIOS DE REDES E INFORMÁTICA.**

a) Se recomienda la reubicación de los laboratorios de Redes e Informática a las nuevas instalaciones que la ESPE extensión Latacunga, esta por construir en el nuevo campus politécnico ubicado en el sector de Belisario Quevedo.
b) Si se procede a la realización de mejoras o remodelamientos el material utilizado no deberá ser inflamable o combustible Ejemplo: bases de aceites para pinturas, solventes lacas, gases inflamables etc.

- **INSTALACIONES ELÉCTRICAS DE LOS LABORATORIOS DE REDES E INFORMÁTICA.**

a) Se deben realizar inspecciones anuales a las instalaciones eléctricas.
b) Para mantener un adecuado funcionamiento de los equipos informáticos se debe considerar lo siguiente:
    1. Fallas producidas por la falta de energía
    2. Altas y bajas de voltaje

- **DETECTORES Y ALARMAS DE LOS LABORATORIOS DE REDES E INFORMÁTICA**

Los laboratorios de Redes e Informática deben instalar un sistema de alarmas y detectores de incendios.

- **PLANOS ESTRUCTURALES DE LOS LABORATORIOS DE REDES E INFORMÁTICA**

Mantener una actualización permanente de los planos estructurales, arquitectónicos y eléctricos en un lugar seguro y a cargo de un responsable.

- **ESQUEMA DE CABLEADO ESTRUCTURADO DE LOS LABORATORIOS DE REDES E INFORMÁTICA**

a) Mantener actualizados los diagramas de red
b) Se debe etiquetar los puntos de red de los laboratorios de Redes e Informática
c) Elaboración de un cronograma para el mantenimiento del cableado

- **ACCESO Y CONTROL DE INGRESOS FÍSICOS A LOS LABORATORIOS DE REDES E INFORMÁTICA**

a) Se debe implementar un sistema más riguroso para el acceso a cada uno de los laboratorios como tarjetas magnéticas o lector de huellas dactilares.
b) Se debe implementar medidas de seguridad tales como: puertas electrónicas y cámaras de seguridad que controlen el ingreso y salida a los laboratorios de Redes e Informática

- **SALIDAS DE EMERGENCIA DE LOS LABORATORIOS DE REDES E INFORMÁTICA**

La evacuación del personal debería realizarse por las escaleras que se encuentran en la parte frontal del ingreso de los bloques de aulas, el único inconveniente es que la escalera se encuentra compartida para los tres bloques de aulas cada bloque de cuatro pisos.

Se debe instalar señaléticas tales como salida de emergencia y números de teléfonos de emergencia en cada uno de los laboratorios.

2.2 MEDIDAS DE PREVENCIÓN PARA HARDWARE

2.2.1 SERVIDORES Y EQUIPOS INFORMÁTICOS

Fallas en los equipos informáticos

Se debe establecer un cronograma y grupos de mantenimiento a cargo de la Sección de TIC’s para que efectúen el mantenimiento

de los equipos de los diferentes laboratorios de Redes e Informática de la ESPE-EL., lo cual se cumplirá con:

- Mantenimiento preventivo
- Mantenimiento correctivo

Los TIC's deben mantener un stock mínimo de repuestos para los equipos informáticos como: tarjetas de red, discos duros, memoria, bus de datos, fuentes de poder, cables, etc.

Los TIC's deben establecer los contratos respectivos para el mantenimiento preventivo de los servidores.

Equipos

- Realizar backups de la información necesaria e indispensable para los laboratorios de Redes e Informática.
- Designación de un responsable en los TIC's para que realice un inventario de equipos informáticos indicando el estado del mismo.
- Disponer de los servicios profesionales de las diferentes empresas proveedoras ya que en caso de producirse una contingencia la ESPE-EL procederá a la adquisición de los servidores de igual o superior características técnicas

FALLAS HUMANAS

- Mantener al recurso humano en un ambiente de trabajo armónico para que se realice un buen desempeño laboral.
- Disponer con el recurso humano que reúna los perfiles necesarios para el correcto funcionamiento de los laboratorios de Redes e Informática

DESASTRES NATURALES

El término desastre suele asociarse con los fenómenos naturales por ejemplo (terremoto, erupción volcánica, etc.) combinando con sus efectos nocivos (pérdidas de vidas, destrucción de edificios, pérdida de información provocada por daños irreparables a los distintos equipos informáticos).

2.3 MEDIDAS DE PREVENCIÓN PARA EL SOFTWARE BASE / APLICACIÓN

Los datos son uno de los recursos más valiosos de Los laboratorios de Redes e Informática aunque los mismos sean intangibles, necesitan ser analizados y controlados con el mismo cuidado que los demás inventarios de los laboratorios de Redes e Informática por lo cual se debe tener presente ya que una vez realizado el análisis de riesgos se han establecido como medidas de prevención lo siguiente:

SISTEMAS

- Se debe asignar responsabilidad del manejo de los datos a los usuarios los cuales tienen un perfil para el manejo de la información.
- Los Administradores de Base de Datos deben llevar un control actualizado y seguro de los datos, evitando duplicidad de los mismos.
- Contar con los respaldos y duplicados, archivos necesarios para que puedan funcionar los laboratorios en caso de contingencia.

- Conservar los respaldos en lugares seguros con un mínimo de 2 copias.
- Actualizar las versiones de los antivirus.

2.4 MEDIDAS DE PREVENCIÓN ADMINISTRATIVAS Y DE DOCUMENTACIÓN

- Mantener debidamente documentado todos los programas y archivos para disminuir la pérdida de la información.
- Establecer manuales de respaldo y duplicados de los sistemas, programas y archivos.
- Mantener actualizada la documentación necesaria para prevenir desastres.
- Disponer de la respectiva documentación acerca de la configuración de los equipos informáticos correspondiente a hardware y software.
- Realizar los respectivos manuales de emergencia de los servicios auxiliares tales como energía eléctrica, UPS.
- Proveer a los diferentes laboratorios de Redes e Informática una lista de emergencia como: Policía, bomberos, cruz roja, hospitales, ambulancias, servicios de ayuda y rescate general, en lugares visibles para cualquier emergencia que se produzca.
- Establecer grupos de evaluación de desastres, los cuales deberán documentar las acciones que se lleven a cabo en caso de una emergencia.
- Implementar el Manual de Políticas de Seguridad Informática para la Red

- Los respaldos de los programas fuentes y ejecutables deben ser almacenados en un lugar externo al bloque de aulas.

POLÍTICAS DE SEGURIDAD Y CONTROL DE LA INFORMACIÓN

SEGURIDAD INFORMÁTICA

- Seguridad Informática es el conjunto de reglas, planes y acciones que permiten asegurar la información contenida en un sistema computacional.
- Seguridad informática es un conjunto de soluciones técnicas a problemas no técnicos.

