PLAN DE CONTINGENCIAS PARA EL ÁREA DE TECNOLOGÍAS DE LA INFORMACIÓN DE CTT-ESPE-CECAI INNOVATIVA SEDE SANGOLQUI.

Alcívar, Lilian

Departamento de Ciencias de la Computación; Universidad de las Fuerzas Armadas, Sangolquí, Ecuador

Resumen: Previo a la elaboración del plan de Contingencias para INNOVATIVA, se realizó el estudio de factibilidad, del que se concluyó que dicho plan se elabora bajo las premisas y condiciones que se detallan a continuación.

- **Factibilidad técnica**.- es factible elaborar un plan de contingencia con el personal técnico con el que se cuenta actualmente y el mismo estará en la capacidad de ejecutarlo.
- **Factibilidad tecnológica.-** Se recomienda realizar un convenio con la Universidad de las Fuerzas Armadas para que se pueda operar en uno de sus servidores caso de algún desastre o contingencia.
- **Factibilidad operativa.-** El espacio físico con el que cuenta Innovativa es suficiente para poder implementar algunas medidas de seguridad necesarias como el colocar extintores de incendios.
- **Factibilidad operacional.-** El objetivo principal de este plan contingencias es asegurar continuidad de las operaciones de Innovativa. Y para garantizar su operacionalidad se tomarán en cuenta cuatro etapas evaluación, planificación, ejecución y recuperación.
- **Factibilidad económica.-** Los gastos más importantes ya han sido cubiertos y se encuentran en marcha proyectos de adquisición de los equipos necesarios.
- **Factibilidad legal.-** Las normas que deben tomarse en cuenta para la ejecución del plan de Contingencia son: Normas de Control Interno para el Sector Público, NFPA 10 Norma para extintores portátiles contra incendios y NFPA 75 Norma para la protección de equipos de Tecnología de la Información.
- **Factibilidad ética.-** Este proyecto será totalmente ético ya que será desarrollado a la vista de todos y estará disponible para todos los interesados, además se regirá a todas las leyes, normas y reglamentaciones para que el Estado Ecuatoriano y la normativa interna de la empresa exijan.

En su parte medular, el Plan de Contingencias se ha estructurado en tres matrices de control, matriz de controles de prevención, de mitigación y de recuperación. Cada una de estas matrices consta de un código, la descripción del control y el responsable de ejecutarlo.

Palabras clave: factibilidad, plan, contingencias, controles, prevención, mitigación, recuperación

Abstract: A feasibility study was conducted prior to the development of the Contingency Plan for INNOVATIVA. The conclusion of the study was that the mentioned plan was developed based on the premises and conditions listed below.

- **Technical feasibility:** Feasibility of the development of a contingency plan with the help of the current available technical staff. This staff will have the ability to run it.
- **Technological feasibility**: It is recommended to establish an agreement with the University of the Military Forces so that they can operate in one of their servers in case of any disaster or contingency.
- **Operational feasibility:** The physical area available in INNOVATIVA is enough to implement some required security measures such as installing fire extinguishers.
- **Operational feasibility:** The main objective of this contingency plan is to ensure the continuity of INNOVATIVA operations. To ensure their operability four assessment stages will be considered: planning, execution, and retrieval.
- **Economic feasibility:** The major expenses have already been considered and projects have been developed to acquire the necessary equipment.
- **Legal feasibility:** The rules to be taken into account for the implementation of the Contingency Plan are: Internal Control Standards for the Public Sector, NFPA 10 Standard for Portable Fire Extinguishers and NFPA 75 Standard for protecting the Information Technology Equipment.
- **Ethical feasibility:** This project will be totally ethical as its development will be known by many people and the mentioned project will be available to all stakeholders. In addition, the the project will be governed by the laws, rules and regulations established by the Ecuadorian government as well as the enterprise internal regulations.

At its core, The Contingency Plan has been structured into three control matrices: a matrix for prevention, one for mitigation, and another for retrieval. Each of these matrices has a code, a control description, and a responsible for running it.

