GOBIERNO REGIONAL LAMBAYEQUE
SEDE REGIONAL

GRPP

RESOLUCIÓN GERENCIAL GENERAL REGIONAL

No. 003 –2006-GR.LAMB/GGR

Chiclayo, 18 ENE. 2006

VISTO:

El informe Nº 014-2006-GR.LAMB/GRPP, emitido por la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial;

CONSIDERANDO:

Que, el Instituto Nacional de Estadística e Informática; mediante Oficio No 011-2003-INEI/DINP, da cuenta sobre el esquema para elaborar el Programa de Control de Hardware y Software – PCHS de forma bianual, instrumento de gestión que brinda procedimientos para el control de la parte física y lógica de este Parque Informático para el salvamento de información ante cualquier actividad orientados a mejorar la seguridad de la información;

Que, la Sede del Gobierno Regional Lambayeque, ha elaborado el respectivo Proyecto de "Programa de Control de Hardware y Software" el mismo que requiere ser aprobado;

Estando a lo actuado, con las visación de la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial; así como en uso de las atribuciones conferidas por el Reglamento de Organización y Funciones del Gobierno Regional, aprobado con Ordenanza Regional No.002-2003-GR.LAMB y modificatorias Ordenanzas Regionales Nos. 011, 021 y 024-2003-GR.LAMB/CR;

SE RESUELVE:

ARTÍCULO 1º.- Aprobar el Programa de Trabajo para el presente año denominado "Programa de Control de Hardware y Software" para la Sede del Gobierno Regional Lambayeque", el mismo que esta conformado por diecinueve (11) folios, cuyo texto integro forma parte de la presente resolución.

ARTICULO 2º.- Transcribir el contenido de la presente a la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial.

ARTICULO 3º.- Publicar el Programa de Trabajo en el Portal Institucional y distribuirlo en los correos institucionales de los trabajadores para conocimiento.

REGÍSTRESE Y COMUNÍQUESE.

ING° JULIO RIOS SOUSA
GERENTE GENERAL REGIONAL

INDICE

Introducción

El reconocimiento que la información es un activo valioso para la Sede del Gobierno Regional Lambayeque es un proceso difícil. Aceptamos como una realidad que los datos están disponibles, son confiables y estén protegidos de divulgación indebida; sin embargo, muchas veces no se capta el nivel de dependencia que la Sede del Gobierno Regional Lambayeque puede tener de estos datos hasta que la misma faltan o son afectados de algún modo.

La diversidad y la heterogeneidad de los sistemas de información que requiere actualmente la Sede del Gobierno Regional Lambayeque, sumando a la globalización a la que nos enfrentamos al conectar nuestros sistemas al mundo de internet, genera un sinfín de incertidumbres en lo referente a la seguridad de la información.

Por ello la Sub Gerencia de Racionalización e Informática, responsable de la seguridad tanto de hardware como software, debe desarrollar distintas estrategias de seguridad tomando en cuenta al tiempo, dinero y esfuerzo que hay que invertir para desarrollar las directivas y controles apropiados.

Aunque una estrategia de seguridad puede ahorrar mucho tiempo a la Sede del Gobierno Regional Lambayeque y proporcionar importantes recomendaciones de lo que se debe hacer, la seguridad no es una actividad puntual, es una parte integrante del ciclo vital de los sistemas y deben ser actualizadas permanentemente.

La Sede del Gobierno Regional Lambayeque como institución pública, necesita dar protección y prever de posibles amenazas internas y externas que afectan la disponibilidad, integridad y confidencialidad de los datos. Para ello se ha desarrollado el presente Plan de Control de Hardware y Software que contiene un análisis de la situación actual tanto del nivel físico como lógico. Análisis que permite plantear estrategias de protección para el hardware y software institucional.

Se han descrito en este documento estrategias que permiten orientar al personal técnico para brindar seguridad física y lógica a los datos.
También se incluye los criterios de programación y la distribución de actividades de acuerdo a las funciones que realiza cada área de ésta Sub Gerencia.

PLAN DE CONTROL DE HARDWARE Y SOFTWARE

1. Objetivo

Orientar a la prevención y protección de hardware y software de la Sede del Gobierno Regional Lambayeque, a través de estrategias de seguridad física y lógica.

2. Periodo de Vigencia

Hasta el 31 de Julio del 2004.

3. Análisis de la Situación Actual

3.1. Inventario de Hardware

EQUIPO	CANTIDAD
Servidor PDC	01
Servidor BDC	01
Servidor EPO	01
Servidor Firewall	01
Servidor Webmail	01
Estaciones de trabajo	158
Impresoras	87
Switch	05
Hub	13
Router	01
Plotter's	02
Escanner's	03

3.2. Hardware en Garantía

UNIDAD CENTRAL DE PROCESO – CPU					
CODIGO	Nº INVENT.	SERIE	FECHA ADQUISICION	UBICACION	RESPONSABLE
74089950	210		37585	Sub Gerencia de Racionalización e Informática	Galan Santisteban, Juan
74089950	211		37585	Oficina de Contabilidad	Valqui Tapia, Maria
74089950	212	INTEL INSIDE	37591	Oficina de Contabilidad	Contreras Benites, Carlos
74089950	213	1S2134L6T78P7102	37617	Oficina de Desarrollo	Rojas Cordova, Jorge
74089950	214		37711	Oficina de Contabilidad	Lluncor Granados, Silvia
74089950	215		37711	Sub Gerencia de Programación e Inversiones	Callirgos Coico, Marcos
74089950	216		37711	Oficina de Contabilidad	Soraluz Juarez, Angel S.
74089950	217	INTEL INSIDE	37711	Sub Gerencia Racionalización e Informática	Galan Santisteban, Juan
74089950	218		37711	Sub-Gerencia de Programación e Inversiones	Zapata Villamonte
74089950	219	INTEL INSIDE	37711	Oficina de Patrimonio Fiscal	Ramirez Reto, Wiliam H.
74089950	220	COMPATIBLE	37767	Gerencia Reg. Desarrollo Económico	Farroñan Santisteban,
74089950	221	INTEL INSIDE	37771	Sub Gerencia de Racionalización e Informática	Cardenas Del Aguila,
74089950	222	INTEL INSIDE	37771	Sub Gerencia de Racionalización e Informática	Cardenas Del Aguila, Edward
74089950	223	INTEL INSIDE	37771	Sub Ger. de Gestión Presupuestaria Y Tributación	Montes Mattos, Ronald
74089950	224	INTEL INSIDE	37771	Oficina de Contabilidad	Rojas Bonilla, Maria Nora
74089950	225	INTEL INSIDE	37771	División de Gestión Documentaria	Segundo Cajo, Miguel
74089950	226		37802	Sub Ger. de Planif. Estrat. Ordenamiento Territorial	Portocarrero Rodriguez,
74089950	227	COMPATIBLE	37809	Gerencia Reg. Desarrollo Económico	Melendez Malatesta, Rosa
74089950	228		37809	Sub. Gerencia de Programación e Inversión	Bernuy Del Castillo,
74089950	229	COMPATIBLE	37809	Sub Ger. de R.N. Areas Proteg. y Medio Ambiente	Sanchez Ramirez, Oscar R.
74089950	230	COMPATIBLE	37819	Sub Ger. de R.N. Areas Proteg. y Medio Ambiente	Reyes Gonzáles, Regis
74089950	231	COMPATIBLE	37862	Gerencia Reg. Desarrollo Económico	Tejada Tem, Itala
74089950	232		37862	Sub Gerencia de Programación e Inversión	Segura Murga Teresa
74089950	233		37877	Sub Gerencia de Estudios y Obras	Panta Samillan, Juan
					TOTAL CPU ----------> 24