COMPONENTES DE UNA POLÍTICA DE SEGURIDAD

- Una política de privacidad
- Una política de acceso
- Una política de autenticación
- Una política de contabilidad
- Planes para satisfacer las expectativas de disponibilidad de los recursos del sistema
- Una política de mantenimiento para la red y los sistemas de la organización
- Directrices para adquirir tecnología con rasgos de seguridad requeridos y/o deseables.
- Sanciones para quien infrinjan la política de seguridad
- Una política de reporte de incidentes y de divulgación de información

ASPECTOS QUE SE DEBE TENER EN CUENTA

- Confidencialidad
- Contraseñas de administradores
- Claves de software con licencia
- Integridad de la información
- Disponibilidad
- Consistencia
- Control
- Auditoría

CONFIDENCIALIDAD

- Significa proteger la información de ser leída o copiada por cualquiera usuario que no tenga los permisos adecuados (definición de perfiles de usuario) Responsable Administrador de Aplicaciones, Sistemas Operativos y Redes de datos.
- Debe cuidarse no solo el acceso a la información confidencial sino también a otras áreas sensibles que puedan servir para inferir información clasificada

INTEGRIDAD DE LA INFORMACIÓN

- Significa proteger la información, incluyendo los programas, de ser borrados o modificados sin conocimiento y consentimiento del dueño de la información mediante los

niveles de acceso de los usuarios. Responsable Administrador de Base de Datos, Administrador de Aplicaciones, Sistemas Operativos y Redes de datos

DISPONIBILIDAD

- Significa proteger la calidad de los servicios y acceso a los datos de no ser degradada o negada sin la autorización correcta.
- Los daños causados por ataques de Negación de Servicio son un ejemplo común de problemas de seguridad que degradan la disponibilidad de servicios y datos. Responsable Administrador de Base de Datos, Administrador de Aplicaciones, Sistemas Operativos y Redes de datos

CONSISTENCIA

- Significa que los sistemas y aplicaciones en explotación hagan siempre lo que se espera del mismo.
- También puede entenderse como la existencia controlada de datos en el sistema de forma que no existan copias diferentes referentes a los mismos datos. Responsables Administrador de Aplicaciones, Administrador de Base de datos

CONTROL

Significa regular el acceso al sistema y sus recursos.

Incluye elementos tales como:

- Control de acceso de los usuarios
- Control de utilización de los recursos
- Control de comportamiento del sistema
- Control de servicios disponibles para uso de los usuarios

CONSIDERACIONES PARA ESTABLECER UNA ADECUADA POLÍTICA DE SEGURIDAD

- Identificar los elementos que desea asegurar o proteger.
- Identificar las amenazas
- Identificar quienes y de qué forma tienen acceso a la información.
- Identificar los sitios vulnerables de acceso
- Fiscalizar periódicamente los sistemas en explotación
- Establecer un plan acción al detectar una violación de seguridad
- Difunda las políticas y eduque a los usuarios y conviértalos en sus mejores aliados

IDENTIFICAR LOS ELEMENTOS A PROTEGER

Identificar todos los elementos que pueden ser afectadas por un problema de seguridad:

- Personal: usuarios, administradores, técnicos.
- Datos e Información: en ejecución, en línea, almacenada, respaldos, bases de datos, procesos en ejecución, etc.

- Software: programas fuente, paquetes, bibliotecas, sistemas operativos, aplicaciones, servicios, claves de instalación etc.
- Hardware: CPUs, dispositivos de interconexión, discos, líneas de comunicación, estaciones de trabajo, si son elementos críticos, disponer de elementos redundantes (Servidores, Routers, etc.)
- Documentación: configuración de servicios, procedimientos administrativos, equipos, programas, respaldos (sitios alternos de almacenamiento de información)
- Accesorios: papel, cartuchos de impresión, cartuchos de respaldo.
- Edificaciones: ubicación, formas de acceso, sitios de almacenamiento local y remoto.

COMO SE HACEN EFECTIVAS LAS AMENAZAS!

Tipos de ataques:

- Intervención pasiva:

  Espionaje, no se perturba la red, son prevenibles y detectables

- Intervención activa:

  Modifica la información y/o perturba la operación de la red no se pueden prevenir, pero se pueden detectar, disponer de planes de acción inmediatos ante determinada circunstancia

DIFUSIÓN DE LAS POLÍTICAS DE SEGURIDAD

Realice un documento sencillo y fácil de entender por cualquier usuario dentro de la organización donde establezca con claridad:

- Porque es importante la seguridad
- Comprometa a todos por igual a velar por la seguridad de la Información
- Como detectar algún elemento sospechoso
- Que hacer al detectar un posible problema de seguridad
- A quien debe informarse de un potencial peligro
- Las vías en que los usuarios pueden hacerle llegar sus comentarios y sugerencias referentes a la seguridad
- Incentive a que se elaboren otros documentos más especializados con los temas específicos de cada área o sector. (Área de desarrollo, área de Servidores, área de mantenimiento de aplicaciones, etc.)
- Procure dar la información únicamente necesaria, informe no explique

DIVULGACIÓN DE LA POLÍTICA DE SEGURIDAD ATRAVES DE UNA RED

- Establezca un sitio en la red donde sus empleados puedan ser informados sobre nuevos peligros y como protegerse.
- Mantenga este sitio actualizado con información confiable pero concisa.
- Informe a sus usuarios de los cambios

PLAN DE ACCIÓN ANTE UN ATAQUE A LA SEGURIDAD DE LA INFORMACIÓN

Existen dos paradigmas:

- Detener y proteger
- Proteger y continuar

COMO MANEJAR INCIDENTES DE SEGURIDAD

Debe definirse un plan y una política de manejo de incidentes de seguridad

Objetivos del plan:

- Averiguar cómo ocurrió el incidente
- Averiguar cómo evitar la generación nuevamente del incidente
- Determinar el impacto y daño del incidente (limitarlo)
- Recuperar el sistema del incidente (retomar el control)
- Actualizar la política de seguridad y sus procedimientos
- Averiguar quién provocó el incidente

MANTENIMIENTO DE LA SEGURIDAD

- Las redes y sistemas de una organización no son entes estáticos
- Surgen nuevas amenazas que pueden afectarla
- Periódicamente hay que revisar las políticas y procedimientos de seguridad de una organización

- Proteger el sistema contra aquellas amenazas que aplican a las tecnologías empleadas

QUIENES PUEDEN AYUDAR

Su equipo de trabajo y sus usuarios, mediante la concientización y adiestramiento en la aplicación de las políticas de seguridad

CAPÍTULO III PLAN DE CONTENCIÓN

En el Plan de Contención se tomará en cuenta las acciones que deben ser ejecutadas inmediatamente cuando se presenta el siniestro o desastre, para minimizar los daños que se provoquen cuando los laboratorios dejen de operar, los cuales afectarán al normal funcionamiento de la ESPE-Extensión Latacunga, produciéndose dentro de las horas de clase como fuera de ellas.

Durante la contingencia se deberá salvaguardar y proteger la seguridad del personal civil y militar, equipo informático de comunicaciones y los archivos de información que posee los laboratorios de Redes e Informática. Una vez presentada la contingencia o siniestro se deberá ejecutar:

3.1 PLAN DE EMERGENCIA

En este plan se establecen las acciones que se deben realizar cuando se presente el Siniestro, así como la difusión de las mismas.

Es conveniente prever los posibles escenarios de ocurrencia del siniestro.

- Durante el día
- Durante la noche o madrugada

Este plan incluye la participación de actividades a realizar por todas y cada una las personas que se pueden encontrar presentes en el área donde ocurre el siniestro debiendo detallar:

- Vías de salida o escape.
- Plan de Evacuación del personal (Incluye personal civil y militar)

- Ubicación y señalización de los elementos contra el siniestro (extintores, cobertores contra agua, etc.)
- Teléfonos de emergencia (Bomberos, Cruz Roja, Hospitales, Policía, etc.) en caso de siniestro, además tener a la mano: Elementos de iluminación (Linternas).