Keywords: feasibility plan, contingencies, controls, prevention, mitigation, retrieval.

Introducción

Innovativa, institución adscrita a la Escuela Politécnica del Ejército ESPE cuya misión es realizar transferencia de tecnología mediante el desarrollo de proyectos y prestación de servicios de capacitación, asesoría y consultoría para contribuir al desarrollo del país; sustentados en el conocimiento, innovación y estímulo de la investigación científica, cuenta con el Departamento de Tecnologías de Información, que es el encargado de Coordinar, supervisar, gestionar y ejecutar los procesos que permitan fortalecer la plataforma tecnológica de hardware y software de INNOVATIVA, mediante el uso de herramientas de tecnologías de información y comunicaciones, que faciliten la administración y aseguramiento de la información institucional.

Sin embargo el Área de TI, no tiene al momento un plan de contingencias que permita resolver inmediatamente los problemas que se suscitan, lo cual implica que este departamento no pueda aportar adecuadamente al cumplimiento de los objetivos estratégicos institucionales y conlleva a un mal uso de los recursos. Además las líneas de negocio que mantiene Innovativa, dependen directamente del correcto funcionamiento de la tecnología y de una pronta recuperación de posibles fallos.

Por lo tanto es necesario poner en marcha un plan de contingencias, que sea fiable y seguro para poder cumplir con los objetivos del negocio y satisfacer las necesidades del cliente eficientemente.

I. Metodología

1.1. La situación actual de Innovativa

Existe un manual de procedimientos el cual se encuentra subutilizado debido a la falta de socialización del mismo entre el personal.

Las instalaciones donde se desarrollan las actividades de Innovativa prestan vulnerabilidades en cuanto a la seguridad, por lo cual si se produjera un flagelo, los funcionarios no podrían ser prevenidos ni tendrían los elementos para mitigarlo, esto es un riesgo tanto para los equipos, para la información que ellos guardan y la integridad de las personas que ahí laboran.

ES necesario definir claramente el proceso de generación de respaldos, además los respaldos que generan reposan únicamente en las mismas instalaciones de Innovativa.

En lo que tiene que ver con la provisión de energía eléctrica las instalaciones que brinden poca seguridad a personal y equipos en cuanto a la cantidad y calidad de suministro; se pueden observar instalaciones, pero no existe la evidencia de que estén funcionando y prestando servicio a Innovativa.

La infraestructura de comunicaciones y redes de datos ha sido construida sin seguir estándares y no claramente definida.

1.2. Estudio de Factibilidad de elaborar el plan de contingencias para Innovativa

1.2.1. Factibilidad técnica

Para la parte desarrolladora los requerimientos de conocimiento del tema están cubiertos a satisfacción, debido a la formación académica, capacitación y experiencia profesional. Considerando las funciones y la capacitación del personal involucrado por parte de Innovativa se ha valorado al personal como muestra la Tabla 1 y la Tabla 2.

Tabla 1: Capacitación del personal

Cargo	Capacitación área	Capacitación alternativa	Capacitación en Seguridad y Contingencias	Capacitación en temas administrativos y otras
Diseñador Multimedia 1	Diseño de Páginas Web Diseño de Páginas Web Avanzado Suficiencia en Informática Técnicas y Tecnologías en la Educación	Redes LAN Redes WAN Inalámbricas Cableado Estructurado CISCO I y II Instalación, Configuración, Manejo de Linux Certificación Internacional de Microsoft IC3	Seguridades en Internet.	Negocios usando Internet Contabilidad Computarizada Relaciones humanas y Motivación
Diseñador Multimedia 2	Cursos de Moodle Cursos de Hot Potatoes	Curso de Power Builder V 7.0 Curso de Visual Basic V 6.0 Manejo de Administradores de Base de Datos SQL Server, Access.		Seminario de productos EPSON Seminario de Productos HP Seminario de la Microsoft (S.O Windows Stard Edition) Seminario de Productos Microsoft DeskTop, Servers Licensing Seminario de la Microsoft (Sales Specialist 2007, Productos Office 2007 Windows Vista y Servidores).
Jefe de Sistemas	Entrenamiento Asterisk Advanced dCAP Digium CISCO CCNA1 CISCO CCNA2 Administración “Microsoft Dinamycs Axapta 3.5” Integrador de Voice over IP		Taller de planificación de recuperación ante desastres	
Web Master	Entornos Virtuales de Aprendizaje Creación de entornos virtuales para el aprendizaje basados en la Web 2.0	Autocad Principiantes		Planificación Estratégica

