ELABORACIÓN DE UN PLAN DE SEGURIDAD DE INFORMACIÓN EN LA UNIVERSIDAD

Iván Casilla Rondan[1]; Marleni Barrientos Lazo[2]

RESUMEN

El presente tema nos da la idea de cómo debemos tener un plan de seguridad en las universidades, ya que tanto ellas como las empresas tienen información relevante, así como también equipos que son de suma importancia para el buen funcionamiento de las labores académicas y administrativas de la Universidad.

También nos da una visión de qué acciones debemos tomar en caso de incidentes (considérese cualquier desastre); es decir tener un plan de contingencia alterno al plan original y cómo deberíamos actuar en tales casos. Casi siempre el aspecto burocrático es el que imposibilita tomar acciones que van en contra del tiempo, los cuales pueden ser fatales.

ABSTRACT

The present fears us he/she gives the idea we should have a plan of security in the Universities since so much of how they as the companies, have excellent information as well as teams that are of supreme importance for the good operation of the academic and administrative works of the university.

He/she also gives us a vision and that you work we should take in the event of incidents (considers you any disaster), that is to say to have an alternating contingency plan to the original plan and like we should act in such cases, the bureaucratic aspect is almost always the one that disables to take actions that go against the time, which can be fatal.

I. INTRODUCCIÓN

La Universidad hoy en día no aplica medidas de seguridad consistentes para guardar información, y esto se ve en las diferentes áreas u oficinas, a veces uno no se preocupa mucho por los siniestros que pudieran ocurrir, o los daños que causarían los virus. A partir de ello se crea la necesidad de adoptar planes de contingencia. Aunque no aplican en su totalidad, es necesario resaltar esto porque los siniestros pueden suceder en cualquier instante, es prioritario contar con un plan de contingencia que sea parte esencial de una efectiva estrategia de seguridad. Sobre todo para las oficinas de la universidad, la cual tiene áreas críticas.

II. OBJETIVOS

- Promover y generar una mayor conciencia sobre la importancia de la seguridad de información.

- Reducir costos por perjuicios en caso de ocurrir siniestros.

- Mejorar la comunicación y las relaciones entre las diferentes oficinas.

Etapas en la elaboración de planes de contingencia

Las partes involucradas en el desarrollo de un plan de contingencia deben saber escuchar y comunicarse. Aunque existen algunas etapas importantes de desarrollo, mantener un buen plan significa repetir continuamente estas etapas, volver a evaluar el plan y revisarlo.

1. Determinación del objetivo: El punto de partida para el desarrollo de un plan de contingencia es determinar un objetivo claro. Los jefes de cada área así como los decanos de las facultades deben identificar el objetivo operativo en caso de una emergencia en materia de seguridad. Por ejemplo, determinar si el objetivo es proteger cierta información y bienes, es mantener las operaciones académicas y administrativas. El objetivo ayudará a cada oficina a definir un plan estratégico de acción y determinar la información y los recursos que se deben proteger primero.

2. Realización de un inventario completo: Se deben identificar las principales herramientas de las oficinas,

(1) Ingeniero de Sistemas
(2) Analista Programador de Sistemas

los recursos y las tareas necesarias para realizar negocios y atender las funciones críticas establecidas en el objetivo de la elaboración de planes de contingencia. El inventario debe incluir recursos auxiliares como suministros de energía y recursos de respaldo.

3. Análisis de riesgos: Evalúe los perjuicios totales que pudieran ocurrir como resultado de una brecha del sistema de seguridad. También analice amenazas a la seguridad y los perjuicios que potencialmente podrían ocasionar a varios departamentos y operaciones.

4. Desarrollo de un plan de acción: Repase los escenarios detallados de "qué pasaría si..." que implican diferentes amenazas a la seguridad y los efectos posibles en las operaciones. Para cada escenario potencial de disminución de riesgos, tenga en cuenta a las personas involucradas, sus responsabilidades, las consideraciones presupuestales, etc.

5. Prevea un "Plan Alterno": Aunque los mejores planes de contingencia encuentran problemas técnicos, trate de anticiparse a estos problemas y crear soluciones alternas.

6. Planeación de las comunicaciones y compras: Los mejores planes son efectivos solo si los empleados tienen en cuenta su importancia y entienden sus mensajes y procesos. Los departamentos de recursos humanos, de aspectos jurídicos y finanzas deben revisar y responder a los planes de contingencia de seguridad en cada etapa de desarrollo, sin descuidar la parte académica.

III. ESPECIFICACIONES DEL PLAN DE ACCIÓN

Los planes de contingencia variarán dependiendo del tipo específico de brechas del sistema de seguridad, como el ataque de virus que podría afectar las operaciones de la Universidad de manera diferente a como lo haría una negación de servicio.

Debido al rango de amenazas a la seguridad, los planes de contingencia deben ser adaptables. Sin embargo, todos los planes efectivos deben responder por lo siguiente:

· **Pérdida de la información:** Eventualmente las fallas en el fluido eléctrico, los virus, los hackers u otras fuerzas perjudicarán la información importante de una compañía o la hará inaccesible. Prepárese para lo inevitable haciendo copias de seguridad del sistema y de la información.