3.1.1 PELIGROS POTENCIALES

3.1.1.1 INCENDIO

Un incendio es una ocurrencia de fuego no controlada que puede abrazar algo que no está destinado a quemarse. Puede afectar a estructuras y a seres vivos. La exposición a un incendio puede producir la muerte, generalmente por inhalación de humo, por intoxicación o por quemaduras graves.

Para que se inicie un fuego es necesario que se den conjuntamente estos tres factores: combustible, oxigeno, y calor o energía de activación.

Los incendios en los edificios pueden empezar por fallos en las instalaciones eléctricas, cortocircuitos y otras fuentes como velas y cigarrillos.

PREVENCIÓN DE INCENDIOS.

Mantener apropiadamente las instalaciones físicas para disminuir posibles causas de incendio, siendo responsabilidad del personal de los laboratorios cualquier sospecha de incendio.

Una vez implementado el sistema de alarmas y detectores de incendios las personas encargadas de los laboratorios de Redes e Informática, protegerán los equipos de daños, costos de reparación.

El personal debe conocer la clasificación de incendios, como utilizar los extintores y procedimientos a seguir.

CLASIFICACIÓN DE INCENDIOS

Fuegos clase A.- Son los fuegos en materiales combustibles comunes como: madera, tela, papel, caucho y plásticos.

Fuegos clase B.- Son los fuegos de líquidos inflamables y combustibles, grasas de petróleo, alquitrán, bases de aceites para pinturas, solventes lacas, alcoholes y gases inflamables.

Fuegos clase C.- Son incendios en sitios donde están presentes equipos eléctricos y energizados y donde la no conductividad eléctrica del medio de extinción es importante.

Fuegos clase D.- Son aquellos fuegos en materiales combustibles como Magnesio, Titanio, Circonio, Sodio, Litio y Potasio.

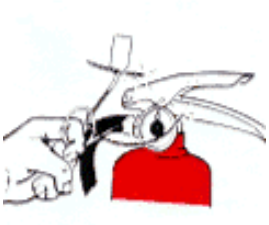
Fuegos clase K.- Fuegos en aparatos de cocina que involucren un medio combustible como aceites y grasas vegetales y/o animales.

COMO UTILIZAR LOS EXTINTORES

Todo el personal debe conocer muy bien las instrucciones de cualquier extinguidor en caso de llegar a usarlo.

A continuación se describe gráficamente el procedimiento para el uso de extinguidores en caso de incendio.

HALE



1.- Hale el pasador de Seguridad, rompiendo el sello de garantía

PRESIONE

2.- Sujete la manguera y presione las manijas de la válvula

APUNTE / FORMA DE ABANICO

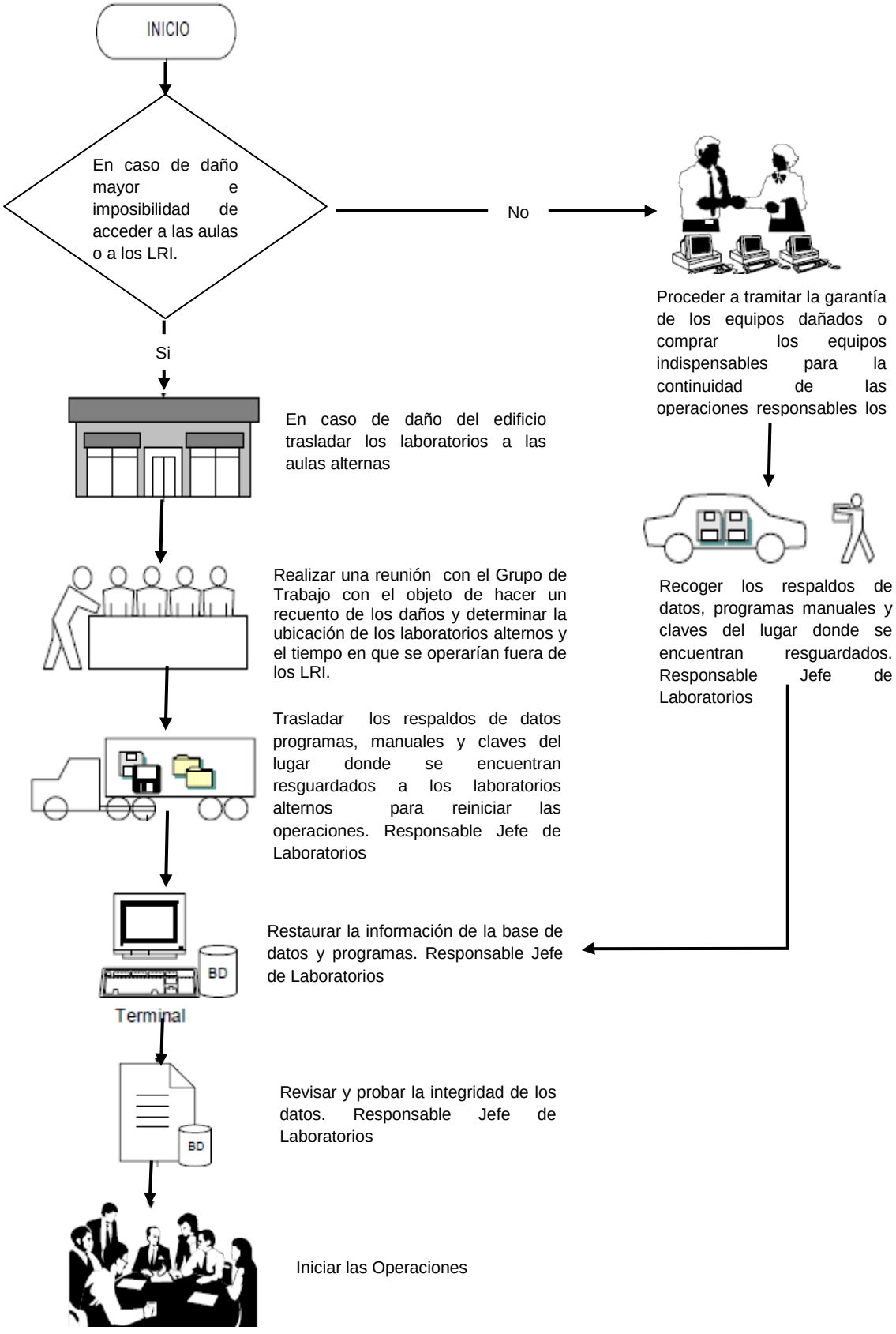
3.- Apunte a la base del fuego y el chorro de izquierda a derecha

PROCEDIMIENTO

El personal de los laboratorios de Redes e Informática, debe conocer los procedimientos a seguir en el Plan Contra Incendios establecido por la ESPE-Extensión Latacunga, el cual contempla:

- Alerta de incendio a todo el personal que labora en la ESPE-Extensión Latacunga
- Evacuación del personal militar y civil que labora en las instalaciones, estipulado en el "Plan de Seguridad de la ESPE-EL"
- Llamar al cuerpo de bomberos de Latacunga
- Formación de equipos contra incendios.
- Evacuación de los equipos informáticos y documentación.