Tabla 2: Valoración de Capacitación del personal

Recursos	Especialista de Sistemas	Jefe de Sistemas	Web Master	Maestrante	Promedio
Conocimiento de Primeros Auxilios	10%	50%	10%	50%	30.0 %
Conocimiento de Normas Legales	60%	90%	50 %	90%	72.5 %
Conocimiento de Redes	80%	90%	90%	90%	87.5 %
Conocimiento de Hardware	80%	90%	90%	90%	87.5 %
Conocimiento de Software	80%	90%	70%	90%	82.5 %
Conocimiento de Estándares	80%	80%	70%	90%	80.0 %
				Total Promedio	73.33 %

De lo expuesto, se puede concluir que es factible elaborar un plan de contingencia con el personal técnico con el que se cuenta actualmente y el mismo estará en la capacidad de ejecutarlo.

1.2.2. Factibilidad tecnológica

De los requerimientos mínimos para desarrollar este proyecto es indispensable contar con los recursos que se detallan en la tabla 3.

Tabla 3: Capacidad Tecnológica vs la requerida para una buena prestación de servicios.

Recursos	Requeridos	Existentes	Porcentaje
Servidores	2	1	50%
Equipos de Escritorio	27	27	100 %
Portátiles	9	9	100%
Impresoras y Escáneres	7	7	100%
Swicth	1	1	100%
Modem	1	1	100%
Gateway	1	1	100%
Router	1	1	100%

Se han considerado que físicamente deben existir dos Servidores para poder tener uno de respaldo en un sito alterno, el cual permita operar en caso de algún desastre o contingencia, debido al costo que puede tener adquirir un servidor, se recomienda realizar un convenio con la Universidad de las Fuerzas Armadas para que se pueda operar en uno de sus servidores.

1.2.3. Factibilidad operativa

Innovativa tiene mucho interés en que se cumpla con este requerimiento de contar con un plan de contingencias en el área de TI por lo cual existe el apoyo total en cuanto a facilitar los accesos a la información necesaria

El espacio físico con el que cuenta Innovativa es suficiente para poder implementar algunas medidas de seguridad necesarias como el colocar extintores de incendios.

El hecho de contar con un Data Center facilitará el implementar normas de control de acceso físico a los equipos más importantes y sensibles que posee Innovativa.

1.2.4. Factibilidad operacional

El objetivo principal de este plan contingencias es asegurar continuidad de las operaciones de Innovativa. Y para garantizar su operacionalidad se tomarán en cuenta cuatro etapas evaluación, planificación, ejecución y recuperación. Las dos primeras hacen referencia al componente preventivo y las últimas a la ejecución del plan una vez ocurrido el siniestro.

El Plan de Contingencias será socializado a las personas responsables de ejecutarlo y también a nivel directivo ya que el lenguaje utilizado contendrá términos técnicos que requieren de cierto conocimiento en el área de tecnologías de la Información, Se distribuirá de manera digital en formato pdf y se contará con dos ejemplares impresos que reposarán en el área de TI bajo la responsabilidad del jefe de área.

1.2.5. Factibilidad económica

Según el análisis realizado es sumamente importante la implementación de un firewall que mantenga resguardada la información de los servidores de Innovativa, esto podría haber sido un inconveniente debido al costo que tiene, pero actualmente se ha firmado ya un contrato para la adquisición e implementación del mismo.