MONITOR

CODIGO	Nº INVENT.	SERIE	FECHA ADQUISICION	UBICACIÓN	RESPONSABLE
74087700	189	207MX07703	37585	Of. Patrimonio Fiscal	Ramirez Reto, Wiliam H.
74087700	190	207MX07719	37585	Oficina de Contabilidad	Valqui Tapia, Maria
74087700	191	207MX07660	37591	Oficina de Contabilidad	Contreras Benites, Carlos
74087700	192	60H7947/55-13265	37617	Gerencia Regional de Desarrollo Social	Chiclayo Domenech, José
74087700	193	207D100085	37711	Sub Gerencia de Programación e Inversiones	Callirgos Coico, Marcos
74087700	194	306DI52839	37802	Oficina de Contabilidad	Rojas Bonilla, Maria Nora
74087700	195	2007DI00180	37711	Sub Gerencia de Racionalización e Informática	Galan Santisteban, Juan
74087700	196	211DIG1001	37711	Sub Gerencia de Racionalización e Informática	Galan Santisteban, Juan
74087700	197	207D10077	37711	Sub Gerencia de Programación e Inversiones	Zapata Villamonte,
74087700	198		37768	Gerencia Reg. Desarrollo Económico	Farroñan Santisteban,
74087700	199		37771	Sub Gerencia de Racionalización e Informática	Cardenas Del Aguila, Edward
74087700	200		37771	División de Gestión Documentaria	Segundo Cajo, Miguel
74087700	201	302DIG8428	37771	Oficina de Contabilidad	Soraluz Juarez, Angel S.
74087700	202	302DIG8462	37771	Sub Ger. de Gestión Presupuestaria y Tributación	Montes Mattos, Ronald
74087700	203		37771	Sub Gerencia de Racionalización e Informática	Cardenas Del Aguila, Edward
74087700	204	304D185667	37802	Sub Ger. de Planif. Estrat. Ordenamiento	Portocarrero Rodriguez,
74087700	205	401DI36232	37802	Sub Gerencia de Racionalización e Informática	Cardenas Del Aguila, Edward
74087700	206	301DI66913	37802	Sub Gerencia de Racionalización e Informática	Cardenas Del Aguila, Edward
74087700	207	304DI85703	37809	Gerencia Reg. Desarrollo Económico	Melendez Malatesta, Rosa
74087700	208	304D185594	37809	Sub Gerencia de Programación e Inversiones	Bernuy Del Castillo,
74087700	209	304D185942	40011	Sub Ger. de R.N. Areas Proteg. y Medio Amb.	Sanchez Ramirez, Oscar R.
74087700	210	304DI85792	37809	Sub Ger. de R.N. Areas Proteg. y Medio Amb.	Reyes Gonzales, Regis
74087700	211	AN17HXAW403638	37877	Sub Gerencia de Estudios y Obras	Panta Samillan, Juan
74087700	212	AN17HXAW403638X-	37862	Sub Gerencia de Programación e Inversiones	Segura Murga Tereza
74087700	213	AN17HXAW403715X-	37862	Gerencia Reg. Desarrollo Económico	Tejada Tem, Itala
					TOTAL MONITORES ------> 25

IMPRESORA MATRIZ DE PUNTO					
CODIGO	Nº INVENT.	SERIE	FECHA ADQUISICION	UBICACION	RESPONSABLE

74084550	89	DZUY023064	37585	Almacén de Mat. Oficina y Const.	La Torre Gomez, Carlos E.
74084550	90	DZU4009090/C423	37680	Dpto. de Servicio Mecánico	Purisaca Jacinto, Ines
74084550	91		37771	Consejeros	Cabrejos Tarrilo, José
74084550	92	DZUY002480	37771	Consejeros	Castañeda Serrano Marco
74084550	93	DZUY01251	37771	Consejeros	Soto Roca Enrique
74084550	94	DZUY012294	37771	Consejeros	Pacherrez Monja Héctor
74084550	95	DZUY012457	37771	Consejeros	Solis Rosas De Aita Maria
					TOTAL IMP. MATRIC---- --> 7

IMPRESORA A INYECCION DE TINTA

CODIGO	Nº INVENT.	SERIE	FECHA ADQUISICION	UBICACION	RESPONSABLE
74083650	14	FAKH00426	37680	División de Imagen Institucional	Chero Negron, Blanca Luz
					TOTAL IMP. INYECCION ---> 1

IMPRESORA LASER

CODIGO	Nº INVENT	SERIE	FECHA ADQUISICION	UBICACIÓN	RESPONSABLE
74084100	28	BRBB006929	37837	Sub Ger.de R.N Areas Proteg. y Medio Amb	Sanchez Ramirez, Oscar R.
74084100	29	BRBB009155	37837	Sub Ger.De R.N. Areas Proteg. y Medio Amb	Reyes Gonzáles, Regis
74084100	30	CNBB429614	37862	Ofic. de Contraloría	Miranda Plasencia, José
					TOTAL IMP. LASER -----> 3

CONCENTRADOR DE RED

CODIGO	Nº INVENT.	SERIE	FECHA ADQUISICION	UBICACION	RESPONSABLE
74081400	24	0100/LW201B00714	37606	Sub. Ger. Supervisión y Liquidaciones	Asalde Sipión, Pedro
74081400	25		37606	Sub Gerencia Estudios	Nizama Paz, Jorge Luis

74081400	26	0100/LW2G1B00724	37591	Gerencia Reg. de Infraestructura	Carrión Rojas, Manuel
					TOTAL HUB ----> 3

SWITCH DE RED					
CODIGO	Nº INVENT.	SERIE	FECHA ADQUISICION	UBICACION	RESPONSABLE
74086030	4		37771	Sub Gerencia Racionalización e Informática	Cardenas Del Aguila, Edward
74086030	5		37771	Sub Gerencia Racionalización e Informática	Cardenas Del Aguila, Edward
74086030	6		37866	Sub Ger. de R.N. Areas Proteg. y Medio Ambiente	Sanchez Ramirez, Oscar R.
					TOTAL SWITCH ----> 3

3.3. Control de Mantenimiento de Hardware

Consolidado de Mantenimientos hechos en los meses de Enero hasta Octubre 2003			
Mes	**Dispositivo**	**Nª Inv**	**Oficina**
Enero	----------		
Febrero	Impresora	74084550-0031	Oficina de Abastecimientos
	Impresora	74084550-0075	Oficina de Abastecimientos
	Teclado	74089500-0155	Oficina de Abastecimientos
	CPU	74089950-0065	Oficina de Abastecimientos
	Teclado	74089500-0155	Oficina de Abastecimientos
Marzo	Impresora		Div. Promoción de Inversiones y CTI
Abril	----------		
Mayo	----------		
Junio	Impresora		Gerencia Regional de Infraestructura
	CPU		Sub. Gerencia de R.N. Proteg. Y Medio Ambiente
	Mouse		Sub. Gerencia de R.N. Proteg. Y Medio Ambiente
	CPU		Sub Gerencia de Estudios y Obras
	Impresora		Sub Gerencia de Estudios y Obras
Julio	Mouse		División de Imagen Institucional
	Impresora		Sub Gerencia de Racionalización e Informática
	Impresora		Sub. Gerencia Planif. Estrat. y Ordenamiento Terr.
	Teclado	74089500-0171	Sub. Gerencia Planif. Estrat. y Ordenamiento Terr.
	CPU	74089950-0125	Gerencia Regional de Desarrollo Social
	Pantalla	74087700-0112	Gerencia Regional de Desarrollo Social
	Teclado	74089500-0149	Gerencia Regional de Desarrollo Social
	Mouse	74088035-0075	Gerencia Regional de Desarrollo Social
Agosto	Impresora	105E118543	Comité de Damas
	CPU	74089950-0003	Oficina de Desarrollo Humano
	Impresora		Presidencia Regional
	CPU		Oficina Regional de Asesoría Jurídica
Septiembre	Impresora	74083650-0024	Sub. Gerencia de R.N. Proteg. Y Medio Ambiente
	Teclado	74089500-0143	Sub Gerencia de Racionalización e Inform. – Soporte
Octubre	Teclado		Gerencia Regional de Infraestructura
	Impresora		Comité de Damas

3.4. Equipos de Seguridad Contra Incendios

a. Actualmente contamos con un extintor de Carbón Dióxido, el cual tiene fecha de vencimiento el 25 de febrero del 2004, este extintor puede ser usado para incendios, como: Sólidos, líquidos inflamables y corriente eléctrica.
b. Falta capacitación sobre uso de extintor, solamente se siguen las instrucciones generales que se reflejan en el extintor.

