Administración segura de la información: Una experiencia de vinculación entre un ente del estado provincial y la U.N.P.A.

Javier Díaz
L.I.N.T.I. – Universidad Nacional de La Plata
Calle 50 y 115 – 1er. Piso – Edificio Bosque Oeste
E-mail: jdiaz@info.unlp.edu.ar
Carlos A. Talay
Alicia E. Santana
Gonzalo Miranda
Unidad Académica Río Gallegos
Universidad Nacional de la Patagonia Austral
Santa Cruz (9400), Argentina
E-mail: ctalay@mixmail.com, alisanjo@hotmail.com, gonza_m1@yahoo.com

RESUMEN

El objetivo de este trabajo es exponer los aspectos fundamentales de un proyecto de investigación destinado a proponer e implementar normas y procedimientos para la administración segura de información, en un contexto de carácter público y confidencial, como lo es un organismo estatal de la Provincia de Santa Cruz.

1. INTRODUCCIÓN

Con el transcurso del tiempo, en el ámbito de la administración pública provincial de Santa Cruz, se ha ido tomando conciencia de la magnitud de los distintos problemas que acarrea la no implementación de adecuadas políticas sobre seguridad en el uso de la información. Esta preocupación ha sido transmitida mediante los permanentes contactos con responsables de áreas informáticas de los distintos entes estatales.

Debido al gran desarrollo de las Tecnologías de la información y comunicaciones, la forma en que los usuarios pueden acceder a la información alojada en servidores es cada vez más variada. El acceso físico a terminales ubicadas en ambientes controlados, que se encuentran conectadas a servidores, ya no es una condición indispensable para lograr el acceso a la información. Nuevos paradigmas generan aplicaciones que definen innovadores modos de relacionarse. Esto conlleva a prestar especial atención a los procesos y a la organización, plantenado la necesidad de extremar las medidas de seguridad, generándose desafíos en este sentido. Esto implica abarcar aspectos de origen legal (por ejemplo, requerimiento de utilización de bases de datos disociadas conforme ley de protección de datos personales o aspectos técnicos exigidos por la ley de firma digital a fin de otorgar valor al documento electrónico, etc.), técnicos (uso de protocolos de seguridad, VPN, duplicación de recursos, etc.) y administrativos (reglamento internos de uso, normas,

procedimientos, definición de misiones y funciones de los responsables de áreas informáticas, etc.). En este sentido, es importante destacar que para lograr los objetivos, las instituciones que han avanzado en estos aspectos han tenido necesariamente que nivelar la infraestructura tecnológica que incluye organización, equipamiento, normativa y realizar planes de capacitación, no sin contar con una adecuada política tecnológica y apoyo de las máximas autoridades que deberán considerar los aspectos de seguridad e implementación de tecnologías de la información con visón estratégica que incluya la definición de políticas internas y presupuestarias.

La ocurrencia de incidentes a nivel de seguridad respecto de los datos procesados en los centros de cómputos, se han produciendo a lo largo del tiempo, aunque no se cuenta con una recopilación de estos datos, que permitan realizar un seguimiento estadístico que pueda darnos una idea concreta acerca de sus orígenes.

En este contexto, se presentó la posibilidad de abordar el caso puntual dentro de una estructura estatal dedicada a la construcción y adjudicación de grupos habitacionales en la Provincia de Santa Cruz, sobre el cual se realizará el desarrollo del proyecto.

De esta manera, se estudiará la problemática del manejo seguro de datos, realizando una propuesta integral que optimice el uso de recursos e información. Esta propuesta abarcará un conjunto de procedimientos y normas de trabajo que contemplarán los aspectos de seguridad lógica, física, legal y administrativa.

Con el fin de alcanzar este objetivo se conformo un equipo de trabajo integrado por: (1) Licenciado en Sistemas, (1) Ingeniero Electricista con orientación en sistemas digitales, (1) Licenciada de Sistemas y Abogada y (1) Lic. en Organización Industrial (Mg. en administración y negocios), (6) Alumnos de las carreras Analista y Licenciatura en Sistemas de la UNPA y (2) empleados del organismo estatal en donde se realizará el proyecto.

