UNIVERSIDAD PERUANA LOS ANDES

FACULTAD DE INGENIERÍA

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

TESIS

DISEÑO DE UN PLAN DE CONTINGENCIA DE SISTEMAS INFORMATICOS PARA LA UNIVERSIDAD PERUANA LOS ANDES

PRESENTADO POR:

Bach. SHERLY CLERY ESPINOZA ASTO

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS Y COMPUTACIÓN

HUANCAYO - PERÚ

2014

Mg. RUBEN TAPIA SILGUERA
PRESIDENTE

……
JURADO

……..
JURADO

……..
JURADO

MG. MIGUEL ANGEL, CARLOS CANALES
SECRETARIO DOCENTE

Mag. Jaime Humberto Ortiz Fernández

ASESOR

Dedicatoria

Al Todopoderoso, por concederme la dicha de la vida y todo lo que soy, por brindarme la sabiduría y el conocimiento de su palabra. A mi madre adorada Marina Asto, por todo su amor y confianza permanente, por inculcarme sus valores y sabios consejos en todo momento. A mi complemento perfecto por su apoyo incondicional y su fuente inagotable de amor.

Espinoza Asto Sherly Clery

INDICE DE CONTENIDO

INDICE DE CONTENIDO v
RESUMEN viii
ABSTRACT ix
INTRODUCCIÓN x
GENERALIDADES 1
CAPITULO I 2
ASPECTOS GENERALES 2
1.1 DESCRIPCIÓN DE LA ORGANIZACIÓN 2
1.3 OBJETIVOS 6
1.4 LIMITACIONES 6
1.5 FACTIBILIDAD 7
CAPITULO II 18
MARCO TEÓRICO 18
2.1 Antecedentes 18
2.2 Bases Teóricas 20
2.2.1 Sistema Viable 20
2.2.2 Los Sistemas de Información 20
2.2.3 El modelo de Nolan/Gibson 21
2.2.4 El modelo de Gartner 22
2.2.5 El modelo de Donovan 24
2.2.6 Qué es un Plan de Contingencia 25
2.2.7 El Plan de Contingencia Informática 25
2.2.8 Base de Datos 30
2.3 METODOLOGÍAS 30
2.3.1 Norma ISO 27001, Guía de buenas prácticas ISO 27002 y necesidad del Plan de Contingencia 30
2.3.2 Modelo de Gobierno TI Basado en COBIT 33
2.3.3 Estándar para la Gestión de Servicios Informáticos ITIL 36
2.4 ELECCIÓN DE METODOLOGÍA DE SOLUCIÓN 38
PRESENTACIÒN DE RESULTADOS 40
CAPITULO III 41

IDENTIFICACIÓN DEL SISTEMA VIABLE 41
3.1 Diagnóstico de la Universidad basado en el Enfoque de Sistema Viable 41
3.2 Diagnóstico 43
3.3 Antecedente de Diagnóstico Sistémico 44
3.3.1 Organigrama Relacional de la Oficina Universitaria de Informática 45
3.3.2 La Gestión de Proyectos 46
3.3.3 Activos Intangibles 46
DISCUCIÒN DE RESULTADOS 51
CAPITULO IV 52
DIAGNÓSTICO Y PROPUESTA DE CAMBIO 52
4.1 Diagnostico del Sistema (Oficina Universitaria de Informática) 52
4.2 Propuesta de Cambio con ISO 27001 60
4.2.1 FASE 01 PLANIFICACION 61
4.2.2 FASE 02 HACER 3
4.2.3 FASE 03 VERIFICAR 15
4.2.4 FASE 04 ACTUAR 32
CONCLUSIONES 40
RECOMENDACIONES 41
BIBLIOGRAFÍA 43
ANEXOS 46

INDICE DE CUADROS

Cuadro 1 Clasificación de los Activos Intangibles 48
Cuadro 2 Tecnologías 54
Cuadro 3 Equipos de informática y software básico 54
Cuadro 4 Comunicaciones y redes 54
Cuadro 5 Sistemas de información 55
Cuadro 6 Infraestructura de servidores 55
Cuadro 7 Actividades para el Plan de Contingencia Informática para la Oficina de Informática 2
Cuadro 8 Análisis de Evaluación y riesgos 4
Cuadro 9 Matriz de planificación de contingencia 7
Cuadro 10 Tareas para ubicar soluciones a Contingencias 15
Cuadro 11 CUADRO DE LISTA DE RIESGOS QUE SE PUEDE ENCONTRAR 17
Cuadro 12 Cuadro Valoración de riesgos 19
Cuadro 13 Cuadro Clasificación de Riesgos 22

Cuadro 14 Relación de los Sistemas de Información con los que cuenta 24
Cuadro 15 Equipos de Cómputo 25
Cuadro 16 Cuadro de Riesgos 30

INDICE DE GRAFICOS

Grafico 1 Modelo de Nolan para la Implementación de tecnologías en las organizaciones 22
Grafico 2 Estado de madurez de organización en TI 24
Grafico 3 Áreas de enfoque del gobierno de TI 35
Grafico 4 Ciclo de vida ITIL 38
Grafico 5 Organigrama Relacional deInformatica 45
Grafico 5 Curva de Nolan adaptado resultado de la calificación de las tecnologías. 56
Grafico 6 Organigrama Estructural y Funcional 62
Grafico 7 Identificación de Soluciones Preventivas 11

RESUMEN

El presente trabajo es una propuesta para el Plan de contingencia de la UPLA en su local ubicado en la Av. Giráldez que busca mejorar el rendimiento, la confiabilidad y aumentar el nivel de seguridad en las comunicaciones en la institución, debido a que la infraestructura de red disponible actualmente no posee las características necesarias para la implantación de nuevas tecnologías, con este proyecto se busca fortalecer los procesos y medidas mediante un plan de contingencia, facilitando una herramienta para mejorar la productividad con la utilización de tecnología y cumpliendo con la innovación y desarrollo que deben tener las instituciones de educación superior.

El trabajo está apoyado en una metodología basada en el enfoque sistémico, ITIL, COBIT Estándares ISO donde se obtiene la información necesaria de los usuarios y se plantea una solución a la problemática existente; está basado en la Metodología de Ciclo de Vida de Sistemas.

ABSTRACT

This research is a proposal for the contingency plan at your local UPLA located at Av Giráldez looking to improve performance, reliability, and increase the level of communications security in the institution, because the network infrastructure currently available does not have the features necessary for the implementation of new technologies, this project seeks to strengthen the processes and measures through a contingency plane, providing a tool to improve productivity through the use of technology and compliance with innovation and development must be institutions of higher education.

Work is supported by a methodology based on the ecosystem approach, ITIL, COBIT ISO Standards where necessary user information is obtained and a solution to the existing problem arises, is based on the methodology of Life Cycle Systems.

INTRODUCCIÓN

Todas las organizaciones, de cualquier tamaño, naturaleza, actividad económica, etc., son susceptibles de mejora en algunos de sus procesos de negocio o de apoyo. Conscientes de esto, tomamos la determinación de aprovechar nuestra experiencia y aplicar los conocimientos adquiridos durante la especialización para promover la mejora en el proceso de Tecnologías de Información y Comunicación (TIC) en la UPLA.

No se puede mejorar lo que no se conoce, por lo que el punto de partida definido fue realizar un acercamiento a la UPLA, conocer su proceso de TIC y comprender la visión del recurso humano del área de Sistemas sobre el estado informático de la organización. Posteriormente, se plantea la necesidad de evaluar la madurez informática de la institución, para lo cual se analiza también la percepción del usuario final o cliente interno, buscando tener una idea objetiva y evitar opiniones sesgadas.

Con el análisis de la información recolectada, el equipo consultor y el grupo de trabajo de Sistemas de la institución detectan las problemáticas de TI y generan las estrategias orientadas a promover la mejora del área y de los servicios informáticos para beneficio de la organización.

El equipo consultor sugiere también una propuesta de mejoramiento, basada en guías de buenas prácticas de TI y en su propia experiencia.

Este documento presenta el desarrollo del mencionado proceso de consultoría y los resultados obtenidos representados en una propuesta de mejoramiento y un plan de contingencia de TI.

Para el logro de la presente investigación de proyecto factible, se utilizó como metodología a ITIL, COBIT y buenas Practicas ISO, con un nivel de investigación descriptivo. Estructurándose el trabajo en cinco capítulos los cuales se describen a continuación:

Capítulo I: ASPECTOS GENERALIDADES.
Se explica el planteamiento del problema, el alcance y las limitaciones encontradas durante el desarrollo del proyecto.

Capítulo II: MARCO TEÓRICO.
Está conformado por el marco teórico, se especifica los antecedentes de la investigación, el área de estudio y el área de investigación.

Capítulo III: IDENTIFICACIÓN DE LOS SISTEMAS VIABLES.
Este capítulo comprende el análisis de datos para las diferentes técnicas aplicadas de forma clara para así poder determinar cuáles son los requerimientos y necesidades en general.

Capítulo IV: DIAGNÓSTICO Y PROPUESTA DE CAMBIO.
Este capítulo comprende las fases de la metodología utilizada, se presenta un análisis detallado de los resultados obtenidos de la investigación y obteniendo el desarrollo de procesos y manuales de contingencia. Finalmente se presentan las conclusiones, recomendaciones, la bibliografía y los anexos que complementan el contenido del presente trabajo.

La Estudiante

GENERALIDADES

CAPITULO I

ASPECTOS GENERALES

1.1 DESCRIPCIÓN DE LA ORGANIZACIÓN

Las universidades son organizaciones de formación superior, representan el avance y desarrollo tecnológico del ámbito regional donde estas se encuentren ubicadas y deben ser consideradas guías tecnológicos en el mundo competitivo, el uso de mecanismos de interconexión de redes facilita sus comunicaciones a nivel mundial y se convierten en una ventaja competitiva en el mercado global.

La Universidad Peruana Los Andes, también conocida como UPLA, es una universidad ubicada en la ciudad de Huancayo, Perú. Fue creada el 30 de diciembre de 1983. Reconocida como una de las universidades más prósperas de la Región Junín.

La institucionalización, que fue otorgada por la Asamblea Nacional de Rectores (ANR) el 18 de junio de 1993, mediante Resolución N° 446-93-ANR. Autorización

definitiva que deviene del informe evaluado por la Comisión de Coordinación Interuniversitaria, órgano autónomo de la ANR. Actualmente su población estudiantil bordea los 20000 alumnos, funciona en varias sedes y Filiales el local principal o Administrativo está ubicado en la Av. Giráldez N°231 Huancayo, su infraestructura es material noble, los ambientes son divididos y aquí funcionan las oficinas administrativas, cuenta con otros locales, el principal está en la ciudad universitaria de chorrillos, cuenta con aulas y laboratorios.

Jerárquicamente los sistemas de información como el Contable y Académico y otros están administrados por la Dirección de Informática de la UPLA y en conjunto con la Dirección Universitaria de Desarrollo Académico, y la Oficina de Economía.

En el local de la Av. Giráldez N° 231- Huancayo; implementada la mayoría de sus sistemas las que más valor poseen. Se cuenta con servidores que alojan a los diferentes sistemas y la red LAN que se han implementado de acuerdo a la necesidad, año tras año -según la disponibilidad de recursos- se ha ido ampliando su cobertura hasta llegar a conectar a todas las computadoras administrativas,.

Actualmente la conexión inalámbrica se realiza a través de cables de par trenzado CAT 5, en su mayoría, y otras conexiones con CAT 6, el uso principal que se le brinda es para ingresar al Internet y en menor grado para compartir recursos, los equipos de conectividad –switchs- son de diferentes configuraciones y velocidades, demostrándose que la prioridad era lograr la conectividad con los recursos disponibles sin respetar estándares o protocolos mínimos de seguridad.

Se tiene acceso a Internet, además de una línea VPN de 900Kbps conectada al local central de las facultades, ésta línea sólo es utilizada por la oficina de asuntos académicos para conectarse al sistema académico de la universidad con mayor velocidad.

La organización Institucional se encuentra conformada por la Asamblea Universitaria, el Consejo Universitario, Rector, el Consejo Universitario, Rector y los Decanos de las Facultades.

Las facultades y/o carreras desde el año 1995, se encuentran organizadas como facultades, programas, educación a distancia y escuela de post grado

El plan de contingencia es una propuesta para el área de informática del local central de la UPLA que funciona en la ciudad de Huancayo, para lograr una mejora en los planes estratégicos de la institución.

1.2 PLANTEAMIENTO DEL PROBLEMA

1.2.1 Situación Problemática

Actualmente la Universidad Peruana Los Andes; tiene una población estudiantil que bordea los 20000 estudiantes, funciona en varias sedes y filiales. Jerárquicamente los sistemas de información como el Contable y Académico, entre otros se encuentra administrada por la Dirección de Informática de la UPLA y en conjunto con la Dirección Universitaria de Desarrollo Académico, y la Oficina de Economía. Es por ello la necesidad incrementar la seguridad en la información tanto Académico como Contable en caso se presente diferentes tipos de contingencias ya sean desastres naturales o producidos directamente por manos ajenas, es muy importante recalcar la necesidad de contar con un adecuado plan que pueda asegurar la continuidad de las operaciones en caso se presente una caída de sistema o pérdida parcial o total de la información.

El alcance del presente informe corresponde al local central de la Av. Giráldez Nº231 Huancayo. Toda la información se encuentra almacenada en los servidores que resguardan a los diferentes sistemas y la red LAN que poco a poco ha sido implementado y ampliado de acuerdo a la disponibilidad de recursos, por lo cual se llegó interconectar a todas las computadoras administrativas mediante conexión alámbrica de par trenzado CAT5, en su mayoría, y otras conexiones con CAT 6, principalmente para ingresar a Internet y en menor grado para compartir recursos, los equipos de conectividad switchs son de diferentes configuraciones y velocidades, observando que la prioridad era la de lograr la conectividad de acuerdo a los recursos existentes y disponibles sin respetar estándares o protocolos mínimos de seguridad. Ya interconectadas todas las computadoras podemos observar que la seguridad de la información se encuentra abierta a todos los usuarios, para lo cual necesitamos generar diferentes acciones de restricción y

protección de datos, copias de respaldo, restructuración del cableado, mantenimiento de los servidores, actualización de equipos, entre otros; que describiremos en los siguientes capítulos.

Es fundamental precisar que para obtener la Acreditación Universitaria la ANR estipula que toda institución debe contar con un adecuado plan de contingencia para sus sistemas informáticos asegurando confiabilidad y seguridad a nivel general en todos sus equipos.

1.2.2 Definición del problema

El problema es la falta de un plan de contingencia de sistemas para la Universidad Peruana Los Andes que puede ocasionar problemas directos tanto en el software como en el hardware, de presentarse un sismo, terremoto, incendio, inundación, virus, hackers, desencadenando en la pérdida total o parcial de la información, por tal motivo es recomendable contar con una herramienta a disposición del personal como lo ordenan los entes, leyes y normas donde especifique y evalué los peligros y riesgos, que describan las medidas de prevención y/o control con la que toda organización debería de contar.

Frente a este problema, el presente trabajo de investigación plantea una solución a través del diseño de un plan de contingencia de sistemas para la Universidad Peruana Los Andes para minimizar la probabilidad de ocurrencia de incidentes y riesgos, en tal sentido que la organización continúe con sus actividades de manera normal sin mayores pérdidas, de presentarse diferentes tipos de contingencias. Siendo indispensable contar con un adecuado plan que asegure la protección y recuperación de la información, contribuyendo así con la Acreditación Universitaria.

1.3 OBJETIVOS

1.31 OBJETIVO GENERAL

-Diseñar un plan de contingencia de sistemas informáticos para la Universidad Peruana Los Andes.

1.3.2 OBJETIVOS ESPECÍFICOS

- Determinar los activos a proteger en caso se presenten los eventos en los sistemas informáticos de la Universidad Peruana Los Andes.

-Definir los riesgos que pueden causar daño al Hardware y Software en los sistemas informáticos de la Universidad Peruana Los Andes.

- Establecer medidas de prevención y/o control que se requieren para minimizar los riesgos en los sistemas informáticos de la Universidad Peruana Los Andes.

1.4 LIMITACIONES

-La investigación se llevará a cabo en la Av. Giráldez N°231 - Local Central de la UPLA, en la ciudad de Huancayo.

-La propuesta se basará específicamente en los sistemas informáticos de la Oficina de Informática – Local Central de la UPLA.

-Los manuales y/o propuestas de Contingencia son sujetas a modificaciones en caso así lo requieran.

-La investigación plantea una propuesta económica para implantar un plan de contingencia el cuál puede variar en el tiempo por los factores de depreciación y valorización.

1.5 FACTIBILIDAD

1.5.1 Factibilidad Técnica

La factibilidad técnica estima recursos tecnológicos que tiene a disposición para ser considerada y aprovechada.

A continuación se muestra el software y hardware disponible para el rendimiento de la investigación.

a.-Software utilitario para el desarrollo del proyecto

Se muestra de forma detallada el software a utilizar en el desarrollo del proyecto, así como las herramientas de apoyo en la realización de cada una de las actividades que se ejecutarán para el desarrollo del sistema.

Cuadro Nº1: Requerimientos de Software para el desarrollo del proyecto de investigación.

Recursos de Software	Software	Descripción	Requerimientos de Hardware
Herramienta de administración de proyectos	Project Professional 2007 (Español)	Utilizado para la programación de tareas, recursos y creación de cronogramas.	Procesador: 700 MHz RAM: 512 MB HD: 1.5 GB
Suite de ofimática	Microsoft Office PYME 2007	Se usará para realizar procesamiento de texto, gráficos y presentaciones, entre otras actividades	Procesador: 500 MHz RAM: 256 MB HD: 1.5 GB
Software de edición de imágenes y animaciones	Adobe Fireworks CS5 trial version Adobe Flash CS5 trial version	Servirá para crear interfaces, imágenes y animaciones.	Procesador: Pentium 4 1.5Ghz RAM: 1 GB HD: 3.5 GB
Software generador de diagramas	Visio Professional 2007 (Español)	Estas herramientas serán utilizadas para la	Procesador: 500 MHz RAM: 256

	Poseidon for UML 8.0 trial version	creación de diagramas	MB HD: 1.5 GB
Sistema operativo	Windows XP Profesional SP3 (Español)	Sistema operativo que se utilizará para las máquinas de desarrollo.	Procesador: 800 MHz RAM: 128 MB HD: 3.0 GB
Navegador Web	Mozilla Firefox 3.6	Se utilizará como navegador web	Procesador: 500MHz RAM: 128 MB HD: 52 MB

Nota: fuente Elaboración Propia

a.-Hardware utilitario para el desarrollo del proyecto.

Análisis del equipo informático para el desarrollo y producción. En el cuadro siguiente se muestra una comparación entre el equipo que se necesita y el equipo disponible para el desarrollo del proyecto.

Cuadro Nº2: Requerimientos de hardware para el desarrollo del proyecto de investigación

Equipo disponible	Equipo requerido (básico)	Cumple requisito
Intel Celeron 1.8 GHz RAM: DDR2 1GB Monitor: CRT 15” HD: 80 GB CD-RW/DVD-R	Procesador: Pentium 4 1.5Ghz. RAM: 1 GB HD: 3.5 GB	APROBADO

Nota: fuente Elaboración Propia.

También se cuenta con Impresora Multifuncional, valido para las impresiones, escaneos y copias.

RESTRICCIONES:

En cuanto al equipo que la investigación propone dependerá de la institución la adquisición pero se presenta la propuesta al ser considerada en la Factibilidad Técnica.

1era OPCIÓN

Compra de Servidor Dell para implementar servidor redundante.

Es preciso acotar que se necesita 02 servidores adicionales para implementar el sistema automático para copia de seguridad que se realizaría en la Ciudad Universitaria de Chorrillos, esto no incluye costos de uso de Red. O VPN.

Cuadro Nº3: 1ra opción de Compra Sistema Operativo Servidor Redundante

Recursos de Software	Software	Descripción	Requerimientos de Hardware
s/1000.00 soles: 5 licencias cliente $/ 3.999 dólares: con 25 licencias cliente.	Windows Server 2008 Standard	Se usará para realizar respaldo de información del Local Central en la Ciudad Universitaria de Chorrillos	Arquitectura Servidor: Mínimo 2 procesadores tecnología Xeon.

Nota: fuente Elaboración Propia.