3.5. Alimentación Eléctrica y Pozos a Tierra

a. A la fecha se cuenta con conexiones antiguas que constituyen peligro para los usuarios.
b. Se cuenta con un generador de energía eléctrica, pero que abastece limitadamente la Sede del Gobierno Regional Lambayeque.
c. Solamente las oficinas de Contabilidad, Finanzas, Planificación y Programación e Inversiones tienen conexiones para poso a tierra.
d. Existen seis pozos a tierra de los cuales dos(02) están activos.

3.6. Inventario de Software en Uso

Actualmente los softwares que se están usando en las diferentes computadoras personales de la Sede Regional son los siguientes:

3.6.1. Módulos Informáticos de Propiedad del Gobierno Regional

a. Sistema de Gestión Documentario (SISGEDO).
b. Sistema de Control Contable (SISCONT).
c. Sistema de Tesorería (SISTESO).
d. Sistema Control Presupuestal(SISPOPP).
e. Sistema Control de Fondos para Pago en Efectivo(SISCAJA).
f. Sistema de Abastecimientos(SISABAS).
g. Sistema de Patrimonio Fiscal(SISPAT).
h. Sistema de Plan Operativo(SISPOP).
i. Sistema de Planillas(SISPLL).
j. Sistema de Cesantes(SISCESE).
k. Sistema de Confrontación de Operaciones Autodeclaradas(SISCOA).
l. Sistema de Racionalización(SISRACIO).
m. Sistema de Cooperación Técnica Internacional(SICTI).
n. Sistema de Resoluciones(STRES).
o. Sistema de Control de Personal(SISCOPER).
p. Portal Web Gobierno Regional Lambayeque.

3.6.2. Aplicativos Comerciales

a. Windows NT/95/98/Millenium/2000 PRO.
b. Office 97/2000/XP.
c. Arc View 3.1
d. Total Virus Defense McAfee Ver. 4.5.1.
e. Vstudio Ver. 6.
f. Foxpro para DOS Ver. 6.

3.6.3. Sofware Libre

a. Linux
b. PHP
c. MySQL
d. Apache

3.6.4. Software que proviene de otras instituciones del Estado

a. Sistema de Presupuesto: Provisto por el Ministerio de Economía y Finanzas (MEF).
b. Sistema Integrado de Administración Financiera (SIAF): Provisto por el Ministerio de Economía y Finanzas.
c. ADCOA: Provisto por la Superintendencia de Administración Tributaria.
d. Sistema de Registro de Inventario Físico: Provisto por la Contraloría General de la República.
e. Sistema Integrado de Administración Financiera-Módulo Gerencial: Provisto por el Ministerio de Economía y Finanzas.

3.7. Redes y Comunicaciones

3.7.1. Equipo Informático

La red informática del Gobierno Regional Lambayeque esta implementada bajo el sistema operativo Microsoft Windows NT Server 4.0 con 02 servidores que son:

a. CONTROLADOR DE DOMINIO PRINCIPAL (PDC): Servidor principal ubicado en los ambientes del SGRI, el cual contiene toda la información de los sistemas y usuarios.
b. CONTROLADOR DE DOMINIO DE RESPALDO (BDC): Servidor de respaldo o redundante, ubicado en los ambientes

de Soporte Técnico, que realiza copias en línea de la información procesada por el PDC: Ambos servidores están conectados las 24 horas del día, y cada usuario puede acceder con un LOGIN y un PASSWORD de acuerdo a una política de acceso establecida por la administración de la Red.

c. SERVIDORES PARA INTERNET

El Gobierno Regional Lambayeque tiene implementado un enlace dedicado con un ancho de banda de 128 kbps el cual permite contar con acceso a Internet los 365 días del año, y este servicio lo proporciona la Empresa TELEFONICA S.A.

La comunicación a Internet, los servicios Web y Correo Electrónico (E Mail) se han implementado bajo el Sistema Operativo Linux Red Hat, con 02 servidores:

Web / Mail: Servidor configurado para almacenar todas las cuentas de E Mail, paginas Web y servicios de FTP.

Proxy / Firewall: Servidor configurado como una base de datos de las páginas mas visitadas de manera que permita acelerar aun más el acceso a Internet y ampliar la cobertura de numero de PC's con salida a Internet.

Así mismo, su principal función es crear una barrera de fuego "Firewall" que impida el acceso de personas mal intencionadas a la Red.

3.7.2. Actualmente la red de comunicación de datos tiene problemas con la velocidad de transmisión de datos por las siguientes razones:

a. Excesivo número de usuarios que en este último año se han incrementado.
b. Existencia de equipos de comunicación de datos y equipos de cómputo que a la fecha ya han cumplido su tiempo de vida útil y por lo tanto su velocidad de procesamiento han disminuido.
c. La existencia de un diseño de red que esta desfasado y no cumple con los estándares establecidos.
d. La implantación de al red se realizó sin ningún previo estudio o proyecto.

3.7.3. A la fecha solo se han adquiridos tres(03) switch para la transmisión de datos, los que han sido ubicados en zonas estratégicas.

3.7.4. Carece de un plan de expansión de la red. Existe documentación limitada de la configuración de la red y su expansión ha originado cierto desorden tanto a nivel de cableado (que en algunos casos se encuentra expuesto al medio ambiente) como a nivel de estaciones de red (asignando valores disponibles de una forma arbitraria).

3.7.4. Las políticas de seguridad de la red están en proceso de implementación.

3.8. Acceso a las instalaciones informáticas

a. El acceso está restringido a la sala de servidores sin la autorización previa de la jefatura.
b. Las visitas a las instalaciones de Informática son guiadas por un personal asignado por la jefatura.
c. La limpieza en las oficinas son supervisadas por un personal asignado por la jefatura, para evitar incidentes.
d. Cada una de las oficinas están etiquetadas con su respectivo nombre, de acuerdo a las labores que se realizan.

4. Estrategias de Seguridad Física

4.1. Medidas de acceso a las instalaciones informáticas

a. Evitar que personas extrañas ingresen a la sala de servidores sin previa autorización.
b. Evitar que los equipos de cómputo y comunicaciones sean manipulados sin autorización previa de la jefatura de la SGRI.
c. Las visitas al centro de procesamiento de datos se hará acompañado de una persona debidamente autorizada. Además se debe registrar en una ficha como mínimo los siguientes datos: apellidos y nombres, empresa, motivo de la visita, hora de entrada y salida y nombre de la persona que atendió.
d. El jefe de la SGRI es el encargado principal del control y seguimiento de los registros y accesos y deberá actuar en consecuencia ante sospechas de violaciones de la misma.

e. La entrada de cualquier persona al centro de procesamiento de datos fuera del horario habitual de trabajo, deberá estar autorizado formalmente y registrada en la bitácora o ficha de ingresos.
f. Las tareas de limpieza en la SGRI serán supervisados por una persona responsable de la Sub. Gerencia que pueda advertir y evitar incidentes accidentales o intencionales sobre los equipos.