2. PLANIFICACIÓN Y MÉTODO

El organismo donde se planificó ejecutar el proyecto, posee un centro informático en el cual se desarrollan sistemas para ser utilizados por las diferentes áreas.

Posee una importante cantidad de equipos instalados en la ciudad de Río Gallegos y demás dependencias distribuidas en el interior provincial de Santa Cruz, que generan y procesan información en forma local para luego enviarla a la administración central, donde es organizada, registrada, integrada y almacenada.

Esta información es variada y conforma en la actualidad distintas bases de datos sobre las cuales se proyectan las tareas administrativas internas y también define políticas estratégicas.

En este contexto, las autoridades se encuentra realizando una planificación que implica la revisión de los sistemas informáticos existentes, la implementación de nuevos sistemas de manejo de información y la integración con las delegaciones distribuidas en el interior de la provincia mediante la puesta en marcha de una red interconectada de datos, que una todas las dependencias y que permita el manejo integrado y en

línea de la información. Existe la posibilidad que esto se realice mediante la integración a una red provincial de datos que se encuentra actualmente en etapa de ejecución.

A partir de la decisión de realizar estas tareas de enlace entre todas las dependencias del interior con la administración central y la red provincial, las autoridades están determinadas a mejorar, formalizar e implementar circuitos y procedimientos que ordenen el manejo de la información para todo el sistema, a fin de lograr un nivel de calidad en su tratamiento y resguardo de la información.

Teniendo en cuenta las consideraciones expuestas, se definió un plan de trabajo que contempla las siguientes etapas:

a) Revisión del estado del arte y fase de relevamiento

En esta etapa se realizará una revisión el estado del arte, recopilando bibliografía y documentos relacionados a modelos de políticas de seguridad que el estado ha definido para entes públicos. Se proporcionará a los alumnos los conceptos teóricos básicos necesarios para formarlos en los aspectos de seguridad a través de cursos impartidos al efecto y se organizará los aspectos del planeamiento general del trabajo. Luego, se dará inicio al relevamiento del escenario sobre el cual se llevará a cabo el proyecto.

b) Análisis y procesamiento de los datos obtenidos

Una vez recabada la información, en la etapa anterior, se procederá a compendiar y organizar los datos de la manera más adecuada, de tal manera que se puedan apreciar los aspectos relevantes, lográndose de esta manera, detectar las interacciones que se producen en forma puntual y general dentro de la estructura existente.

c) Planificación de mejoras del funcionamiento

Una vez analizados los datos, el grupo de trabajo procederá a determinar los aspectos relevantes a tener en cuenta sobre las opciones de mejora de los procedimientos que se deberían implementar, intentando de esta manera, optimizar el funcionamiento para lograr integrar los procesos en un correcto funcionamiento de conjunto. En esta etapa se generara un documento con propuestas de esos procedimientos, que tendrán como ejes centrales:

- ✓ Clasificación y descripción de los activos, tanto físicos como a nivel de recursos humanos. Se plantearán las posibles amenazas que hay sobre ellos y se identificarán las vulnerabilidades.
- ✓ Ubicación física de los equipos, el tipo de accesibilidad física y lógica que se produce sobre ellos. El tipo de interconexión a nivel de redes internas y con el exterior.
- ✓ Configuración de servidores. Servicios que proporcionan a los usuarios y tipos de bases de datos utilizadas.
- ✓ Monitoreo mediante software de diagnóstico de la red. Verificación de frecuencia y calidad de tráfico. Análisis de rendimiento.

- ✓ Políticas de acceso, registro de usuarios, gestión de cuentas (ABM), definición de privilegios y responsabilidades. Sugerencias al personal sobre uso y especificación de claves personales.
- ✓ Fuentes de generación de información. Análisis de los circuitos de información. Confidencialidad, integridad y disponibilidad de la información.
- ✓ Controles criptográficos. Cifrado. Firma digital. Servicios de no repudio.
- ✓ Análisis de acceso remoto y a través de servicios disponibles por INTERNET. Política de utilización de los servicios de red. Servicios seguros. Autentificación de usuarios en conexiones externas. Configuraciones que implica la definición una plataforma adecuada para brindar estos servicios (Subdivisión de redes, Host Bastión, autentificación de nodos, autentificación de usuarios para conexiones externas, Firewalls, protección de los puertos y monitoreo de tráfico hacia y desde el exterior).
- ✓ Análisis de integración con la red provincial de informática. Compatibilidad de datos y servicios integrados.
- ✓ Resguardos de información. Políticas de resguardo. Tipo de soporte físico. Disposición final.
- ✓ Manejo de incidentes. Registro de eventos. Plan de contingencia.
- ✓ Análisis de planes de continuidad sobre la actual propuesta, teniendo como base la actual plataforma de trabajo (cursos, asistencia técnica, auditorias, planificación estratégica, etc.).