Cuadro Nº4: 1ra opción de Compra Sistema Operativo Servidor Redundante

Recursos de Hardware	Hardware	Descripción	Precio
Servidor Procesador Intel® Xeon® E5-2620 2.00GHz, 15M Cache, 7.2GT/s QPI, Turbo, 6C 95W 8GB RDIMM, 1600MT/s,	Microsoft Office PYME 2007	Se usará para realizar procesamiento de texto, gráficos y presentaciones, entre otras actividades	S/. 15,099

Low Volt, Dual Rank, x4 Data Width Disco Duro Hot Plug 500GB 7.2K RPM Near-Line SAS 6Gbps 2.5 pulgadas ProSupport Plus: 3 Year Next Business Day Onsite Service PowerEdge T620, Intel® Xeon® E-26XX Processors			

Nota: fuente Elaboración Propia.

Este costo no incluye el servicio de red (internet o VPN) para interconectar los servidores.

2da OPCIÓN

Servidor Dedicado x mes $289.00

289 x 12 = $3468 x año

3468 x 2,70 = 9363,6 soles x año aproximadamente.

Revisar: https://secure.iweb.com

Configuración del Servidor

CPU Intel® Xenon® E3-1230V3-4 Núcleos – 3.3GHz- H/T

RAM 16 GB DDR3

Disco duro 4 TB SATA3 + 4 TB SATA3 + RAID1 – SW

Ancho de banda 100 Mbps, 33.000GB Incluido, $0,00 x GB adicional

Puerto APC Puerto de inicio remoto APC

KVM/IP Comnutador KVM a pedido durante 24 horas

Sistema Operativo Windows 2012 R2 Estándar Edition EN

Panel de control Microsoft Web Platform Installer

Administración del Servidor Unmanaged

Monitoreo Monitoreo Ping

Software Idera Server Backup Manager – 1 Licencia de Servidor Físico

IP Hasta 5 direcciones IP en uso

1.5.2 Factibilidad Económica

En este apartado se determina si el sistema de información proporcionará beneficios mayores que los costos de su desarrollo y operación, además se detalla si es posible obtener los recursos económicos para el desarrollo del proyecto o si ya se cuenta con el hardware adecuado para la operación del sistema

BENEFICIOS INTANGIBLES

Según Kendall y Kendall, los beneficios intangibles se pueden definir como: "los que se acreditan a la organización mediante el uso del sistema de información y son difíciles de medir pero aun así son importantes". A continuación se presenta un listado de beneficios intangibles que se tendrán con la implementación del plan de contingencia de sistemas informáticos.

La copia de seguridad de los sistemas informáticos, representa millones de soles puesto que allí se almacenan las deudas y pensiones de los estudiantes, y las notas de los mismos en el sistema académico que constantemente lo solicitan los estudiantes para obtener sus certificado de estudios, etc.

Beneficios tangibles	**(S/año)**
Reducción del tiempo gastos por recuperación de datos	60000,00

Reducción del tiempo invertido para la elaboración de los informes consolidados a partir de documentos manuales	300000,00
Total	360000,00

-5 personas expertas en recuperación de datos (lo que queda), para saber matriculados, pensiones, etc. Con un sueldo de 3000 cada uno x mes.

-60000 soles x año.

-10 personas encargadas de reformular, reingresar datos manuales donde figuren actas de notas, etc. Para restaurar el sistema académico.

-Con un sueldo de 2500 soles x mes 300000 soles x año.

IMPORTANTE

No se incluyen los perjuicios de perdida de información, que esto puede representar millones de soles ya que en la base de datos se registran las cuentas por cobrar de muchos estudiantes, las deudas, etc.

BENEFICIOS TANGIBLES

Según el autor del libro Análisis y Diseño de Sistemas, define beneficios tangibles como: "Son las ventajas que se pueden medir en dólares que se acreditan a la organización mediante el uso del sistema de información". En la Tabla se presentan los beneficios tangibles asociados con el sistema a desarrollar.

Tipo	Monto(S/.)	Total (S/.)
COSTOS DE RECURSOS HUMANOS		
ASESORIA	500	
Sub Total		**500**
COSTOS DE RECURSOS TECNOLÓGICOS		
HARDWARE	2517	
SOFTWARE	1120	
Sub Total		**3637**
COSTOS FIJOS		
COSTOS FIJOS	624	

Sub Total		**624**
INSUMOS		
COSTOS EN MEDIOS DE ALMACENAMIENTO	68,75	
COSTOS DE RECURSOS CONSUMIBLES	433	
ALQUILER DE RETROPROYECTOR	54	
OTROS COSTOS	2936	
Sub Total		**3491,75**
SUBTOTAL		**8252,75**
IMPREVISTOS (10%)		**825,275**
TOTAL		**9078,025**

Nota: fuente Elaboración Propia

Restricción:

En caso la universidad desea adquirir la implementación se adjunta los precios promedio a enero -2014.

02 COSTOS DE RECURSOS TECNOLÓGICOS ADICIONAL		
HARDWARE (servidor)	30,018,00	
SOFTWARE	1000,00	
OTROS	2000,00	
Total	33,018,00	

Nota: fuente Elaboración Propia

Evaluación Costo – Beneficio

En caso la universidad decida invertir en el proyecto, se hallará el VAN del proyecto. En 5 años.

COSTO TOTAL		
COSTOS 01	33,018,00	
COSTOS 02	**9078,025**	
Total INVERSION	42096,025	
ANUALIDADES (Costo Mantenimiento)	800,00	
(Costos fijos)	9000,00	51896,025

Nota: fuente Elaboración Propia

Valor presente de los costos y beneficios: Se utilizará la siguiente fórmula del valor presente para lograr obtener, en un solo punto en el tiempo, las anualidades y los beneficios relacionados con el sistema propuesto y así poder sumarlos y compararlos:

$$Valor\ presente = A\left[\frac{(1+i)^n - 1}{i(1+i)^n}\right]$$

Donde:

A: Anualidad, se estima como una serie uniforme de costos o ingresos.

i : Tasa de interés.

N : Vida útil.

$51896{,}025\left[(1+10\%)_5 - 1/10\%(1+10\%)_5\right]$

Valor Presente Costos = 196 726,765

Valor presente de los beneficios= 1364 683,24

Beneficios – Costos = 1167 956,47

El monto representa un beneficio económico de 1 167 956,47 soles. Por lo que es muy rentable. Sin considerar las perdidas por datos dañados en la base de datos financieros.

1.5.3 Factibilidad Social

La factibilidad social va enmarcada, en la concientización de los operadores de los equipos de la UPLA y de los entes encargados haciendo que estos con los diferentes avances tecnológicos; implementen una nueva forma de recolectar, procesar y distribuir los diferentes procesos de los sistemas.

Este proyecto es factible socialmente ya su impacto seria de gran beneficio a los administrativos de la UPLA, docentes y alumnos a su vez traería las reducción de riesgos de equipos.

1.5.4 Factibilidad Operativa

Para determinar si el plan de contingencia a desarrollar será útil para la organización, es necesario descubrir el impacto que éste tendrá en el entorno institucional, y determinar si el desarrollo del sistema es factible operativamente.

¿El plan de contingencia operará luego de instalarse?

El sistema estará instalado y será ejecutado de preferencia en un servidor Espejo de la Ciudad Universitaria de Chorrillos.

¿El plan de contingencia es necesario?

Es de vital importancia para mejorar y reducir el riesgo, ya que en otras instituciones ya cuentan con este tipo de planes informáticos, el cuál puede servir para lograr disminuir perdidas de datos tangibles como intangibles.

¿Existe el recurso humano para operarlo?

Sí existen ingenieros expertos en el área de Informática capacitados en Tecnología de Servidores Windows.

1.5.5 Alternativas o Planteamiento de la Solución

Se tiene dos opciones de implantación de seguridad:

La primera a implementar es el Servidor Espejo en la ciudad Universidad de Chorrillos.

La segunda opción contratar un servidor dedicado con tecnología Windows para guardar la información directamente en el Servidor dedicado. El control del acceso de los usuarios con respecto a los equipos y la información deberá estar limitado para garantizar que los datos y la información que se obtenga sea veraz y presentada de acuerdo a las necesidades y niveles de usuario, para que esta información no sea manipulada o utilizada para fines distintos a las normas y ética establecida, ya que la información debe ser protegida y libre de cualquier divulgación. Además de esto se presentará información que apoye a la toma de decisiones basada en datos fidedignos del área de Informática.

Proteger a nivel general tanto el hardware como el software en la medida que sea posible frente a las diversas contingencias que se pudieran presentar. Con la obtención de información veraz y oportuna de los datos de seguridad se podrá tener la información en tiempo real y de manera segura.

1.6 JUSTIFICACIÓN

La universidad contará con una solución estructurada para mantener operativas las funciones que son fundamentales para la organización, cuando una contingencia afecte la infraestructura en TI instalada. Le ayudará a determinar acciones preventivas, reduciendo el grado de vulnerabilidad y exposición al riesgo, así como dimensionar el riesgo potencial y tomar decisiones rápidas ante fallas.

Toda institución está en riesgo ante cualquier fenómeno de la naturaleza que se presentan, afectando al personal administrativo, docentes y estudiantes, poniendo

en riesgo el patrimonio de la Universidad.

El personal administrativo utiliza los sistemas contable y académico en especial para emitir diferentes constancias que requiere el estudiante, desde una boleta de notas hasta una constancia de no adeudar.

La investigación planteó el diseño de un plan de contingencia de sistemas para la Universidad Peruana Los Andes propone tener un plan de acción antes, durante y después del incidente de seguridad ya sean propios de la naturaleza ò inducidos por agentes externos y así estar prevenidos ante cualquier contingencia que pueda generarse en la institución.

En la investigación se establecerá un procedimiento metodológico que servirá de referencia para futuros trabajos en el área.

CAPITULO II

MARCO TEÓRICO

2.1 Antecedentes

Ramírez Robayo Maritza, Londoño Rúa Edwin, Gómez Gómez Jairo (Bogotá, Colombia - 2012) "*Propuesta de Mejoramiento y Contingencia de Sistemas Informáticos en la Empresa T*" - UNIVERSIDAD EAN - ESPECIALIZACIÓN GERENCIA INFORMÁTICA.

Las instituciones son susceptibles de mejora en algunos de sus procesos de negocio o de apoyo. Conscientes de esto, tomamos la determinación de aprovechar nuestra experiencia y aplicar los conocimientos adquiridos durante la especialización para promover la mejora en el proceso de Tecnologías de Información y Comunicación (TIC) en una compañía de nuestro interés, que en adelante llamaremos "T", a través de la metodología de la consultoría, mediante el proceso de Contingencia de los Sistemas de Información.

De esta investigación tomaremos gran parte de la estructura en la implementación de los procesos para la Contingencia en la Universidad Peruana Los Andes

Granda Andrea (Cuenca, Ecuador - 2005),"*Diseño de un Plan de Contingencias de Tics para La Empresa Eléctrica Centrosur.*" para optar el grado de maestría en gerencia de sistema de información.

Los procedimientos manuales, si es que existen, sólo serían prácticos por un corto período. En caso de un desastre, la interrupción prolongada de los servicios de TI puede llevar a pérdidas financieras significativas, lo más graves que se puede perder la credibilidad del público o de los clientes y, como consecuencia, la imagen corporativa de la empresa lo que conllevaría a un fracaso total. ..

De esta investigación tomaremos la referencia el Plan de Contingencia de TI, para la empresa Eléctrica Centrosur.

Quiroz García Nestor (Mexico DF, Mexico - 2008),"*Sistema de Apoyo para el control y la Administración de un proceso de entrega de servicios informáticos*". para optar el grado de maestría en Ciencias en informática.

Se trata de la aplicación de Sistemas de para el control y administración de procesos de servicios informáticos.

De esta investigación tomaremos los procesos de entrega de servicios informáticos.

Salazar Villalobos Jorge(San José, Costa Rica - 2008), "*Guía para crear un Plan de recuperación en caso de desastre en el Sistema Informático del Centro de Datos de un grupo Financiero*".para optar el titulo de Master en Administración de Proyectos.

Esta investigación se proyecta en un Plan de recuperación en caso de desastre, que contempla a ITIL para su desarrollo.

De esta investigación tomaremos la referencia el Plan de Recuperación el cual contempla las buenas practicas ITIL.

Alfaro Paredes Emigdio (Lima, Perú - 2008),"*Metodología para La Auditoría Integral de la Gestión de la Tecnología de Información*". - Tesis para optar por el Título de Ingeniero Informático.

Aplica la Metodología de varias secciones como COBIT, ISO, ITIL para la auditoría de Tecnologías de Información.

De esta investigación tomaremos la referencia de Tecnologías referente a COBIT, ISO, ITIL.

Sub-Jefatura de Informática (Lima, Perú - 2011)," *Guía Práctica para el Desarrollo de Planes de Contingencia de Sistemas de Información*". - Instituto Nacional de Estadística e Informática.

Aplica Metodología para el desarrollo de una Guia de Plan de contingencia.

2.2 Bases Teóricas

2.2.1 Sistema Viable

Aquel que es capaz de mantener una existencia independiente. Es decir, posee su propia capacidad para sobrevivir, para responder a las condiciones cotidianas y para resolver eventos inesperados.

Modelo de Sistema

De acuerdo a la propuesto por el Dr. Stanffor Beer "es aquel que representa el meta-modelo que describe la auto-organización y la auto-construcción de cualquier sistema, biológico, social o mecánico".

El Enfoque de Sistemas Viables (VSA) se focaliza en el análisis de las relaciones entre entidades socio-económicas en busca de condiciones viables de interacción (Barile, 2000; Golinelli, 2000). Según el VSA, cada entidad (sea una empresa o un individuo) puede ser considerada como un sistema de muchas partes o estructuras (Parsons, 1971) formadas por un grupo de sub-componentes interrelacionados, con el objetivo de lograr una meta común.

2.2.2 Los Sistemas de Información

Un Sistema Informático (Laudon y Laudon 2008) utiliza ordenadores para almacenar los datos de una organización y ponerlos a disposición de su

personal. Pueden ser tan simples como en el que una persona tiene una computadora y le introduce datos, los datos pueden ser registros simples como ventas diarias, se produce una entrada por cada venta.

Los sistemas de información tienen muchas cosas en común. La mayoría de ellos están formados por personas, equipos y procedimientos. Al conjugar una serie de elementos como hombres y computadoras se hace imprescindible tomar medidas que nos permitan una continuidad en la operatividad de los sistemas para no ver afectados los objetivos de las mismas y no perder la inversión de costos y tiempo.

2.2.3 El modelo de Nolan/Gibson

El modelo de Nolan/Gibson trata de explicar las diferentes etapas de asimilación de las nuevas tecnologías por las organizaciones. Considera que las instituciones tienen una cartera de tecnologías de la información diferentes y que cada tecnología pasa a través de las siguientes fases:

Fase 1: Inversión/proyecto de la nueva tecnología. Esta fase se inicia con la decisión de invertir en una tecnología nueva de tratamiento de la información, que implica el desarrollo de algún proyecto y la formación inicial de las personas. Estos proyectos se caracterizan por su imprecisión presupuestaria, gran incertidumbre y por una gran dosis de aprendizaje.

Fase 2: Aprendizaje de la tecnología y adaptación. Se pretende aprender cómo adaptar la nueva tecnología a unas determinadas tareas más allá de las que se identificaron en la propuesta inicial. Los ciclos de vida del proyecto en esta fase se presentan difíciles para la planificación.

Fase 3: Racionalización/control de gestión. Esta fase trae el desarrollo de controles precisos que guían el diseño e implantación de los sistemas que utilizan estas tecnologías (para asegurar que las aplicaciones posteriores puedan hacerse con mayor eficacia en costes que las primeras).

Fase 4: Madurez/difusión generalizada de la nueva tecnología e integración. Esta fase final puede verse como un programa de difusión tecnológica. Aquí, las instituciones recogen la experiencia conseguida en una división operativa y extienden su empleo a toda la firma.

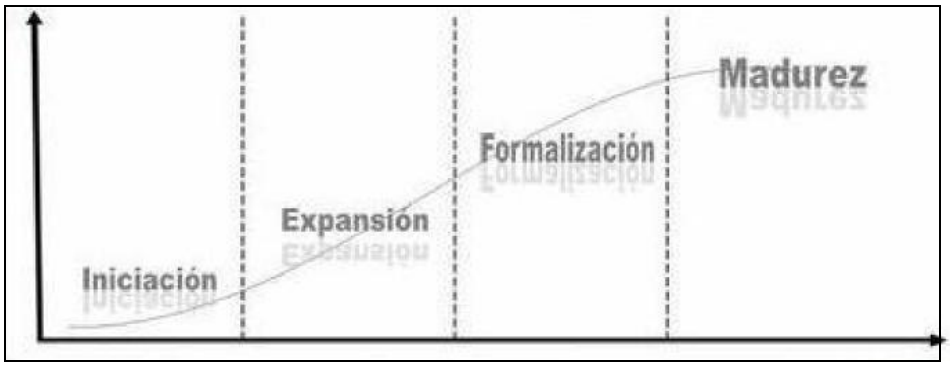


Grafico 1 Modelo de Nolan para la Implementación de tecnologías en las organizaciones

Descargado de **Fuente:** http://sistemas-de-informacion-gerencial.wikispaces.com/Modelo+de+etapas+de+Nolan

2.2.4 El modelo de Gartner

Gartner define cinco etapas en las que una organización de TI puede existir: Caótico, Reactiva, Proactivo, Servicio y Valor. En cada etapa la organización de TI se define por un conjunto de características. Estas características ilustran los tipos de actividades y comportamientos que se observan en la cultura de la organización.

Chaotic (Caótico)

- No existe documentación
- Infraestructura Impredecible
- No hay procesos comunes o workflow
- Cero monitoreo
- No funcional, no se efectúa planeación o presupuesto.

Reactive (Reactiva)

- Mínima documentación o nada.
- Naciente control de cambio.
- Incentivo a apagar incendios.
- Disponibilidad de solo monitoreo.
- Funcionando, pero sin planeación.

Proactive (Proactivo)

- Documentación de configuración.
- Documentación y aceptación de cambios de control.
- Se Incentiva la planeación sobre incendios.
- Monitoreo de disponibilidad y rendimiento, con predicción de pre-fallas.
- Funcionando, pero tecnología centrada en planeación/presupuesto.

Service (Servicio)

- Documentación de Configuración y SLA.
- Documentación y aceptación de cambios de control.
- Incentivo de servicio de calidad sobre tecnología.
- Monitoreo a nivel de Servicio.
- Funcionando, servicio alineado planeación/presupuesto.

Value (Valor)

- Configuración, SLA, y documentación vinculada al negocio.
- Documentación y aceptación de cambios de control, con vinculación al negocio.
- Incentivo al rendimiento del negocio y calidad de servicio.
- Monitoreo a nivel de Servicio y de Negocio.
- Funcionando, negocio alineado con la planeación/presupuesto.

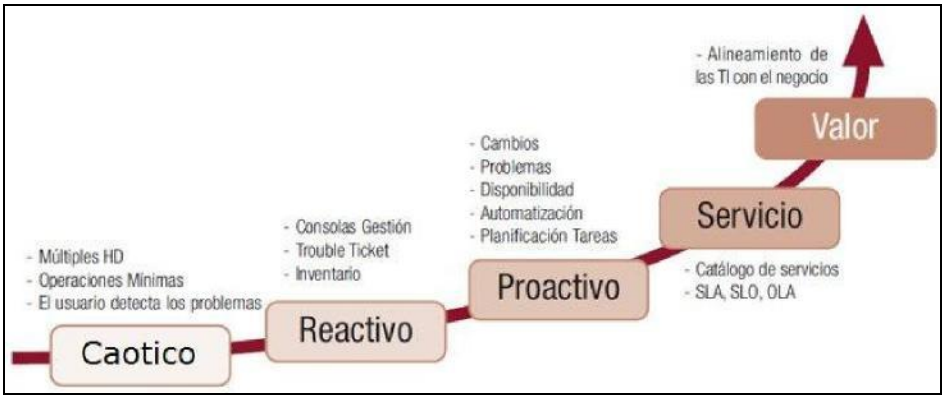


Grafico 2 Estado de madurez de organización en TI

Fuente: AbastConsulting. Gestión de TI (ITIL, ISO 20000, CobiT).

2.2.5 El modelo de Donovan

Este modelo, en vez de tomar como variable la inversión realizada en informática, toma como referencia la evolución desde la informática centralizada hacia la descentralizada.