4.2. Medidas de protección de los equipos y medios de comunicación de la red de datos.

Es necesario realizar un proyecto de cableado estructurado, para evitar se deteriore tanto los equipos de comunicación de datos como los medios de transmisión. Al implementar cableado estructurado y un diseño de red eficaz, estamos asegurando una adecuada velocidad de transmisión, un mantenimiento sencillo e inmediato, así como también la detección de errores de manera rápida. Este proyecto de cableado estructurado debe comprender los siguientes aspectos:

a. Diario de ingeniería.
b. Topología lógica.
c. Topología física.
d. Plan de distribución.
e. Matrices de solución de problemas.
f. Tomas rotuladas.
g. Tendidos de cable rotulados.
h. Resumen del tendido de cables y tomas.
i. Resumen de dispositivos, direcciones MAC y direcciones IP.
j. Diagrama de flujo incluyendo:
    1. Instalación de tomas
    2. Instalación de jacks.
    3. Tendido de cables (Protegidos con canaletas u otros medios).
    4. Inserción a presión de cables en los paneles de conexión.
    5. Prueba de cables.
    6. Documentación de los cables.
    7. Instalación de las NIC.
    8. Instalación de hubs, switches, puentes y routers con sus respectivos gabinetes y closets.
    9. Configuración de routers.
    10. Instalación y configuración de los PC.

4.3. Sistema informático de control de Software y Hardware

Implementar el Sistema de Control de Hardware y Software, a fin de obtener información oportuna sobre:

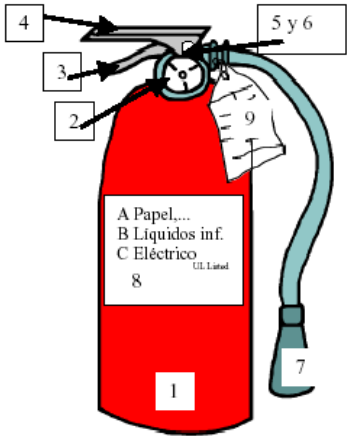
a. Inventario actualizado.
b. Mantenimiento preventivo y correctivo actualizado.
c. Listado de fallas y soluciones de hardware y software.
d. Número de Ip's asignados y por asignar.
e. Mantenimiento de Pozos a Tierra.

4.4. Definiciones y recomendaciones para enfrentar un incendio accidental.

4.4.1. Deberán existir extintores portátiles de fuego ubicados en posiciones estratégicas en todo el ambiente de procesamiento. Los mismos tendrán una etiqueta de inspección con la indicación de la clase de incendios a los que extinguen y la fecha de vencimiento.

4.4.2. Programar un curso de capacitación para el uso del extintor.

4.4.3. Queda establecido que el extintor es un artefacto que se puede transportar de un lugar a otro, cuyo peso varía desde 5 hasta 50 libras. Contiene una sustancia que, al echarla sobre un incendio pequeño, en la forma correcta, puede extinguirlo totalmente y evitar su propagación. La forma de los extintores, salvo variaciones minúsculas, es casi siempre en forma cilíndrica.



4.4.4. Las partes que componen el extintor son:

1. Cilindro: Recipiente donde se almacena el agente extintor.

2. Manómetro: Es un indicador de presión en el extintor. Indica cuan lleno o vacío está. Contiene tres secciones a saber; empty - vacío, full – lleno, overcharged –sobrecargado. No todos los

extintores tienen este indicador. En los que no tienen manómetro, existen otros medios para determinar si están llenos o vacíos.

3. Mango: Parte metálica fija por la cual se agarra el extintor cuando se utiliza.

4. Palanca: Parte por la cual se pone en acción el extintor. Al presionarla se abre la válvula de escape y sale el agente extintor.

5. Pasador de seguridad: Metal que fija la palanca y evita que se accione el extintor accidentalmente.

6. Abrazadera o Precinta de seguridad: Se utiliza para evitar que el pasador se salga de lugar. Normalmente, se utiliza como indicador de si se utilizó o no el extintor.

7. Manga o boquilla (trompeta): Parte por donde sale el agente extintor y con la cual se guía éste hacia el incendio.

8. Panel de instrucciones: Placa que contiene la información acerca del extintor, precauciones de uso y cualquier otra información pertinente.

Aquí dice el tipo de extintor: A, B, C, AAB, ABC. (Busque el extintor más cerca de usted y verifique su clasificación).

9. Tarjeta de mantenimiento e inspección: Tarjeta atada al extintor, donde se anota la fecha en que se recargó, se inspeccionó y las iniciales de la persona que lo hizo. Es un Registro de Mantenimiento y Servicio.

4.4.5. Elección del agente extintor

El agente extintor debe ser apropiado a la clase de fuego que vaya a combatir, es decir, a los combustibles existentes y las operaciones industriales que existan en el riesgo, con el fin de que su acción se manifieste más eficaz.

Además, hay que tener en cuenta, en el momento de la elección del agente extintor, la posible toxicidad de los gases producidos en la descomposición, por el calor, de algunos agentes extintores cuando se emplean en locales pequeños o mal ventilados.

Así mismo, hay que prestar especial atención a los riesgos en los que la protección se realiza sobre elementos bajo tensión eléctrica.

Se consideran adecuados, para cada una de las clases de fuego definidas en UNE 23010, A (sólidos), B (líquidos), C (gases), D (metales), los siguientes agentes extintores:

AGENTE EXTINTOR	CLASE DE FUEGO			
	A	B	C	D
AGUA A CHORRO	XXX	X	X	X
AGUA PULVERIZADA	XXXX	XX	X	X
ESPUMA FÍSICA	XXX	XXX	X	X
POLVO POLIVALENTE	XXX	XXX	XXX	X
POLVO SECO		XXXX	XXX	X
NIEVE CARBONICA (ANHÍDRIDO CARBONICO)	XX	XX	X	X
DERIVADOS HALOGENADOS	XX	XXX	X	X
PRODUCTOS PARA FUEGOS EN METALES	X	X	X	XXX

CALIFICACIÓN	EXCELENTE	BUENO	ACEPTABLE	NO ACEPTABLE
COLOR	XXXX	XXX	XX	X

4.4.6. Uso del extintor

1. Quite el seguro.
2. Colóquese a la distancia adecuada.
3. Accione la palanca.
4. Dirija el chorro a la base del fuego.
5. Utilice el extintor siempre a favor del viento, o sea, con al viento a su espalda.
6. Dirija el agente extintor a la base del fuego.
7. Es mejor utilizar todos los extintores que se necesiten al mismo tiempo.
8. En las acciones combinadas todo el agente extintor se debe dirigir a la base del fuego.
9. Nunca hay que darle la espalda al fuego, verifique su extinción total pasado un buen tiempo.
10. El equipo extintor se descarga en forma completa en 30 segundos aproximadamente.

4.5. Recomendaciones ante un desastre natural y desastre de entorno

4.5.1. Terremoto.- Es el desastre natural menos probable en el departamento de Lambayeque, se debe tener en cuenta ciertas medidas de prevención como:

a. Evitar la ubicación de equipos delicados en superficies muy elevadas (aunque tampoco es bueno situarlos a ras de suelo, como veremos al hablar de inundaciones). Si lo hacemos, un pequeño temblor puede tirar desde una altura considerable un complejo *hardware*, lo que con toda probabilidad lo inutilizará; puede incluso ser conveniente (y barato) utilizar fijaciones para los elementos más críticos, como las CPUs, los monitores o los *routers*. De la misma forma, tampoco es recomendable situar objetos pesados en superficies altas cercanas a los equipos, ya que si lo que cae son esos objetos también dañarán el *hardware*.

b. No situar equipos cerca de las ventanas: si se produce un temblor pueden caer por ellas, y en ese caso la pérdida de datos o *hardware* pierde importancia frente a los posibles accidentes - incluso mortales - que puede causar una pieza voluminosa a las personas a las que les cae encima.

