ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"PROPUESTA DE UN PLAN DE CONTINGENCIA Y CONTINUIDAD DEL NEGOCIO PARA EL DEPARTAMENTO TIC EN UNA INSTITUCIÓN DE EDUCACIÓN ESTATAL UBICADA EN LA PROVINCIA DE SANTA ELENA"

EXAMEN DE GRADO (COMPLEXIVO)

Previo a la obtención del título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

KARINA ALEXANDRA VILLAO RODRÍGUEZ

GUAYAQUIL- ECUADOR

AÑO 2016

AGRADECIMIENTO

Primeramente a Dios, por darme la bendición de permitirme ingresar a estudiar y culminar esta maestría.

Sincero agradecimiento a todos y cada uno de los profesores del MSIA IV, por su valiosa enseñanza que me servirá en el campo profesional, al Ing. Lenin Freire, por brindar su guía y apoyo en el proceso de culminación.

Gratitud a mis compañeros de maestría, a los diferentes grupos establecidos dentro del aula, principalmente a los que compartieron sus conocimientos, a los compañeros de la ESPOL, de igual manera a mis compañeros de proyectos y a quienes me ofrecieron su amistad, siempre los recordare a todos.

Karina Villao R.

DEDICATORIA

A mi familia, especialmente a mis padres queridos, a quien les debo lo que soy, mi mami por darme su voz de aliento y fortaleza para que siga adelante en los estudios, siempre brindando su ayuda y anhelando lo mejor para sus hijos.

De igual manera a mi apreciada tía Luz Amada, por brindarme constantemente su apoyo incondicional, además de demostrarme afecto.

Karina Villao R.

TRIBUNAL DE SUSTENTACIÓN

ING. LENIN FREIRE

DIRECTOR MSIA

MGS. ALBERT ESPINAL

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

MGS. RONNY SANTANA

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

RESUMEN

El presente trabajo muestra un análisis realizado al Departamento TIC de una Institución de Educación Estatal, ubicada en la Provincia de Santa Elena, donde se determina los riesgos a los que puede estar expuesto debido a ciertos factores sean naturales o inducidos.

Se determinó las vulnerabilidades existentes y se analizaron las posibles amenazas que podrían afectar los servicios académicos que utilizan sus estudiantes y los docentes

En el presente trabajo se indican estrategias para la Continuidad de Negocio y se propone un Plan de Contingencia.

Finalmente se indica el procedimiento para el retorno a las instalaciones principales del Departamento TIC, sin que se vean afectados los servicios después de un incidente.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

IBM	International Business Machines Corp.
TIC	Tecnologías de la información y comunicación

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Hoy en día, las diferentes entidades dependen mucho de la tecnología en el desarrollo de sus actividades normales, por lo que es fundamental contar con un Plan de Contingencia y Continuidad del Negocio, para en el caso de que se presente algún acontecimiento natural o de cualquier otra índole poder restaurar los equipos y sistemas lo más pronto posible.

Motivo por el cual se decide realizar la propuesta de este plan para el Departamento de Tecnología de Información y Comunicación TIC de la Institución de Educación Estatal, ubicada en la Provincia de Santa Elena, teniendo en cuenta la importancia de tener acceso a la información actualizada mediante el uso de las aplicaciones.

A través del presente trabajo se analiza las vulnerabilidades además de los posibles riesgos, obteniendo un plan con estrategias que permitan la prevención de daños en los equipos y sistemas ante un incidente, brindará orientación en la restauración del Departamento de tal manera que puedan

continuar con los procesos indispensables, como registro de notas, consultas de record académico de estudiantes, control de planes de clase, distributivos docentes, fichas de datos personales para docentes y estudiantes.

