

# **PROPUESTA PARA LA CONSTITUCION Y ESTRUCTURACION DE LA DIRECCION DE SEGURIDAD DE LA INFORMACION DE LA OFICINA DE TECNOLOGIAS DE INFORMACION**

Autor: Jorge Eduardo Sznek<sup>(1)</sup>

El presente artículo está basado en un documento de trabajo redactado para la Dirección Provincial de la Oficina de Tecnologías de Información (OTI) de la provincia del Neuquén, donde se propone la constitución y estructuración de una Dirección de Seguridad de la Información.

La OTI es un ente gubernamental creado a través de un decreto en el año 2004. Surge como una fusión de 2 organismos preexistentes: la Dirección Provincial de Informática y la Dirección Provincial de Telecomunicaciones y, entre otras facultades, se establece que debe ser el "ente rector en materia de tecnologías de la información y de las comunicaciones en el ámbito de la provincia del Neuquén". En su estructura básica aparece la Subdirección Provincial de Planeamiento, dependiendo de la Dirección Provincial, y dentro de esa Subdirección Provincial figura un sector denominado Seguridad Informática. Sin embargo esa área de Seguridad Informática nunca fue estructurada.

A instancias del actual Director Provincial, se ha planteado la necesidad de elevar a las autoridades provinciales una propuesta para constituir y estructurar dicho sector, tarea que le fuera encomendada al autor del presente artículo, dados sus conocimientos en el tema de Seguridad de la Información.

En este artículo se extraen las principales consideraciones volcadas en dicho documento de trabajo, las que pueden ser tomadas como una base general para situaciones de naturaleza similar.

## **1. La información**

Se puede definir el término Información como "toda comunicación o representación de conocimiento presentada en cualquier forma (textual, numérica, gráfica, cartográfica, narrativa o audiovisual), y en cualquier medio (magnético, en papel, en pantallas de computadoras, audiovisual u otro) que se utiliza para la toma de decisiones de diferente especie y naturaleza.

Antes de la existencia de las computadoras, la información era tratada manualmente por el conjunto de personas que la requerían para cumplir sus metas, manejándola esencialmente en forma escrita; quedaba claro quien accedía a cada porción de información y que acciones debía realizar a partir de la toma de conocimientos de la misma.

Con el advenimiento de las computadoras, se produce un cambio sustancial en el manejo, tratamiento y conocimiento de la información, tanto en lo cualitativo como en lo cuantitativo, pues ahora era posible "procesar" mucha mayor cantidad de información que cuando se trataba manualmente.

Por otra parte, al irse multiplicando los ambientes informatizados, va creciendo el acceso a la información por parte de los individuos que forman parte de una organización, resultando mucho más dificultoso el establecimiento de responsabilidades sobre quién puede acceder a cuál porción de información y, por sobre todo, controlar el cumplimiento de esas responsabilidades.

Es allí donde comienzan a avizorarse los primeros conceptos de Seguridad de la Información.

Desde un punto de vista organizacional, la información es un activo muy importante (si no el de mayor importancia) del que en muchos casos depende la supervivencia de la propia organización. Y por ello se deberán establecer aspectos para protegerla.

## **2. La Seguridad de la Información**

Se puede definir como "*el conjunto de políticas, métodos y controles que tienen la finalidad de mantener la confidencialidad, integridad y disponibilidad de la información de una organización y de todos los elementos tecnológicos que la contienen*".

La confidencialidad o privacidad se refiere a como proteger información de la publicación no autorizada y como preservarse del uso no autorizado de los recursos del sistema tales como CPU, programas y otro tipo de equipamiento. Brinda la certeza de que la información no va a ser revelada a individuos o procesos no autorizados.

La integridad se refiere a como preservar los objetos para hacerlos confiables y verosímiles, evitando la modificación no autorizada de los objetos. Brinda la certeza de que la información no va a ser alterada por individuos o procesos no autorizados.

La disponibilidad garantiza que los recursos sean accedidos por las personas que están autorizadas para hacerlo en el momento que los requieran.

La disponibilidad es la base de la Seguridad de la Información: si no existe disponibilidad, no se puede determinar si hay confidencialidad e integridad.

La Seguridad de la Información comprende aspectos relacionados con políticas, estándares, buenas prácticas, controles, valuación de riesgos, capacitación y otros elementos necesarios para la adecuada administración de los recursos tecnológicos y de la información que se maneja por esos medios.