Donovan analiza el proceso tomando tres variables que son:

- El grado en que una organización distribuye el hardware desde su sede central a sus oficinas remotas.
- El grado en que se descentralizan las decisiones referentes a la informática.
- El grado en que se descentraliza la facultad de desarrollar con autonomía nuevas aplicaciones.

Según el valor de estas variables se tienen los siguientes tipos de organizaciones:

- Dinosaurios. Organizaciones con un gran ordenador central, donde las decisiones se toman en la sede central, y todos los programas se gestan en la misma.
- Gran Hermano. Lo único descentralizado es el hardware. Las decisiones y los programas se siguen adoptando y desarrollando en la sede central.

- Mano amiga. Se descentraliza el hardware y las decisiones, permitiendo a los usuarios formar la parte activa. Sin embargo, algunos usuarios avanzados construyen sus propias aplicaciones, con lo que información se dispersa.
- Perro vigilante. Se ha descentralizado el software y el desarrollo de software, pero las decisiones son tomadas desde un organismo central, lo que incluye la adopción de estándares, normas de desarrollo, etc.
- Red o malla. Los tres puntos están descentralizados.

Según Donovan, todas las organizaciones tienden hacia el modelo de malla.

2.2.6 Qué es un Plan de Contingencia

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

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

2.2.7 El Plan de Contingencia Informática

Es un instrumento de gestión que contiene las medidas técnicas, humanas y organizativas para que una organización garantice la continuidad de la operación en caso de cualquier incidente o situación que impida la operación habitual de la plataforma informática. Esta herramienta requiere la identificación de aquellos sistemas de información y/o recursos de TIC’s

críticos que son susceptibles de riesgo de deterioro, violación o pérdida, ya sea por causa física o humana, con el propósito de estructurar y ejecutar procedimientos y asignar responsabilidades que salvaguarden la información y permitan su recuperación garantizando la confidencialidad, integridad y disponibilidad de ésta, en el menor tiempo posible, a unos costos razonables y minimizando las pérdidas.

Algunas instituciones emprenden el gran proyecto de la implementación de un SGSI (Sistema de Gestión de Seguridad de la Información) generalmente apoyándose en la norma ISO 27001 y en la guía de buenas prácticas ISO 27002 que son un conjunto de estándares que proporcionan un marco de gestión de la seguridad de la información. Estas sirven como guía metodológica para diseñar los controles necesarios para proteger los activos de información, basada en el análisis de riesgos, buscando implementar, establecer, operar, monitorear, revisar, mantener y mejorar la seguridad de la información en cualquier institución. Esta decisión requiere un fuerte compromiso de la alta dirección de la institución y demanda una alta asignación de recursos.

Consideraciones de implementación

Toda organización debe planear y desarrollar un Plan de Contingencia cuando todavía no es necesario, es decir, antes de que los eventos ocurran. La planificación aumenta la habilidad y capacidad de la organización para "sobrevivir" y mantener las operaciones en caso de incidentes o desastres, sirviendo como punto de partida y aportando una guía de acciones que se deben ejecutar para una adecuada respuesta en caso de emergencia.

Etapas para elaborar un Plan de Contingencia

Las etapas básicas para elaborar el Plan de Contingencia informática de una organización son:

Análisis y valoración de riesgos

En primer lugar se debe realizar un análisis del impacto que causaría en la organización una falla e incidente en la plataforma tecnológica o un desastre

natural. Se identifican los procesos críticos y las consecuencias que se presentan en caso de no estar en funcionamiento. El primer componente del Plan de Contingencia debe ser una descripción del servicio y el riesgo para ese servicio. También es recomendable determinar el costo que representa para la organización experimentar estos incidentes.

La evaluación del nivel de riesgo de la información sirve para:

- Determinar la relación costo/beneficio y tener argumentos para decidir entre aceptar la pérdida de información o invertir en implementar sistemas de contingencia.
- Clasificar los componentes de la plataforma tecnológica en términos de riesgo (alto, medio, bajo) e identificar aquellos que representen mayor riesgo.
- Cuantificar el impacto en el caso de suspensión del servicio.
- Determinar la información que pueda representar pérdidas considerables para la organización o que impida una adecuada toma de decisiones.

Este análisis de posibles riesgos permitirá identificar las fortalezas, oportunidades, debilidades y amenazas, y profundizar en las medidas que se deben tomar para gestionarlas, de manera que en caso de incidentes se pueda recuperar la operatividad en el menor tiempo posible.

Jerarquización de las aplicaciones

Es indispensable definir con anticipación cuáles son las aplicaciones primordiales para la organización. Teniendo en cuenta que para cada departamento o área funcional de la organización, su operación es la más importante, la jerarquización debe estar avalada y respaldada por un comité de contingencia o por la alta dirección, procurando objetividad y minimizando el conflicto de intereses.

El plan debe incluir una lista de los sistemas, aplicaciones y prioridades, así como identificar aquellos elementos informáticos (hardware, software base, software de aplicaciones, telecomunicaciones) que puedan ser críticos ante

cualquier incidente o desastre, jerarquizándolos de acuerdo al orden de importancia dentro de la organización. Se deben incluir los problemas generados por ausencia de fuentes de energía, mala administración o uso de dispositivos de backup o cualquier otro daño de origen físico que pueda provocar la pérdida masiva de información.

Establecimiento de requerimientos de recuperación

Esta etapa busca determinar lo que se debe hacer para lograr una óptima solución, especificando las funciones con base en el estado actual de la organización. Es necesario realizar las siguientes actividades: profundizar la definición del problema, analizar áreas o componentes problema, comunicaciones y sus flujos, formulación demedidas de seguridad necesarias dependiendo del nivel de seguridad requerido, justificación del costo de implantar las medidas de seguridad, análisis y evaluación del plan de contingencia actual (si lo hay), determinar los recursos humanos, técnicos y económicos necesarios para desarrollar el plan, definir un tiempo prudente y viable para lograr que el sistema se libere y pueda entrar en operación.

Ejecución

Una vez finalizado el plan, es conveniente elaborar un informe final con los resultados de su ejecución cuyas conclusiones pueden servir para mejorar éste ante eventualidades que se puedan presentar con posterioridad. En esta etapa se debe tener presente que el plan de contingencia no busca resolver la causa del problema, sino asegurar la continuidad de las tareas críticas de la institución.

Para garantizar el éxito del plan de contingencia es conveniente que en su elaboración participen la alta dirección de la organización, personal técnico y operativo de los procesos y los usuarios, ya que los recursos necesarios para la puesta en marcha del plan, demandan mucho esfuerzo técnico, económico y organizacional y se requiere observar el sistema, la plataforma tecnológica y la operación de la institución desde diversos puntos de vista.

Pruebas y simulaciones

Es necesario definir y generar simulaciones que permitan poner a prueba el plan de contingencia, el personal y los recursos necesarios para su realización. El propósito es intentar valorar el impacto real de un problema dentro de los escenarios establecidos como posibles. En caso de que los resultados obtenidos difieran de los esperados, se debe analizar si el resultado varió por un problema en el ambiente de pruebas del plan, en cuyo caso se podrá corregir el problema y repetir la prueba, o si el plan tiene vacíos o carencias en su definición. Es indispensable la capacitación y participación del equipo de contingencia para detectar y evidenciar posibles carencias del plan, así como una buena documentación para facilitar la ejecución de las pruebas.

Documentación

Aunque esta etapa demanda un esfuerzo significativo, ayudará a comprender otros aspectos del sistema y puede ser apoyo para la institución en caso de ocurrir un incidente o desastre. Debe incluir los procedimientos detallados que expliquen el paso a paso de las tareas de instalación y recuperación necesarias, procurando que sean entendibles y fáciles de seguir.

La documentación del plan de contingencia se debe desarrollar a medida que se avanza en la definición del plan y desde el mismo momento que nace, pasando por todas sus etapas; en ningún caso se debe dejar de lado esta labor, esperando a realizarla cuando se concluyan las pruebas y su difusión, pues se correría el riesgo de que la documentación resulte inexacta, difusa y que cualquier aspecto importante se pase por alto.

Difusión y mantenimiento

Con el plan de contingencia probado y documentado, surge la necesidad de su difusión y capacitación entre las personas encargadas de llevarlo a cabo. El mantenimiento del plan comienza con una revisión del plan existente y se examina en su totalidad realizando los cambios en la información que pudo haber ocasionado una variación en el sistema y realizando los cambios que

sean necesarios. La generación del plan no muere aquí, por el contrario es el inicio de un ciclo de revisión, ajuste y divulgación constante que suministre a la organización la tranquilidad de estar preparada y lista ante cualquier incidente.

2.2.8 Base de Datos

Una base de datos es un conjunto de datos organizados, entre los cuales existe una correlación y que además, están almacenados con criterios independientes de los programas que los utilizan.

También puede definirse, como un conjunto de archivos interrelacionados que es creado y manejado por un Sistema de Gestión o de Administración de Base de Datos (Data Base Management System - DBMS).

Las características que presenta un DBMS son las siguientes:

- Brinda seguridad e integridad a los datos.
- Provee lenguajes de consulta (interactivo).
- Provee una manera de introducir y editar datos en forma interactiva.
- Existe independencia de los datos, es decir, que los detalles de la organización de los datos no necesitan incorporarse a cada programa de aplicación.

2.3 METODOLOGÍAS

2.3.1 Norma ISO 27001, Guía de buenas prácticas ISO 27002 y necesidad del Plan de Contingencia

La norma ISO 27001 es un estándar internacional diseñado por la ISO/IEC (Organización Internacional para la Estandarización y la Comisión Electrotécnica Internacional, que busca proporcionar un modelo para establecer, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). El diseño e implementación

de un SGSI debe corresponder a las necesidades de la organización, de manera que se proporcionen los controles de seguridad que protejan los activos de información y que aporten confianza a las partes interesadas.

La Norma ISO 27001 plantea el modelo PDCA (Plan – Do – Check – Act), en español, PHVA (Planear – Hacer- Verificar – Actuar), que las organizaciones deben seguir como metodología para gestionar el SGSI. De esta manera la norma ISO 27001 define que la organización debe:

Planear

- Definir el alcance y los límites del SGSI en términos de las características del negocio, la organización, su ubicación, activos, tecnología.
- Definir una política SGSI en términos de las características del negocio, la organización, su ubicación, activos, tecnología.
- Definir el enfoque de valoración del riesgo de la organización
- Identificar los riesgos
- Analizar y evaluar los riesgos
- Identificar y evaluar las opciones para el tratamiento de los riesgos
- Seleccionar objetivos de control y controles para el tratamiento de los riesgos - Obtener la aprobación de la Gerencia para los riesgos residuales propuestos - Obtener la autorización de la Gerencia para implementar y operar el SGSI - Preparar un enunciado de aplicabilidad

Hacer

- Formular un plan de tratamiento de riesgo que identifique la acción gerencial apropiada, los recursos, las responsabilidades y prioridades para manejar los riesgos de la seguridad de información.
- Implementar el plan de tratamiento de riesgo para lograr los objetivos de control, incluyendo asignación de roles y responsabilidades
- Implementar los controles seleccionados para satisfacer los objetivos de control
- Definir los mecanismos para medir la efectividad de los controles
- Implementar programas de capacitación y conocimiento
- Manejar las operaciones del SGSI

- Manejar recursos para el SGSI
- Implementar procedimientos y controles capaces de permitir detectar y responder oportunamente a incidentes de seguridad

Verificar

- Ejecutar procedimientos de monitoreo y revisión para detectar errores en resultados de procesamiento, identificar incidentes, eventos y violaciones de seguridad, determinar la efectividad de las acciones tomadas para resolver estas fallas.
- Realizar revisiones periódicas de la efectividad del SGSI y de los controles de seguridad.
- Medir efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad
- Revisar las evaluaciones del riesgo, nivel de riesgo residual, y riesgo aceptable tomando en cuenta cambios en la organización, la tecnología, los objetivos y proceso comercial, nuevas amenazas, efectividad de los controles, y regulaciones, leyes, contratos.
- Realizar auditorias internas al SGSI
- Realizar una revisión gerencial del SGSI
- Actualizar los planes de seguridad teniendo en cuenta los resultados de las actividades de monitoreo y evaluación
- Registrar acciones y eventos que podrían tener impacto en la efectividad o desempeño del SGSI.

Actuar

- Implementar las mejoras identificadas en el SGSI
- Tomar acciones preventivas y correctivas
- Aplicar lecciones aprendidas de las experiencias de seguridad de otras organizaciones y de la organización misma.
- Comunicar resultados y acciones a todas las partes interesadas.
- Asegurar que las mejoras logren los objetivos.

Por su parte la ISO 27002:2005[16] es una guía de buenas prácticas de seguridad de la información que presenta los objetivos de seguridad que sería ideal

alcanzar, una extensa serie de controles a tener en cuenta para cada objetivo y un conjunto de sugerencias o recomendaciones para cada control. Esta guía comprende 11 dominios, 39 objetivos de control y 133 controles.

Los 11 dominios son:

- Política de seguridad
- Aspectos organizativos de la seguridad de la información
- Gestión de Activos
- Seguridad ligada a los Recursos Humanos
- Seguridad Física y del entorno
- Gestión de comunicaciones y operaciones
- Control de acceso
- Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
- Gestión de Incidentes en la Seguridad de la Información
- Gestión de la Continuidad del Negocio
- Cumplimiento

El propósito de la norma 27001 es que la organización determine cuáles son sus requerimientos, defina un alcance de lo que desea implementar y aborde los controles necesarios para satisfacer sus necesidades de seguridad. En ningún caso la guía de buenas prácticas ISO 27002 debe considerarse como un listado de controles que la organización está obligada a alcanzar para lograr la estandarización, y por ende la certificación ISO 27001.

Los planes de contingencia surgen entonces a partir de la necesidad de las organizaciones de mantener la continuidad de los sistemas de información frente a eventos o incidentes, atendiendo los dominios de Gestión de incidentes en la seguridad de la información y la Gestión de la Continuidad del negocio.

2.3.2 Modelo de Gobierno TI Basado en COBIT

Creado por la Asociación para la Auditoría y Control de Sistemas de Información, (ISACA, en inglés: Information Systems Audit and Control Association), y el Instituto de Administración de las Tecnologías de la Información (ITGI, en inglés: IT Governance Institute) en 1992.

Los Objetivos de Control para la Información y la Tecnología relacionada (COBIT por sus siglas en inglés: Control Objectives for Information and related Technology) brindan buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. Las buenas prácticas de COBIT representan el consenso de los expertos. Están enfocadas fuertemente en el control y menos en la ejecución. Estas prácticas ayudarán a optimizar las inversiones habilitadas por TI, asegurarán la entrega del servicio y brindarán una medida contra la cual juzgar cuando las cosas no vayan bien.

Para que TI tenga éxito en satisfacer los requerimientos del negocio, la dirección debe implementar un sistema de control interno o un marco de trabajo. El marco de trabajo de control COBIT contribuye a estas necesidades de la siguiente manera:

- Estableciendo un vínculo con los requerimientos del negocio.
- Organizando las actividades de TI en un modelo de procesos generalmente aceptado.
- Identificando los principales recursos de TI a ser utilizados.
- Definiendo los objetivos de control gerenciales a ser considerados.

La orientación al negocio que enfoca COBIT consiste en alinear las metas de negocio con las metas de TI, brindando métricas y modelos de madurez para medir sus logros, e identificando las responsabilidades asociadas de los dueños de los procesos de negocio y de TI.

El enfoque hacia procesos de COBIT se ilustra con un modelo de procesos, el cual subdivide TI en 34 procesos de acuerdo a las áreas de responsabilidad de planear, construir, ejecutar y monitorear, ofreciendo una visión de punta a punta de la TI. Los conceptos de arquitectura institucional ayudan a identificar aquellos recursos esenciales para el éxito de los procesos, es decir, aplicaciones, información, infraestructura y personas.

Grafico 3 Áreas de enfoque del gobierno de TI

Fuente: http://cafrancavilla.wordpress.com/tag/problemas-it/

- **Alineación Estratégica:** se enfoca en garantizar la alineación entre los planes de negocio y de TI, en definir, mantener y validar la propuesta de valor de TI, y en alinear las operaciones de TI con las operaciones de la institución.
- **Entrega de Valor:** se refiere a ejecutar la propuesta de valor a todo lo largo del ciclo de entrega, asegurando que TI genere los beneficios prometidos en la estrategia, concentrándose en optimizar los costos y en brindar el valor intrínseco de la TI.
- **Administración de Recursos:** se trata de la inversión óptima, así como la administración adecuada de los recursos críticos de TI: aplicaciones, información, infraestructura y personas. Los temas claves se refieren a la optimización de conocimiento y de infraestructura.
- **Administración de Riesgos:** requiere conciencia de los riesgos por parte de los altos ejecutivos de la institución, un claro entendimiento del apetito de riesgo que tiene la institución, comprender los requerimientos de cumplimiento, transparencia de los riesgos significativos para la institución, y la inclusión de las responsabilidades de administración de riesgos dentro de la organización.

- **Medición del Desempeño:** rastrea y monitorea la estrategia de implementación, la terminación del proyecto, el uso de los recursos, el desempeño de los procesos y la entrega del servicio, con el uso, por ejemplo, de balanced scorecards que traducen la estrategia en acción para lograr las metas medibles más allá del registro convencional.

2.3.3 Estándar para la Gestión de Servicios Informáticos ITIL

La Biblioteca de Infraestructura de Tecnologías de la Información (ITIL) fue desarrollada en 1980 por la CCTA (Agencia Central de Telecomunicaciones), buscando estandarizar la operación de todos los proveedores de tecnología (internos y externos) para el gobierno del Reino Unido. El resultado fue una guía que esta formada por una serie de "Mejores prácticas" procedentes de todo tipo de suministradores de servicios de TI.

ITIL especifica un método sistemático que garantiza la calidad de los servicios de TI. Ofrece una descripción detallada de los procesos mas importantes en una organización de TI, incluyendo listas de verificación para tareas, procedimientos y responsabilidades que pueden servir como base para adaptarse a las necesidades de cada organización.

ITIL pertenece a la OGC (Oficina de comercio gubernamental), entidad que en 2001 absorbió a la CCTA, pero es de libre utilización.

En junio de 2007, la OGC público la última actualización a ITIL, conocida comúnmente como ITIL V3. Esta consta de 5 libros basados en el ciclo de vida del servicio: Estrategia del Servicio, Diseño del Servicio, Transición del Servicio, Operación del Servicio, Mejora Continua del Servicio.

A lo largo de todo el ciclo de los productos TI, la fase de operaciones alcanza cerca del 70% al 80% del total del tiempo y de los costos, el resto se invierte en el desarrollo de productos o servicios. De esta manera, los procesos eficaces y eficientes de la Gestión de Servicios TI se convierten en esenciales para el éxito de los departamentos de TI. Esto se aplica a cualquier tipo de organización, grande o pequeña, pública o privada, con servicios TI

centralizados o descentralizados, con servicios TI internos o suministrados por terceros. En todos los casos, el servicio debe ser fiable, consistente, de alta calidad, y de costo aceptable.

El ciclo de vida ITIL

El ciclo de vida ITIL, consta de cinco fases, cada una con sus respectivas funciones y procesos, que indican la manera de implementar las mejores prácticas, con el fin de obtener un servicio TI de alta calidad. Estas fases son:[19]

- **Estrategia del servicio:** esta fase del ciclo de vida ITIL, define directrices para el diseño, desarrollo e implantación de la gestión del servicio como un recurso estratégico. Es fundamental en el contexto de los procesos que se siguen en las otras fases del ciclo de vida del servicio. Su principal función es mejorar la sincronización entre TI y las estrategias institucionales.
- **Diseño del servicio:** se ocupa del diseño y desarrollo de servicios y sus procesos relacionados. Afecta tanto a los nuevos servicios, como a los que han sido modificados. Entre sus objetivos están: contribuir con los objetivos del negocio, ahorrar (en lo posible) tiempo y dinero, minimizar riesgos y evaluar y mejorar la eficiencia de los servicio de TI.
- **Transición del servicio:** convierte las especificaciones de la fase anterior, en un servicio nuevo o modificado, reduciendo las variaciones en el rendimiento y los errores conocidos y garantizando que este cumple con los requisitos del negocio. Para lograr esto, se vale de los siguientes pasos: planificación y preparación, construcción y pruebas, pilotos, y planificación y preparación del despliegue.
- **Operación del servicio:** tiene como objetivos la coordinación y ejecución de las actividades y procesos necesarios para entregar y gestionar servicios para usuarios y clientes con el nivel especificado. También tiene la responsabilidad de gestionar la tecnología necesaria para la prestación y el soporte de los servicios.