DIAGRAMA DE RESPUESTA DE EMERGENCIA DE "INCENDIO"



3.1.1.2 TERREMOTO/ ERUPCIONES

TERREMOTO

Los terremotos son movimientos fuertes de las capas de tierra que no podemos predecir.

Normas de Comportamiento en caso de terremoto.- Las personas que laboran en los laboratorios de Redes e Informática así como en la ESPE-Extensión Latacunga, deben conocer y entender las normas de seguridad, recomendaciones y procedimientos que deben llevar a cabo en estas situaciones como:

- Mantener la calma
- Alejarse de vidrios y de objetos que puedan caer.
- Tratar de proteger la integridad física.
- Permanecer en áreas de estructura resistente, tales como debajo de dinteles o junto a columnas.
- Las áreas más seguras son los interiores evitando permanecer cerca de ventanas o en las azoteas.

ERUPCIONES

Las Erupciones son comportamientos de los volcanes difiere uno de otro, sin embargo, la mayoría emiten señales de alerta antes de una erupción.

3.1.2 ALERTA EN CASO DE UNA ERUPCIÓN

Es la declaración formal de ocurrencia cercana o inminente, está dada en función del tiempo estimado desde que este se avisa hasta que el evento catastrófico ocurra. Lo principal de cada grado de Alerta es saber ***¿QUE HACER?*** cuando se dé el aviso de cada una de ellas.

3.1.3 TIPOS DE ALERTAS

Existen varios tipos de alertas según los vulcanólogos de menor a mayor riesgo, estas son cuatro: Blanca, Amarilla, Naranja y Roja para la elaboración del Plan de Contingencias de los Laboratorios de Redes e Informática se tomo en cuenta las de mayor riesgo.

3.1.3.1 NARANJA.- Aumenta la probabilidad que el evento catastrófico ocurra en días o semanas.

Las acciones que implica la declaratoria de la alerta naranja son las siguientes:

- Reunir al personal de los laboratorios para tomar las medidas de seguridad.
- Ubicar los puntos críticos y de evacuación, con base a los riesgos.

- Adquisición de cobertores para proteger los equipos informáticos, ductos de comunicación y todo equipo que no se encuentre protegido.
- Adquisición de cintas adhesiva para sellado de puertas.
- Dependiendo del grado de acumulación de ceniza se procederá a la limpieza de alcantarillas, sifones y desagües.

3.1.3.2 ROJA.- Las condiciones de desequilibrio de la Amenaza aumentan y la probabilidad de ocurrencia del evento catastrófico se espera que ocurra en horas o días.

Las acciones que implica la declaratoria de la alerta roja son las siguientes:

- Evacuación del personal de alumnos y docentes de los laboratorios de Redes e Informática a las áreas de seguridad.
- Libertad de horarios de trabajo.
- Mientras dure la alerta roja, no habrá asistencia normal del personal, laborarán solo los grupos establecidos en el Plan de Contingencias hasta el momento mismo de la erupción.
- De producirse la erupción, el personal asignado para la emergencia será el encargado de poner en recaudo los servidores y la información en el Nuevo Campus Politécnico.

3.1.4 PLANIFICACIÓN DE UNA EVACUACIÓN EN CASO DE ERUPCIÓN

- Mantenerse alerta a los comunicados de la magnitud del desastre en caso de ser necesaria una evacuación.
- Establecer conversaciones acerca de la posibilidad de una evacuación, para determinar las acciones a tomar como son: salidas de emergencia, medio de transporte, a qué lugar dirigirse una vez realizada la evacuación.

3.1.5 ACCIONES INMEDIATAS DESPUÉS DEL SINIESTRO

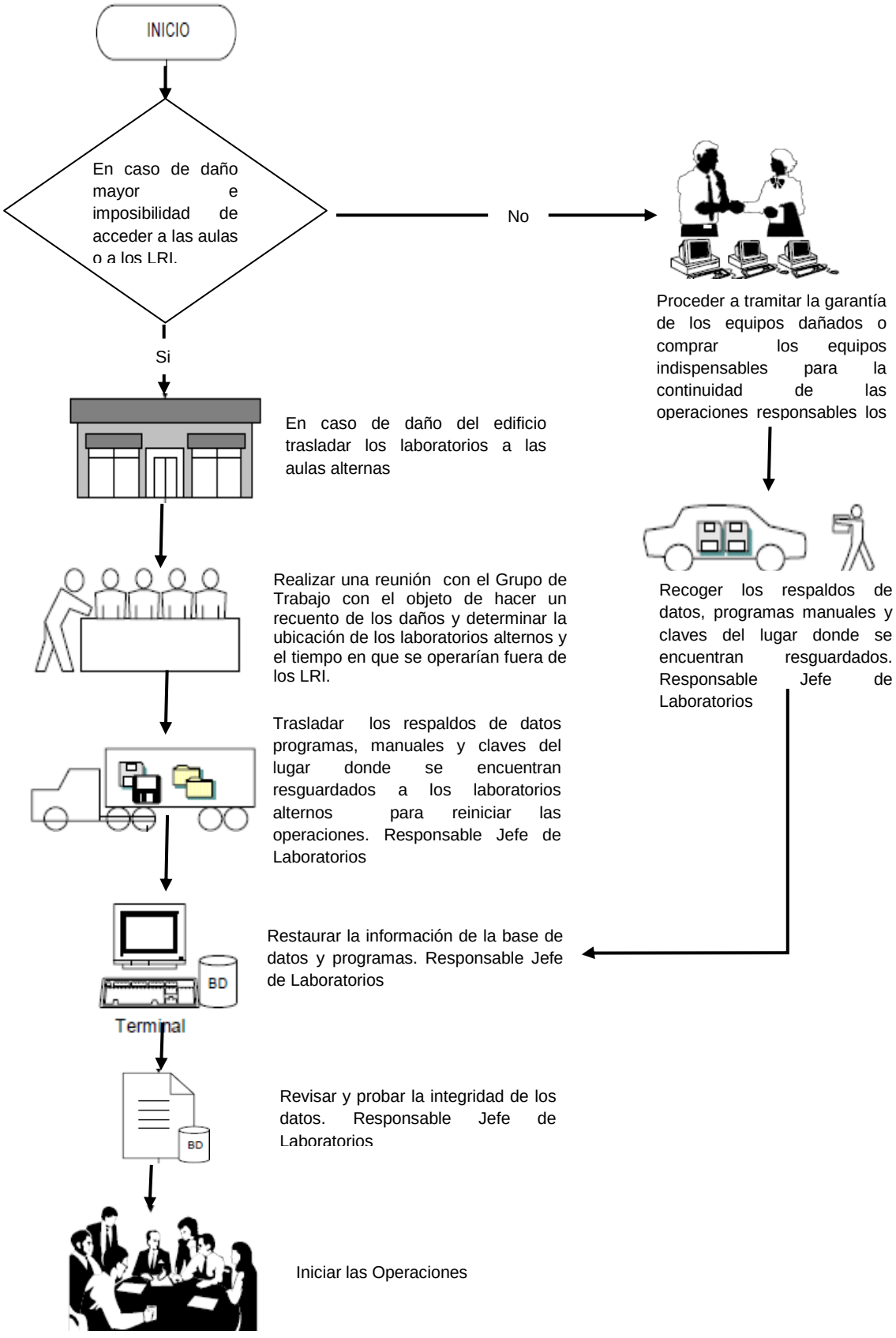
Una vez terminado el siniestro se evacuará los laboratorios de Redes e Informática, evitando atravesarse por áreas donde la estructura aparente estar frágil y por donde caen objetos.