La Seguridad de la Información establece métricas para resguardar a los activos contra daños, destrucción, adulteración, uso no autorizado o robo, permitiendo que la información electrónica sea oportuna, precisa, confiable y completa para ayudar a alcanzar las metas institucionales y permitir el uso eficiente de los recursos tecnológicos destinados para el procesamiento de la información.

### **3. La informática en la Administración Pública Provincial**

La Administración Pública Provincial también evolucionó tecnológicamente, desde contar con un Centro de Cómputos central hasta el modelo actual de innumerables redes locales en los diferentes organismos, utilización de sistemas informáticos centrales, generalización del uso del correo electrónico y de Internet, etc.

Cada vez es mayor la demanda de sistemas de información que los responsables de los organismos solicitan a sus áreas de Informática a los efectos de satisfacer sus necesidades de información para la gestión y la toma de decisiones.

Una gran debilidad que presenta este modelo es el del crecimiento caótico, sin directrices claras, produciendo muchas veces duplicación de esfuerzos y falta de interoperabilidad de información.

Los aspectos de Seguridad de la Información son tenidos en cuenta escasamente, careciéndose también de referencias y de líneas estándares. Esto redundará necesariamente en el aumento de los riesgos a los que se expone la información y los objetos físicos que la contienen, ocasionándose pérdidas importantes de activos.

### **4. La Seguridad de la información en las organizaciones**

Hoy en día la mayoría de las organizaciones, sean públicas o privadas, cuenta en su organigrama con un área de Tecnología de la Información (TI), la que adopta innumerables designaciones tales como Sistemas, Computación, Informática, etc.

Si bien abarcan una gran cantidad de tareas específicas, dependiendo del volumen y envergadura de la organización, en esencia podemos encontrar dentro de ellas los siguientes sectores:

- Tecnología: se ocupa de controlar el adecuado funcionamiento de la infraestructura tecnológica de la organización, ya sea mediante la administración de las redes, la provisión de conectividad, etc.
- Desarrollo: se ocupa de llevar adelante proyectos de sistemas de información a partir de las necesidades que posee la organización. Es acá donde se pueden encontrar los sectores de análisis de sistemas, de programación y de implementación.

- Soporte: se ocupa de asistir al conjunto de individuos usuarios de los diferentes recursos tecnológicos, ya sea en el uso de los elementos como en la operación de los sistemas de información.

En los últimos años se ha incorporado a esta estructura básica una nueva área: la de Seguridad de la Información, con metas bien definidas en lo referido a proteger y preservar los activos de la organización, habida cuenta de la enorme importancia que adquirió la información para las organizaciones.

Antes de esto, las "tareas de seguridad" estaban diseminadas entre las áreas de Tecnología y Soporte –y en menor medida de Desarrollo–, sin una clara diferenciación de las responsabilidades.

Sin embargo, a nivel mundial se han desarrollado ampliamente los conceptos de Seguridad de la Información, al punto de la aparición de estándares internacionales que regulan estos aspectos (Common Criteria, COBIT, ISO 17799) y de instituciones que fuerzan la aplicación de medidas a diferentes clases de organizaciones (como ejemplo, basta mencionar las circulares del BCRA en lo referido a Seguridad Informática para las entidades bancarias de la Argentina).

A grandes rasgos, la Seguridad de la Información abarca:

- **Ambito físico**: espacios donde residen equipos de procesamiento de datos. Incluye aspectos de control del perímetro y control de acceso físico.
- **Hardware**: Instalaciones físicas adecuadas, regulación de la humedad, control de la temperatura, no exposición de cables a la intemperie, fuentes de poder siempre disponibles, tipo de infraestructura seleccionada, tipo de cables, tipo de computadoras, etc.
- **Software**: los Sistemas Operativos que se tienen y las aplicaciones que se corren (las que son de misión crítica no pueden permitirse la ocurrencia de errores).
- **Recursos Humanos**: personas que utilizan los medios tecnológicos, tanto los especializados en informática como aquellos que utilizan esos medios para el cumplimiento de sus tareas habituales, sean internos o externos a la entidad.

## **5. Aspectos de la Seguridad de la información**

Como se mencionó más arriba, la Seguridad de la Información apunta a preservar la confidencialidad, integridad y disponibilidad de la información.