- **Mejora continúa del servicio:** se centra en las actividades que mejoran la calidad del servicio. Para esto utiliza el ciclo "Planear, hacer, verificar actuar", que establece una fase de consolidación para cada mejora, con el fin de incorporar nuevos procedimientos en la organización. Las medidas y análisis son muy importantes, ya que permiten identificar los servicios rentables y aquellos que se pueden mejorar.

Grafico 4 Ciclo de vida ITIL

Fuente: Secure and IT proyectos. ITIL / ISO 20000.

2.4 ELECCIÓN DE METODOLOGÍA DE SOLUCIÓN

Todo trabajo de investigación debe estar enmarcado dentro de una metodología, es decir, una serie de pasos que guíen el desarrollo del proyecto, a tal efecto, después de la revisión de varias de ellas se ha decidido aplicar como metodología la norma ISO 27001 y el ISO 27002 (la guía de buenas prácticas).

Planear

Aquí se define el alcance y los límites del SGSI en términos de las características del negocio, la organización, su ubicación, activos, tecnología.

Se Identificar los riesgos, se analiza y evaluar los riesgos.

Hacer

En esta etapa se formula un plan de tratamiento de riesgo que identifique la acción gerencial apropiada, los recursos, las responsabilidades y prioridades para manejar los riesgos de la seguridad de información.

Verificar

Se ejecuta procedimientos de monitoreo y revisión para detectar errores en resultados de procesamiento, identificar incidentes, eventos y violaciones de seguridad, determinar la efectividad de las acciones tomadas para resolver estas fallas.

Actuar

Se implementa las mejoras identificadas en el SGSI y se toma las acciones preventivas y correctivas.

El propósito de la norma 27001 es que la organización determine cuáles son sus requerimientos.

Los planes de contingencia surgen entonces a partir de la necesidad de contar con un sistema de seguridad de información fuera del local central de la UPLA, para proteger y disminuir el riesgo de alguna contingencia que puede ocurrir.

PRESENTACIÒN DE RESULTADOS

CAPITULO III

IDENTIFICACIÓN DEL SISTEMA VIABLE

Dentro de la Universidad Peruana Los Andes el sistema viable en estudio es la Oficina Universitaria de Informática donde se almacena los sistemas Académico y Contable, La organización está constituida por componentes que tienen roles, actividades y objetivos específicos que son llevados adelante en un entorno de normas, reglas y limitaciones. Los sistemas emergen de las estructuras mediante la transformación de las relaciones en interacciones dinámicas con los sub-sistemas (oficinas).

3.1 Diagnóstico de la Universidad basado en el Enfoque de Sistema Viable

Organización: "**UNIVERSIDAD PERUANA LOS ANDES**"

Componentes del Modelo

Sistema 1 – Implementación: Este modelo y las estrategias se deben desarrollar en los procesos misionales, en conjunto con los colaboradores. Se espera poder incluir las sugerencias de estos.

Sistema 2 – Coordinación: Se utilizará la gestión documental para garantizar la estandarización de los documentos que se generen a partir del modelo, junto con un sistema en línea. Se propondrá crear redes de conocimiento con reuniones periódicas.

Sistema 3* – Monitoreo: Se generarán indicadores de gestión alineados con el Plan Estratégico y el Modelo de Desarrollo y Desempeño, los cuales se aplicarán en las actividades, asimismo se plantearán auditorías de conocimiento para asegurar la continuidad y el mejoramiento del modelo.

Sistema 3 – Control: La información que se genere a partir del modelo, se asegurará en un procedimiento, lo aportará a la estrategia en el largo plazo.

Sistema 4 – Inteligencia: Se analizará la coherencia entre el modelo, para asegurar la viabilidad del proyecto.

Sistema 5 – Política: Se utilizarán las directrices establecidas como base para establecer las estrategias de los demás sistemas.

Este modelo presenta estos cinco sistemas:

Sistema 1. Implementación
Sistema 2. Regulación y coordinación
Sistema 3. Control

Sistema 4. Planeación

Sistema 5. Definición de políticas.

Todos relacionados entre sí y con las mismas características internas repetidas, es decir, que dentro de cada uno de estos sistemas existen los mismos 5 sistemas pero más pequeños.

Todo esto alude a la forma fractal con la que cuenta la naturaleza para mantenerse en el tiempo.

CONTEXTO PROBLEMÁTICO DE LA UNIVERSIDAD Las diferentes dependencias de la Universidad Peruana Los Andes (UPLA), se desenvuelven a través de una estructura orgánica "piramidal", que es una combinación del modelo lineal y el modelo funcional, que generan centralización de poder en la toma de decisiones, los diferentes órganos y unidades orgánicas desarrollan sus actividades en forma independiente y muchas de ellas duplicando funciones, ejecutando tareas innecesarias y omitiendo las que si son indispensables.

3.2 Diagnóstico

Fase 1. IDENTIFICACIÓN DEL SISTEMA BAJO ESTUDIO: qué sistema (sistemas más amplios, ambientes) pertenece el sistema focalizado. Qué proceso cumple el sistema focalizado. El sistema focalizado previo es el subsistema de Informática en el cual está enfocada nuestra investigación.

Fase 2. DIAGNÓSTICO DE PROCESOS BASADO EN EL ENFOQUE DE SISTEMA VIABLE: Existen varios subsistemas independientes y relacionados con otros, para nuestro caso debemos concentrarnos en el Área de Informática del Local Central, que vendría ser como el cerebro de la Universidad, donde se desea implementar el plan de Contingencia.

EL SISTEMA 1: LAS OPERACIONES

Es necesario identificar el entorno de los procesos, estas son las entradas y salidas respectivas. Así también las gerencias representativas para cada uno de ellos. Es necesario identificar las porciones del entorno sobre las cuales las unidades operacionales trabajan.

EL SISTEMA 2: COORDINACIÓN El sistema 2 es el encargado de proporcionar estabilidad entre los procesos misionales, mediante coordinaciones, acuerdos, etc.

EL SISTEMA 3 Y 3*: COHESIÓN Y MONITOREO Se encargan de optimizar la labor de los procesos misionales a través de mecanismos, controles y recursos necesarios. Actualmente viene dado por procesos de Soporte con oficinas como: Asesoría Legal, Informática, Economía.

EL SISTEMA 4: INTELIGENCIA Esta dado por la oficina de Informática quienes almacenan los procesos económicos más importantes por salvaguardar la información de la universidad.

EL SISTEMA 5: POLÍTICA Encargado de supervisar a la organización entera. Por tanto se debe tener cuidado al momento de estudiarlo. La Asamblea Universitaria en conjunto con el rector son los responsables de brindar las políticas generales, a través de normas y lineamientos.

3.3 Antecedente de Diagnóstico Sistémico

La Oficina de Informática de la Universidad Peruana Los Andes organizó un curso aplicado al estudio sistémico de organizaciones y comprendió el fundamento teórico de los modelos computacionales y SocLab que es la herramienta que permite modelar y siendo este un laboratorio virtual es decir un meta modelo computacional

multiagente que puede usarse para el estudio de relaciones y poder en las organizaciones sociales, indicó el docente Mag. Jowel Cabrera Padilla.

El fundamento teórico de dicho meta modelo es la sociología de la acción organizada (SOA en inglés) desarrollada por Crozier y Friedberg (también se llama análisis estratégico). De esta manera el SOA busca develar el funcionamiento (sistémico) de una organización partiendo más allá de sus estructuras formales (reglas y normas que la codifican), tomando en cuenta también la dinámica de poder que se da entre los distintos actores organizacionales.

El evento contó con la presencia del Dr. Hernán López Garay (Venezuela) Ph. D. en Teoría de Sistemas, Planeamiento y Administración de la Wharton School, Universidad de Pennsylvania, EE.UU., M.A. en Sistemas Gerenciales por la Universidad de Lancaster, Inglaterra. M.Sc. en Ingeniería de Sistemas por el Instituto de Tecnología, Cleveland, Ohio. Ingeniero Eléctrico y de Sistemas de Control por la Universidad de Los Andes, Colombia.

Profesor del Programa de Graduados en Sistemología Interpretativa, Universidad de los Andes, Venezuela. Miembro fundador del Departamento de Sistemología Interpretativa y Coordinador del Programa Doctoral en Sistemología Interpretativa, Universidad de los Andes, Venezuela. Expositor en la Escuela de Sistemas, Universidad de los Andes. Ha sido consultor en Planeamiento y Desarrollo Organizacional para el Rector de la Universidad de Los Andes, Venezuela.

3.3.1 Organigrama Relacional de la Oficina Universitaria de Informática

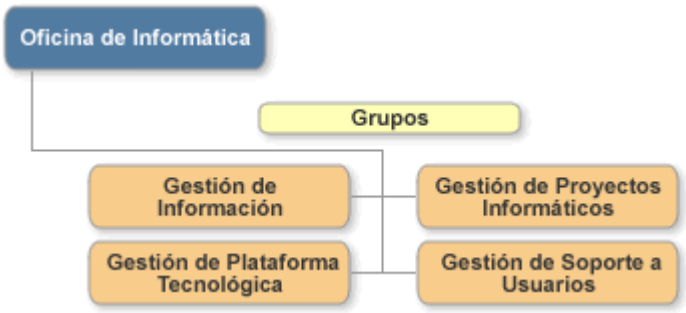


Grafico 5 Organigrama Relacional de Informática

3.3.2 La Gestión de Proyectos

En los proyectos informáticos la gestión ha demostrado a través de la experiencia que a lo largo de su ciclo de desarrollo es necesario estudiar las posibles perturbaciones y su riesgo, y poder así planificar los proyectos y gestionarlos teniendo en cuenta dicho riesgo Ashton J. (2006) .

Los Directores de Proyectos han de tomar decisiones similares cuando manejan los riesgos que amenazan el éxito de su proyecto. El riesgo está siempre presente por definición en un proyecto, pues toda realización futura implica cierto grado de incertidumbre.

La Identificación de los Riesgos es el aspecto más importante del estudio, pues los riesgos no identificados son los que causan los problemas del proyecto. Otras vías para identificar posibles riesgos suelen ser: los planes de producción y evaluación del proyecto; las actividades de control de calidad; las auditorías del proyecto y de su calidad; las propias reuniones del equipo del proyecto para ver su progreso; las sesiones de evaluación del cambio e incluso las de generación de ideas.

Los proyectos son sistemas integrados por subsistemas interrelacionados los cuales se ven afectados por los niveles de la toma de decisión administrativa que inciden horizontalmente sobre el sistema organizacional. Los proyectos como sistemas son importantes para el cumplimiento de metas y objetivos específicos, utilizando diversos recursos como el factor humano.

3.3.3 Activos Intangibles

Este capítulo tiene como objetivo determinar que son los activos intangibles, cómo se definen y cómo pueden clasificarse. En el mismo, analizaremos la naturaleza de los activos intangibles y su relevancia en la utilidad de la información contable, en

la valoración de la empresa, en el desarrollo de ventajas competitivas y en la formación de precios de mercado.

El valor de las empresas en la actualidad, tanto en el sector industrial como en el de comercio o servicios, no reside solamente en sus instalaciones, maquinaria o edificios, sino en aspectos inmateriales como la capacidad de desarrollar relaciones estables con sus clientes y conseguir su fidelización, su capacidad para innovar e introducir nuevos productos o servicios al mercado, o la competencia técnica y motivación de su personal. Por ello, es que se puede afirmar que el valor de las empresas en la actualidad viene dado por el conjunto de sus activos tangibles y el de sus intangibles.

En los últimos años, han surgido diversas definiciones y clasificaciones de activos intangibles con el propósito de ofrecer una mejor comprensión del concepto, alcanzar una valoración fiel de las inversiones en estos activos y promover la comunicación entre investigadores, directivos de empresas, usuarios de la información contable y organismos emisores de normas contables.

En cuanto a la definición de Activos Intangibles, a continuación podemos citar a varios autores. En primer lugar, se encuentra el concepto de Sosa Gómez (2002). Dada la gran diversidad de activos intangibles, este autor identifica como tales aquellos que realmente representan agregación de valor a la empresa.

Vargas Montoya (2000), los denomina Recursos intangibles: aquellos que no tienen soporte físico, lo que hace muy compleja su identificación y valoración.

Según Navas y Guerras (1998), sus características básicas son las siguientes:

–Son activos que se sustentan en información.

–Esta información no es siempre codificable.

–Los derechos de propiedad de estos recursos no siempre están bien definidos.

Dentro de este tipo de recursos, se puede distinguir entre recursos intangibles humanos (en función de que estén vinculados al factor humano que forma parte de la organización) y recursos intangibles no humanos.

Cuadro 1 Clasificación de los Activos Intangibles

Recursos intangibles	**No separables del individuo** (Recursos humanos)	**Separables del individuo**	
Defendibles en un contexto legal	(Recursos con opacidad voluntaria) Beneficios del capital humano apropiables pormedios legales	(Recursos tecnológicos) (Recursos conopacidad voluntaria) PatentesSecreto industrial	(Recursos comerciales) (Recursos transparentes) Imagen corporativa y reputación Marcas Nombre comercial Rótulo del establecimiento
No defendibles en un contexto legal (Recursos conopacidad intrínseca)	Beneficios del capital humano no apropiables por medios legales	(Recursos organizativos) Rutinas organizativa Cultura empresarial	(Recursos comerciales) Clientes Proveedores

Nota: Fuente: Vargas Montoya, 2000, p. 8

El criterio de clasificación es la que proponen los autores Serrano y Chaparro (2001), según los cuales los activos intangibles se pueden agrupar en activos intangibles de Recursos Humanos, de organización interna y de estructura externa.

Activos Intangibles de Recursos Humanos, según se refieran a las aptitudes y conocimiento de los recursos humanos de la empresa.

Activos Intangibles de Estructura Interna, como la capacidad de los sistemas de información de que dispone la empresa; o

Activos Intangibles de Estructura Externa, como la clientela o las marcas.

A continuación sólo detallaremos:

Activos Intangibles de Estructura Interna

Los activos intangibles de estructura interna se refieren a la estructura organizativa formal e informal, a los métodos y procedimientos de trabajo, a los sistemas de dirección y gestión, la cultura de la empresa y la filosofía de gestión. El análisis de la cadena de valor proporciona una guía para su medición. Los más comunes son la organización de los sistemas de información y los índices relacionados con la investigación y desarrollo que realiza la empresa.

a) **La organización de los sistemas de información**. La empresa puede tener un activo intangible en la organización de sus sistemas de información, software, bases de datos o el uso eficiente de tecnologías de la comunicación. Podemos comparar el uso diferente que dos empresas o personas hacen del mismo equipamiento informático: para unos puede ser una carga: "la informática es un problema, no puedo obtener un simple informe", dicen, mientras que para otras puede ser una ventaja estratégica, un activo.

   Para valorar su capacidad, se utilizan indicadores que analizan la utilización de la tecnología de punta en la empresa, el uso de Intranet, Extranet, sistemas EDI (Electronic Data Interchange), los beneficios que se obtienen de estos sistemas, etc.

b) **Investigación y desarrollo**. La investigación y desarrollo es también un activo intangible para la empresa. Es uno de los que ya se recoge en la contabilidad, aunque desde la perspectiva del capital intelectual se critican sus normas de valoración. Se incluyen también los activos intelectuales de propiedad intelectual como las patentes, copyrights, diseños, secretos. Se pueden obtener bastantes indicadores como el número de patentes y su coste de mantenimiento, el porcentaje de recursos que destina la empresa a Investigación y Desarrollo

(I+D) o su incremento, el porcentaje de I+D dedicado a investigación básica, etc.

Pucich y otros (2001) proponen como indicadores de estructura interna aquellos que miden el aprovechamiento de la tecnología de información y los indicadores de innovación.

Indicadores que miden el aprovechamiento de tecnología de la información:

–**Fechas de actualización de las bases de datos de los clientes.** Dado que las mismas carecen de valor si no se mantienen actualizadas, la que contendrá el perfil de nuestros clientes, su profesión, sus lugares de fin de semana, sus pasatiempos, sus preferencias con respecto a bienes del hogar, entre otros. Este indicador podría informar acerca de la intención de una empresa de conocer las necesidades de sus clientes.

–**Grado de conocimiento de tecnologías de información por parte de los administradores.** En general, dichos recursos son expuestos en los informes contables a su costo y no como están siendo utilizados por la organización para obtener resultados y brindar soluciones que contribuyan a un buen manejo de la información.

–**Existencia de planes para adoptar tecnologías de información**

–Indicadores de innovación. Como los siguientes.

–**Relación de las Ventas de nuevos productos y las ventas totales.** Consideran Pucich y otros (2001) que este indicador muestra el éxito de una empresa en el mercado.

–**Tiempo que duran los ciclos de vida de los productos.** Con respecto al tiempo que tarda la empresa en lanzar nuevos productos o modificar su diseño y características.

DISCUCIÒN DE RESULTADOS

CAPITULO IV

DIAGNÓSTICO Y PROPUESTA DE CAMBIO

4.1 Diagnostico del Sistema (Oficina Universitaria de Informática)

Activos de los Sistemas de UPLA

a) Inventario de Base de Datos

Sistema Académico

Dbseguridad – Auditoria

DBCampusNet – Data del Sistema Académico

ASPState – Control de usuarios

Aspnetdb – Control de Usuarios

Sistema Financiero

SGA – Data Financiera

Sistema Patrimonio

DBPATRIMONIO –Data de Bienes Patrimoniales

Sistema de Asesoría Legal

dbAsesoria – Data de documentos de procesos legales

Sistema de Personal

DBPERSONAL – Data de procesos laborales

Sistema de Trámite Documentario

dbTramDoc_SITD data del proceso de trámite de documentos

b) Inventario de Aplicativos

Sistema Financiero FOXPRO

Sistema Academico ASP Net

Sistema Grados y Títulos – PHP

Sistema de Contabilidad – Fox Pro

Sistema Logistica- Fox Pro

Sistema Patrimonio – Power Bilder

Sistema Personal – Visual Studio . Net y Visual Fox Pro

Sistema Asesoría Legal – Visual Studio . Net

Sistema de Almacen Fox Pro

c) Inventario de Servidores

Servidor IBM x3850 – Servidor de Base de Datos

Servidor IBM x3850 – Servidor de Aplicativos

Storage IBM DS3500 – Almacena los Backups de todas las base de datos

Evaluación de la madurez de TIC en la UPLA

Esta evaluación de madurez intenta determinar el estado actual de las TIC al interior de la organización, haciendo uso del modelo Nolan adaptado. Las calificaciones se obtuvieron ponderando los resultados de la encuesta a usuarios finales (Ver Anexo 1), visita a las instalaciones de la institución y entrevista con los miembros de la Oficina de Informática. Estas herramientas permitieron la clasificación de las tecnologías usadas por la institución, para su análisis individual.

Cuadro 2 Tecnologías

T1	Equipos de informática y software básico
T	Comunicaciones y redes
T	Sistemas de información
T	Infraestructura de servidores

Nota: fuente Elaboración Propia

Evaluación de las tecnologías

Cuadro 3 Equipos de informática y software básico

Número	Criterio	Calificación
CR1	Grado de cubrimiento en la organización	4
CR2	Dominio de los usuarios	3
CR3	Soporte del área informática	4
Total		**3.67**

Nota: fuente Elaboración Propia

Cuadro 4 Comunicaciones y redes

Número	Criterio	Calificación
CR1	Grado de cubrimiento en la organización	3
CR2	Dominio de los usuarios	2
CR3	Soporte del área informática	3
Total		**2.67**

Cuadro 5 Sistemas de información

Número	Criterio	Calificación
CR1	Grado de cubrimiento en la organización	3
CR2	Dominio de los usuarios	3
CR3	Soporte del área informática	3
Total		3

Cuadro 6 Infraestructura de servidores

Número	Criterio	Calificación
C R1	Grado de cubrimiento en la organización	4
C R2	Dominio de los usuarios	3
CR3	Soporte del área informática	3
Total		**3.33**

Nota: fuente Elaboración Propia

Tecnologías	Calificación
Equipos de informática y software básico	3.67
Comunicaciones y redes	2.67
Sistemas de información	3
Infraestructura de servidores	3.33
Total	**3.23**

Nota: fuente Elaboración Propia

La conclusión a que se llega en la evaluación de las tecnologías, ubica a la organización entre las etapas de “Integración de la información” y “Madurez”, con una tendencia cercana a la primera.