El Director indicará la gravedad del siniestro, así como el impacto que este causó sobre las personas, equipo informático, de comunicación e instalaciones.

Se procederá a la rehabilitación o periodo de transición en el cual se restablecerán los servicios indispensables de los laboratorios de Redes e Informática.

La reconstrucción se caracterizará por las acciones que se realizarán con el fin de reparar la infraestructura afectada, restaurar el sistema, así como la información para superar el nivel de desarrollo previo al siniestro.

DIAGRAMA DE RESPUESTA DE EMERGENCIA DE "TERREMOTO/ERUPCIONES"



3.1.5.1. ANÁLISIS DE LA SITUACIÓN INMEDIATA DESPUÉS DEL SINIESTRO

El Director conjuntamente con el personal que labora, llevará a cabo la evaluación de la magnitud del siniestro, solicitando ayuda a las diferentes brigadas de Emergencia establecidas en la ESPE-Extensión Latacunga.

3.1.5.2. ACCIONES PARA CASOS DE EMERGENCIA DE LOS EQUIPOS INFORMÁTICOS

- Emergencias Físicas

Caso A: Error Físico de Disco de un Servidor.

Dado el caso crítico de que el disco presente fallas, tales que no pueden ser reparadas, se debe tomar las siguientes acciones:

1. Ubicar el disco malogrado.

2. Avisar a los usuarios que deben salir del sistema.

3. Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.

4. Bajar el sistema y apagar el equipo.

5. Retirar el disco malo y reponerlo con otro del mismo tipo, formatearlo y darle partición.

6. Restaurar el último backup en el disco, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad.

7. Instalar aplicaciones y realizar configuraciones necesarias.

8. Habilitar las entradas al sistema para los usuarios.

Caso B: Error de Memoria RAM

En este caso se dan los siguientes síntomas:

- El servidor no responde correctamente, por lentitud de proceso o por no rendir ante el ingreso masivo de usuarios.
- Arroja errores con mapas de direcciones hexadecimales.
- Es recomendable que el servidor cuente con ECC (error correct checking), por lo tanto si hubiese un error de paridad, el servidor se auto corregirá. 0
- Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por la Jefatura de Laboratorios, a menos que la dificultad apremie, cambiarlo inmediatamente.
- Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las acciones siguientes:
    1. Avisar a los usuarios que deben salir del sistema.
    2. El servidor debe estar apagado, dando un correcto apagado del sistema.
    3. Ubicar las memorias malogradas.

4. Retirar las memorias malogradas y reemplazarlas por otras iguales o de similares características.
5. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
6. Probar los sistemas que están en red en diferentes estaciones.
7. Finalmente luego de los resultados, habilitar las entradas al sistema para los usuarios.

Caso C: Error de Tarjeta(S) Controladora(S) de Disco

Se debe tomar en cuenta que ningún proceso debe quedar cortado, debiéndose ejecutar las siguientes acciones:

1. Avisar a los usuarios que deben salir del sistema.
2. El servidor debe estar apagado.
3. Ubicar la posición de la tarjeta controladora.
4. Retirar la tarjeta con sospecha de deterioro y tener a la mano otra igual o similar.
5. Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que al encender el sistema, los usuarios ingresen.
6. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
7. Al final de las pruebas, luego de los resultados de una buena lectura de información, habilitar las entradas al sistema para los usuarios.

Caso D: Caso de Incendio Total

En el momento que se dé aviso de alguna situación de emergencia general, se deberá seguir al pie de la letra los siguientes pasos, los mismos que están encausados a salvaguardar la seguridad personal, de los equipos informáticos y los archivos de información que se posea en backups.

- Se recomienda conservar la serenidad. Es obvio que en una situación de este tipo, impera el desorden, sin embargo, es muy recomendable tratar de conservar la calma, lo que repercutirá en un adecuado control de nuestras acciones.
- En ese momento cualquiera que sea(n) el (los) proceso(s) que se esté(n) ejecutando en el Servidor Principal, se deberá enviar mensajes (si el tiempo lo permite) de "Salir de Red y Apagar los Computadores", seguidamente digitar Down en el (los) servidor(es).
- Se apagará (poner en OFF) la caja principal de corriente de los laboratorios.
- Tomando en cuenta que se trata de un incendio de mediana o mayor magnitud, se debe tratar en lo posible de trasladar el servidor fuera del local, se abandonará el edificio en forma ordenada, lo más rápido posible, por las salidas destinadas para ello.
- Retirar el CD o DVD con el que arrancó el computador e insertar el CD o DVD antivirus, luego activar el programa de tal forma que revise todos los archivos y no sólo los ejecutables.

Caso E: Caso de Inundación

- Para evitar problemas con inundaciones se ha adquirido un rack de Servidores para la ubicación de los servidores. De esta manera evitaremos inconvenientes como el referido.
- En lo posible, los tomacorrientes deben ser instalados a un nivel razonable de altura.
- Dado el caso de que se obvió una conexión que está al ras del piso, ésta debe ser modificada su ubicación o en su defecto anular su conexión.
- Para prevenir los corto circuitos, asegurarse de que no existan fuentes de líquidos cerca a las conexiones eléctricas.

Caso F: Caso de Fallas de Fluido Eléctrico

Se puede presentar lo siguiente:

1. Si fuera corto circuito, el UPS mantendrá activo los servidores y algunas estaciones, mientras se repare la avería eléctrica.
2. Para el caso de apagón se mantendrá la autonomía de corriente que el UPS nos brinda corriente de emergencia, hasta que los usuarios completen sus operaciones.
3. Cuando el fluido eléctrico de la calle se ha restablecido se tomarán los mismos cuidados para el paso de grupo electrógeno a corriente normal (o UPS).

- Llámese corriente de emergencia a la brindada por grupo electrógeno y/o UPS.
- Llámese corriente normal a la brindada por la compañía eléctrica.
- Se contará con transformadores de aislamiento (nivelan la corriente) asegurando que la corriente que entre y salga sea 110v, evitando que los equipos sufran corto circuito por elevación de voltaje (protegiendo de esta manera el equipo informático y de comunicación).

Caso G: Caso de Virus

Dado el caso crítico que se presente virus en los equipos informáticos se procederá a lo siguiente:

Para los Servidores:

- Se contará con antivirus para el sistema que aíslan el virus que ingresa al sistema llevándolo a un directorio para su futura investigación
- El antivirus muestra el nombre del archivo infectado y quién lo usó.
- Estos archivos (exe., com., ovl., nim., etc.) serán reemplazados del CD original de instalación o del backup.
- Si los archivos infectados son aislados y aún persiste el mensaje de que existe virus en el sistema, lo más probable es que una de las estaciones es la que causó la infección, debiendo retirarla del ingreso al sistema y proceder a su revisión.

Para Computadoras Fuera de la Red:

Se revisará las computadoras que no estén en red con antivirus.