Estas propiedades corren riesgo de perderse, ocasionando diversos tipos de perjuicios debido a las vulnerabilidades, amenazas y ataques.

Las vulnerabilidades son aquellos puntos débiles de los sistemas y de los elementos; como ejemplo se puede mencionar los "bugs" de las aplicaciones, las fallas de materiales en los elementos de hardware, etc.

Las amenazas pueden ser vistas como potenciales violaciones de seguridad, y existen debido a las vulnerabilidades.

Los ataques o incidentes de seguridad son la concreción de las amenazas; la ocurrencia de incidentes de seguridad suele producir diversos tipos de daños, resultando a veces en pérdidas significativas de información, recursos y dinero.

Hay dos clases básicas de ataques o incidentes de seguridad: los intencionales y los accidentales.

Los intencionales, como el término lo indica, son realizados con total conciencia por parte del agresor con el objeto de obtener algún recurso del sistema de información: robo de partes de equipos, obtención de datos confidenciales, averiguación de contraseñas, introducción de virus informático, etc. Este tipo de agresores pueden ser personas pertenecientes a la organización o ajenas a la misma

(vale señalar que hoy en día la conectividad que provee Internet facilita ampliamente este tipo de acciones desde el exterior).

Los incidentes de seguridad accidentales son, en su mayoría, producto de la falta de capacitación de los individuos en la utilización de los recursos que proveen los sistemas de información: borrado de datos, divulgación de contraseñas, envío de correo electrónico con información confidencial sin encriptar, etc.

Puede agregarse a esto que existe otra clasificación respecto al tipo de incidentes de seguridad: los hay pasivos y activos.

Los pasivos son aquellos que se realizan monitoreando los sistemas para recolectar información, ya sea para llevar adelante otra agresión o para obtener datos significativos. En general, no dejan ningún rastro que los permita identificar.

Los activos tienen como objetivo producir algún cambio en el comportamiento del sistema. Por su característica, dejan rastros que permiten detectar su ocurrencia.

## **6. Ámbito de aplicación de la Seguridad de la información**

La seguridad de la Información tiene 3 ámbitos de aplicación claramente definidos: seguridad física, seguridad lógica y seguridad de las comunicaciones.

La seguridad física está destinada a proteger los componentes físicos de los sistemas, tales como salas de servidores, instalaciones de energía y de comunicaciones, medios físicos que soportan datos, los equipos, etc.

La seguridad lógica está destinada a la protección de datos y programas contenidos en los distintos soportes físicos, tanto magnéticos como en papel, en pantallas, etc.

La seguridad de las comunicaciones combina métodos de seguridad física y lógica ya que está destinada a proteger a los medios de comunicación y a la información que circula por ellos.

La Seguridad de la Información se aplica también a las propias organizaciones, tanto en sus aspectos organizativos, metodológicos y procedurales, como en los recursos humanos que las componen.

## **7. Roles de Seguridad de la información**

La Seguridad de la Información posee 3 funciones claramente diferenciadas: de definición y coordinación (de políticas, normas, procedimientos, estándares, etc.); de aplicación (de las definiciones); y de verificación (control de aplicación de las definiciones).

La función de definición consiste en establecer las directrices generales (políticas, estándares, procedimientos, etc.) que guían el funcionamiento de la entidad en materia de Seguridad de la Información.

La función de aplicación consiste en, justamente, aplicar los procedimientos de Seguridad de la Información previamente establecidos. Hay que tener en cuenta que esta tarea es competencia de **todo el personal** de la organización, cada uno en su rol correspondiente.

La función de verificación puede dividirse a su vez en interna y externa. La verificación interna consiste en chequear el cumplimiento de las pautas establecidas por parte de los diferentes sectores de la organización. La verificación externa, normalmente conocida como auditoria externa, consiste en verificar con una mirada objetiva el cumplimiento de las políticas por parte de la organización en cada una de sus áreas.