4.5.2. Vibraciones

Las vibraciones, incluso las más imperceptibles, pueden dañar seriamente cualquier elemento electrónico de nuestras máquinas, especialmente si se trata de vibraciones continuas: los primeros efectos pueden ser problemas con los cabezales de los discos duros o con los circuitos integrados que se dañan en las placas. Para hacer frente a pequeñas vibraciones podemos utilizar plataformas de goma donde situar a los equipos, de forma que la plataforma absorba la mayor parte de los movimientos; incluso sin llegar a esto, una regla común es evitar que entren en contacto equipos que poseen una electrónica delicada con *hardware* más mecánico, como las impresoras: estos dispositivos no paran de generar vibraciones cuando están en funcionamiento, por lo que

situar una pequeña impresora encima de la CPU de una máquina es una idea nefasta.

4.5.3. Tormentas eléctricas

Al igual que los terremotos, es menos probable que sucedan, pero no resulta de más tomar ciertas medidas como:

a. Son predecibles con más o menos exactitud, lo que permite a un administrador parar sus máquinas y desconectarlas de la línea eléctrica.
b. Otra medida de protección contra las tormentas eléctricas hace referencia a la ubicación de los medios magnéticos, especialmente las copias de seguridad, almacenar lo más alejados posible de la estructura metálica de las instalaciones. Un rayo en la propia Sede Regional, puede inducir un campo electromagnético lo suficientemente grande como para borrar de golpe todas nuestras cintas o discos, lo que añade a los problemas por daños en el *hardware* la pérdida de toda la información de nuestros sistemas.

4.5.4. Inundaciones

En caso de inundaciones, lo más económico resulta la instalación de un falso suelo por encima del suelo real, o simplemente tener la precaución de situar a los equipos con una cierta elevación respecto al suelo, pero sin llegar a situarlos muy altos por los problemas que podrían ocurrir en caso a posibles terremotos y vibraciones.

4.5.5. Desastres de Entorno

1. Electricidad

a. Ante los cortocircuitos, picos de tensión, cortes de flujo que a diario amenazan la integridad tanto del *hardware* como de los datos que almacena o que circulan por él, se recomienda utilizar tomas de tierra para asegurar aún más la integridad; estos mecanismos evitan los problemas de sobretensión desviando el exceso de corriente hacia las instalaciones donde se encuentran instalados los pozos a tierra.

b. Para los excesivos voltajes se debe usar estabilizadores de tensión y para picos eléctricos usar filtros o estabilizadores con filtro incorporado.
c. Para bajadas de tensión es recomendable utilizar una SAI (Servicio de Alimentación Ininterrumpido).
d. Se recomienda usar UPS para protección de los Servidores, por ser equipos especiales y responsables de la prestación de recursos.
e. Evitar tocar con la mano la parte metálica de teclado o un conductor de una placa, debido a que la energía estática puede destruir un equipo completamente. Se trata de corriente de muy poca intensidad pero un altísimo voltaje, por lo que aunque la persona no sufra ningún daño - sólo un pequeño calambrazo - el ordenador sufre una descarga que puede ser suficiente para destrozar todos sus componentes, desde el disco duro hasta la memoria RAM.
f. Los técnicos de soporte a menudo deben usar *spray* antiestático o pulseras antiestáticos con la finalidad de evitar destruir los componentes de un equipo de cómputo o comunicaciones.

2. Ruido eléctrico

Su incidencia relacionada con la corriente de otras máquinas que pueden afectar al funcionamiento de la nuestra.

Para prevenir los problemas que el ruido eléctrico puede causar en nuestros equipos lo más barato es intentar no situar *hardware* cercano a la maquinaria que puede causar dicho ruido; si no tenemos más remedio que hacerlo, podemos instalar filtros en las líneas de alimentación que llegan hasta los ordenadores. También es recomendable mantener alejados de los equipos, dispositivos emisores de ondas, como teléfonos móviles, transmisores de radio o *walkie-talkies*; estos elementos puede incluso dañar permanentemente a nuestro *hardware* si tienen la suficiente potencia de transmisión.

3. **Humo**

   Evitar fumar cerca de los equipos de cómputo y comunicaciones, el humo afecta a los dispositivos magnéticos, ópticos y circuitos integrados en general.

4.5.6. Temperaturas extremas

a. Las temperaturas extremas, ya sea un calor excesivo o un frió intenso, perjudican gravemente a todos los equipos. Es recomendable que los equipos operen entre 10 y 32 grados Celsius, aunque pequeñas variaciones en este rango tampoco han de influir en la mayoría de sistemas. Para controlar la temperatura ambiente en el entorno de operaciones nada mejor que un acondicionador de aire.

b. Otra condición básica para el correcto funcionamiento de cualquier equipo que éste se encuentre correctamente ventilado, sin elementos que obstruyan los ventiladores de la CPU. La organización física del computador también es decisiva para evitar sobrecalentamientos: si los discos duros, elementos que pueden alcanzar temperaturas considerables, se encuentran excesivamente cerca de la memoria RAM, es muy probable que los módulos acaben quemándose.

4.6. Seguridad ambiental dentro de la sala de servidores

a. Todos los servidores del ambiente de procesamiento de la Sub. Gerencia deberán contar con estabilizadores de tensión y/o UPS (Uninterruptible Power Supply), estar instalados de acuerdo a las instrucciones del proveedor y montados en un Rack donde los cables estén asegurados de manera tal de evitar accidentes no intencionales. Todos los dispositivos se probarán periódicamente en los días y horarios que determine el responsable del ambiente de procesamiento.

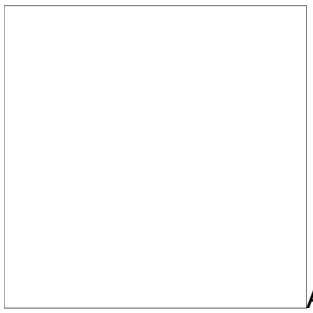
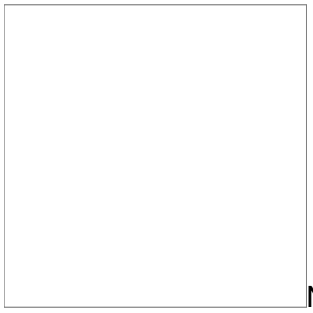
b. Preferentemente deberán existir dos llaves de desconexión eléctrica de emergencia, una dentro de la sala de la Sub. Gerencia y la otra cerca, pero fuera de la misma. Deberán estar claramente identificadas, ser de fácil acceso y estar protegidas de personas no autorizadas a fin de evitar que se las active en forma accidental. Estos dispositivos se probarán junto con los de suministro eléctrico.

c. La instalaciones de Informática de la Sub. Gerencia deberá estar limpio y ordenado, adecuadamente ambientado con aire acondicionado a fin de mantener estable la temperatura de los equipos y el piso deberá estar cubierto con alfombra antiestática.
d. La SGRI deberá contar con un sistema de detección de incendios. Dicho sistema deberá producir una señal audible cuando sea activado tanto manual como automáticamente y deberá estar conectado a la caseta de vigilancia a fin de comunicar al Departamento de Bomberos del incidente.
e. No se almacenará material combustible innecesario dentro o cerca de la sala de servidores, tales como papeles, cajas, etc.
f. Está prohibido comer, beber y/o fumar dentro de la sala de servidores de la Sub. Gerencia.

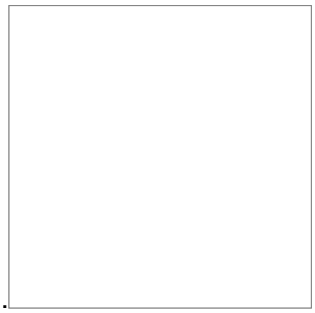
4.7. Medidas de seguridad eléctrica

Preferentemente la instalación deberá estar alimentada por dos líneas de suministro de electricidad, de forma tal que la interrupción por accidentes ambientales de una (agua, incendio, rayos, corte, etc.) no afecte a la otra.