1.2.6. Factibilidad legal

Las normas que deben tomarse en cuenta para la ejecución del plan de Contingencia son las siguientes:

a. *Normas de Control Interno para el Sector Público***.-** Al ser Innovativa una entidad pública y encontrarse bajo el ámbito de competencia de la Contraloría General del Estado, debe regirse a esta norma que en su apartado 400-09 habla sobre la seguridad general en los centros de procesamiento de datos y dice “Los centros de procesamiento de datos de la institución, establecerán mecanismos que protejan y salvaguarden contra pérdidas y fugas de los medios físicos (equipos y programas) y la información.”.

b. *NFPA 10 Norma para extintores portátiles contra incendios.- Esta norma está* dirigida a la selección, instalación, inspección y mantenimientos y prueba de equipos de extintores portátiles, se deberá tomar en cuenta todo lo que la misma considera para ser aplicada en el plan de contingencias.

c. NFPA 75 Norma para la protección de equipos de Tecnología de la Información.- El propósito de esta norma es el de establecer los requisitos mínimos para la protección del equipamiento de Tecnología de la Información y de las áreas para los equipos de tecnología de la información, de los daños ocasionados por el fuego o por sus efectos asociados, es decir, humo, corrosión, calor y agua.

1.2.7. Factibilidad ética

Este proyecto será totalmente ético ya que será desarrollado a la vista de todos y estará disponible para todos los interesados, además se regirá a todas las leyes, normas y reglamentaciones para que el Estado Ecuatoriano y la normativa interna de la empresa exijan.

1.3. Diseño del Plan de Contingencias para Innovativa

En la fase del análisis de riesgo, se consideran tres elementos que permiten aproximar un valor objetivo de riesgo de la lista de riesgos principales: el tipo, la probabilidad y grado de impacto del riesgo. Estos elementos permitirán categorizar los riesgos, lo que a su vez le permite dedicar más tiempo y principalmente a la administración de los riesgos más importantes.

Los tipos de riesgos se han clasificado en tres grupos: naturales Tecnológicos y sociales.

La probabilidad el riesgo es la posibilidad de que una condición se produzca realmente, la tabla 4 muestra la clasificación que se la ha dado para la elaboración de este plan.

Tabla 4: Probabilidad del riesgo

Probabilidad de ocurrencia	Descripción
Muy Frecuente	Incidentes repetidos
Frecuente	Incidentes aislados
Poco Frecuente	Sucede alguna vez
Remota	Poco probable que suceda

El impacto del riesgo mide la gravedad de los efectos adversos, o la magnitud de una pérdida, causados por la consecuencia. La tabla 5 indica los tipos de impacto considerados.

Tabla 5: Impacto del riesgo

Impacto	Descripción
Muy Severo	Pérdida de información crítica, daño serio, patrimonial
Grave	Pérdida de información sensible, retraso o interrupción, pérdida patrimonial
Moderado	Pérdida de información sensible, pérdida patrimonial
Leve	Pérdida de información y/o equipamiento no sensitivo.

Se detectaron 12 riesgos importantes a los que Innovativa se encuentra expuesta y que deben ser considerandos en el plan de contingencias, para los cuales se ha elaborado la matriz de riesgos que se muestra en la tabla 6.

Tabla 6: Matriz de riesgos

Riesgo	Tipo de riesgo	Probabilidad de ocurrencia	Grado de impacto
Incendios	Tecnológicos	Remota	Muy Severo
Sismos	Naturales	Remota	Muy Severo
Inundaciones	Sociales	Aleatoria	Grave
Fallas en la conexión de red	Tecnológicos	Poco Frecuente	Moderado
Inoperatividad de los Servidores	Tecnológicos	Poco Frecuente	Moderado
Inconvenientes eléctricos.	Tecnológicos	Frecuente	Moderado
Pérdida de Información	Tecnológicos	Poco Frecuente	Grave
Acción de virus informático	Sociales	Poco Frecuente	Grave
Alteración de la información	Sociales	Poco Frecuente	Grave
Robo común de equipos y archivos	Sociales	Remota	Grave
Robo de información y datos	Sociales	Poco Frecuente	Grave
Ausencia del Personal de TI	Sociales	Poco Frecuente	Moderado