De suceder que una computadora se haya infectado con uno o varios virus ya sea en la memoria o a nivel disco duro, se debe proceder a realizar los siguientes pasos:

1. Utilizar un CD que contenga sistema operativo igual o mayor en versión al instalado en el computador infectado. Reiniciar el computador con dicho CD.
2. Retirar el CD con que arranco el computador e insertar el CD antivirus, luego activar el programa de tal forma que revise todos los archivos y no solo los ejecutables.

De encontrar virus, dar la opción de eliminar el virus. Si es que no puede hacerlo el antivirus, recomendará borrar el archivo, tomar nota de los archivos que se borren. Si éstos son varios pertenecientes al mismo programa, reinstalar al término del Scaneado. Finalizado el scaneado, reconstruir el Master Boot del disco duro.

3.1.6 COORDINACIÓN DEL EQUIPO DE SEGURIDAD

Organización de la Seguridad

Administrador General de los Laboratorios de Redes Informática y Laboratoristas

3.1.6.1 LLAMADAS DE EMERGENCIA

Bomberos.....102 - 2813520

Cruz Roja.....3811400 – 2812216

Defensa Civil.....2810148 – 2812-993

Banco de Sangre.....2812220

Hospital General.....147 - 2800332

Policía.....101 - 2812683

3.1.7. FUNCIONES DE LOS EQUIPOS EN CASO DE DESASTRE

Los servidores se encuentran dirigidos por un Jefe Administrador de Laboratorios y controlado por los Laboratoristas.

ADMINISTRADOR DE LOS LABORATORIOS DE REDES E INFORMÁTICA

Será el responsable de tomar las decisiones de seguridad sobre todos los Sistemas que operan en los Laboratorios de Redes e Informática como en la jefatura de Laboratorios.

COORDINADOR DE EMERGENCIA

Es responsable de coordinar las actividades y decisiones que efectuará el equipo de seguridad.

Llevará a cabo una relación directa con la brigada de Bomberos y Defensa Civil.

3.1.8. REORGANIZACIÓN Y OPERACIÓN

3.1.8.1. SITIO DE REUNIÓN DESPUÉS DEL DESASTRE

Si el siniestro fuese de gran magnitud y por tal razón las instalaciones del Campus Politécnico fueran destruidas parcial o totalmente el personal que labora en los laboratorios de Redes e Informática deberá ser contactado para presentarse en el nuevo campus ubicado en Belisario Quevedo.

3.1.8.2. ATENCIÓN MÉDICA

El personal de los laboratorios de Redes e Informática deberá comunicarse de inmediato con el Hospital Regional Latacunga para la coordinación de ambulancias y medicina.

3.1.8.3. TRANSPORTE

En caso de existir una evacuación el personal que labora en los laboratorios será provisto de transporte, debido a que la escuela cuenta con unidades propias que abastecerían a todo el personal.

3.2 ACCIONES HOSTILES

3.2.1 EL ROBO

Los equipos de cómputo son recursos muy valiosos y están expuestos al robo de la misma forma que están los cables de poder, tarjetas, memorias y accesorios en stock.

La información importante o confidencial puede ser fácilmente copiada además el software es una propiedad fácilmente sustraída.

3.2.2 EL FRAUDE

En realidad, el potencial de pérdida a través de fraudes están en aumento en sistemas computarizados y los problemas de prevención y detección del fraude son un reto.

Las tres principales aéreas donde se produce el fraude son:

- Manipulación de información de entrada, fácil de realizar y muy difícil de detectar, al ser los métodos de validación de entrada simples.
- Alteración o creación de archivos de información.
- Transmisión ilegal, interceptar o transferir información

3.2.3 EL SABOTAJE

El peligro más temido por los centros de Procesamiento de datos, es el sabotaje intentar implementar programas de seguridad de alto nivel contra saboteadores es uno de los retos más duros.

La protección contra el sabotaje requiere:

- Una selección rigurosa del personal
- Buena administración de los recursos humanos
- Buenos controles administrativos
- Buena seguridad física donde están los equipos

CAPITULO IV PLAN DE RECUPERACIÓN

Después de ocurrido el siniestro o desastre es necesario realizar las respectivas actividades que se detallan a continuación para recuperar el funcionamiento de los Laboratorios de Redes e Informática.

4.1 EQUIPO HUMANO DE EVALUACIÓN

El personal designado deberá realizar la evaluación de las instalaciones y equipos donde ocurrió el siniestro, y registrar todas aquellas actividades que se estén ejecutando, el tiempo y circunstancia que aligeraron o retrasaron las actividades del Plan de Contención.

El objetivo fundamental es obtener:

- Retroalimentación del Plan de Contingencias.
- Elaboración de una lista de sugerencias para minimizar los riesgos y pérdidas.

4.1.1 RESPONSABILIDADES DEL EQUIPO HUMANO DE EVALUACIÓN

- Estimar el impacto y la situación luego del siniestro respecto a los activos de los Laboratorios de Redes e Informática.
- Dar a conocer a todo el personal involucrado en el funcionamiento de los Laboratorios de Redes e Informática, para ejecutar las actividades detalladas en el Plan de Emergencia.
- Dar a conocer los procedimientos o actividades para ser ejecutadas en el momento de crisis.

4.2 EVALUACIÓN DEL IMPACTO DEL SINIESTRO

Tomando en cuenta la magnitud del impacto del desastre y el tiempo de paralización tenemos:

Interrupción Interna.- Se presenta cuando el impacto del siniestro o desastre ha afectado a uno o más Laboratorios.

Interrupción Externa.- Se presenta cuando el impacto del siniestro ha afectado parcialmente las actividades desarrolladas fuera de los Laboratorios.

Interrupción Total.- Se presenta cuando el impacto paraliza por completo las actividades desarrolladas en los Laboratorios.

Las actividades a ser ejecutadas considerando cualquiera de las anteriores interrupciones mencionadas son:

1. Identificación y localización del siniestro o desastre.
2. Poner en ejecución el Plan de Recuperación dependiendo del impacto del recurso afectado.
3. Ubicar con urgencia al personal técnico.

4.3 DEFINICIÓN DE LAS ACCIONES A EJECUTARSE DESPUÉS DEL DESASTRE

El Administrador de los Laboratorios deberá ejecutar las siguientes actividades que se detallan a continuación:

- Evaluación de daños.- Se evalúa luego de sucedido el desastre para conocer cuáles fueron las aplicaciones afectadas, equipos afectados, y cuales se pueden rescatar.

- Establecer procedimientos prioritarios como:
  - Sistemas de información
  - Equipos informáticos
  - Almacenamiento y obtención de respaldos
  - Normas y Procedimientos de Backups
- Si el desastre fuera de gran intensidad que afecte la integridad del personal que labora en los laboratorios debe ejecutarse de inmediato el Plan de Protección así como los Planes de Seguridad establecidos en la ESPE-L.
- Elaboración de un informe de daños que contendrá los tiempos de paralización.
- Ejecutar el Plan de Recuperación considerando el informe de daños ocurridos.
- Comunicación y activación de los equipos de trabajo.

4.4 EJECUCIÓN DE ACTIVIDADES

Implica al equipo humano de evaluación para realizar las actividades previamente planificadas, cada uno de estos equipos deberán contar con un coordinador que deberá reportar diariamente el avance de los trabajos de recuperación y en caso de presentarse algún problema, reportarlo de inmediato al Jefe a cargo del Plan de Contingencia..

Los trabajos de recuperación constan de 2 etapas que son:

1. La restauración del servicio usando los recursos.
2. 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 el buen servicio del Sistema e imagen Institucional.