CAPÍTULO 1

PLANTEAMIENTO DEL PROBLEMA

1.1 IDENTIFICACIÓN DEL PROBLEMA

La Institución de Educación trabaja diariamente a través de sistemas informáticos con datos de estudiantes y docentes, realizando ingreso y consulta de notas, manejo de sílabos, además como apoyo para las clases usa la plataforma Moodle y Edmode, que se encuentra alojado en servidores dentro del Departamento de las TIC, cuya información debe estar disponible para el personal administrativo, docentes y estudiantes. Es decir cuenta con algunos servicios importantes en su mayoría en línea, para el desarrollo de las actividades, pero lastimosamente carece de infraestructura y seguridades.

La institución está ubicada en la Provincia de Santa Elena, que posee constantes cortes de energía, además debido a la predicción de amenaza natural del fenómeno del niño y al tener la Provincia características físicas del suelo y su topografía casi plana lo hace que algunas áreas sean propensas a inundaciones cuando ocurren lluvias fuertes debido a la baja capacidad de infiltración que posee el suelo, pudiendo ocasionar áreas con agua que pueden pasar meses antes de que el agua se pueda evaporar completamente [5]. Todos estos factores generan riesgos que pueden ocasionar pérdida de datos, servicios, daños de software y hardware, motivos para impulsar la elaboración de un Plan de Contingencia y Continuidad del Negocio, que permita retornar de manera rápida a las actividades académicas frente a un incidente, reduciendo el impacto y evitando exista pérdida de información.

1.2 CONFORMACIÓN DEL DEPARTAMENTAMENTO TIC Y SU UBICACIÓN

1.2.1 DEPARTAMENTAMENTO TIC

El Departamento está conformado por el Director TIC y dos grupos que abarcan los sistemas y las redes.

Figura 1.1: Departamento TIC

Elaborado por: Karina Villao Rodríguez

1.2.2 UBICACIÓN

La Institución de Educación Estatal está ubicada en el cantón La Libertad de la Provincia de Santa Elena.

El Departamento TIC de la Institución se encuentra en una edificación de una sola planta, el área que esta frente al ingreso no se encuentra pavimentado y parece que fuera es un espacio destinado para áreas verdes (tierra).

1.3 ACTIVOS Y SERVICIOS QUE POSEE EL DEPARTAMENTO TIC

El departamento TIC posee los siguientes activos y servicios que se usan para las actividades académicas.

- Redes de Comunicaciones.

- Servidor de Base de Datos.
- Servidor Web.
- Servidor de Aplicaciones.

- Sistema Académico.
- Correo Institucional.
- Sistema de Talento Humano.
- Sistema de Relaciones Externas.
- Sistema de Líneas de Investigación
- Sistema de Vinculación
- Sistema PAPP

Servicios a estudiantes y docentes

Estudiantes

- Consulta de calificaciones
- Matriculación

Docentes

- Registro de calificaciones WEB
- Plan de clase

1.4 LISTADO DE SERVICIOS DE LA INSTITUCIÓN CONSIDERADOS PRIORITARIOS EN EL MOMENTO DE PRESENTARSE UNA EVENTUALIDAD.

A continuación se lista los servicios considerados de mayor prioridad, para ser recuperados ante un siniestro:

- Suministro de Energía
- Documentación de inventarios, diagrama de red.

Hardware y Software

- Conectividad de Red Interna

- Conectividad de Red Externa
- Internet
- Servicio de DNS y DHCP
- Correo Electrónico Institucional
- Controlador de Dominio
- Servidor de Base de Datos Institucionales
- Servidor Web
- Respaldo de Información, instaladores de software, licencias

1.5 ANÁLISIS DE LOS PROCESOS Y LOS RIESGOS

Dentro de las principales actividades diarias que se realizan en la Institución de Educación a continuación se enlistaran las principales con el nivel de impacto en la institución:

Tabla 1: Proceso y su impacto

PROCESO	IMPACTO EN LA INSTITUCIÓN
INGRESO DE NOTAS	ALTO
RECORD ACADEMICO (TODAS LAS NOTAS DE LOS ESTUDIANTES)	ALTO
INGRESO DE SILABO	MEDIO