A fin de garantizar que se realicen copias de seguridad periódicamente, desarrolle una política de seguridad que establezca claramente lo siguiente:

* Los medios que utilizará el personal de la Universidad para hacer las copias de seguridad.

* Quién realizará las copias de seguridad.

* Con qué frecuencia se realizarán las copias de seguridad.

* Los sitios de almacenamiento dentro y fuera del local destinados para las copias de seguridad de la información.

Los servicios de copia de seguridad en línea se están volviendo más comunes. Sin embargo, el personal de la Universidad debe investigar exhaustivamente las herramientas de seguridad más confiables para el almacenamiento y la confiabilidad de las computadoras.

· **Respaldo del hardware:** A las oficinas con computadoras y servidores propios les gustaría contar con equipos de respaldo "rápido", que estén disponibles en caso que el servidor principal se dañe. Aunque en la universidad cada oficinas almacena su información en forma rudimentaria (en disquetes), porque es necesario contar con equipos de respaldo, que estén a la medida de la importancia de la información, a fin de proteger otras prioridades operativas.

· **Suministros de energía de reserva:** Una falla en la energía puede dañar la información y afectar la capacidad de la Universidad para prestar los servicios. Una fuente de energía ininterrumpida o UPS es un componente indispensable de todo plan de contingencia. Algunos modelos de UPS pueden suministrar protección contra los picos y fluctuaciones de corriente y la capacidad para calcular automáticamente las necesidades de energía del personal de cada oficina o área. Los costos de las UPS varían, dependiendo del "tiempo de ejecución" del modelo o del tiempo de energía disponible.

· **Aprobación de fondos:** Las situaciones de emergencia requieren gastos que no están contemplados en el presupuesto. Las partes responsables de elaborar un plan de contingencia deben revisar los estatutos de constitución y el reglamento de la Universidad para determinar quién puede declarar cuando una situación es una emergencia y quién tiene autoridad para asignar los recursos de emergencias. En situaciones de emergencia se debe establecer un proceso de rápida asignación de fondos para las emergencias con el fin de evitar procesos demorados de solicitud y aprobación.

IV. CREACIÓN DE UN DOCUMENTO Y EQUIPO DE RESPUESTAS A INCIDENTES

El documento de respuesta a incidentes explica de manera resumida el "imperio de la ley" para los procedimientos de emergencia y trata los siguientes aspectos:

* ¿Quién reporta a quién?

* ¿Quién es responsable de qué?

* ¿En qué circunstancias debería suspenderse un servicio de correo electrónico o un servidor de Internet?

* ¿Cuáles son los procedimientos para la comunicación y alerta de emergencias?

Un equipo de respuesta a incidentes realiza muchas de las acciones explicadas en el documento de respuesta a incidentes. Los siguientes son los aspectos clave que se deben tener en cuenta cuando se conforma un equipo de respuestas a incidentes:

* ¿Están representados los integrantes de las diferentes oficinas o áreas?

* ¿En qué condiciones actuarían los integrantes del equipo?

* ¿Cuál es la cadena de mando?

* ¿Qué grado de autonomía tienen los integrantes para la toma de decisiones?

V. MEDIDAS DE SEGURIDAD

Los planes de contingencia no son únicamente estratégicos. Mientras que los planes solucionan principalmente escenarios hipotéticos, también necesitan que el personal de la Universidad tome algunas medidas en tiempo real.

- **Seguro:** En caso de una brecha de seguridad, el seguro cibernético puede ayudar a cubrir los costos debido a la pérdida de información, interrupción de las ofinas, gastos en relaciones públicas, demandas de terceros como consecuencia de la negligencia en seguridad, etc.

- **Aplicaciones de la seguridad:** Los antivirus, la detección de intrusos y el software para el filtrado de contenidos de Internet y del correo electrónico pueden ayudar a proteger la red contra una variedad de amenazas a la seguridad como las siguientes:

* Ataques de piratas

* Ataques de virus

* Negación de servicio

* Intrusión de códigos móviles maliciosos

* Fugas de información confidencial

* Correo electrónico y contenidos calumniosos de los sitios web

VI. PLANES DE CONTINGENCIA ESPECÍFICOS

Todas las etapas de análisis e implementación de un plan de contingencia deben respaldar el objetivo del plan. Debido a la variedad de brechas de seguridad, los planes de contingencia deberán ser adaptados a los diferentes escenarios. Sin embargo, el personal de la Universidad debe planear algunas constantes como el suministro de energía, los respaldos de la información, los recursos adicionales del personal de las diferentes oficinas, etc. Los costos para el desarrollo e implementación de un plan de contingencia completo pueden ser significativos, aunque siempre serán mayores los costos de tiempo de inactividad de la compañía y el detrimento a la reputación debido a las brechas de seguridad.

VII. REFERENCIAS BIBLIOGRÁFICAS

1. Caballero Gil, Pino. **Seguridad Informática. Técnicas criptográficas**, 1996.

3. **Instituto Nacional de Estadística e Informática**. 1997.

2. Vicente Aceituno Canal. **Seguridad de la información**, 2002.