ANALISIS DE RIESGO RESPECTO A LA SEGURIDAD INFORMATICA DE UNA ORGANIZACIÓN CORRESPONDIENTE AL SECTOR PÚBLICO 1RA. PARTE

TECNOLOGÍA

SUSANA NOEMÍ TOMASI

INTRODUCCIÓN:

El objetivo de éste trabajo es mostrar la manera de llevar a cabo un análisis del riesgo respecto a la seguridad informática, de un Organismo correspondiente al sector público, que puede adaptarse a cualquier organización.

Para efectuar el análisis del riesgo de una organización es necesario:

1. Evaluar la normativa vigente.

2. La organización de un comité de seguridad.

3. Un relevamiento de los sistemas informáticos, clasificándolos, armando una planilla con el nivel de riesgo e importancia que poseen.

4. Determinar que contingencias pueden surgir a través del contrato con terceros contratados.

5. Evaluación del riesgo a través de la confección de:

a. Una tabla de amenazas.

b. Una tabla de vulnerabilidades - probabilidad de ocurrencia - impacto

c. Una tabla de controles.

d. Una tabla de riesgos

6. Reunión del comité de seguridad a fin de decidir respecto a las modificaciones propuestas por las distintas gerencias y sub gerencias.

El Organismo dependiente de la Administración Pública Nacional se compone de:

- Una Dirección General, a cargo de un Director.

- Dos gerencias.

- Seis subgerencias.

No poseen, hasta el momento, como casi toda la Administración Pública Nacional, una política de seguridad de la información formalizada, sino que han aplicado medidas tendientes a asegurar la información durante los últimos años, y están tratando de cumplir la nueva normativa vigente.

1. DESCRIPCIÓN DE LA NORMATIVA VIGENTE:

Normativa vigente en cuanto a la Seguridad Informática, para la Administración Pública Argentina, es la siguiente:

- Decisión Administrativa 669/2004 (Política de Seguridad de la Información) de la Jefatura de Gabinete de Ministros del 22-12-2004 :

A través de la misma se establece que los organismos del Sector Público Nacional integrados por:

- La Administración Nacional, conformada por la Administración Central y los Organismos Descentralizados, comprendiendo en estos últimos a las Instituciones de Seguridad Social.
- Las Empresas y Sociedades del Estado que abarcan a las Empresas del Estado, las Sociedades del Estado, las Sociedades Anónimas con Participación Estatal Mayoritaria, las Sociedades de Economía Mixta y todas aquellas otras organizaciones empresariales donde el Estado nacional tenga participación mayoritaria en el capital o en la formación de las decisiones societarias.
- Los Entes Públicos excluidos expresamente de la Administración Nacional, que abarca a cualquier organización estatal no empresarial, con autarquía financiera, personalidad jurídica y patrimonio propio, donde el Estado nacional tenga el control mayoritario del patrimonio o de la formación de las decisiones, incluyendo aquellas entidades públicas no estatales donde el Estado nacional tenga el control de las decisiones.
- Los Fondos Fiduciarios integrados total o mayoritariamente con bienes y/o fondos del Estado nacional.

Deberán dictar o bien adecuar sus políticas de seguridad de la información conforme a la Política de Seguridad Modelo a dictarse, dentro del plazo de 180 días.

Que las máximas autoridades de los organismos deberán conformar en sus ámbitos un Comité de Seguridad de la Información integrado por representantes de las Direcciones Nacionales o Generales o equivalentes del organismo, el cual será coordinado por el Subsecretario o su equivalente en cada área Ministerial o Secretaría de la Presidencia de la Nación o por el funcionario designado por las máximas autoridades de cada organismo descentralizado, que tenga a su cargo las áreas de apoyo.

Las funciones del Comité de Seguridad de la Información, serán las siguientes:
1. Revisar y proponer a la máxima autoridad del organismo para su aprobación, la Política y las responsabilidades generales en materia de seguridad de la información.
2. Monitorear cambios significativos en los riesgos que afectan a los recursos de

información frente a las amenazas más importantes.
3. Tomar conocimiento y supervisar la investigación y el monitoreo de los incidentes relativos a la seguridad.
4. Aprobar las principales iniciativas para incrementar la seguridad de la información.
5. Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.
6. Garantizar que la seguridad sea parte del proceso de planificación de la información.
7. Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
8. Promover la difusión y apoyo, a la seguridad de la información dentro del Organismo.
9. Coordinar el proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información del Organismo frente a interrupciones imprevistas.