MATRICULACIÓN EN LÍNEA	MEDIO
INGRESO DE PLANES DE CLASE	ALTO
AULAS VIRTUALES MOODLE	ALTO
SERVICIO DE EDMODO	ALTO
CORREO INSTITUCIONAL	MEDIO
INGRESO Y CONSULTA DE DATOS PERSONALES EN FICHAS DE ESTUDIANTES Y DE DOCENTES	MEDIO

Elaborado por: Karina Villao Rodríguez

1.6 IDENTIFICACIÓN DE AMENAZAS

Se procede a identificar la probabilidad de que ocurran las siguientes amenazas, que podrían ocasionar interrupciones en las actividades relacionadas a la academia. [1]

Tabla 2: Probabilidad de amenaza

DESCRIPCIÓN	PROBABILIDAD DE AMENAZA		
	ALTA	MEDIA	BAJA
Inundación ocasionada por lluvias en el fenómeno del niño	X		
Interrupciones en el sistema eléctrico	X		
Incendio		X	
Falla del acondicionador de aire		X	
Robo de equipos			X
Humedad		X	
Pérdida de Información	X		

Elaborado por: Karina Villao Rodríguez

1.7 IDENTIFICACIÓN DE AMENAZAS

Se presentan escenarios, las vulnerabilidades existentes para el escenario y los riesgos que podrían suscitarse.

Tabla 3: Escenarios y sus vulnerabilidades

ESCENARIO	VULNERABILIDAD	RIESGO
INUNDACIÓN DEL DEPARTAMENTO TIC	• El área frente a donde se ingresa al departamento está por debajo del nivel donde pasa la alcantarilla, por lo que esa área no se puede conectar al alcantarillado de aguas residuales. • Está ubicada en un lugar propenso a desastres naturales. • Cuando llueve con viento el agua ingresa por los filos de las ventanas. No existe protección. • La edificación del Departamento no	En el caso de presentare el fenómeno del niño, al haber constantes lluvias, el agua se queda estancada y podría ingresar agua al Departamento ocasionando daños.

	posee canaleta para agua de lluvia.	
INTERRUPCIONES EN EL SISTEMA ELÉCTRICO	• Inestabilidad en la energía eléctrica, aumenta o disminuye su voltaje, o el servicio se pone intermitente, cuando existen constantes lluvias. • La Institución de Educación no posee equipos necesarios para la protección de equipos y para suministrar energía y seguir operando. • Carece de un Plan de recuperación.	Fallo en sistemas y daño de equipos. Dejan de funcionar los sistemas y se deja de prestar los servicios.
FUEGO OCASIONADO POR CORTOCIRCUITO	• En el departamento hay materiales inflamables, papel, cartones de periféricos, con rollos de cable. • No existe instalado un sistema de alarma contra incendio y detector de humo.	Por inundación o por fallos eléctricos se puede generar un cortocircuito, ocasionando un incendio. Puede haber pérdidas materiales y humanas

FALLA DEL ACONDICIONADOR DEL AIRE	• En la Institución no existe una planificación de mantenimiento preventivo y correctivo.	Los equipos pueden presentar daños al no estar en la temperatura adecuada.
ROBO DE EQUIPOS EN HORAS NO LABORABLES	• Escasos guardias. • El Departamento carece de instalación de alarmas y cámaras de seguridad. • No posee una adecuada protección de equipos.	Ingreso de personal a robar equipos.
HUMEDAD	• No existe detector de humedad.	Puede existir falla en los equipos.
PÉRDIDA DE INFORMACIÓN	• No se cuenta con un sitio alterno de respaldo. • No se cuenta con un servicio de backup externo para continuidad del negocio.	Pérdida parcial o total de la información.