En general, es notorio el interés de la organización por implementar tecnologías de información y comunicación que apoyen y cubran en alto grado todas las actividades tácticas y operativas, con el fin de mejorar la operación y brindar valor tanto a los usuarios internos, como a los clientes externos. Los usuarios en general tienen un buen grado de aceptación y dominio de las tecnologías que apoyan sus labores, pero se notan debilidades en el uso de las comunicaciones y redes, porque se desconoce el uso y las bondades adicionales que éstas pueden ofrecer.

El soporte del área de Sistemas tiene una buena calificación, pero la falta de metodologías impide un cubrimiento total y evidencian un sentimiento de retraso en las tareas de soporte por parte de los clientes internos. La parte operativa y administrativa de las tecnologías es atendida por dos funcionarios que tienen bajo su responsabilidad atender los soportes y requerimientos solicitados por los demás usuarios, impidiendo que se dedique tiempo a actividades de evaluación e investigación de nuevos usos tecnológicos o a la explotación de los que ya existen, lo que le da un carácter al área más reactivo que proactivo.

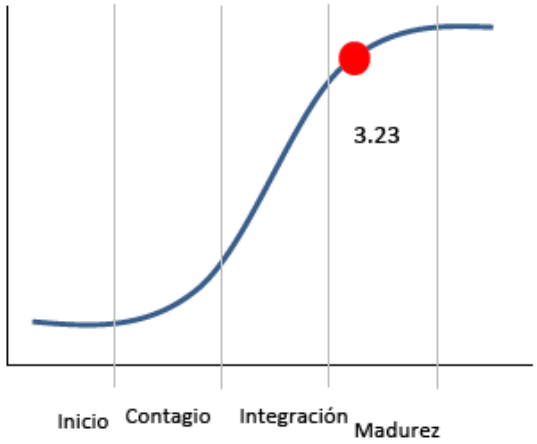


Grafico 6 Curva de Nolan adaptado resultado de la calificación de las tecnologías.

Procesos de gestión de los sistemas de información

- **Desarrollo y Mantenimiento del Sistema de Información:** El área se encarga de la gestión y análisis de requerimientos que solicitan los usuarios, correcciones de errores del software y ajustes o nuevos desarrollos para adaptar el sistema a las necesidades del negocio. Efectúa el diseño y análisis de las soluciones, desarrollo de código o programación, realiza las pruebas o verificación del software, y luego, libera el resultado o software a ambiente de producción.
- **Administración de Implantación de Software:** La Oficina de Informática gestiona cualquier instalación, implementación o actualización ejecutada sobre los sistemas de información. El propósito es asegurar que la implantación de software soporta las necesidades de la institución y que el nuevo software o las actualizaciones sobre uno ya existente no alterarán el desempeño normal de la operación.

  La gestión de software también incluye la instalación y actualización de otros programas y aplicaciones como sistemas operativos, paquetes de oficina (Microsoft Office), programas de diseño (Autocad, visores de CAD), programas para gestión de proyectos, y cualquier otro tipo de software.

  También incluye actividades realizadas para el control de licenciamiento e inventario de software.
- **Soporte del Sistema de Información:** El área se encarga de brindar soporte técnico al usuario sobre los módulos del sistema de información corporativo.

  También presta un servicio de soporte funcional básico. En caso de que se requiera un soporte más avanzado, se gestiona una solicitud de servicio mediante un sistema de servicio al cliente ante el partner del fabricante del software en Colombia.
- **Administración de la Operación del Sistema de Información:** Es responsabilidad del área velar por la disponibilidad y correcta operación del sistema. Esto incluye instalación periódica de paquetes de software, revisión de servicios, administración y mantenimiento de las Bases de Datos, revisión y administración

de desempeño y carga de los recursos de los servidores, generación de backups, gestión de seguridades del Sistema, administración de usuarios y perfiles.

Evaluación del estado de tecnologías en la UPLA

Con el propósito de evaluar el estado de las tecnologías de información y comunicación en la institución, el equipo de trabajo definió y aplico como metodología la construcción de dos matrices estratégicas muy conocidas que permiten obtener una visión global e integral de la situación y facilitan el análisis de la información recogida. Estas dos matrices son:

Identificación de necesidades de TI en la UPLA

El análisis realizado a lo largo del capítulo permite enunciar las siguientes necesidades de TI detectadas al interior de la organización:

- Es conveniente crear servidores espejo en la Ciudad universitaria de Chorrillos para tener respaldos de los sistemas en caso de cualquier inconveniente u desastre natural.
- Generar espacios para que los integrantes del equipo de Sistemas aprendan de nuevas tecnologías y dispositivos Linux.
- Es conveniente definir mecanismos para garantizar el respaldo del recurso humano en caso de ausencia de cualquier miembro del equipo.
- Se requiere enfocar esfuerzos en el desarrollo de **procesos de planeación y organización del área de TI que incluyan: elaboración de plan estratégico de TIC**, control presupuestal, definición de políticas y **procedimientos del área,** estructura del área, planeación de capacitación, establecimiento de indicadores de gestión y evaluación de desempeño del área. También se debe elaborar, divulgar y oficializar las políticas de TIC de la institución.
- Es indispensable **desarrollar, probar, documentar**, divulgar y mantener un Plan de contingencia de TIC que permita continuar la operación en caso de fallas.
- Es necesario generar una política clara de soporte y mantenimiento controlando los requerimientos sobre el sistema de información (los sistemas académico y contable). Se debe establecer un estándar para solicitud y recepción de requerimientos, contar con un proceso definido de levantamiento, recepción, documentación, aceptación, entrega y control de cambios, y definir un proceso

para la planeación, ejecución y monitoreo de los proyectos de desarrollo de software.

- Se requiere la implementación de una herramienta de helpdesk que permita el registro, control y documentación del soporte técnico ofrecido.
- Se requiere la implementación de una herramienta sistematizada para controlar el inventario de Hardware y Software de la institución.
- Es necesario evaluar y licenciar una herramienta de control y monitoreo remoto de equipos.
- Se requiere el desarrollo de mecanismos de captura de información a través de dispositivos móviles para facilitar la operación de los usuarios y fortalecer el ingreso en tiempo real de la información.
- Es importante generar herramientas para proporcionar información a las partes interesadas a través del portal corporativo.
- Es necesario promover la integración de sistemas CRM, BI y BPM que apunten a fortalecer la gestión y consolidación de la información y la toma de decisiones estratégicas en la organización.
- Se hace relevante cambiar el esquema de servicios de impresión, digitalización y fotocopiado y desarrollar una campaña para promover el buen uso de los recursos, evitando la impresión innecesaria.
- Es necesario repotenciar y mejorar la configuración de los equipos de cómputo de la institución, lo que se puede lograr implementando la renta de equipos de cómputo como mecanismo que permite renovación tecnológica y actualización frecuente, evitando costos de depreciación.
- Se debe sacar más provecho a la infraestructura tecnológica actual fomentando los programas de capacitación a través de las herramientas de trabajo colaborativo y las redes LAN.
- Es indispensable pensar en el futuro e ir evaluando los esquemas de cloudcomputing y virtualización para una futura migración de los sistemas de información.
- Resulta conveniente implementar redes inalámbricas seguras en cada uno de los puntos remotos de la institución y canales alternos de comunicación en los

puntos donde la relación costo/beneficio resulte conveniente garantizando conectividad en caso de fallas del canal primario.

- Desarrollar mecanismos o puntos de control dentro del sistema de información (los sistemas académico y contable), evitando que los controles sean realizados en papel, rompiendo la cultura de imprimir todo.
- Realizar un monitoreo de la red, detectar y corregir vulnerabilidades para proteger la infraestructura y la red de ataques.

- Tomar medidas para mantener los componentes del sistema los sistemas académico y contable y/o minimizar el impacto que ocasiona una falla. Algunas medidas pueden ser: contratar una firma de consultoría especializada en Base de Datos los sistemas académico y contable y garantizar una revisión y mantenimiento periódico de la Base de Datos, realizar validaciones y pruebas de efectividad de los backupslos sistemas académico y contable para garantizar efectividad de las copias en caso de fallas en los servidores.

4.2 Propuesta de Cambio con ISO 27001

El presente plan de contingencia pretende indicar los procedimientos a seguir en caso de falla en cualquier componente de la plataforma tecnológica que soporta el sistema de información actual de la institución, es decir, los sistemas académico y contable.
Los procedimientos específicos, en caso de contingencia, de cada una de las áreas de la institución que gestionan su información en los sistemas académico y contable, serán elaborados y documentados por cada líder de área y junto con este Plan de Contingencia de TI, conformarán el Plan de Contingencia Integral de la Organización.

La metodología empleada para el desarrollo y aplicación del plan de contingencias de los sistemas de información de la UPLA, está basado en e ISO 27001 e inspirado en el Plan de contingencias del Instituto Nacional de Estadística e Informática.
La presente metodología se podría resumir en cuatro fases de la siguiente manera:

PLANIFICAR

–preparación y aprobación de esfuerzos y costos.

HACER

–**Identificación de riesgos:** funciones y flujos del proceso de la empresa.

–**Identificación de soluciones:** Evaluación de Riesgos de fallas o interrupciones.

–**Estrategias:** Otras opciones, soluciones alternativas, procedimientos manuales.

VERIFICAR

–**Documentación del proceso:** Creación de un manual del proceso.

–**Realización de pruebas:** selección de casos soluciones que probablemente funcionen.

ACTUAR

–**Implementación:** creación de las soluciones requeridas, documentación de los casos.

–**Monitoreo:** Probar nuevas soluciones o validar los casos.

4.2.1 FASE 01 PLANIFICACION

Diagnóstico

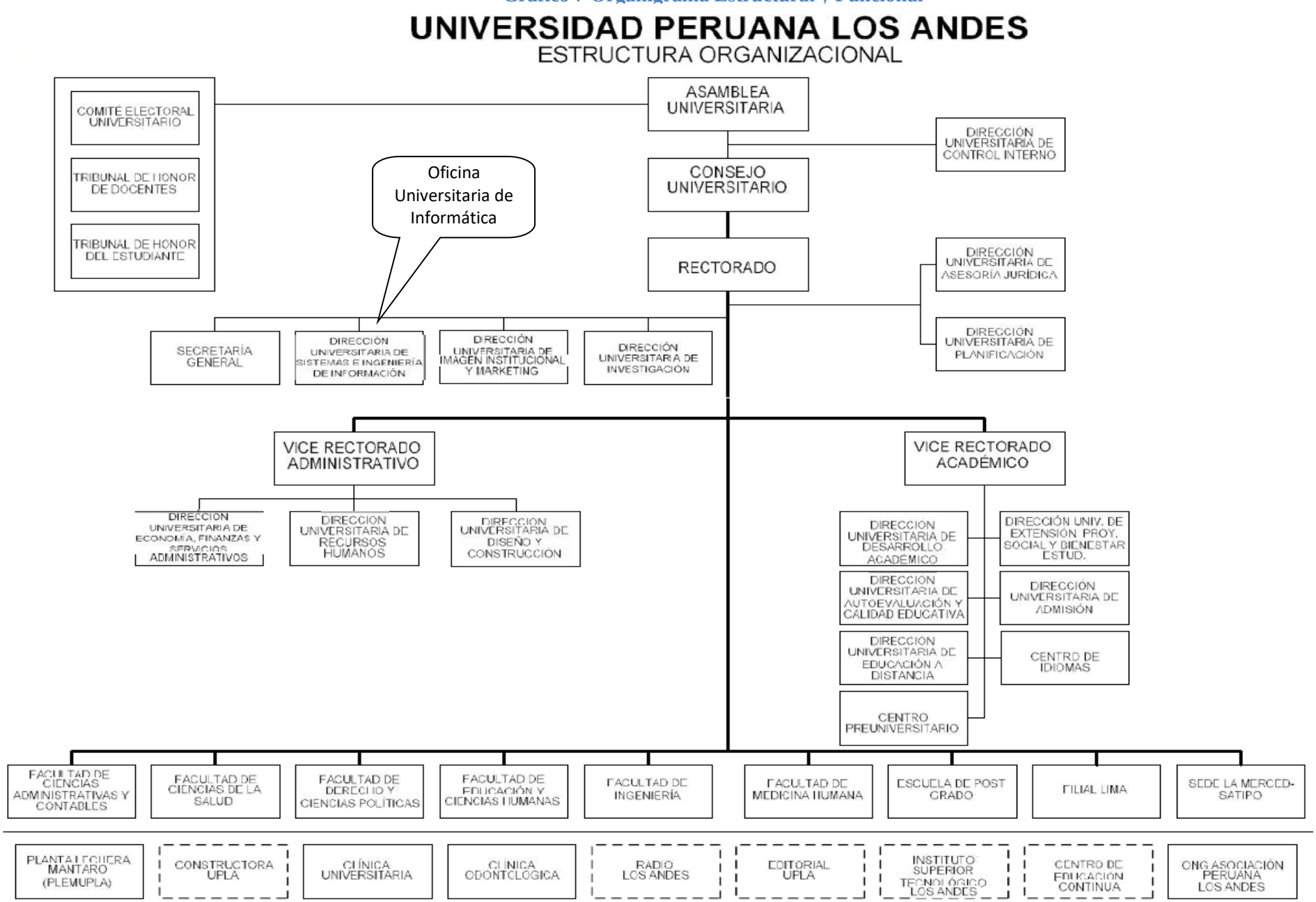
La Universidad Peruana Los Andes lleva sus procesos y actividades muchas veces de manera descuidada, el 28 de Febrero del 2014 fue multado por no cumplir con las normas de seguridad por INDECI, las razones pueden ser muchas entre ellas el alto grado de demora en sus procedimientos.

La Oficina Universitaria de Informática lleva sus procesos sin manuales de buenas prácticas, y almacena sus bases de datos en el mismo local Central sin tener un resguardo fuera del mismo, careciendo de seguridad de datos, en caso pueda ocurrir algún desastre natural o artificial.

Organización Estructural y Funcional.

En este aspecto se deben describir y analizar las Direcciones, Gerencias o dependencias en las que se divide la institución haciendo referencia de las funciones más importantes que desempeñan cada una de ellas, priorizando tales funciones en relación al sistema productivo de bienes o servicios que desarrollan.

Grafico 7 Organigrama Estructural y Funcional



Servicios Académicos.

La UPLA depende directamente de las pensiones de los estudiantes y por que ofrece servicios académicos.

Servicios y Materiales Utilizados.

Utiliza materiales, aulas, laboratorios para la investigación y formación de los estudiantes.

Inventario de Recursos Informáticos.

El inventario de recursos informáticos se realizará por dependencias y en forma clasificada:

- **Servidores:** Computadoras, actuales.
- **Programas:** De sistemas operativos, procesadores de textos, hojas de cálculo, lenguajes de programación, software de base.
- **Aplicativos Informáticos:** Del sistema de Contabilidad, de Trámite.

Activos de los Sistemas de UPLA

Inventario de Base de Datos

Sistema Académico

Dbseguridad – Auditoria

DBCampusNet – Data del Sistema Académico

ASPState – Control de usuarios

Aspnetdb – Control de Usuarios

Sistema Financiero

SGA – Data Financiera

Sistema Patrimonio

DBPATRIMONIO –Data de Bienes Patrimoniales

Sistema de Asesoría Legal

dbAsesoria – Data de documentos de procesos legales

Sistema de Personal

DBPERSONAL – Data de procesos laborales

Sistema de Trámite Documentario

dbTramDoc_SITD data del proceso de tramite de documentos

Inventario de Aplicativos

Sistema Financiero FOXPRO

Sistema Académico ASP Net

Sistema Grados y Títulos – PHP

Sistema de Contabilidad – Fox Pro

Sistema Logística- Fox Pro

Sistema Patrimonio – Power Bilder

Sistema Personal – Visual Studio . Net y Visual Fox Pro

Sistema Asesoría Legal – Visual Studio . Net

Sistema de Almacén Fox Pro

Inventario de Servidores

Servidor IBM x3850 – Servidor de Base de Datos

Servidor IBM x3850 – Servidor de Aplicativos

Storage IBM DS3500 – Almacena los Backups de todas las base de datos

Planificación

La fase de planificación es la etapa donde se define y prepara el esfuerzo de planificación de contingencia/continuidad. Las actividades durante esta fase incluyen:

Cuadro 7 Actividades para el Plan de Contingencia Informática para la Oficina de Informática

Actividades programadas	Meses				
	01	02	03	04	05
Levantamiento de Información de los bienes de Software	X				
Levantamiento de Información de los bienes de Hardware	X				
Programación de Implantación del Servidor de	X	X			

Respaldo					
Programación de Instalación y Configuración	X	X	X		
Análisis y redacción de las Guías de Buenas Practicas	X	X	X	X	
Programa de Implantación de Servidor de Respaldo de Información	X	X	X	X	X

Nota: fuente Elaboración Propia

Estrategias:

- Utilizar los medios de comunicación existentes.
- Utilizar la propuesta mas adecuada planteada en la factibilidad técnica.

- Utilizar tecnología Microsoft ya que el inventario de bienes de Software y Hardware se encuentran en esa tecnología.

Identificación de Roles:

-Si la universidad apuesta por la implementación se precisará de los encargados de informática, con participación del investigador.

Definición de términos clave:

Se deberá hacer el plan de contingencia de informático que beneficie a los usuarios del local central, en especial al área de informática

4.2.2 FASE 02 HACER

a) Identificación de Riesgos

El objetivo principal de la Fase de Reducción de Riesgo, es el de realizar un análisis de impacto económico y legal, determinar el efecto de fallas de los principales sistemas de información y producción de la institución o empresa.

Análisis y Evaluación de Riesgos

Es necesario reconocer y reducir de riesgos potenciales que afecten a los productos y servicios; es por ello que se considera dentro de un Plan de

Contingencia, como primer paso la Reducción de Riesgos, para favorecer el cumplimiento de los objetivos institucionales.

Cuadro 8 Análisis de Evaluación y riesgos

	Impacto	Nivel A	Nivel B	Proceso Critico
Inventario de Base de Datos				
Sistema Académico	alto	**X**		**X**
Dbseguridad – Auditoria				**X**
DBCampusNet – Data del Sistema Académico				**X**
ASPState – Control de usuarios				**X**
Aspnetdb – Control de Usuarios				**X**
Sistema Financiero	alto	**X**		**X**
SGA – Data Financiera				**X**
Sistema Patrimonio	medio	**X**		
DBPATRIMONIO –Data de Bienes Patrimoniales				
Sistema de Asesoría Legal	medio	**X**		
dbAsesoria – Data de documentos de procesos legales				
Sistema de Personal	alto	**X**		
DBPERSONAL – Data de procesos laborales				
Sistema de Trámite Documentario	bajo		**X**	
dbTramDoc_SITD data del proceso de tramite de documentos				
Inventario de Aplicativos				
Sistema Financiero FOXPRO			**X**	

Sistema Académico ASP Net			**X**	
Sistema Grados y Títulos – PHP			**X**	
Sistema de Contabilidad – Fox Pro			**X**	
Sistema Logística- Fox Pro			**X**	
Sistema Patrimonio – Power Bilder			**X**	
Sistema Personal – Visual Studio . Net y Visual Fox Pro			**X**	
Sistema Asesoría Legal – Visual Studio . Net			**X**	
Sistema de Almacén Fox Pro			**X**	
Inventario de Servidores				
Servidor IBM x3850 – Servidor de Base de Datos	alto	**X**		**X**
Servidor IBM x3850 – Servidor de Aplicativos	alto	**X**		**X**
Storage IBM DS3500 – Almacena los Backups de todas las base de datos	alto	**X**		**X**

Nota: fuente Elaboración Propia

Identificar los Procesos Críticos

Base de Datos del Sistema Académico

Base de Datos del Sistema Financiero

Análisis de las Operaciones Actuales

Todo el proceso de administración de los servidores de Base Datos es Manual, no cuenta con Servidor de Respaldo fuera del local Central, las copias de seguridad son sólo en Medios de almacenamiento, como Cd, DVD.

Todos los procesos académicos son repetitivos desde la adquisición (áreas administrativas e intermedias) pueden y deben controlarse, en gran parte.