4.5 INSTALACIÓN FÍSICA Y ELÉCTRICA

TABLA 4.5.1 DESCRIPCIÓN DE LAS ACTIVIDADES DE RECUPERACIÓN CON RESPECTO A LA INSTALACIÓN FÍSICA Y ELÉCTRICA

TIPO SINIESTRO	PROCESAMIENTO DE RECUPERACIÓN	RESPONSABLE
Daño Catastrófico	Si el impacto del desastre es catastrófico se procede habilitar lo más rápido posible los Laboratorios, en otra Dirección en este caso en el nuevo Campus Politécnico. Dar a conocer al personal involucrado en el funcionamiento de los Laboratorios de Redes de Informática para que apliquen el proceso de recuperación.	Jefe Laboratorista
Daño en el Sistema Eléctrico	Solicitar al personal encargado de la empresa eléctrica para que determine el impacto del daño y las medidas a tomar para su normal funcionamiento.	Jefe Administrativo

4.6 HARDWARE

TABLA 4.6.1 DESCRIPCIÓN DE LAS ACTIVIDADES DE RECUPERACIÓN CON RESPECTO AL HARDWARE

TIPO SINIESTRO	PROCESAMIENTO DE RECUPERACIÓN	RESPONSABLE
Falla en los componentes internos de los Servidores	El personal encargado del funcionamiento de los servidores llevará un registro del estado de los mismos para evitar daños en los componentes. En el caso que se presenten fallas técnicas que el personal responsable no pudiera reparar se llamará a la empresa responsable con la cual se mantienen los respectivos contratos vigentes.	Jefe Laboratorista
Daños en los Equipos	El personal encargado de los Laboratorios debe hacer una revisión física de los equipos para realizar un reporte de los daños. Una vez obtenido el reporte el personal revisara si los equipos dañados tienen garantía o están asegurados y si la garantía o el seguro está vigente.	Jefatura Laboratorista

4.7 SOFTWARE

TABLA 4.7.1 DESCRIPCIÓN DE LAS ACTIVIDADES DE RECUPERACIÓN CON RESPECTO AL SOFTWARE

TIPO SINIESTRO	PROCESAMIENTO DE RECUPERACIÓN	RESPONSABLE
Problema en los servidores.	El personal que Administra los servidores llevarán un registro del estado del software para evitar daños en la configuración del Sistema Operativo así como de la Base de Datos. En el caso que se presenten fallas técnicas que el personal responsable no pudiera reparar se llamará a la empresa responsable con la cual se mantienen los respectivos contratos vigentes para solicitar el servicio técnico respectivo.	Jefe Laboratorista.

4.8 EVALUACIÓN DE RESULTADOS

Una vez concluidas las labores de recuperación de los equipos y sistemas que fueron afectados por el siniestro se deben evaluar objetivamente todas las actividades realizadas ejecutándose en forma correcta, que tiempo tomaron, que circunstancias modificaron aceleraron o entorpecieron las actividades del Plan de Contención, como se comportaron los equipos informáticos.

4.9 RETROALIMENTACIÓN DEL PLAN DE ACCIÓN

Con la evaluación de resultados del siniestro se elaborarán las recomendaciones referentes a la retroalimentación y optimización del Plan de Contingencias y una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionaron el siniestro, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente.

CAPITULO V NORMALIZACIÓN DESPUÉS DE LAS EMERGENCIAS

Una vez puesto en ejecución los planes de Prevención, Contención y Recuperación y/o obtenido el informe de daños de las instalaciones y equipos informáticos se procederá a tramitar las garantías y seguros vigentes de los equipos informáticos dañados, y si las garantías y seguros no están vigentes se procederá a tramitar la adquisición de nuevos equipos informáticos, para poner en normalidad los Laboratorios de Redes e Informática.

5.1 PROCEDIMIENTOS A SEGUIR PARA LA NORMALIZACIÓN DE LOS LABORATORIOS DE REDES E INFORMÁTICA.

Si las casas comerciales y aseguradoras entregan los equipos informáticos nuevos.

a) Se procede adaptar físicamente a la nueva instalación con la base de datos y reinstalar nuevamente las aplicaciones en cada uno de los laboratorios.
b) Se Coordinara con los TIC's el servicio técnico respectivo para los equipos.

Si la Escuela Politécnica del Ejercito Extensión Latacunga compra nuevos equipos informáticos.

a. Se designara un personal para la revisión y evaluación de los equipos nuevos y estos remitirán un informe técnico.
b. Los nuevos equipos informáticos se darán ingreso en los activos fijos de los Laboratorios

c. Se procede adaptar físicamente a la nueva instalación con la base de datos y reinstalar nuevamente las aplicaciones en cada uno de los laboratorios.

5.2 PROBLEMAS CON LOS EQUIPOS INFORMÁTICOS

Los problemas a solucionar en los equipos informáticos son los siguientes:

- Equipos informáticos dañados por los desastres
- Equipos informáticos nuevos.

Equipos informáticos dañados por los desastres

Con el informe técnico de daños en los equipos se procederá a tener presente lo siguiente:

- Los equipos informáticos que se encuentren catalogados en recuperación deberán ser llevados a los TIC's.
- Los equipos dañados totalmente su hardware se procederá a dar la baja de los activos de los Laboratorios y se realizara el trámite para la adquisición de nuevos equipos.

Equipos informáticos nuevos

- Si los equipos nuevos presentaran fallas en su Hardware se procederá a realizar el cambio inmediato del equipo.
- Si los equipos tienen fallas en el Software se solicitara el servicio técnico a la empresa responsable.
- Si los equipos no cumplen con las características solicitadas se realizar el trámite para su entrega.

CAPITULO VI GUÍAS PARA LA EJECUCIÓN DE PRUEBAS

Se debe tener presente que la ejecución del Plan de Contingencias no solo se ejecuta en casos de emergencias, sino se debe realizar pruebas regularmente y en coordinación con las brigadas responsables (Cuerpo de Bomberos, Defensa Civil etc.), es necesario trabajar con el responsable del Plan de Contingencia y el personal designado para la ejecución del mismo los cuales deben ejecutar las siguientes actividades:

En el caso de existir actualizaciones al Plan de Contingencias o Procedimientos, se deberá llevar a cabo pruebas que afirmen su funcionalidad. Las Actividades a seguir para la ejecución de estas pruebas-simulacros se describen a continuación:

a) Planificación de la ejecución de la prueba-simulacro
b) Realización de la prueba-simulacro
c) Revisión de la prueba-simulacro
d) Definición de los planes de acción para los problemas detectados
e) Actualizar la documentación

Las pruebas pueden ser de dos tipos: anunciadas o no anunciadas. Estas últimas son las más reales y se realizan normalmente luego de algunas pruebas avisadas.

6.1 OBJETIVOS

El objetivo de las pruebas es verificar los procedimientos establecidos, probar y reanudar operaciones en sitios alternos o con elementos reducidos, determinar el conocimiento que tienen las personas de su

función en dichos procedimientos, establecer los tiempos de recuperación y, en general, detectar fallas y aplicar correctivos.

El objetivo de realizar las pruebas es:

- Que el Plan se encuentre totalmente actualizado.
- Garantizar su funcionalidad, el Plan debe tener un periodo de prueba lo cual garantizará que cuando se produzcan una Contingencia se encuentre al tanto de dichas actividades.