Una vez elaborada la matriz, con ayuda de Los Objetivos de Control para la Información y la Tecnología Relacionada (Cobit) que garantiza que los riesgos de TI se administran apropiadamente definiendo objetivos de control para los 34 procesos que ha definido previamente y de la norma ISO 17799:2005 la cual ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización y establece once dominios de control que cubren por completo la Gestión de la Seguridad de la Información. Además se han considerado la Norma Extintores contra incendios NFPA 10 cuyas Las estipulaciones se dirigen a la selección, instalación, inspección, mantenimiento y prueba de equipos de extinción portátiles. Y la Norma para la protección de equipos de Tecnología de la Información NFPA 75, cuyo propósito es el de establecer los requisitos mínimos para la protección del equipamiento de Tecnología de la Información y de las áreas para los equipos de tecnología de la información, de los daños ocasionados por el fuego o por sus efectos asociados, es decir, humo, corrosión, calor y agua.

Se han definido 95 controles de prevención, 39 controles de mitigación y 12 controles de recuperación. Al ser el primer plan de contingencias con el que Innovativa contará, se hizo hincapié en que sus instalaciones sean seguras tanto para el personal y para los activos de TI. Los controles de prevención sugeridos, permitirán reducir la probabilidad de ocurrencia de los riesgos y su impacto sobre las operaciones y prestación de servicio de Innovativa. A continuación se muestra un ejemplo de cómo funciona el Plan de contingencias, para lo cual se ha seleccionado el riesgos de **Acción de virus informático**, si se observa la matriz de controles de prevención, existe el código 14 para el activo Sofware, entonces se debe ir a la tabla 7, de controles de prevención y buscar el código 14 que dice "Tener respaldos de la información en un sitio remoto, se recomienda llenar una ficha con los datos del sitio en donde reposarán los respaldos ver Anexo 3 y Anexo 8". ese debe ser el control a implantar, y así para cada uno de los códigos para los diferentes tipos de control.

Acción de virus informático

Activos	Controles de prevención	Controles de Mitigación	Controles de recuperación
Equipos eléctricos y electrónicos	16,28,32,33,34,57,62	9,18,19,20	6
Servidores	21,32,33,34,35,61,62	9	6
Software	13,14,15,16,33,34,35		3,6
Información	12,13,14,15,16,42,48		6
Personal	27,31,36,37,38,43,45	1	11,12
Instalaciones	5		

Tabla 7: Tabla de Controles de prevención

Nº	Control de prevención	Responsable
14	Tener respaldos de la información en un sitio remoto, se recomienda llenar una ficha con los datos del sitio en donde reposarán los respaldos ver Anexo 3 y Anexo 8.	Especialista en Sistemas
33	Recopilar información sobre la configuración inicial y establecer líneas base Cobit DS9	Especialista en Sistemas
62	Realizar evaluaciones de vulnerabilidad de manera regular Cobit DS5	Especialista en Sistemas

Tabla 8: Controles de mitigación

Nº	Control de mitigación	Responsable
18	Desconectar la estación infectada de la red.	Especialista en Sistemas
19	Entregar al usuario un equipo de reemplazo hasta que se solucione el problema.	Especialista en Sistemas
20	Verificar que no existan más estaciones de trabajo infectadas.	Especialista en Sistemas

Tabla 9: Controles de Recuperación

Nº	Control de Recuperación	Responsable
3	Ejecutar proceso para identificar bienes afectados ver Anexo 9.	Subdirector Administrativo
6	Ejecutar proceso para control de virus informático ver Anexo 12	Especialista en Sistemas

II. Trabajos relacionados

Existen varios planes de contingencia, de los cuales se ha tomado referencia y se han adaptado algunos controles para ser usados en el área de TI de Innovativa.