## **8. Funciones de la Dirección de Seguridad de la información**

La Dirección de Seguridad de la Información debe atender las siguientes funciones y tareas:

- Elaborar un plan de seguridad de Tecnología de Información.
- Definir los requerimientos de la Seguridad de la Información.
- Elaborar políticas de Seguridad de la Información.
- Diseñar estándares, normas y procedimientos de seguridad informática.
- Implementar la división de funciones.
- Participar en la planificación de los métodos de aseguramiento.
- Proponer medidas para la identificación, autenticación y acceso a los sistemas informáticos.
- Establecer modelos de seguridad para el acceso a datos en línea.
- Participar en la clasificación de los datos y en la asignación de responsables de datos.
- Implementar reportes de actividades de seguridad.
- Coordinar los incidentes de seguridad.
- Analizar los riesgos de seguridad asociados al ciclo de vida de los sistemas.
- Establecer las medidas de seguridad para el almacenamiento de los respaldos.
- Establecer criterios para evitar el "no repudio".
- Asegurar la protección adecuada del hardware y software de seguridad.
- Administrar las claves criptográficas.
- Elaborar un marco de referencia para la prevención, detección y corrección de software malicioso.
- Establecer criterios de seguridad para la configuración de las arquitecturas de firewalls y conexiones a redes públicas.
- Recomendar medidas de seguridad para las pruebas de software de aplicación
- Verificar la seguridad del software del sistema.
- Calcular el costo de la seguridad.
- Participar en la elaboración de contratos con proveedores externos para verificar el cumplimiento de los aspectos de Seguridad de la Información.
- Controlar el cumplimiento de las políticas, estándares, normas y procedimientos de Seguridad de la Información.
- Asesorar en materia de Seguridad de la Información.
- Entrenar y capacitar al personal de la organización en materia de Seguridad de la Información.

## 9. Políticas de Seguridad de la Información

Establecen las normas generales y operativas de seguridad física y lógica para el uso de los recursos tecnológicos. La Dirección de Seguridad de la Información es la responsable de la coordinación de su implementación, seguimiento, y control del cumplimiento de las mismas.

Las políticas de seguridad examinarán particularmente las cuestiones relativas al acceso, autenticidad, privacidad, integridad, aceptación, control, fiabilidad y recuperación después de desastres.

Una política de Seguridad de la Información es una forma de comunicarse con los usuarios y los directivos. Establece el canal formal de actuación del personal en relación con los recursos y servicios informáticos importantes de la entidad.

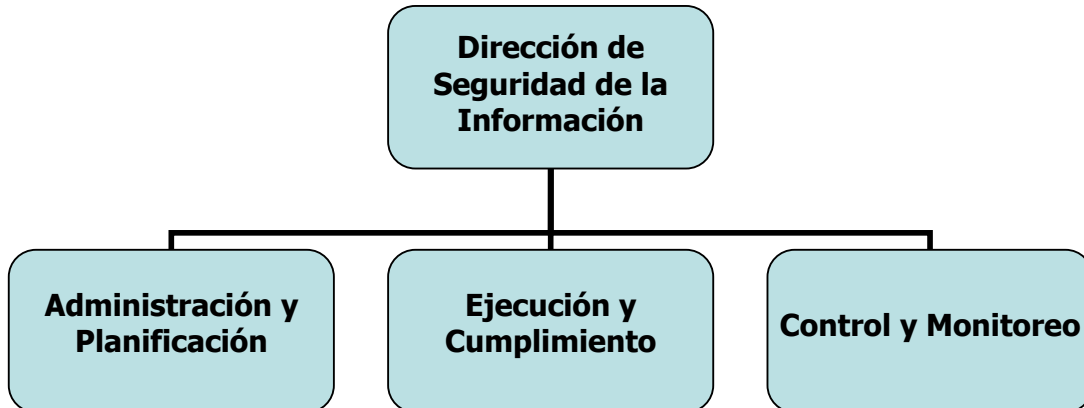
Se trata que cada uno de los miembros de la organización logre reconocer la información como uno de sus principales activos para que adopte una posición conciente y vigilante por el uso y limitaciones de los recursos y servicios informáticos críticos de la entidad.

Las políticas de seguridad deben constituir un proceso continuo y retroalimentado que observe la concientización, métodos de acceso a la información, monitoreo de cumplimiento y renovación, aceptación de las directrices y estrategia de implementación, que lleven a una formulación de directivas institucionales que logren aceptación general.