PROCESOS INMERSOS

- Manejo de índices.
- Diseño de componentes de cable
- Prueba de diseño
- Revisión de documentos
- Diseño del sistema de energía
- Requerimiento del sistema

b) Identificación de Soluciones

Fase de Reducción de Riesgos

Para reducir el riesgo del inventario de los bienes críticos como son las base de Datos y los servidores, es preciso y **urgente implementar un sistema** de Respaldo fuera del local Central, se sugiere la ciudad universitaria de Chorrillos vía conexión VPN. Si prefieren la 2da opción el contratar un servidor dedicado, sin embargo se tiene que pagar a los proveedores mensual y/o anualmente.

Fase de Recuperación de Contingencia

En caso ocurriera algún desastre natural o artificial, al estar interconectado el servidor principal del local central con el servidor de respaldo el de respaldo tomaría el control y los datos estarían a salvo, aun si se destruye el servidor principal, se puede restaurar del servidor de respaldo hasta el último segundo de transacción realizada.

Fase de Organización de un Sistema de Alerta contra Fallas

Si ocurriera algún desastre natural o artificial el sistema antifallas deberá activarse automáticamente por ello se precisa de 02 servidores adicionales uno de ellos se comportará como arbitro el que detectará el error y deberá activar el servidor de respaldo automáticamente comportándose este como principal.

Cuadro 9 Matriz de planificación de contingencia

OPCIONES	OPERACIÓN MANUAL	REEMPLAZO	EXTERNALIZACION DEL SERVICIO
Reparación rápida y de defecto	Recurra al proceso manual sólo en caso de clientes prioritarios. Asegure que contará con personal que tengan acceso al laboratorio.	Tenga disponible software de repuesto que cumpla con los requisitos	Use personal temporalmente para llenar brecha
Reparación parcial	Use hojas de cálculo o base de datos paraofreceralguna dela funcionalidad original delsistema (	Use base de datos paquetes COTS par reemplazar la funcionalidad del sistema	Haga que el contratista procese los pagos en sus propias instalaciones
Reparación total	Ofrezca operaciones totalmer Funcionales a través del proceso manual, utilizando personal adicional si es necesario	Elimine esfuerzos de reparación e implemente un sistema comercial funcional, rápidamente	Entregue el manejo de la plantilla de pago a una firma comercial especialista

Nota: fuente Elaboración Propia

Identificación de Alternativas

Como indicamos anteriormente, un buen método para identificar alternativas consiste en revisar los planes de administración de emergencia o recuperación de fallas. Estos son algunos ejemplos de alternativas que pudieran ayudarle al inicio del proceso de preparación.

- En local Central se deberá contar con los encargados de reparar levantar la data en caso de que el servidor tuviera problemas
- Deberá activarse generadores si no tiene acceso a la red de energía pública.
- Disponga del suministro adicional de combustible para los generadores, en caso de fallas eléctricas prolongadas.
- Disponga de bombas manuales de combustible y úselas si fallan las electrónicas.
- Elaborar un programa de vacaciones que garantice la presencia permanente del personal.
- No haga nada y vea qué pasa – esta estrategia es algunas veces llamada

arreglar sobre falla.

Identificación de Eventos Activadores

El evento activador de la protección de las base de datos y servidores de sistemas es el servidor árbitro, que todo el día esta sincronizado y chequeando alguna caída del servidor:

- Fallo de la infraestructura regional (energía, telecomunicaciones, sistemas financieros)

  ○Cabe mencionar que, para desarrollar este proyecto es necesario conocer los lineamientos generales del sistema afectado, es decir el tipo de producción al cual pertenece pudiendo pertenecer al sector de bienes o al sector servicios. Una vez establecido a que rubro de la producción pertenece, identificamos el departamento u área ligada y las funciones que en ella realiza, las áreas principales pueden ser:

- Académico
- Finanzas
- Asesoría Legal

Fallas Potenciales

-caída de la base de datos y aplicación del Sistema Académico

-caída de la base de datos y aplicación del Sistema Contable

Soluciones

El objetivo es reducir el costo de encontrar una solución en la medida de lo posible, a tiempo de documentar todos los riesgos identificados.

Actividades importantes a realizar:

- Clasificar los riesgos.
- La elaboración de soluciones de acuerdo con el calendario de eventos.
- La revisión de la factibilidad de las soluciones y las reglas de implementación.
- La identificación de los modos de implementación y restricciones que afectan a las soluciones.

Seguridad en Redes

En el intento de proteger una red de computadoras, existen varias funciones comunes a las cuales deben dirigirse. La siguiente es una lista de cuatro problemas básicos:

a. El anfitrión promiscuo

El anfitrión promiscuo es uno de los principales problemas de seguridad y uno de los problemas más urgentes de cualquier red. Si un intruso es paciente, él puede simplemente mirar (con una red debugger o anfitrión promiscuo) que los paquetes fluyen de aquí para allá a través de la red. No toma mucha programación el análisis de la información que fluye sobre la red.

Un ejemplo simple es un procedimiento de login remoto. En el procedimiento login, el sistema pedirá y recibirá el nombre y contraseña del usuario a través de la red.

b. Autenticación

El procedimiento de login remoto ilustra el problema de autenticación. ¿Cómo presenta usted credenciales al anfitrión remoto para probar que usted es usted?.

c. Autorización

Aun cuando usted puede probar que usted es quien dice que es, simplemente, ¿Qué información debería permitir el sistema local accesar desde a través de una red?. Este problema de autorización parecería ser simple en concepto, pero considerar los problemas de control de acceso, cuando todo el sistema tiene su identidad remota de usuario, el problema de autorización sería un problema de seguridad bastante serio.

Componentes de Seguridad

Para un intruso que busque acceder a los datos de la red, la línea de ataque más prometedora será una estación de trabajo de la red. Estas se deben proteger con cuidado. Debe habilitarse un sistema que impida que usuarios

no autorizados puedan conectarse a la red y copiar información fuera de ella, e incluso imprimirla.

A continuación se sugiere un sistema en tres niveles:

- **Nivel de administración.** Aquellos que diseñan, mantienen o ponen en marcha la red. Este debe estar constituido sólo por el administrador o por un pequeño grupo de personal de soporte y administración.
- **Usuarios fiables.** Aquellos usuarios que cumplen las normas y cuyo trabajo se pueda beneficiar de una mayor libertad de acceso a la red.
- **Usuarios vulnerables.** Aquellos que muestran falta de competencia, son excesivamente curiosos o beligerantes, o los que por alguna razón no se puede confiar.

Control de Acceso a la Red

Restringir el acceso a las áreas en que están las estaciones de trabajo mediante llaves, tarjetas de identificación, tarjetas inteligentes y sistemas biométricos.

Protección del Servidor

La copia automática del servidor de respaldo que funcione en Chorrillos deberá complementarse con la copia manual de datos.

Dada la importancia del servidor y la cantidad de datos que pasan por él, es necesario efectuar copias de seguridad, del servidor. Cabe recordar que las copias de seguridad del servidor de archivos son un elemento especialmente valioso, debiéndose quedar guardados en un lugar cerrado, seguro y con las condiciones ambientales necesarias. Un conjunto de copias de seguridad se debe trasladar regularmente a otro lugar seguro (de preferencia otro local).

c) Estrategias

Las estrategias de contingencia están diseñadas para identificar prioridades y determinar en forma razonable las soluciones a ser seleccionadas en primera instancia o los riesgos a ser encarados en primer lugar. Hay que decidir si se adoptarán las soluciones a gran escala, como las opciones de recuperación de desastres para un centro de datos.

Actividades Importantes

–La revisión de procesos, flujos, funciones y opciones de importancia crítica.

–La revisión / depuración del cronograma maestro, incluyendo prioridades, fechas importantes en el calendario de eventos y dependencias cruzadas en diversos proyectos o áreas.

–La consolidación de soluciones de acuerdo a las funciones o áreas de negocios más importantes e identificar las estrategias globales.

–La identificación de los impactos de las soluciones y estrategias para ahorrar costos, como puede ser la selección de una solución para cubrir varios riesgos, Se deben de considerar varios elementos de costo: como el costo de crear la solución, el costo de implementar la solución, y el costo de mantener vigente dicha solución. Debido a que la continuidad de las operaciones de la organización constituye el enfoque primordial, la estrategia de la empresa rige el análisis de costos.

Grafico 8 Identificación de Soluciones Preventivas

Los puntos que deben ser cubiertos por todos las áreas informáticas y usuarios en general son:

–Además del servidor de Contingencia que se propone se recomienda copias

adicionales periódicas.

–Respaldar toda la información importante en medio magnético, ya sea en disquetes, cintas o CD-ROM, dependiendo de los recursos con que cuente cada área. Acordamos que lo que debe respaldarse es INFORMACION y no las aplicaciones.

MEDIDA DE PRECAUCIÓN Y RECOMENDACIÓN

En Relación al Centro del Local Central

–Es recomendable que el Centro de Cómputo este restringido solo a personal autorizado.

–Se deben evitar, en lo posible, los grandes ventanales, los cuales además de que permiten la entrada del sol y calor (inconvenientes para el equipo de cómputo), puede ser un riesgo para la seguridad del Centro de Cómputo.

–Otra precaución que se debe tener en la construcción del Centro de Cómputo, es que no existan materiales que sean altamente inflamables, que despiden humos sumamente tóxicos o bien paredes que no quedan perfectamente selladas y despidan polvo.

–Se deberá estar al día con las disposiciones de INDECI, para minimizar los riesgos.

–Se recomienda que al momento de reclutar al personal se les debe hacer además exámenes psicológicos y médico y tener muy en cuenta sus antecedentes de trabajo, ya que un Centro de Cómputo depende en gran medida, de la integridad, estabilidad y lealtad del personal.

–El acceso a los sistemas compartidos por múltiples usuarios y a los archivos de información contenidos en dichos sistemas, debe estar controlado mediante la verificación de la identidad de los usuarios autorizados.

–Establecer políticas de control de entrada y salida del personal, así como de los paquetes u objetos que portan.

–Los controles de acceso, el acceso en sí y los vigilantes deben estar ubicados de tal manera que no sea fácil el ingreso de una persona extraña. En caso que ingresara algún extraño al centro de Cómputo, que no pase desapercibido y que no le sea fácil a dicha persona llevarse un archivo.

–Las cámaras fotográficas no se permitirán en ninguna sala de cómputo, sin permiso por escrito de la Dirección.

Respecto a al almacén de Datos de respaldo

Debe ser administrada bajo la lógica de un almacén. Esto implica ingreso y salida de medios magnéticos (sean cintas, cartuchos, Discos removibles, CD's, etc.), obviamente teniendo más cuidado con las salidas.

Existen dos tipos de activos en un Centro de Cómputo. Los equipos físicos y la información contenida en dichos equipos. Estos activos son susceptibles de robo o daño del equipo, revelación o destrucción no autorizada de la información clasificada, o interrupción del soporte a los procesos del negocio, etc.

El valor de los activos a proteger, está determinado por el nivel de clasificación de la información y por el impacto en el negocio, causado por pérdida o destrucción del Equipo o información. Hay que distinguir los activos en nivel clasificado y no clasificado. Para los de nivel no clasificado, no será necesario control. Cualquier control debe basarse únicamente en el valor del equipo y servicios que ellos prestan.

Recomendaciones para el Mantenimiento de los Discos Duros

Aunque el conjunto de cabezales y discos viene de fábrica sellado herméticamente, debe evitarse que los circuitos electrónicos que se encuentran alrededor se llenen de partículas de polvo y suciedad que pudieran ser causa de errores.

El ordenador debe colocarse en un lugar donde no pueda ser golpeado, de preferencia sobre un escritorio resistente y amplio.

Se debe evitar que la microcomputadora se coloque en zonas donde haya acumulación de calor. Esta es una de las causas más frecuentes de las fallas de los discos duros, sobre todo cuando algunas piezas se dilatan más que otras.

No se debe mover la CPU conteniendo al disco duro cuando esté encendido, porque los cabezales de lectura-escritura pueden dañar al disco.

Una de las medidas más importantes en este aspecto, es hacer que la gente tome conciencia de lo importante que es cuidar un Microcomputador.

Respecto a los Monitores

La forma más fácil y común de reducir la fatiga en la visión que resulta de mirar a una pantalla todo el día, es el uso de medidas contra la refección.

Generalmente éstos vienen en forma de una pantalla con un terminado áspero o algún tipo de capa contra brillo con una base de sílice, sobre la superficie de la pantalla del monitor.

Se recomienda sentarse por lo menos a 60 cm. (2 pies) de la pantalla. No sólo esto reducirá su exposición a las emisiones (que se disipan a una razón

Recomendación para el Cuidado del Equipo de Cómputo

Teclado. Mantener fuera del teclado grapas y clips pues, de insertarse entre las teclas, puede causar un cruce de función.

Cpu. Mantener la parte posterior del cpu liberado en por lo menos 10 cm. Para asegurar así una ventilación mínima adecuada.

Mouse. Poner debajo del mouse una superficie plana y limpia, de tal manera que no se ensucien los rodillos y mantener el buen funcionamiento de éste.

Protectores de pantalla. Estos sirven para evitar la radiación de las pantallas a color que causan irritación a los ojos.

Impresora. El manejo de las impresoras, en su mayoría, es a través de los botones, tanto para avanzar como para retroceder el papel.

Mantener las Areas Operativas Limpias y Pulcras

Todas las razones para mantener las áreas operativas limpias y pulcras son numerosas, para enunciarlas aquí. Sin embargo, algunos de los problemas

que usted puede evitar son: el peligro de fuego generado por la acumulación de papeles bajo el falso piso, el daño potencial al equipo por derramar el café, leche o chocolate en los componentes del sistema, el peligro de fuego que se presentan por el excesivo almacenamiento de hojas continuas, el peligro por fumar y las falsas alarmas creadas por detectores de humo. Estos son solamente algunos de los problemas encontrados en las áreas operativas con reglas poco estrictas de limpieza.

4.2.3 FASE 03 VERIFICAR

a) DOCUMENTACION DEL PROCESO

Como puntos importantes que debe de incluir esta documentación podremos citar las siguientes:

Cuadro 10 Tareas para ubicar soluciones a Contingencias

Inventario de Base de Datos	Llamar Experto	**Reiniciar Sistema para restaurar**	Recuperar Copia de Medios de Almacenamiento	Recuperar de Copia de Seguridad DB	**Recuperar y reparar otros**
Sistema Académico	SI	**X**	**X**	**X**	
Dbseguridad – Auditoria	**X**	**X**	**X**	**X**	
DBCampusNet – Data del Sistema Académico	**X**	**X**	**X**	**X**	
ASPState – Control de usuarios	**X**	**X**	**X**	**X**	
Aspnetdb – Control de Usuarios	**X**	**X**	**X**	**X**	
Sistema Financiero	**X**	**X**	**X**	**X**	

SGA – Data Financiera	**X**	**X**	**X**	**X**	
Sistema Patrimonio	**X**	**X**	**X**	**X**	
DBPATRIMONIO –Data de Bienes Patrimoniales	**X**	**X**	**X**	**X**	
Sistema de Asesoría Legal	**X**	**X**	**X**	**X**	
dbAsesoria – Data de documentos de procesos legales	**X**	**X**	**X**	**X**	
Sistema de Personal	**X**	**X**	**X**	**X**	
DBPERSONAL – Data de procesos laborales	**X**	**X**	**X**	**X**	
Sistema de Trámite Documentario	**X**	**X**	**X**	**X**	
dbTramDoc_SITD data del proceso de tramite de documentos	**X**	**X**	**X**		
Inventario de Aplicativos					
Sistema Financiero FOXPRO		**X**	**X**		
Sistema Academico ASP Net		**X**	**X**		
Sistema Grados y Títulos – PHP		**X**	**X**		
Sistema de Contabilidad – Fox Pro		**X**	**X**		
Sistema Logistica- Fox Pro		**X**	**X**		
Sistema Patrimonio – Power Bilder		**X**	**X**		
Sistema Personal – Visual Studio . Net y Visual Fox Pro		**X**	**X**		
Sistema Asesoría Legal – Visual Studio . Net		**X**	**X**		
Sistema de Almacen Fox Pro		**X**	**X**		
Inventario de Servidores					
Servidor IBM x3850 – Servidor de Base de Datos	**X**	**X**	**X**	**X**	**X**

Servidor IBM x3850 – Servidor de Aplicativos	**X**	**X**	**X**	**X**	**X**
Storage IBM DS3500 – Almacena los Backups de todas las base de datos	**X**	**X**	**X**	**X**	**X**

Nota: fuente Elaboración Propia

Cuadro 11 CUADRO DE LISTA DE RIESGOS QUE SE PUEDE ENCONTRAR

Riesgos	Check
No existe caja de breakers de los circuitos del aula.	
No existen sistemas contra incendios.	
Los usuarios no son capacitados en el uso adecuado de extintores.	
No existen sistemas de censores de humo.	
No existen sistemas Extractores de calor.	
No existen sensores de Temperatura.	
No existen controles sobre el acceso de personas al aula.	
No hay un control de asistencia sobre los responsables del aula.	
No hay sistemas de vigilancia para detectar posibles movimientos fraudulentos a los equipos de cómputo.	
Faltan definir políticas para la asignación de contraseñas de los equipos de cómputo.	
No se lleva un registro detallado de los usuarios que hacen uso de los equipos.	
No hay una hoja de vida de la existencia de los equipos.	
No se llevan bitácoras para la realización de procesos de mantenimiento.	

No existe personal encargado del mantenimiento de los equipos.	
La ventilación del aula no es la adecuada.	
No se ha asignado un espacio locativo para el ejercicio del mantenimiento preventivo y correctivo.	
No se ha definido un protocolo para la organización de los equipos dependiendo que clase de mantenimiento se procederá a efectuar.	
No se hace monitoreo sobre la prestación de servicios de mantenimiento de hardware contratados por la institución educativa.	
No se hace inventario de existencias de equipos de cómputo.	
No se lleva monitoreo de la capacidad del hardware con el fin de asegurar que siempre exista una capacidad justificable para procesar las cargas de trabajo.	
No se realiza un escaneo para evitar intrusiones en la red.	
El rack no posee las medidas de seguridad necesarias.	
No se definen fechas para cambios del proveedor de servicios de internet.	
No se hace monitoreo sobre la prestación de servicios del ISP contratado.	

Nota: fuente Elaboración Propia

VALORACIÓN DE RIESGOS

De acuerdo a los riesgos citados, se realiza la valoración de los riesgos teniendo en cuenta la probabilidad de ocurrencia y el impacto del riesgo dentro de la red de la Oficina de informática del local Central.

Cuadro 12 Cuadro Valoración de riesgos

Riesgos / Valoración		Probabilidad			Impacto		
		A	M	B	L	M	C
Eléctricos							
R1	No existe conexión de polo a tierra			x	x		
R2	No existe instalación de sistema eléctrico regulado			x	x		
R3	No existe sistema de protección en caídas de energía			x	x		
R4	No hay medidores de voltaje eléctrico en sus tres fases			x	x		
R5	La fase neutra no se encuentra bien identificada			x	x		
R6	No existe caja de breakers de los circuitos del aula			x	x		
Siniestros y Catástrofes							
R7	No existen sistemas contra incendios	x					x
R8	Los usuarios no son capacitados en el uso adecuado de extintores		x		x		
R9	No existen sistemas de censores de humo	x					x
R10	No existen sistemas Extractores de calor	x					x
R11	No hay un control de asistencia sobre			x	x		

	los responsables del aula						
R12	No hay sistemas de vigilancia para detectar posibles movimientos fraudulentos a los equipos de cómputo.		x			x	
R13	No se lleva un registro detallado de los usuarios que hacen uso de los equipos		x			x	

Manejo y Control de Hardware

14	No hay una hoja de vida de la existencia de los equipos		x			x	
R15	No se llevan bitácoras para la realización de procesos de mantenimiento		x			x	
R16	No existe personal encargado del mantenimiento de los equipos	x					x
R17	La ventilación del aula no es la adecuada		x			x	
R18	no se hace monitoreo sobre la prestación de servicios de mantenimiento de hardware contratados por la institución educativa			x	x		
R19	no se hace inventario de existencias de equipos de computo	x					X
R20	no se lleva monitoreo de la capacidad del hardware con el fin de asegurar que siempre exista una capacidad justificable para procesar las cargas de trabajo	x					X

Manejo y Control de Redes

R21	No se realiza un escaneo para evitar intrusiones en la red	x					x
R22	El rack no posee las medidas de seguridad necesarias		x				x
R23	no se hace monitoreo sobre la prestación de servicios del ISP contratado		x		x		

Nota: fuente Elaboración Propia

Probabilidad	Impacto
Alta: A	Catastrófico: C
Media: M	Moderado: M
Baja: B	Leve: L

MATRIZ DE RIESGOS

De acuerdo a la valoración que se hace a los riesgos encontrados en la visita que se realiza a y sirve para estar preparado para las visitas de INDECI.