Elaborado por: Karina Villao Rodríguez

CAPÍTULO 2

DESARROLLO DEL PLAN DE CONTINGENCIA

2.1 ESTRATEGIAS DE CONTINUIDAD

Para mantener la continuidad de los servicios ante posibles riesgos, se debe cumplir con los siguientes requerimientos, necesarios para salvaguardar la integridad de los activos mediante el respaldo y aseguramiento de equipos. [2] [3]

Seguridad del Edificio

- Se debe instalar en el departamento cámaras de seguridad.
- Instalar detector de humo, alarma contra incendio.
- Instalar sensores de humedad
- Colocar canaletas para agua de lluvia

- Sellar las uniones de las ventanas y los boquetes con silicona.
- Realizar mantenimiento preventivo de acondicionadores de aire, además de tener sistemas de acondicionadores de aire con exceso de capacidad.
- Mantener lleno los extinguidores de incendio tipo C.

Seguridad de Fallos Eléctricos

- Instalación de UPS de características que proporcione energía de reserva a corto plazo a todos los componentes del sistema.
- Generadores eléctricos diesel o a gasolina para proveer energía a largo plazo.

Seguridad de Activos Informáticos

Se debe asegurar de tener en el lugar alterno o un lugar seguro la siguiente documentación:

- Tener el inventario actualizado de equipos del área.
- Copia de licencias de software.
- Tener las configuraciones de los equipos y de la red.

- Listado de números de teléfono de empresa de seguro de equipos, de proveedores de venta de repuestos o la empresa que preste los servicios de backup.

Para poder asegurar el uso de todos los sistemas y servicios de la Institución, deberá realizar copias de seguridad o backup de lo siguiente:

- Sistemas Operativos
- Software y Lenguajes de programación
- Sistemas Comprados incluir licencias
- Sistemas Desarrollados por el departamento TIC con su respectivo programa fuente.
- Base de Datos

Además se deberá:

- Adecuar un sitio que sirva para operar como Departamento TIC Alterno
- Centro de replicado
- Contratar un seguro de equipos informáticos.

- Realizar copias de seguridad de los servidores, mediante backup éste respaldo será guardado en una bóveda, que debe cumplir con las medidas de seguridad necesarias. Se lo realizará dos veces al año que cubrirán la culminación de periodos académicos.

De ser posible de acuerdo a la factibilidad de la Institución deberá considerar contratar una Empresa que gestione y proteja los activos de datos como **IBM Spectrum Protect**, que realiza copia de seguridad, recuperación, archivado y recuperación tras desastre. Esta sería una solución completa.