Los principales objetivos del simulacro son los siguientes

- Prevenir o minimizar el peligro para las vidas del personal que labora en los Laboratorios de Redes e Informática.
- Determinar la capacidad del equipo humano para volver a la normalidad después del desastre.

Considerando la importancia de los simulacros en los Laboratorios de Redes e Informática se llega a establecer la ejecución de estos periódicamente por las siguientes razones:

1. Se comprueba la conciencia y preparación del personal para afrontar los posibles desastres.
2. Se identifican las omisiones en el Plan de Prevención
3. Se pueden verificar que los planes establecidos en los Laboratorios funcionan correctamente.
4. Iniciar los procedimientos de recuperación inmediatamente y lo más ordenadamente posible.
5. Minimizar el número de decisiones a tomar tras un desastre.
6. Minimizar la dependencia sobre una persona en particular durante el proceso de recuperación.
7. Minimizar la necesidad de probar acciones de recuperación corriendo el riesgo de cometer errores cuando ocurra una emergencia o desastre.

6.2 ACTIVIDADES

Luego de cada prueba el coordinador de contingencia hará un informe completo, dirigido a los participantes, en el que se contemple toda la información acerca de la prueba, escenarios, objetivos, importancia, y se informen los resultados de la misma.

A continuación se describen las actividades más importantes a ejecutarse:

- Se identificará una de las aplicaciones consideradas críticas para ser ejecutadas en un sitio alterno.
- Identificar al personal involucrado en la ejecución del Plan de Contingencia.
- Plantear acciones del estado de simulacro que contenga:
  a) Declarar el estado de emergencia
  b) Evaluación de la situación y del impacto del desastre
  c) Establecer el escenario lo más real posible
- Documentar los resultados de la prueba y las mejoras realizadas a los planes.

CAPÍTULO VII ACTUALIZACIÓN Y MANTENIMIENTO

La actualización y mantenimiento de los planes definidos es con el fin de garantizar su efectividad en una emergencia, velando por que su información se encuentre actualizada, completa y precisa. Así mismo se implementan mecanismos que aseguren que el plan es consistente.

7.1 OBJETIVO

- Divulgar y distribuir las nuevas modificaciones en los planes para que todas las personas conozcan.
- Cumplir con los plazos establecidos para la revisión y actualización del Plan de Contingencia.
- Actualizar el Plan de Contingencia ante cambios significativos en los recursos de los Laboratorios, registrando todas las actualizaciones realizadas.
- Planificar pruebas del Plan de Contingencia y establecer los plazos, motivos y responsable de las mismas.
- Realizar pruebas puntualmente dejando constancia documental corrigiendo fallos detectados.
- Para llevar a cabo una actualización y mantenimiento debe tomarse en cuenta aspectos como Hardware, software, comunicaciones y recurso humano.

7.2 DIRECTRICES PARA MANTENER ACTUALIZADO EL PLAN

Designar un responsable para la actualización y mantenimiento del Plan de Contingencia el cual contendrá:

1. Establecer revisiones periódicas de los planes los cuales pueden ser semestrales, anuales.

2. Mantener relación paralela entre los planes desarrollados en la ESPE-Extensión Latacunga y el Plan de Contingencias de los Laboratorios de Redes e Informática.
3. Participar al personal de cambios o modificaciones realizadas en el Plan de Contingencias.
4. Documentar todos los cambios o modificaciones realizadas en el Plan de Contingencias.
5. Mantener actualizados todos aquellos inventarios de hardware y software tomando en cuenta las adquisiciones que se efectúen.
6. Capacitar al personal permanentemente para obtener resultados satisfactorios.

CAPÍTULO VIII CONCLUSIONES Y RECOMENDACIONES

8.1 CONCLUSIONES

a. El desarrollo de un buen Plan de Prevención fortalece el Plan de Contención en caso de siniestros, para superarlos en el menor tiempo y costo posible.
b. La implementación y mantenimiento de este Plan de Contingencias debe ser una de las prioridades primordiales para los Laboratorios de Redes e Informática.
c. La información proporcionada por las instituciones de socorro y seguridad es incompleta en algunos aspectos dados el carácter de reservado que mantiene cada una de ellas.
d. Se ha demostrado que no existe una salida de emergencia y señaléticas respectivas en los laboratorios de Redes e Informática.
e. El Plan de Contingencias lo debe conocer todo el personal involucrado en la administración de los laboratorios como usuarios.

8.2 RECOMENDACIONES

- Se recomienda Ejecutar los simulacros del Plan de Contingencias por lo menos 2 veces al año.
- Designar al personal capacitado para el mantenimiento y actualización del Plan de Contingencias.
- Para que el Plan de Contingencias tenga mejor implementación se debe realizar el estudio e Instalación de un sistema contra incendios.

- Implementar en los Laboratorios de Redes e Informática las recomendaciones establecidas en el Plan de Prevención para su óptimo funcionamiento.
- Se recomienda la capacitación del personal que labora en los Laboratorios de Redes e Informática con el Cuerpo de Bomberos y Defensa Civil en la utilización de extintores y en desastres naturales.
- Es recomendable al momento de adecuar las instalaciones, se lo haga con la asesoría de un técnico.

BIBLIOGRAFÍA

http://es.wikipedia.org/wiki/Plan_de_Contingencias

http://www.monografias.com/trabajos15/software/software.shtml

http://www.trucoswindows.net/conteni7id-22-Que-es-el-Hardware.html

http://www.unisdr.org/eng/public_aware/world_camp/2004/booklet-spa/page9-spa.pdf

http://www.miportal.edu.sv/NR/rdonlyres/8C2DB97E-722C-467E-B84D-2D8D4F31EB4C/0/ManualdeContingenciadelasAIV1.pdf

http://www.inei.gob.pe/web/metodologias/attach/lib611/733.htm

http://www.buenastareas.com/ensayos/Plan-De-Contingencia/246182.html

http://www.inei.gob.pe/web/metodologias/attach/lib611/anex11.HTM

http://www.cuc.uncu.edu.ar/upload/cuc_plan_de_contingencia_20104.pdf

http://es.wikipedia.org/wiki/Incendio

http://www.unirioja.es/servicios/sprl/pdf/tipos_extintores.pdf

MITNICK, KEVIN El Arte de la Instrucción: la verdadera historia de las hazañas de HACKERS, Intrusos e Impostores, Alfa-Omega 2007

Rodríguez Luis Ángel Seguridad de la Información en Sistemas de Computo, Madrid, Ventura 1995

LARDDENT, Alberto, Sistemas de Información para la gestión Empresarial, Procedimientos, Seguridad y auditoria. Buenos Aires PEARSON Education 2001

ESCUELA POLITÉCNICA DEL EJERCITO EXTENSIÓN LATACUNGA

CARRERA DE SISTEMAS E INFORMÁTICA

REFRENDACIÓN

Este proyecto fue elaborado por:

_____

PEÑALOZA O. ROBINSON G.
C.I. 1803416344

_____

ING. JOSE LUIS CARRILLO
COORDINADOR DE LA CARRERA DE SISTEMAS E INFORMÁTICA

_____

DR. RODRIGO VACA CORRALES
SECRETARIO ACADÉMICO

Latacunga, marzo del 2011