Cuadro 13 Cuadro Clasificación de Riesgos

	LEVE	MODERADO	CATASTROFICO
ALTO		R16	R7,R9,R10,R17, R19, R20
MEDIO	R24,R8,R11	R12,R13,R15, R21	R22, R23
BAJO	R1,R2,R3,R4,R5,R6,R18	R14	

Nota: fuente Elaboración Propia

Lista de Contactos de emergencia, en caso de riesgo mayor que atente con la seguridad de las personas y equipo.

DELEGACIÓN POLICIAL

Policía Nacional del Perú (Huancayo)

Av. Ferrocarril 555

Teléfonos: 211653 – 200230 – 200758

Policía Ecológica y de Turismo

Av. Ferrocarril 580

Teléfono: 219851

SERENAZCO HUANCAYO

Teléfonos: 200103 – 200104 – 200106

BOMBEROS Y DEFENSA CIVIL

Compañía de Bomberos Voluntarios Huancayo

Jr. Ancash 603

Teléfonos: 249319 – 211020

Emergencia #116

OTROS

Policía Nacional del Perú #105

Defensa Civil #115

Defensoría del Pueblo Huancayo Teléfono: 217261

HOSPITALES Y CLÍNICAS

Hospital de EsSalud Huancayo

Teléfonos: 248336 – 481120

Hospital Daniel Alcides Carrión

Av. Daniel Alcides Carrión 1150 – 1552

Hospital El Carmen

Jr. Puno 911

Teléfonos: 233691 – 233371

Hospital David Guerrero Duarte

Jr. 9 de Julio s/n – Concepción

Teléfono: 581043

Clínica Ortega

Teléfonos: 232921 – 235430

Clínica Santo Domingo

Teléfonos: 218084 – 213143

Clínica Cayetano Heredia

Teléfonos: 247087 – 252998

Clínica Ruhr Goyzueta

Teléfono: 233051

b) REALIZACION DE PRUEBAS Y VALIDACION

Plan de Recuperación de Desastres

Plan de Recuperación de Desastres se pueden clasificar en tres etapas:

- Actividades Previas al Desastre.
- Actividades Durante el Desastre.
- Actividades Después del Desastre.

Actividades Previas al Desastre

Establecimiento de Plan de Acción

En esta fase de Planeamiento se debe de establecer los procedimientos relativos a:

Sistemas e Información.

Equipos de Cómputo.

Obtención y almacenamiento de los Respaldos de Información (BACKUPS).

Políticas (Normas y Procedimientos de Backups).

a) Sistemas e Información. Relación de los Sistemas de Información con los que cuenta.

Cuadro 14 Relación de los Sistemas de Información con los que cuenta

	Impacto	Nivel A	Nivel B
Inventario de Base de Datos			
Sistema Académico	alto	X	
Dbseguridad – Auditoria			
DBCampusNet – Data del Sistema Académico			
ASPState – Control de usuarios			
Aspnetdb – Control de Usuarios			
Sistema Financiero	alto	X	
SGA – Data Financiera			
Sistema Patrimonio	medio		X
DBPATRIMONIO –Data de Bienes Patrimoniales			
Sistema de Asesoría Legal	medio		X
dbAsesoria – Data de documentos de procesos legales			
Sistema de Personal	medio		X
DBPERSONAL – Data de procesos laborales			
Sistema de Trámite Documentario	bajo		X

dbTramDoc_SITD data del proceso de tramite de documentos			
Inventario de Aplicativos			
Sistema Financiero FOXPRO		X	
Sistema Academico ASP Net		X	
Sistema Grados y Títulos – PHP		X	
Sistema de Contabilidad – Fox Pro		X	
Sistema Logistica- Fox Pro		X	
Sistema Patrimonio – Power Bilder		X	
Sistema Personal – Visual Studio . Net y Visual Fox Pro		X	
Sistema Asesoría Legal – Visual Studio . Net		X	
Sistema de Almacen Fox Pro		X	

Nota: fuente Elaboración Propia

b) Equipos de Cómputo. Aparte de las Normas de Seguridad que se verán en los capítulos siguientes, hay que tener en cuenta:

Cuadro 15 Equipos de Cómputo

Inventario de Servidores		Nivel A	
Servidor IBM x3850 – Servidor de Base de Datos	alto	X	
Servidor IBM x3850 – Servidor de Aplicativos	alto	X	
Storage IBM DS3500 – Almacena los Backups de todas las base de datos	alto	X	

Nota: fuente Elaboración Propia

c) Obtención y Almacenamiento de los Respaldos de Información (BACKUPS).

Backups del Sistema Operativo

Backups del Software Base (Paquetes y/o Lenguajes de Programación con los cuales han sido desarrollados o interactúan nuestros Aplicativos Institucionales).

Backups del Software Aplicativo (Considerando tanto los programas fuentes, como los programas objetos correspondientes, y cualquier otro software o procedimiento que también trabaje con la data, para producir los resultados con los cuales trabaja el usuario final).

Backups de los Datos (Bases de Datos, Indices, Cuadros de validación, passwords, y todo archivo necesario para la correcta ejecución del Software Aplicativo de nuestra Institución).

Backups del Hardware. Se puede implementar bajo dos modalidades:

Modalidad Externa. Se presentó en la factibilidad financiera la posibilidad de alquilar un servidor dedicado.

Modalidad Interna. Se presentó en la factibilidad financiera la implementar el sistema de Respaldo automático. A través el servidor primario como el servidor espejo mantienen una copia de la base de datos y el registro de transacciones, mientras que el tercer servidor, llamado el servidor árbitro.

d) Políticas (Normas y Procedimientos de Backups)

Política de backups

Determinar los **costes** de las posibles pérdidas de datos

El **tiempo** que se tardaría en la recuperación

Valorar los **recursos** disponibles (hardware, velocidad de la red, discos remotos, etc.)

Analizar **qué** es imprescindible copiar y qué no.

Guardado y retención de backups

Esto es distinto del ***archiving***, que consiste en mover datos antiguos que no se están utilizando a una localización distinta. Un backup es siempre una copia, mientras que el *archiving* consta de los datos originales que son trasladados porque no se utilizan pero no se quieren eliminar definitivamente.

Aunque hay diversas opciones de *storage* es interesante considerar **el servicio *Glacier* de Amazon**. Su bajo coste es una gran ventaja, pero el hecho que la restauración no esté asegurada en un tiempo concreto y que pueda tardar algunas horas lo descarta para el *vaulting* mientras que lo convierte en interesante candidato para *archiving*, donde no hay exigencias de recuperación de datos en tiempos limitados.

Restauración

RTO (*Recovery Time Objective*)

Es el tiempo máximo en el que se debe alcanzar un nivel de servicio mínimo tras una caída del servicio (por ejemplo, debido a pérdida de datos) para no causar consecuencias inaceptables en el negocio.

RPO (*Recovery Point Objective*)

Es el periodo de tiempo máximo en el que se pueden perder datos de un servicio. Si el periodo de tiempo es de 6 horas, se deben realizar backups cada menos tiempo y poder recuperar la información antes de agotar el periodo.

El tiempo de restauración de un backup en caso de pérdida de datos forma parte del tiempo en que no hay servicio, por lo que cuanto menos tarde antes se restablecerá el proceso de negocio.

Herramientas

Las herramientas nos **permiten implementar la política de backup**. Dada la variedad de plataformas, se han creado muchísimas herramientas que actúan a diferentes niveles.

Sincronización

Este tipo de backup permite que **dos directorios en localizaciones distintas (en la misma máquina o en hosts separados) contengan los mismos ficheros**.

Rsync: la herramienta más conocida de sincronización de ficheros, tiene muchas opciones que dan gran flexibilidad.

Duplicity: se basa en la librería de rsync para realizar backups de ficheros comprimidos y encriptados.

Unison: permite la sincronización de directorios aprovechando características de distintos sistemas y herramientas.

Copias

El sistema básico de realizar backups es la **copia de los ficheros a un espacio aparte**. En este caso, se pueden utilizar herramientas de un gran rango de diversidad y complejidad.

fwbackups: herramienta con una interfaz simple pero con muchas opciones, permite programar backups a distintos niveles.

Bacula: herramienta muy completa que permite realizar backups de varios niveles (total, diferencial, incremental), de distintos clientes (linux, solaris, windows) y a diversos soportes (cinta y disco). Es software libre aunque tiene opción de soporte comercial.

Mondorescue: este software permite realizar backup de una instalación entera, y puede dejar las copias en numerosos soportes físicos.

Bases de datos

Las bases de datos piden un trato especial. Por ello, **cada servidor suele proporcionar un sistema de copias de seguridad**, a menudo basadas en volcados de datos en distintos formatos.

MySQL: *mysqldump* realiza un volcado en los datos de la base de datos en SQL. Esto permite realizar backups y crear esclavos entre otros usos.

PostgreSQL: *pg_dump* hace, igual que mysqldump, un volcado de los datos en lenguage SQL.

SQL Server: el servidor de bases de datos de Microsoft ofrece la utilidad SQL Server Management Studio que permite programar las distintas tareas de backups, además de tareas previas y posteriores, especificando cuándo, de qué y a qué nivel se realiza la copia de seguridad de forma que sea consistente y fácilmente recuperable.

Snapshots

Los snapshots son **"fotografías"**:

Sistema de ficheros: hay sistemas de ficheros que permiten realizar backups en forma de snapshots. ZFS dispone de esta utilidad.

Volúmen de disco: LVM ofrece esta posibilidad para recuperar volúmenes.

Máquinas virtuales: muchos gestores de máquinas virtuales permiten realizar snapshots de las mismas. KVM, Xen o VMWare entre otros disponen de esta característica.

Ficheros: con rsnapshot se pueden realizar backups en forma de snapshot aprovechando el rsync y mediante hardlinks de forma transparente. Back In Time también realiza snapshots de directorios, aunque únicamente para entornos de escritorio.

Continuous Data Protection

AIMstor: permite definir fácilmente políticas mediante una interfaz gráfica y soporta distintos tipus de backup, replicación y *archiving*.

RecoverPoint: soporta replicación remota de datos mediante protocolos síncronos y asíncronos.

InMage DR-Scout: tiene un repositorio de capacidad optimizada y soporta diversas plataformas (Windows, Linux, Solaris,…).

A tener en cuenta

Instalación: ¿Está paquetizada o es necesario compilar? ¿Es fácil de instalar? ¿Tiene requerimientos especiales?

Configuración y mantenimiento: ¿Es fácil de mantener? ¿Es capaz de implementar la política? ¿Cuánto tiempo de aprendizaje requiere? ¿Tiene interfaz gráfica?

Restauración: ¿La restauración es fácil y rápida? ¿Puede un usuario restaurar un fichero suyo o debe ser siempre el administrador?

Compatibilidad: ¿Sirve para todos los sistemas de la plataforma? ¿El servidor debe correr en un sistema concreto?

Soporte físico: ¿Permite backup a cinta, DVD, sistemas de ficheros remotos, disco?

Licencia: ¿Es software libre o comercial? ¿Dispone de soporte para empresas?

Actividades Durante el Desastre

Plan de Emergencias.

Formación de Equipos.

Entrenamiento.

a) Plan de Emergencias

Durante el día.

Se deberá llamar e informar a los teléfonos de emergencia en caso de que el siniestro atente con la vida de las personas y los bienes, en especial a los bomberos.

Durante la Noche o madrugada.

Vías de salida o escape.

Plan de Evacuación del Personal.

Plan de puesta a buen recaudo de los activos (los más importantes de

Secuencia de llamadas en caso de siniestro, tener a la mano: elementos de iluminación (linternas), lista de teléfonos de Bomberos / Ambulancia, Jefatura de Seguridad y de su personal (equipos de seguridad) nombrados para estos casos.

b) Formación de Equipos

El equipo estará formado por los integrantes de la Oficina de Informática en grupos de 03, para distribuirse las tareas.

Entrenamiento

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

Actividad Después del Desastre

a) Evaluación de Daños.

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

Cuadro 16 Cuadro de Riesgos

Tipo de Riesgo	Factor
Robo de hardware	
Robo de información	
Vandalismo	
Fallas en los equipos	
Virus Informáticos	
Equivocaciones	

Accesos no autorizados	
Fraude	
Fuego	
Terremotos	

Nota: fuente Elaboración Propia

Priorización de Actividades del Plan de Acción.

Toda vez que el Plan de Acción es general y contempla una pérdida total, la evaluación de daños reales y su comparación contra el Plan, nos dará la lista de las actividades que debemos realizar, siempre priorizándola en vista a las actividades estratégicas y urgentes de nuestra Institución.

Ejecución de Actividades.

La ejecución de actividades implica la creación de equipos de trabajo para realizar las actividades previamente planificadas en el Plan de acción. Cada uno de estos equipos deberá contar con un coordinador que deberá reportar diariamente el avance de los trabajos de recuperación y, en caso de producirse algún problema, reportarlo de inmediato a la jefatura a cargo del Plan de Contingencias.

Evaluación de Resultados

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

Retroalimentación del Plan de Acción.

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

4.2.4 FASE 04 ACTUAR

a) IMPLEMENTACION

La fase de implementación se da cuando han ocurrido o están por ocurrir los problemas.

De las Emergencia Físicas

CASO A: Error Físico de Disco de un Servidor

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

1. Ubicar el disco malogrado.
2. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
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. Recorrer los sistemas que se encuentran en dicho disco y verificar su buen estado.
8. Habilitar las entradas al sistema para los usuarios.

CASO B: Error de Memoria RAM

En este caso se dan los siguiente síntomas:

- El servidor no responde correctamente, por lentitud de proceso o por no rendir ante el ingreso masivo de usuarios.
- Ante procesos mayores se congela el proceso.
- 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 autocorregirá.

Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por la compañía, 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, utilizar mensajes por red y teléfono a jefes de área.
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 similares.
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. Probar los sistemas que están en red en diferentes estaciones.
8. 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, utilizar mensajes por red y teléfono a jefes de área.
2. El servidor debe estar apagado, dando un correcto apagado del sistema.
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 por los altavoces 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, el equipo y los archivos de información que tenemos en cintas magnéticas.

–Ante todo, 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 Computador Principal, se deberá enviar un mensaje (si el tiempo lo permite) de "Salir de Red y Apagar Computador", seguidamente digitar Down en el (los) servidor(es).

–Se apagará (poner en OFF) la caja principal de corriente del departamento de sistemas.

–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.

CASO E: Caso de Inundación (lluvias)

–Para evitar problemas con inundaciones se ha de instalar tarimas de un promedio de 20 cm de altura 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.

–Proveer cubiertas protectoras para cuando el equipo esté apagado.

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 o se enciende el generador.
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 (para que no corten bruscamente el proceso que tienen en el momento del apagón), hasta que finalmente se realice el By-pass de corriente con el grupo electrógeno, previo aviso y coordinación.
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 220v, evitando que los equipos sufran corto circuito por elevación de voltaje (protegiendo de esta manera las tarjetas, pantallas y CPU del computador).

De las Emergencias Lógicas de Datos CASO

A: Error Lógico de Datos

La ocurrencia de errores en los sectores del disco duro del servidor puede deberse a una de las siguientes causas:

–Caída del servidor de archivos por falla de software de red.

–Falla en el suministro de energía eléctrica por mal funcionamiento del UPS.

–Bajar incorrectamente el servidor de archivos.

–Fallas causadas usualmente por un error de chequeo de inconsistencia física.

En caso de producirse alguna de las situaciones descritas anteriormente; se deben realizar las siguientes acciones:

PASO 1: Verificar el suministro de energía eléctrica. En caso de estar conforme, proceder con el encendido del servidor de archivos, una vez mostrado el prompt de Dos, cargar el sistema operativo de red.

PASO 2: Deshabilitar el ingreso de usuarios al sistema.

PASO 3: Descargar todos los volúmenes del servidor, a excepción del volumen raíz.

De encontrarse este volumen con problemas, se deberá descargarlo también.

PASO 4: Cargar un utilitario que nos permita verificar en forma global el contenido del(os) disco(s) duro(s) del servidor.

PASO 5: Al término de la operación de reparación se procederá a habilitar entradas a estaciones para manejo de soporte técnico, se procederá a revisar que las bases de datos índices estén correctas, para ello se debe empezar a correr los sistemas y así poder determinar si el usuario puede hacer uso de ellos inmediatamente.

Si se presenta el caso de una o varias bases de datos no reconocidas como tal, se debe recuperar con utilitarios.

CASO B: Caso de Virus

Dado el caso crítico de que se presente virus en las computadoras se procederá a lo siguiente:

Para servidor:

–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, nlm, etc.) serán reemplazados del diskett 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 red:

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

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 disquete que contenga sistema operativo igual o mayor en versión al instalado en el computador infectado. Reiniciar el computador con dicho disquete.

2.Retirar el disquete con el que arrancó el computador e insertar el disquete antivirus, luego activar el programa de tal forma que revise todos los archivos y no sólo 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

MONITOREO

La fase de Monitoreo nos dará la seguridad de que podamos reaccionar en el tiempo preciso y con la acción correcta. Esta fase es primordialmente de mantenimiento. Cada vez que se da un cambio en la infraestructura, debemos de realizar un mantenimiento correctivo o de adaptación.

Un punto donde se tiene que actuar es por ejemplo cuando se ha identificado un nuevo riesgo o una nueva solución. En este caso, toda la evaluación del riesgo se cambia, y comienza un nuevo ciclo completo, a pesar de que este esfuerzo podría ser menos exigente que el primero.

Esto es importante ya que nos alimentamos de las nuevas posibilidades de soluciones ante nuevos casos que se puedan presentar.

Podríamos enumerar las actividades principales a realizar:

–Desarrollo de un mapa de funciones y factores de riesgo.

– Establecer los procedimientos de mantenimiento para la documentación y la rendición de informes referentes a los riesgos.

– Revisión continua de las aplicaciones.
– Revisión continua del sistema de backup
– Revisión de los Sistemas de soporte eléctrico del Centro de Procesamiento de Datos.

CONCLUSIONES

1.Es de vital importancia contar con un plan de contingencia que pueda respaldar y salvaguardar tanto la información académica como administrativa teniendo en cuenta las diversas contingencias que se puedan presentar.

2.La falta de un adecuado control y restricción a la información, genera una pérdida total o parcial del record de pagos, deudas por cobrar, notas, datos del padrón de alumnos ingresantes, egresados, traslados internos y externos etc.

3.No se cuenta con equipos adecuados para resguardar la información integra de presentarse un incendio, inundación, sismo, ataques intencionales producidos por personas ajenas al área, observando que hasta el momento se ha trabajado de acuerdo al material existente dejando de lado las guías de las buenas prácticas.

4.No existe un plan único para todas las organizaciones, esto depende mucho de la capacidad de la infraestructura física como de las funciones que realiza en CPD (Centro de Procesamiento de Datos) más conocido como Centro de Cómputo.

5.El estudio de metodologías para la administración, gestión y gobernabilidad de TI, permitió identificar deficiencias generadas por la falta de procedimientos, políticas y estándares, por lo que concluimos que se puede lograr una mejora sustancial adoptando recomendaciones de una guía de buenas prácticas ajustada a las necesidades particulares de la organización.

6.Es necesario aplicar medidas de prevención y protección a nivel de software y hardware para evitar gastos futuros.

7.La Universidad Peruana Los Andes no cuenta con un Plan de Contingencia en sus sistemas informáticos siendo un requisito principal para la acreditación Universitaria.

RECOMENDACIONES

1. Se debe implementar el Servidor Espejo en la ciudad Universidad de Chorrillos para asegurar la confiabilidad, seguridad y viabilidad de los datos cuando estos se requieran luego de presentarse una contingencia en sus sistemas.
2. El control del acceso a los usuarios con respecto a los equipos y la información deberá estar limitado para garantizar que los datos y la información que se obtenga sea veraz y presentada de acuerdo a las necesidades y niveles de usuario, para que esta información no sea manipulada o utilizada para fines distintos a las normas y ética establecida
3. Se recomienda adquirir equipos adecuados que disminuyan los riesgos de pérdidas tanto de información como de materiales en caso se presentara un desastre natural o ataques intencionales producidos por personas ajenas al área.
4. Capacitando adecuadamente al personal en general se puede evitar el mal manejo de la información ya que esto puede traer consigo la pérdida total o parcial de la información almacenada. Conjuntamente depende mucho de la infraestructura física como de las funciones que realiza en CPD (Centro de Procesamiento de Datos) más conocido como Centro de Cómputo.
5. Promover la lectura de los manuales de los diferentes equipos, antes de una instalación y/o reparación del mismo para evitar problemas generados por la mala manipulación o desconocimiento del mismo, donde se detalle los procedimientos, políticas y estándares, por lo que concluimos que se puede lograr una mejora

sustancial adoptando recomendaciones de una guía de buenas prácticas ajustada a las necesidades particulares de la organización.