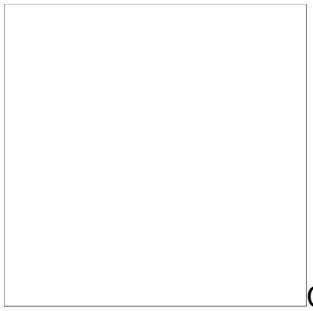
a. Normas básicas para prevenir riesgo eléctrico.

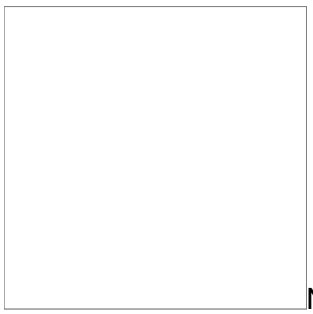
1. Toda instalación eléctrica debe estar provista de disyuntor diferencial en cada sector en que la misma se encuentre dividida.
2.  Antes de utilizar un aparato o instalación eléctrica, asegúrese de su perfecto estado.
3.  No se deben recargar los toma corriente conectando más de un artefacto en cada uno.

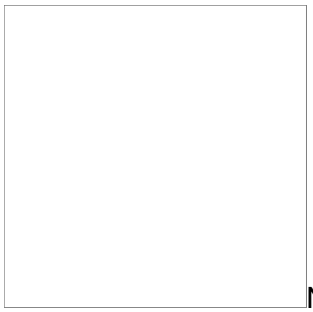
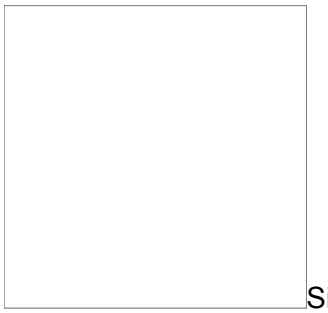
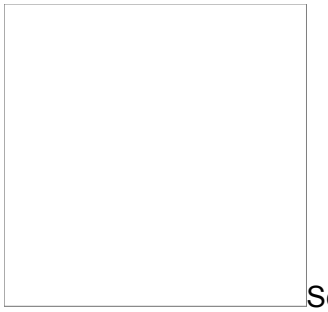
4. No use tomas corriente (enchufes) que se vean deteriorados o quemados.

Usar productos de calidad. 

5. Para desconectar un aparato eléctrico se debe tomar la ficha y nunca tirar del cable de alimentación.

6.  Cortar la corriente eléctrica siempre que se deban hacer trabajos sobre la instalación, aunque solo sea para cambiar una lámpara.

7.  No manipule instrumentos o aparatos eléctricos mojados o húmedos o cuando se tiene las manos y/o pies mojados.

8.  No intente reparar equipos o instalaciones eléctricas en caso de desperfectos. Solicite ayuda a un técnico especializado.
9.  Si alguna persona se electrocuta cortar inmediatamente la corriente eléctrica o utilizar un elemento aislante para auxiliarla. (Por ejemplo un palo de madera, diarios, tirar del pelo, tirar de la ropa suelta, etc.)
10.  Se debe evitar los cables sueltos en pisos.

Si no existe alternativa se deben cubrir con una media caña.
Jamás hacer instalaciones eléctricas "provisorias".

b. Usar pozos a tierra para seguridad de las personas y protección de la inversión de los equipos de cómputo y comunicaciones de datos del Gobierno Regional Lambayeque.

5. Estrategias de seguridad lógica

5.1. Copia de seguridad de datos.

a. Alternativas para realizar backups:

1. Backups transparentes son aquellos que se hacen sin que el usuario conozca que operaciones se están realizando ni como se están realizando. El uso de backups transparentes es mucho mas cómodo ya que su implementación quita trabajo al usuario y posibilidades de que este se equivoque en un proceso tan delicado como el que estamos tratando. Un ejemplo de backups transparente seria uno en el que el usuario simplemente da la orden de backup y el sistema de ficheros se encarga de hacerse una copia de la información que esta contemplando. (Recomendado).
2. Backups manuales son aquellos que se hacen bajo el control y actuación del usuario operación a operación. Es el usuario en todo momento el que tiene que saber que hacer.

   Un ejemplo de backups manuales seria uno en el que el usuario va copiando toda la jerarquía de ficheros del sistema mediante comandos que le ofrece el sistema de ficheros.
3. Mediante hardware es mas fácil ya que el sistema de ficheros no se encarga de nada. Todo el peso de las copias de seguridad lo llevan los mecanismos que se dedican expresamente a ello. Manteniendo

así la información duplicada en varios discos. Para esto se usan los sistemas de discos RAID ("Redundant Array of Independent Disks"). (Recomendado).

4. El uso de software para backups es un tanto mas difícil de manejar y el sistema de ficheros se tiene que encargar de las copias de seguridad, eso hace que el sistema este mas sobrecargado pero también que su uso sea el mas corriente debido a que es mucho mas barato.

b. Determinar el medio y las herramientas correctas para realizar las copias, basándose en análisis de espacios, tiempos de lectura/escritura, tipo de backup a realizar, etc.
c. Los backups deben realizarse en forma periódica(diario, semanal, mensual, trimestral, etc), considerando el volumen de datos que tiene la institución.
d. Los backups realizados en disco o en cinta, deben ser etiquetados y correctamente organizados para conocer en todo momento las últimas versiones y pueda localizarse fácilmente cuando se quiera restablecer los datos en el disco duro.
e. El almacenamiento de los Backups debe realizarse en locales diferentes de donde reside la información primaria. De este modo se evita la pérdida si el desastre alcanza toda la Sede del Gobierno Regional Lambayeque.
f. Verificar, periódicamente, la integridad de los respaldos que se están almacenando. No hay que esperar hasta el momento en que se necesitan para darse cuenta de que están incompletos, dañados, mal almacenados, etc.
g. Garantizar la integridad física de los respaldos, en previsión de robo o destrucción.
h. Garantizar la privacidad de la información que se respalda en medios de almacenamiento secundarios. Por ejemplo, la información se puede encriptar antes de respaldarse.
i. Borrar físicamente la información de los medios de almacenamiento, antes de desecharlos.
j. Mantener equipos de hardware, de características similares a los utilizados para el proceso normal, en condiciones para comenzar a procesar en caso de desastres físicos. Puede optarse por:

1. Modalidad Externa: otra organización tiene los equipos similares que brindan la seguridad de poder procesar la información, al ocurrir una contingencia, mientras se busca una solución definitiva al siniestro producido.
2. Modalidad Interna: se tiene más de un local, en donde uno es espejo del otro en cuanto a equipamiento, características técnicas y capacidades físicas. Ambos son susceptibles de ser usados como equipos de emergencia.
3. En todos los casos se debe asegurar reproducir toda la información necesaria para la posterior recuperación sin pasos secundarios ni operación que dificulte o imposibilite la recuperación.

5.2. Procedimiento para restringir el acceso a los programas, archivos y cuentas de usuario.

a. Elaborar una relación de las cuentas de usuario, programas y archivos a los cuales el usuario tiene acceso autorizado con los privilegios necesarios.
b. Cambiar el passwd cada 3 meses, chequear los passwd de los usuarios contra diccionarios para encontrar passwds fáciles, no dejar repetir passwds, etc.
c. Conviene dar a cada uno de los usuarios del sistema unas ciertas normas sobre el uso de la máquina que podría empezar con la frase de "Todo lo que no esta explícitamente permitido, esta prohibido" y continuar explicando todo lo que está permitido. Si se dejan las cosas claras desde un principio, nos ahorraremos muchos problemas.