d) Revisión externa

A fin de tener una visión externa de los problemas y de las propuestas de mejora, está previsto requerir la opinión de un profesional reconocido en la especialidad, que pueda aportar su experiencia y evaluar los procedimientos elaborados en la planificación.

e) Presentación de informe

Una vez terminadas las etapas precedentes, se procederá a elevar un informe al organismo, en donde se expresen los resultados de los datos relevados, su análisis y las propuestas de mejoras sugeridas.

f) Capacitación del personal

Está previsto un plan integral de capacitación del personal, tanto en las herramientas de software que normalmente utilizan, como así también en los nuevos procedimientos que se definan.

g) Implantación de medidas

Una vez que los procedimientos se encuentran definidos y consensuados, se ha explicado su sentido, su pertinencia y son conocidos los roles a cumplir, se determinará la implantación efectiva de los mismos.

h) Seguimiento y auditorias periódicas

Se tiene previsto realizar la planificación de auditorias periódicas, a fin de mantener un seguimiento de los procedimientos implementados con el objeto de poder brindar a los usuarios el soporte necesario ante dudas o incompatibilidades en la implantación de los procedimientos, como así también llevar un registro de los eventos que se produzcan.

4. CONCLUSIONES PRELIMINARES

El trabajo hasta aquí descrito se encuentra en pleno desarrollo, por tanto no disponemos de resultados totales que permitan concluir con exactitud los beneficios tangibles obtenidos, aunque podemos decir que ya se han podido evidenciar mejoras en la reducción de los incidentes de seguridad que se registran en el centro de cómputos.

Actualmente nos encontramos capitalizado experiencia con la consecuente adquisición de conocimientos en la medida que se avanza en el proyecto.

La transferencia y desarrollo de conocimiento impacta positivamente en la formación de recursos humanos tanto el ámbito universitario representado por nuestros alumnos como en la calificación del personal del organismo interviniente. Particularmente vemos muy positiva la participación de los alumnos, que una vez que recibieron los cursos de capacitación que se les impartió, han podido experimentar cómo son aplicados los conceptos teóricos sobre seguridad informática a una organización.

Otro aspecto necesario de destacar, es lo importante que resulta para ellos la interacción con el personal técnico y administrativo, acercándolos a situaciones reales, con problemas concretos y en algunos de los casos la posibilidad de continuar vinculados mediante al realización de pasantía y eventuales contratos de trabajo.

5. AGRADECIMIENTOS

No queremos finalizar sin dejar de mencionar a los alumnos Andrea Villagra, Fernanda Oyarzo, Mauro Rippa, Cristian Albello, Leonardo Méndez y Diego Enrriquez, pertenecientes a la U.N.P.A. - U.A.R.G., que intervienen en el desarrollo del proyecto y aportan su entusiasmo y dedicación.

6. REFERENCIAS

[1] MODELO DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA ENTES DE LA ADMINISTRACIÓN PÚBLICA NACIONAL, Subsecretaría de la Gestión Pública. Versión 1, Julio-2005

[2] POLITICA DE SEGURIDAD DE LA INFORMACION, Decisión Administrativa 669/2004

[3] Kaeo Merike. *Diseño de seguridad en redes* - Pearson Educación (2003)

[4] Charles P. Pfleeger, Shari Lawrence Pfleeger, *Security in computing* - Prentice Hall (2003)

[5] Maiwald Eric. *Fundamentos de seguridad de redes* - Mc Graw-Hill (2004)

[6] Stallings William. *Fundamentos de seguridad en redes, aplicaciones y estándares* - Pearson Educación (2004)

[7] Charlie Kaufman & Others. *Network security: private communication in a public world* - Prentice Hall (2002)