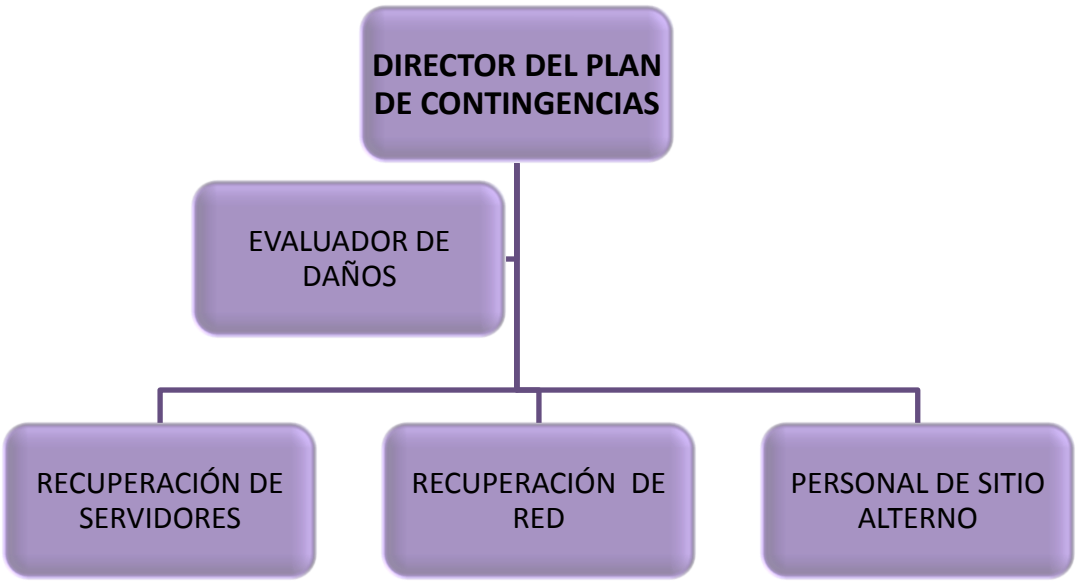
2.2 ASIGNACIÓN DEL PERSONAL DEL PLAN DE CONTINGENCIA

Se debe conformar un equipo capacitado, quienes se encargaran de la recuperación de equipos con los respectivos sistemas, de acuerdo al Plan establecido, permitiendo retornar a las actividades académicas con normalidad en el menor tiempo posible.

El grupo deberá estar integrado por personal asignado de acuerdo a su experiencia y a las actividades que realizan dentro del Departamento, entre los cuales se deberá contar con evaluadores de daños, encargados de recuperación de servidores, equipo de recuperación de red, encargado de poner en funcionamiento el sitio alterno, y otros dependiendo de la magnitud y naturaleza del desastre, estarán bajo las

órdenes del Director del Departamento de TIC, quien será denominado Director del Plan de Contingencia. [1]

Figura 2.1: Personal del Plan de Contingencia



Elaborado por: Karina Villao Rodríguez

2.3 PLAN DE CONTINGENCIA DEL DEPARTAMENTO TIC EN EL CASO QUE SUCEDAN CIERTOS INCIDENTES

Prevención

Incendio

- El director de TIC debe contar con un mapa de salida de emergencia.

- El área debe tener extintores de tipo C (Dióxido de carbono, Polvo Químico Seco o Halon) debidamente cargados, el personal debe conocer su ubicación y estar debidamente capacitado en su uso.
- Tener linternas con batería.
- Tener instaladas alarmas contra incendios.

Referente a los equipos

- Tener respaldos actualizados en el sitio alterno y externamente.
- Tener el inventario de equipos del área.
- Tener las configuraciones de los equipos y de la red.

Humedad

- Revisar periódicamente los techos y paredes propensos a humedad, colocarles impermeabilizantes.
- Ubicar en sitios seguros equipos, software y documentación como los inventarios de equipos, que serán necesarios y de mucha utilidad después de una contingencia.

Para equipos

- Tener plástico de gran dimensión para cubrir los equipos que corran riesgo de humedecerse.

- Tener plástico de gran dimensión para cubrir los equipos que corran riesgo de humedecerse.

Robo

- Colocar cámaras de seguridad y alarma contra robo.

- Prohibición de sacar equipos sin autorización

Inundación

- Revisar que no se encuentren tomacorrientes o regletas en el suelo o muy cerca del suelo, lo aconsejable subir los tomacorrientes a la pared.

- Revisar que las alcantarillas se encuentran limpias.

- Tratar que la edificación tenga conexión a la alcantarilla.

- Alzar equipos que se encuentren en el suelo.

Acciones durante

Incendio

- El personal del área deberá usar los extintores.

- Encender la alarma de incendio.
- Una vez revisado que existen respaldos apagar el equipo.

Humedad

- Verificar de donde proviene la humedad
- Colocar en un lugar seguro lo equipos y documentos.
- Tapar con los plásticos los equipos y documentos.

Robo

- El colaborador deberá indicar sobre el robo suscitado al Director de TIC, a su vez a la Dirección Administrativa y a la Fiscalía General del Estado, para que se dé inicio a la investigación.

Inundación

- El colaborador deberá indicar de la inundación al Director del TIC y demás compañeros revisar que los equipos estén alzados si no desconectar y alzar.

Después

- Analizar los daños.