5.3. Medidas de seguridad de acceso y soporte a los sistemas informáticos.

a. Elaborar una relación del personal y definir los niveles de acceso autorizado a los diferentes sistemas de información, describiendo los derechos que tienen los usuarios a ciertas opciones del sistema informático.
b. Cada cierto período, cambiar las claves de acceso a los diversos sistemas informáticos.
c. Las bases de datos de los sistemas deben contener campos en los cuales se registren los datos antes de ser modificados de un

determinado registro, incluyendo el usuario, la fecha y la hora de efectuado el proceso.

d. Implementar un procedimiento de seguridad en los sistema informáticos, que evite que los sistemas al ser copiados se ejecuten en otros terminales.
e. Implementar un procedimiento automático de regeneración de índices en los sistemas informáticos, el mismo que se ejecutará al detectar que los datos tienen estructuras malogradas.
f. Realizar copia de seguridad de la data de los sistemas informáticos en cintas magnéticas y en el disco duro del usuario que opera el sistema, para evitar perdida de datos ante cualquier falla técnica del sistema.
g. Mantener una copia actualizada de los programas fuentes de los sistemas informáticos, para su uso en el momento de existir fallas técnicas o presencia de virus en el servidor de archivos.
h. Implementar un módulo en cada sistema informático que permite auditar las operaciones realizadas por un determinado usuario.
i. Usar el manual técnico u operativo para realizar mantenimiento a los sistemas informáticos.

5.4. Procedimiento de monitoreo de intrusos y acceso externo no autorizados a la red.

5.4.1. Scaneo de Puertos

Los servicios TCP/IP, como la Web o Ftp, permanecen a la escucha de un puerto determinado. La función de un escaneador de puertos consiste en escanear un rango de direcciones IP en busca de servicios a la escucha en algún puerto. En una gran red puede ser posible que existan servicios ilegales escuchando en algún puerto poco frecuente, de manera que algún trabajador utilice la red de datos institucional de la sede para montar su propio servidor Web o servidor de ficheros, sin pagar a un proveedor de servicios.

Para detectar este tipo de abusos, que pueden llegar a comprometer seriamente la seguridad o ser el resultado de un ataque previo, conviene correr de vez en cuando un escaneador de puertos como UltraScan o Saint.

5.4.2. Conservar las huellas de los intrusos

La mayoría de los sistemas mantienen una serie de registros de log, donde queda almacenada la actividad de los usuarios, procesos, conexiones, etc. Si un intruso penetrara en nuestro sistema, siempre dejará alguna huella en el mismo, que nos permitirá rastrear sus pasos. Por este motivo, los intrusos más sofisticados contarán con herramientas para borrar silenciosamente toda traza de su incursión. Si se requiere que se vuelva imposible para un atacante borrar sus huellas, se puede redirigir la salida de los ficheros de log a otra máquina del sistema, de manera que se dificulte la labor de borrado de rastro de los atacantes. Para ello se debe modificar adecuadamente el fichero syslog.conf o similar, indicando que debe reenviar a otra/s máquina/s los mensajes deseados.

Para una mayor seguridad, se pueden redirigir a una impresora, de manera que queden registrados en papel. Si es demasiado el volumen de papel que se podría generar, se puede adoptar otra solución igual de eficaz, como redirigir el fichero a un puerto serie y conectar ahí mediante un cable modem nulo alguna vieja máquina que ya nadie utilice, guardando en el disco los ficheros.

Para cazar a un intruso, nada como conservar bien seguros todos sus pasos por nuestro sistema.

5.4.3. Cómo controlar por dónde navegan los usuarios

Para controlar el uso que los usuarios hacen del navegador instalado en los ordenadores de su sistema, se puede activar el asistente de contenidos.

En Internet Explorer, debes acudir a:

Ver --> Opciones de Internet... --> Contenido --> Restricciones --> Activar

En Netscape Communicator 4.5, se hace pulsando el comando NetWatch del menú Ayuda.

Una vez dentro, no se tiene más que seguir las instrucciones para activar las restricciones que se impondrán sobre los contenidos que a partir de este momento se podrá visualizar en el ordenador.

5.5. Medidas de seguridad en el uso de los servicios de la Red Informática Institucional.

5.5.1. Administrador:

a. Imprimir una hoja con las medidas de seguridad básicas o la política del sistema, y entregar una copia a cada usuario al crear su cuenta.
b. Desconfiar de cualquier sub programa desconocido que se encuentra en el sistema; utilizar programas del CD-ROM del sistema operativo, o versiones estáticas de los mismos, para tracear las actividades del intruso.
c. Si es posible, reinstalar el sistema operativo completo y aplicarle los parches de seguridad que el fabricante pone a nuestra disposición; permanecer atentos a los directorios de usuarios y a los programas que éstos contienen.
d. Si pensamos que la integridad del sistema peligra mucho, desconectar directamente el cable de red.
e. Obviamente, antes de poner el sistema de nuevo a funcionar en red, estar completamente seguro que los problemas de seguridad que el atacante aprovechó están solucionados.
f. **Seguridad para Windows 95/98/ME**

Seguridad en red

1. No comparta recursos si no es necesario.
2. Si necesita compartirlos, se debe hacer con una buena contraseña y asegurarse de que el recurso se comparte con los usuarios que lo necesitan y no esté accesible para todo el mundo.
3. Siempre que sea posible, compartir como de "sólo lectura". Así se evitará que, accidentalmente o por maldad, borren información o llenen el disco duro escribiendo en el directorio compartido.
4. NUNCA debe compartirse el disco duro con privilegios de escritura ni siquiera con contraseña. Aunque se comparta con contraseña, hay programas que realizan diversos tipos de ataque (de fuerza bruta, diccionario, etc..) hasta que dan con la contraseña correcta. Un hacker tiene todo

el tiempo del mundo para probar, y Windows no avisa que lo está haciendo.

En general, se recomienda no compartir información importante de forma permanente por este método, pues no proporciona demasiada seguridad.

g. Seguridad para Windows NT

Actualizar el S.O. con los últimos parches para disminuir los riesgos al que se expone el sistema.

Passwords en NT

Pregunta: ¿Cuál es el eslabón más débil de la cadena de seguridad en sistemas informáticos?

Respuesta: El usuario final.

Dale a un usuario la oportunidad de elegir libremente su password e inventará palabras de paso como juan98 (se llama Juan, claro) o leire93 (su esposa y el año de su boda). Con esa clase de passwords, las medidas de seguridad más extremas a menudo no sirven de nada.

Windows NT 4.0 Service Pack 2 incluye una nueva DLL (Passfilt.dll) que permite obligar que los usuarios introduzcan passwords fuertes, al incorporar la siguiente política:

1. Los passwords deben tener una longitud mínima de 6 caracteres.
2. Los passwords deben contener caracteres de al menos tres de las siguientes cuatro clases: a) Letras mayúsculas b) Letras minúsculas c) Números d) Caracteres especiales no alfanuméricos, como signos de puntuación
3. Los passwords no podrán contener el nombre de usuario ni otra parte del nombre completo del usuario.

5.5.2. Usuarios:

1. No elegir claves de menos de seis caracteres, y combinar mayúsculas, minúsculas, números, signos de puntuación o cualquier otro caracter que permita el teclado.
2. No apuntar nuestras claves ni compartirlas con otras personas.