Además las máximas autoridades de los organismos, deberán asignar las funciones relativas a la seguridad de sus sistemas de información a un funcionario de su planta dentro del plazo de 180 días de aprobada la Política de Seguridad Modelo, y la asignación de funciones relativas a la seguridad informática y la integración del Comité de Seguridad de la Información, no deberá implicar erogaciones presupuestarias adicionales.

Resolución 45/2005, de la Subsecretaria de Gestión Pública, del 24 de junio del 2005, a través de la cual se faculta al Director Nacional de la Oficina Nacional de Tecnologías de Información a aprobar la Política de Seguridad de la Información Modelo y dictar las normas aclaratorias y complementarias que requiera la aplicación de la Decisión Administrativa 669/2004.

Disposición 6/2005, de la Oficina Nacional de Tecnologías de la Información (ONTI), del 3 de agosto del 2005, a través de la cual se aprueba la "Política de Seguridad de la Información Modelo" que como Anexo I forma parte de la presente Disposición, y que se encuentra publicada en la dirección de Internet http://www.sgp.gov.ar/sitio/PSI_Modelo-v1_200507.pdf , y que servirá como base para la elaboración de las políticas de seguridad a dictarse por cada organismo alcanzado por la Decisión Administrativa 669/2004.

Este modelo debe ser interpretado como un compendio de mejores prácticas en materia de seguridad de la información para las entidades, públicas y adaptada a la realidad y recursos de cada organismo, y las funciones a las que hace alusión la Política de Seguridad Modelo deberán ser asignadas de acuerdo a las particularidades y operatoria de cada organismo, siendo que dicha asignación deberá realizarse evitándose la duplicación de tareas y asegurando la segregación de funciones incompatibles siempre que sea posible, o bien mediante la implementación de controles para mitigar dicho riesgo.

2. ORGANIZACIÓN DE UN COMITÉ DE SEGURIDAD:

Por lo cual y para dar cumplimiento a la Política de Seguridad se ha conformado un Comité de Seguridad con representantes de las 2 gerencias, (Administrativa y de Prestaciones) las 6 subgerencias (Contable/ Impositiva – De personal – de Sistemas – de Compras) (De prestaciones – De atención a los ciudadanos)- , el director general, siendo designado el Director General del Organismo coordinador general de dicho comité, como indica la normativa.

1ra. Reunión del Comité de Seguridad – Temas tratados:

- Relevancia del comité, funciones que va a cumplimentar, notificación al personal del Organismo respecto al mismo, (que queda a cargo del Sub -Gerente de Personal) acta correspondiente, fecha de la nueva reunión.
- Seguridad de la información, para que sirve, que urgencia tiene su implementación.
- Análisis de la normativa vigente para la Administración Pública Nacional respecto a la Seguridad Informática.
- Implementación de un área dentro de la estructura organizacional del Organismo, que proteja los activos de información, de manera tal que administre y controle la seguridad sobre el acceso lógico y físico de sus distintos ambientes tecnológicos y recursos de información.

- Recursos disponibles humanos y económicos para efectuar dicha implementación.
- Evaluación del estado en que se encuentra el Organismo respecto a las políticas de seguridad, con que documentación cuentan y quienes se van a hacer cargo de dicha evaluación.
- Evaluación del riesgo posible por la tercerización con una empresa por la provisión y mantenimiento (remoto y on-site) de los enlaces WAN, y por el hosteo de la página WEB del Organismo, que cuenta con un sistema on-line de registro donde se almacena información personal de los ciudadanos. La base de datos que almacena la información también se archiva en los equipos del proveedor. Modificaciones a efectuar en el contrato vigente.
- Acuerdos, términos y condiciones de confidencialidad de los datos, para todo el personal propio y contratados por los terceristas.
- Se decide la división por temas entre los 6 gerentes y sub-gerentes, y una nueva reunión de urgencia en 30 días.