6. Adecuar el plan de contingencia ante los riesgos latentes para proteger a nivel general tanto el hardware como el software para asegurar el normal funcionamiento de los equipos y evitar gastos o pérdidas.
7. Es indispensable contar con un adecuado plan de contingencia en los sistemas informáticos de la UPLA ya que de esta manera contribuiremos con la acreditación Universitaria.

BIBLIOGRAFÍA

Meza, Francisco, Obregón Miguel (1997). Manual de Formación de Consultoría. IBM Educación.

Reyes, Fredy (2011). Indicadores para el Diagnostico de Madurez Informática. Guías de Clase del módulo de Gerencia de Sistemas Informáticos. Especialización de Gerencia Informática. Universidad EAN.

TienekeVerheijen, Annelies Van Der Veen, Ruby Tjassing, Mike Pieper, Axel Kolthof, Arjen de Jong, &Jan Van Bon. (2010). Fundamentos de ITIL V3. Van Harenpublishing.

Textos de Consulta:

Meza, Francisco; Obregón Miguel (1997). Manual de Formación de Consultoría. IBM Educación.

Reyes, Fredy (2011). Indicadores para el Diagnostico de Madurez Informática. Guías de Clase del módulo de Gerencia deSistemasInformáticos.Especialización de Gerencia Informática. Universidad EAN.

TienekeVerheijen, Annelies Van Der Veen, Ruby Tjassing, Mike Pieper, Axel Kolthof, Arjen de Jong, & Jan Van Bon. (2010). Fundamentos de ITIL V3. Van Harenpublishing.

Sitios Web:

–Universidad de Medellín, Centro Integral de Asesoría y Consultoría. http://www.udem.edu.co/UDEM/Extension/CentroAsesoriasCo

–Álvarez, Luis F; Zayas Enrique; Pérez Marisol. Consultoría Organizacional. http://www.monografias.com/trabajos15/consultoriaorganizacional/consultoria-organizacional.shtml

–Álvarez, Luis F (2005). Proceso de Consultoría Organizacional. http://www.gestiopolis.com/recursos4/docs/ger/econsultoria.ht m

–Codina, Alexis (2006). La consultoría: difusión de tecnología y formación gerencial. http://www.degerencia.com/articulo/la_consultoria_difusion_de _tecnologia_y_formacion_gerencial

–Álvarez, Luis F (2005). Proceso de consultoría organizacional. http://www.gestiopolis.com/recursos4/docs/ger/econsultoria.ht m

–Francavilla, Carlos (2009). Problemas de TI. http://cafrancavilla.wordpress.com/tag/problemas-it

–Fundación Iberoamericana del Conocimiento. Modelo Nonaka. http://www.gestiondelconocimiento.com/modelo_nonaka.htm

–Canales, Roberto (2005). Calidad en el desarrollo de Software. CMMI. http://www.adictosaltrabajo.com/tutoriales/tutoriales.php?pagin a=cmmi

–Tamayo, Alonso; Tamayo Johnny (2006). Guía para la formulación de un Plan de Contingencias. http://www.cibersociedad.net/congres2006/gts/comunicacio.php?id=309

–Secure and IT Proyectos (2012). ITIL / ISO 20000. http://www.secureit.es/index.php?page=seguridad&subpage=i so20k

–Osiatis S.A. ITIL – Gestión de Servicios de TI. http://itil.osiatis.es/Curso_ITIL

–Find the best (2012). Compare Help Desk Software http://help-desk-software.findthebest.com/compare/15-17-59/Request-Tracker-vs-Spiceworks-vs-Free-Help-Desk-Software

–Spyceworks (2012). Free PC & Network Inventory Software. http://www.spiceworks.com/free-pc-network-inventorysoftware/

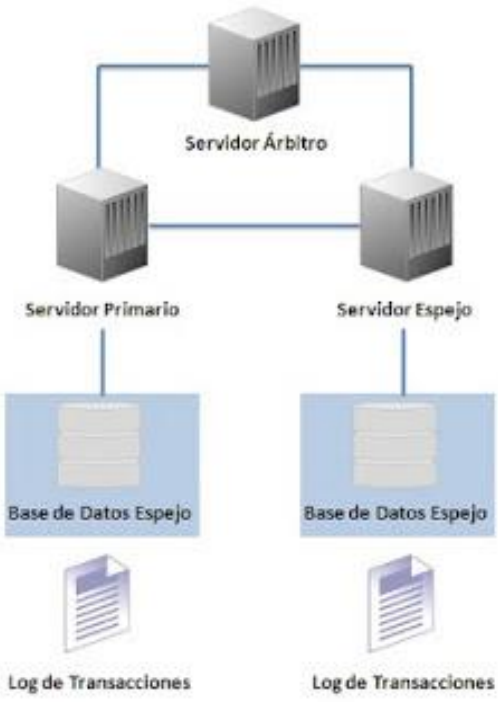
–Find the best (2012). Compare Remote Desktop Software. http://remote-desktop.findthebest.com/compare/1-3- 23/TeamViewer-vs-LogMeIn-Pro-vs-GoToMyPC-Pro

ANEXOS

Anexo 1 Manual para crear Servidor Espejo en Bases de Datos

Base de Datos Espejo (Database Mirroring) es una configuración donde dos o tres servidores de base de datos, ejecutándose en equipos independientes, cooperan para mantener copias de la base de datos y archivo de registro de transacciones (log).

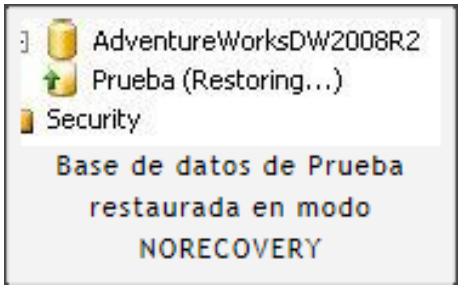
Tanto el **servidor primario** como el **servidor espejo** mantienen una copia de la base de datos y el registro de transacciones, mientras que el tercer servidor, llamado el **servidor árbitro**, es usado cuando es necesario determinar cuál de los los otros dos servidores puede tomar la propiedad de la base de datos. El árbitro no mantiene una copia de la base de datos. La configuración de los tres servidores de base de datos (el primario, el espejo y el árbitro) es llamado Sistema Espejo (Mirroring System), y el servidor primarioy espejo juntos son llamados Servidores Operacionales (Operational Servers) o Compañeros (Partners).



Para hacer el mirror, es necesario como mínimo 2 instancias y como máximo 3. Si utilizamos 2 instancias, una de ellas contiene la base de datos y la otra la espejo.
El detalle de esta configuración es que el failover no es automático y se necesita intervención humana. Si utilizamos 3 instancias, entonces utilizamos una de ellas como witness server y permite que el failover sea automático, osea que cuando una caiga, la otra se ponga en marcha. Para ello el witness server se encarga de "mirar" el estado de las 2 instancias y cuando una de ellas cae, pone la otra en marcha.
Hacer el mirror son dos pasos principales:
1. Copiar y restaurar la base de datos de la que queremos hacer el mirror desde una instancia a la otra
2. Configurar el asistente de configuración del mirror.
Vamos un ejemplo paso a paso.
Lo primero que tenemos que hacer es hacer un reflejo de nuestra base de datos en otra instancia. En nuestro ejemplo esta base de datos se denomina prueba.

Debemos hacer copia de seguridad de la base de datos y del log (Ojo, la base de datos debe estar en modo Full) con estas sentencias:
Backup Database Prueba to Disk='D:\prueba.bak';
Backup Log Prueba to Disk='D:\logprueba.bak;
Una vez hecha la copia de seguridad, copiamos los ficheros y los restauramos otra instancia donde queremos hacer el reflejo con estas sentencias
Restore Database Prueba from Disk='D:\prueba.bak' with NORECOVERY;
Restore Log Prueba from Disk='D:\logprueba.bak with NORECOVERY;

Fijémonos que tanto la restauración del fichero de datos como el del log, son con el parámetro NORECOVERY. Esto es muy importante porque estamos diciendo al SQL Server que restauramos la base de datos pero que no la ponga en marcha y que la deje lista para poder aplicar más logs, osea los logs que vendrán de la otra base de datos cuando comience el mirror.

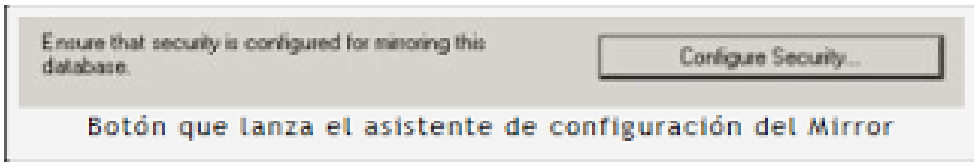


Base de datos de Prueba restaurada en modo NORECOVERY

Una vez tenemos hecha la restauración de la base de datos que queremos reflejar en la otra instancia, ya podemos configurar el mirror. Para ello, pulsamos en la primera instancia con el botón derecho del ratón sobre la base de datos, y seleccionamos **Propiedades**. En el cuadro de diálogo de las propiedades de la base de datos, seleccionamos la opción **Mirror**.

Opción Mirror de las propiedades de la base de datos

Vemos que aparece un cuadro de diálogo con las opciones de configuración del mirror. Para comenzar a configurarlo, seleccionamos el botón **Configure Security**.

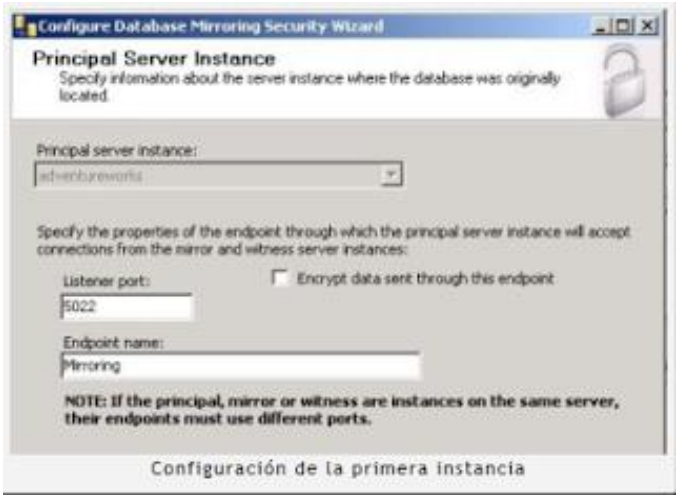


Botón que lanza el asistente de configuración del Mirror

Vemos que aparece el asistente de configuración del mirror. Lo primero que nos pregunta es si queremos utilizar un witness server. Indicamos que sí. Después debemos indicarle que queremos configurar las 3 instancias para poder hacer el failover automáticamente.

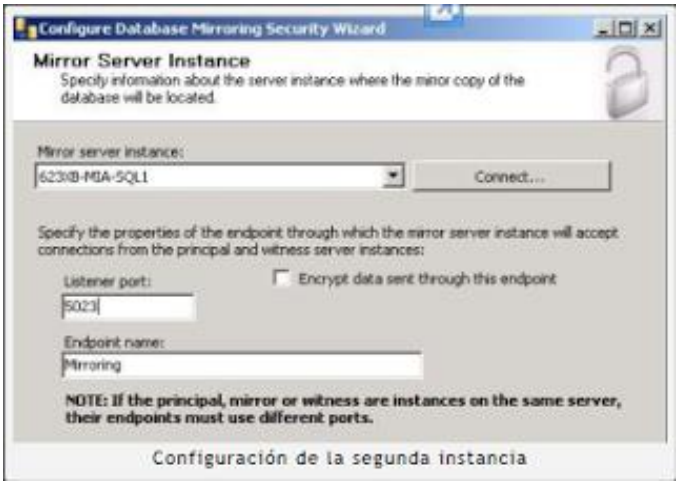
Configuración de las 3 instancias del mirror

Seguidamente indicamos la instancia que contendrá la base de datos en sí. Fijémonos que por defecto, el asistente abre el puerto 5022 para comunicarse con el resto de instancias. Dicho puerto y el resto que se configuran en el asistente, deben estar abiertos en los firewalls de windows. Fijémonos también que hemos quitado la opción de cifrado, ya que en esta configuración, no tenemos habilitado el cifrado de la base de datos.



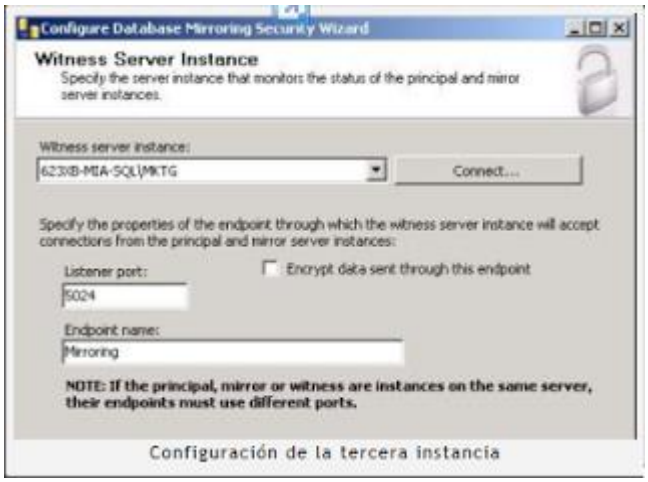
Configuración de la primera instancia

Seguidamente configuramos la segunda instancia que será la que contendrá el reflejo de la base de datos. Fijémonos que por defecto configura el puerto 5023.



Configuración de la segunda instancia

Por último nos queda configurar el witness server que estará en una tercera instancia. Fijémonos que por defecto configura el puerto 5024.

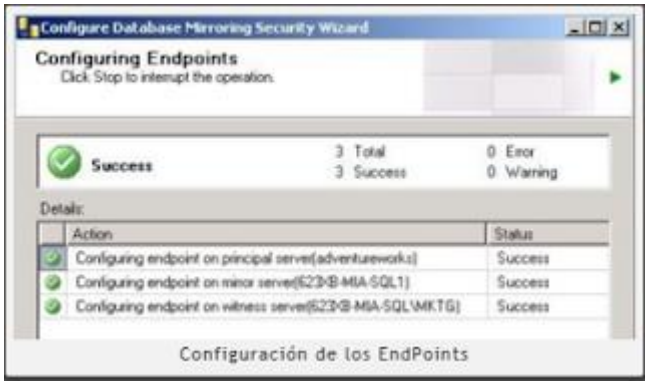


Configuración de la tercera instancia

Un último paso en el asistente es configurar la seguridad. Aquí debemos indicar una cuenta con permisos para acceder al SQL Server. Por ejemplo, podemos indicar la cuenta con la que arrancan los servicios de las instancias.

Configuración de la seguridad del mirror

Para acabar con el asistente pulsamos en **Finish**. El asistente se pondrá a configurar los puertos (Endpoints) en cada instancia y acabará.



Configuración de los EndPoints

Anexo 2 Manual de buenas prácticas de Servidores y Sistemas

A pesar de los esfuerzos de los administradores de sistemas en muchas ocasiones la información sensible, los sistemas y redes pueden comprometerse por acciones maliciosas que pasan inadvertidas.

Se indican a continuación unos consejos de administración de sistemas sencillos, de forma que sea más fácil fiabilizar el sistema con un número mínimo de interrupciones de servicio a los usuarios. Este documento proporciona un conjunto de recomendaciones para ayudar a

mantener un nivel de seguridad aceptable en términos de confidencialidad, integridad, disponibilidad y autenticación mutua.

A lo largo de este documento el término "servidor" se utiliza para indicar una combinación de hardware, sistema operativo, servicio de red, software de aplicación y conexión de red.

1. **Aprenda sobre su sistema**
   - Lea los boletines de seguridad de los fabricantes que estén disponibles
   - Suscribase a los boletines de seguridad de fabricantes y otras fuentes de información relevantes en materia de seguridad
   - Comprenda las problemáticas de seguridad en relación a su configuración y entorno
   - Monitorice la información de los websites de forma rutinaria en busca de información relativa a sus sistemas y actualizaciones de seguridad
2. **Defina los equipos críticos**

   Un equipo crítico es un equipo, el cual, si se compromete, podría producir daños significativos en la red local o en el exterior: dañar la reputación, interrupción de tareas críticas, revelación de información confidencial o incumplimiento de la ley vigente, por ejemplo, un servidor que contiene datos confidenciales, registros médicos, información de pagos, números de la seguridad social, etc. "¿Qué es lo que se trata de proteger?" es una buena pregunta para definir los equipos críticos.

3. **Actualizar el software de antivirus**

   Es importante disponer de software de detección de antivirus y eliminar las amenazas de los servidores. Las actualizaciones automáticas del software de antivirus son fundamentales para asegurar que se detectan los nuevos virus de forma sistemática. Es la responsabilidad del administrador de sistemas el asegurar que el software de detección contiene definiciones actualizadas de los patrones de virus.

4. **Protección de passwords**
   - Utilice passwords de longitud suficiente, preferiblemente caracteres de diferentes grupos entre letras mayúsculas, minúsculas, números y simbolos.
   - Utilice passwords que sean fáciles de recordar, pero que sean difíciles de adivinar por otros
   - No utilice palabras de diccionario
   - Nunca almacene passwords como texto plano o las escriba e nun papel
   - Configure opciones de caducidad de passwords
   - Almacene las passwords cifradas
5. **Configure únicamente los servicios esenciales**
   - Instale únicamente los componentes y servicios esenciales, los que se requieren para lanzar servicios y aplicaciones
   - Ofrezca solo servicios de red y del sistema operativo imprescindibles en el servidor
   - Cierre los puertos UDP/TCP abiertos que sean innecesarios
   - Elimine las cuentas antiguas
   - No proporcione más permisos de acceso a los recursos del sistema que el usuario necesita
6. **Actualice sus sistemas**
   - Mantenga al día la instalación de parches y actualizaciones
   - Lea la información sobre los parches antes de aplicarla
   - Acuerdese de aplicar actualizaciones después de una instalación
   - Actualice también las aplicaciones, no solo los sistemas operativos
7. **Proteja sus sistemas de spyware**
   - El spyware y adware amenaza la privacidad y la productividad. Es importante protegerse de este software malicioso y protege rnuestros sevidores (cuando es posible) con herramientas anti-spyware.
8. **Utilice un firewall** El firewall gestiona el tráfico de red entrante y saliente de la misma, y sirve como primera línea de defensa contra las amenazas externas. Es importante documentar los cambios realizados en la configuración del firewall.
   - Defina una política de seguridad en el acceso

- Configure autenticación de usuario
- Configure los servidores con controles de acceso a archivos y dispositivos.
- Configure el servidor para administración remota segura

9. **Asegure la seguridad e integridad de los datos**
    - Cifre los datos sensibles cuando sea necesario y posible
    - Reemplaza los programas inseguros con programas seguros
    - Evite almacenar las passwords y claves privadas en texto claro
    - Elimine datos de forma segura de los sistemas de almacenamiento
10. **Monitorice su sistema**
    - Lea su archivos de logs (lso hackers también los leen)
    - Utilice analizadores de logs
    - Escanee sus sistemas de forma periodica con herramientas apropiadas (escanear, evaluar, actualizar, corregir y reescanear)
    - Refuerce sus políticas de control de acceso/restricciones de usuario
    - Elimine las cuentas antiguas de los servidores
11. **Documente configuraciones y elabore un plan de contingencia**
    - Documente cambios en la configuración de sistema
    - Documente (en pasos) un plan de contingencia y compártalo con el resto del personal IT
12. **Disponga de un plan de backup**
    - Asegurese que ha verificado su estrategia de recuperación de información
    - Actualice su plan de backup anualmente
    - Forme a los operadores que trabajan con usted (si hay)
    - Contemple un plan de contingencia
    - Debe realizarse copia de seguridad de los datos al menos una vez al día, otros datos pueden necesitar copias de seguridad
    - Las copias de seguridad deben de almacenarse en lugar seguro para evitar robo o daño de los datos almacenados.