3. No utilizar nuestra contraseña de acceso en otros sistemas, especialmente juegos en red o equipos Windows.
4. Sustituir telnet y ftp por ssh y scp o similares.
5. Nunca ejecutar programas que nos envíen por correo o que consigamos a partir de fuentes poco fiable como un “amigo” que nos pasa un programa por IRC). Tampoco ejecutar órdenes cuyo funcionamiento desconocemos, especialmente si alguien desconocido nos indica teclear “algo” para ver el resultado.
6. Desconfiar de llamadas telefónicas o correo electrónico que nos incita a realizar cualquier actividad dentro del sistema, especialmente cambiar nuestra clave; si estas situaciones se producen, indicarlo inmediatamente al responsable de seguridad del equipo, mediante teléfono o en persona.
7. Ante cualquier actividad sospechosa que se detecte es recomendable ponerse en contacto con el responsable de seguridad o el administrador, a ser posible por teléfono o en persona.

5.6. Medidas de seguridad ante un acceso interno no autorizado hacia la red.

Habilitar el sistema de auditorias(cuentas de usuario, sistema de archivos e impresoras) para rastrear sucesos que ocurren dentro del sistema en el servidor. En caso de no contar con el módulo de auditorias del sistema, realice la adquisición a dicho proveedor.

5.7. Medidas de seguridad para formatear y configurar un hard disk de un servidor

a. Realizar una copia espejo del sistema y la data, antes de proceder a dar formato al hard disk.
b. Preparar un disco de arranque del sistema operativo que permitirá iniciar el sistema, ante cualquier falla técnica que se pueda presentar.
c. Anotar la estructura y el tamaño de la partición de los hard disk principales y Raid de discos instalados en el servidor, en caso existan.
d. Revisar los manuales técnicos que acompaña al software de Raid de discos, para una instalación correcta.
e. Revisar los manuales técnicos que acompaña al sistema operativo del servidor, para una instalación correcta.

f. Configurar el sistema a medida que avanza la instalación del sistema operativo de red.

5.8. Medidas de seguridad para instalar una aplicación a los servidores

a. Exigir al proveedor una exposición del software o aplicativo a instalar, dirigida al personal técnico, de tal forma que se exponga los riesgos que correría al poner en marcha dicho programa y las medidas que se tomarían ante cualquier falla técnica.
b. Realizar una copia espejo del sistema y la data, antes de proceder a realizar la instalación.
c. Leer detenidamente las características técnicas del software o aplicativo a instalar.
d. Instalada la aplicación, realice las pruebas para verificar que el software esta ejecutándose normalmente y que no consuma demasiado recursos en la red, que pueda hacer colapsar todo el sistema.

5.9. Procedimiento para la detección y eliminación de virus

5.9.1. Síntomas más comunes de virus

Incluso el mejor software antivirus puede fallar a la hora de detectar un virus. La educación del personal sobre cuáles son posibles síntomas de virus informáticos puede ser la diferencia entre un simple dolor de cabeza y un gran problema. Veamos algunos síntomas:

a. Los programas comienzan a ocupar más espacio de lo habitual.
b. Aparecen o desaparecen archivos.
c. Cambia el tamaño de un programa o un objeto.
d. Aparecen mensajes u objetos extraños en la pantalla.
e. El disco trabaja más de lo necesario.
f. Los objetos que se encuentran en la pantalla aparecen ligeramente distorsionados.
g. La cantidad de espacio libre del disco disminuye sin ningún tipo de explicación.
h. Se modifican sin razón aparente el nombre de los ficheros.
i. No se puede acceder al disco duro.

5.9.2. Para detectar y/o eliminar los virus presentes en un computador, es necesario realizar el siguiente procedimiento:

a. Crear un disco de arranque en un computador del que se tenga certeza que no tiene virus.
b. Copiar en el disco los archivos necesarios para desinfectar el equipo contaminado (por lo general, los programas de antivirus incorporan este procedimiento completo).
c. Asegurar el disco (lockearlo), insertarlo en el PC y bootear el computador desde él.
d. Permitir que el antivirus revise todas las unidades rígidas del PC (discos duros) en busca de virus.
e. Luego de identificar y eliminar el virus, volver a bootear el PC desde el disco antivirus para cerciorarse de que está limpio.

Existe cierto tipo de virus que se aloja en el sector de booteo del disco duro del PC. Para eliminarlos sin necesidad de usar antivirus, a veces basta con usar el comando FDISK /MBR. Se trata de una medida inocua para el funcionamiento del equipo (sobre escribe en el sector de booteo un registro correcto), pero que en caso de existir virus, lo anula.

En otros casos, un antivirus no es capaz de identificar un virus, o si lo identifica, no es capaz de aplicar un antídoto. En tales circunstancias, se debe conseguir las versiones más actualizadas de antivirus que el proveedor pone a disposición en internet o enviarle un mail, detallando el problema.

6. Criterios de programación y asignación de actividades

a. Las estrategias anteriormente descritas deben ejecutarse cada inicio o fin de mes, con la finalidad de verificar ciertas acciones u operaciones de control tanto de hardware como software, si se encuentran implementadas, entonces se debe supervisar que se esté cumpliendo, caso contrario debe procederse de inmediato a su ejecución de las actividades mencionadas.
b. El personal técnico responsable, debe llevar el registro en una ficha de las actividades de control de hardware y software, previamente defino el formato de acuerdo al área que pertenece.
c. Las fichas de control deben ser analizados cada inicio o fin de mes por el personal responsable, con la finalidad de detectar vulnerabilidades en los

sistemas tanto de hardware como software y proponer nuevas estrategias que se agreguen al Plan de Control de Hardware y Software.

d. Asignación de actividades:

Seguridad Física		
Actividad	**Descripción**	**Equipo de Trabajo**
1	Acceso a las instalaciones informáticas	A, B y C
2	Protección de los equipos y medios de comunicación de la red de datos.	A, B y C
3	Actualizar el Sistema informático de control de Hardware y Software.	C
4	Capacitación sobre el uso del extintor en caso de incendio accidental (*)	B
5	Implementar las recomendaciones ante un desastre natural y desastre de entorno	A, B y C
6	Seguridad ambiental dentro de la sala de servidores	C
7	Implementar medidas de seguridad eléctrica (**)	C

Seguridad Lógica		
Actividad	**Descripción**	**Equipo de Trabajo**
1	Copia de seguridad de datos.	C
2	Administración de cuentas de usuario a la red y políticas de acceso a programas y archivos.	C
3	Administración de cuentas de usuario de aplicativos de la Sede Regional.	B
4	Monitoreo de intrusos - acceso interno y externo no autorizados a la red.	C
5	Implementar medidas de seguridad para el uso de los servicios de la red Informática Institucional.	B y C
7	Implementar medidas de seguridad para formatear y configurar un hard disk de un servidor.	C
8	Implementar medidas de seguridad para instalar una aplicación a los servidores.	C
9	Detección y eliminación de virus.	A, B y C
10	Implementación del Sistema de Control de Hardware y Software	A

Leyenda	
A	Desarrollo de Sistemas
B	Producción de Sistemas
C	Soporte Técnico

(*) Coordinar con Sub. Gerencia de Defensa Civil.

(**) Coordinar con la Oficina Regional de Administración.

GOBIERNO REGIONAL LAMBAYEQUE

DR. YEHUDE SIMON MUNARO
PRESIDENTE REGIONAL

ECO. RONALD MONTES MATOS
GERENTE DE PLANEAMIENTO, PRESUPUESTO Y ACONDICIONAMIENTO TERRITORIAL

ING. EDWARD CARDENAS DEL AGUILA
SUB GERENTE DE RACIONALIZACION E INFORMATICA

ING. HERMES MARINO QUINTEROS GONZALES
ANALISTA DE SISTEMAS RESPONSABLE DEL EQUIPO DE DESARROLLO DE SISTEMAS.

EL PRESENTE DOCUMENTO FUE ELABORADO POR EL EQUIPO DE DESARROLLO DE SISTEMAS DE LA SUB GERENCIA DE RACIONALIZACION E INFORMATICA.

CHICLAYO, NOVIEMBRE 2003