***Las políticas por sí solas no constituyen una garantía para la seguridad de la organización, ellas deben responder a intereses y necesidades organizacionales, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos, y a reconocer en sus mecanismos los factores que facilitan la formalización y materialización de los compromisos adquiridos con la entidad.***

## 10. Estructura organizacional

### Organigrama



### Funciones

#### Dirección de Seguridad de la Información:

- Interactuar con el Director Provincial de la OTI, con el subdirector Provincial de Planeamiento, y con las demás subdirecciones a efectos de establecer los lineamientos para los planes de Seguridad de la Información de la entidad.
- Integrar el Comité de Seguridad de la Información del organismo.
- Definir, implementar y mantener actualizado el Plan de Contingencia en conjunto con otros responsables de áreas de la OTI.
- Revisar los aspectos de seguridad en convenios con terceras partes externas.
- Proponer planes de capacitación generales destinados al personal del organismo y planes de capacitación particulares destinados a responsables de infraestructuras informáticas de los organismos de la Administración Pública Provincial.
- Supervisar la definición de Políticas de Seguridad, el seguimiento de las normas y procedimientos y los mecanismos de control del cumplimiento de manera que se garantice la confidencialidad, integridad y disponibilidad de la información.
- Asesorar a los demás organismos de la Administración Pública Provincial en materia de Seguridad de la Información.

#### Administración y Planificación de Seguridad de la Información

- Redactar, mantener y documentar las políticas de Seguridad de la Información.
- Definir, redactar, mantener y documentar los estándares de seguridad de la información.
- Capacitar al personal en las políticas y estándares de Seguridad de la Información vigentes en el organismo.
- Colaborar en la formulación de políticas de seguridad de la información con otros organismos de la Administración Pública Provincial.

#### Ejecución y Cumplimiento

- Redactar, mantener y documentar las normas y procedimientos de Seguridad de la Información de acuerdo a las políticas vigentes.
- Capacitar al personal en normas y procedimientos de Seguridad de la Información vigentes en el organismo.
- Realizar periódicamente análisis de riesgos sobre los recursos críticos de la organización.
- Interactuar con los integrantes de los diversos sectores del organismo para asesorar en temas de seguridad específicos (seguridad en el desarrollo de sistemas, seguridad en administración de redes, etc.)

- Asistir cotidianamente al personal del organismo en las tareas de protección de datos y de recursos.
- Colaborar en la formulación de normas y procedimientos de Seguridad de la Información con otros organismos de la Administración Pública Provincial.

#### Control y Monitoreo

- Definir métricas y procedimientos para el control del cumplimiento de las normativas de seguridad vigentes.
- Releva, documentar e informar el cumplimiento de las normativas vigentes de seguridad de la información.
- Monitorear permanentemente los sistemas para detectar eventos que atenten contra la seguridad implementada.
- Mantener soportes documentales de las actividades relacionadas con la seguridad a efectos de posterior análisis.
- Capacitar al personal en normas y procedimientos de Seguridad de la Información vigentes en el organismo.
- Prestar colaboración con otros organismos de la Administración Pública Provincial en el control de aspectos de Seguridad de la Información.

#### **Recursos Humanos**

Los sectores de La Dirección de Seguridad de la Información deben estar integrados por personal que preferentemente cumpla los siguientes requisitos:

#### Formación y conocimientos

- Profesional universitario en Informática, Ciencias de la Computación, Sistemas o equivalente.
- Conocimientos en Seguridad de la Información. Para determinadas funciones será necesario acreditar experiencia en el área.
- Conocimientos de Estándares Tecnológicos y de normas y estándares mundiales de Seguridad de la Información.
- Conocimientos en Planificación.
- Conocimientos de Organizaciones de TIC's.
- Conocimientos de Auditoría Informática.

#### Capacidades

- Buen manejo de relaciones interpersonales.
- Buena capacidad de trabajo en grupo y de liderar grupos de trabajo.
- Buena disposición a investigar.
- Ordenado y metódico.
- Excelente disposición a aprender.
- Excelente disposición para transmitir lo aprendido.
- Buena capacidad de redacción y síntesis.

<sup>(1)</sup> El autor es graduado en la carrera de Computador Científico egresado de la UBA. Es profesor Adjunto regular en la Universidad Nacional del Comahue en las cátedras de Sistemas Operativos y Seguridad Informática y pertenece al plantel profesional de la Subdirección de Planeamiento de la Oficina de Tecnologías de Información de la provincia del Neuquén.