De los trabajos analizados, se puede observar que los controles se repiten en algunos de los riegos, por lo cual se ha procedido a definir tablas para los controles de prevención, mitigación y recuperación, se les asignó un código y luego se los ha ido aplicando en los diferentes riesgos, lo cual facilita el manejo del plan de contingencias.

III. Conclusiones y trabajo futuro

- Las Normas ISO 17799, COBIT, NFPA 10 Y NFPA 75 han contribuido para poder definir controles que brinden seguridad tanto al personal como a la infraestructura tecnológica del Área de TI de Innovativa.
- Se han determinado 12 contingencias potenciales a las que actualmente INNOVATIVA se expone y que deben ser controladas.
- El plan de contingencias para el Área de TI, está enfocado principalmente en prevenir y reducir los daños causados al suscitarse una contingencia y permitirá reducir de manera razonable la probabilidad y el impacto de los riesgos.
- En lo posible seguir implementado los controles para la seguridad de la infraestructura de TI sugeridos en las Normas ISO 17799, COBIT.
- Documentar los procesos que se deben ejecutar para la recuperación de un desastre.
- Implementar los controles de prevención establecidos en el plan en un periodo máximo de 6 meses.
- Una vez implementados los controles establecer un cronograma de pruebas y ejecutarlo.
- Revisar, evaluar y rehacer el plan de contingencias en el periodo de un año.

Agradecimientos

El desarrollo de este Plan de Contingencias ha sido desarrollado gracias al valioso aporte del Ing. Oswaldo Díaz, el Ing. Germán Ñacato Un especial reconocimiento a INNOVATIVA por las facilidades en cuanto a brindar la información necesaria y el acceso a sus instalaciones.

Referencias Bibliográficas

Claudio Puente, B. A., & Chicaiza Maigua, N. (2003). *Propuesta de un manual de contingencia informático para la U. T. C.* Latacunga.

Dirección de Tecnologías de Información y Comunicaciones. (2007). *Manual para elaborar un Plan de Continuidad del la Gestión en tecnologías de Información y Comunicaciones.* Costa Rica.

Instituto del Mar del Perú. (2012). *Plan de Contingencias Informático 2012-2015.* Callao.

Instituto Nacional de Estadística e Informática. (2001). *Guía práctica para el desarrollo de planes de contingencia de Sistemas de Información.* Lima.

ISO/IEC 17799. (2005).

IT Governance Institute. (2007). *Cobit 4.1.* Estados Unidos.

Llumiquinga Marcillo, C. V., & Vallejo, P. F. (2005). *DISEÑO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y DESARROLLO DEL PLAN DE CONTINGENCIA PARA EL ÁREA DE SISTEMAS DE LA COOPERATIVA DE AHORRO Y CRÉDITO ALIANZA DEL VALLE.*

Maza Anton, G. L. (2009). *Plan de Contingencia Informático y Serguridad de la Información aplicado en al Universidad Nacional de Piura.* Piura.

Municipalidad de la Punta. (2010). *Plan de Contingencia Informático.* Perú.

Paz, C. (s.f.). *Ingeniería en Sistemas*. Obtenido de

http://pazsystemengineering.blogspot.com/2010/05/plan-de-contingencia-informatico.html

Plan de Contingencia Informático de la Empresa Municipal Administradora de Peaje de Lima. (2011). Lima.

Ramirez Robayo, M. Y., Londoño Rúa, E. A., & Gómez Gómez, J. A. (2012). *Propuesta de Mejoramiento y Contingencia de Sistemas Informáticos en la empresa "T".* Bogotá.

Villaón Huerta, A. (s.f.). Obtenido de http://www.shutdown.es/ISO17799.pdf

Yory, J. (2006).

http://www.mvausa.com/Colombia/Presentaciones/INTRODUCCION_ISO_17799.pdf.