- Que el grupo de contingencia realice las acciones pertinentes de acuerdo al plan. [4]

CAPÍTULO 3

PUESTA EN PRÁCTICA LOS PROCEDIMIENTOS DE CONTINUIDAD

3.1 NOTIFICACIÓN DEL INCIDENTE

La persona que se percate de la contingencia, debe dar aviso al Director de TIC, quien a su vez notificará lo suscitado a las autoridades y a su respectivo equipo de contingencia, para poner en marcha el Plan para realizar la recuperación en el menor tiempo posible..

3.2 EVALUACIÓN DE DAÑOS

Lo primero que se necesita hacer es realizar la valoración de los daños, el personal encargado tratará de levantar la mayor información de la situación de los bienes materiales y equipos y sistemas de información

después de un incidente. Lo que será indispensable antes de empezar a tomar acciones.

3.3 EJECUCIÓN DEL PLAN

Se pone en marcha el Plan de contingencia, con el equipo de recuperación, se empezará a movilizar el material necesario para la ejecución del Plan.

3.4 RECUPERACIÓN

Autorizado el inicio de la recuperación, se procede a restablecer los servicios y bases de datos según su importancia, de tal manera que se cuente con el ingreso de notas, record académico (todas las notas de los estudiantes), Ingreso de planes de clase, aulas virtuales Moodle, servicio de Edmodo, correo institucional, ingreso de silabo, Matriculación en línea, ingreso y consulta de datos personales en fichas de estudiantes y docentes, para tener estos procesos se debe:

- Puesta en marcha del Departamento TIC alterno si se tuviera que hacerlo.
- Restaurar los servidores.
- Restaurar el último backup.

Luego se realiza la restauración de sistemas y la comprobación del correcto funcionamiento que permitan brindar los servicios antes indicados.

3.5 RETORNO A LAS INSTALACIONES DEL DEPARTAMENTO TIC AFECTADAS

Luego de restaurar los principales servicios, se debe reunir el equipo de recuperación para planificar el retorno a las instalaciones.

Se identificará de acuerdo al inventario un análisis de lo que se debe recuperar, notificándose el listado al personal pertinente (Director Administrativo), para que se realice su adquisición lo más pronto posible.

El tiempo de retorno a la normalidad de operaciones variará de acuerdo a los daños que se indiquen en el análisis el nivel de afectación de la infraestructura y equipos, lo que se debe mantener durante el tiempo de retorno es la prestación de todos los servicios y que estos cambios no interrumpa las actividades académicas.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Debido a que existen algunos riesgos a los que se podría estar expuesto y la importancia de salvaguardar el Departamento TIC y los servicios que ofrece, se hace necesario la aprobación del Plan de Contingencia y Continuidad del Negocio, con lo que se aseguraría que no exista interrupciones por largo tiempo en sus procesos y estaría prevenido ante cualquier escenario de los que se identificaron.

2. Se obtuvo un listado de vulnerabilidades que tiene la Institución lo que será de ayuda para su corrección.

RECOMENDACIONES

1. Realizar todas las instalaciones que se recomiendan para prevención como: Adquirir y realizar el equipamiento necesario para respaldo y

2. poder contar con el Departamento TIC Alterno, y realizarse las debidas instalaciones eléctricas.

3. Una vez aceptado el Plan de Contingencia debe prepararse al personal y efectuar pruebas y mantenimiento del mismo.

BIBLIOGRAFÍA

[1] Juan Gaspar Martínez, “El Plan de Continuidad del Negocio”. McGraw-Hill Interamericana, 2da Edición.

[2] NTE INEN-ISO 22301, Protección y seguridad de los ciudadanos. Sistema de gestión de la continuidad del negocio (sgcn) especificaciones (ISO 22301:2013, idt).pdf.

[3] ISO 22301, Estándar Internacional, Seguridad de la Sociedad: Sistemas de Continuidad del Negocio - Requisitos

[4] Compendio General ante Desastres. http://www.binasss.sa.cr/poblacion/desastres.htm

[5] Prefectura Provincia de Santa Elena, Plan de Contingencia Ante el "Fenómeno del Niño"