

Autor: José Torres (jtorres@scientech.com.ve)

Director de Tecnología e Información

Scientech de Venezuela

www.scientech.com.ve

Fuente: <http://www.pc-news.com/detalle.asp?sid=&id=11&Ida=1255>

Políticas de Seguridad Informática

Las políticas de seguridad informática representan un tipo especial de reglas de negocios documentadas. Su auge ha sido estimulado por la explosión de tecnologías de manejo de información, incluyendo a los teléfonos celulares, los buscaperonas y los computadores. Los que trabajan en el ambiente empresarial deben recibir instrucciones claras y definitivas que los ayuden a garantizar la seguridad de la información generada en el complejo mundo de los negocios. Definitivamente, es imprescindible mantener reglas claras que enmarquen el desarrollo de las actividades en cualquier actividad comercial, los sistemas de información no escapan de este tipo de documentación.

En general, la seguridad informática depende de la articulación eficiente de varios factores, uno de los cuales es ese conjunto de políticas de seguridad informática, las cuales representan el marco normativo para el establecimiento de cualquier solución de seguridad para las organizaciones.

El ofrecer productos o servicios a través de Internet sin tomar en cuenta la seguridad informática no sólo denota negligencia, sino que constituye una invitación para que ocurran incidentes de seguridad que podrían dañar severamente la reputación de la organización. Para todos nuestros proyectos, las políticas de seguridad informática proporcionan delimitaciones claras que definen un dominio donde se puede encontrar una solución aceptable.

Algunos dicen que la seguridad informática es un problema de personas, mientras que otros dicen que es un problema de tecnología, y podría decirse que ambos tienen razón. Pero antes de que se pueda hacer algo al respecto, la gerencia debe involucrarse en la seguridad informática, asignar suficientes recursos y comunicar claramente a todos los integrantes de su equipo que la seguridad informática realmente sí es importante. Muchas encuestas indican que aquéllos que ejercen la seguridad informática piensan que la llave para alcanzar el éxito de la seguridad informática es la participación de la alta gerencia.

Las políticas son instrucciones gerenciales que trazan una dirección predeterminada o describen la manera de manejar un problema o situación. Las políticas son planteamientos de alto nivel que transmiten a los trabajadores la orientación que necesitan para tomar decisiones presentes y futuras. Las políticas son requisitos generalizados que deben ser escritos en papel y comunicados a ciertos grupos de personas dentro, y en algunos casos fuera, de la organización. Las políticas también pueden considerarse como reglas de negocio. Aunque los documentos de políticas de seguridad informática varían de una organización a otra, un típico documento de este tipo incluye una exposición de motivos, la descripción de las personas a quienes van dirigidas las políticas, el historial de las modificaciones efectuadas, unas cuantas definiciones de términos especiales y las instrucciones gerenciales específicas sobre el tratamiento de las políticas.

Las políticas son obligatorias y pueden considerarse el equivalente de una ley propia de la organización. Se requiere una autorización especial cuando un empleado desea irse por un camino que no está contemplado en la política. Debido a que el cumplimiento es obligatorio, las políticas utilizan palabras como "no se debe hacer" o "se tiene que hacer", ya que estas estructuras semánticas transmiten certeza e indispensabilidad.

Las políticas representan declaraciones instruccionales de más alto nivel que las normas, aunque ambas son de obligatorio cumplimiento. Las políticas proporcionan las instrucciones generales, mientras que las normas indican requisitos técnicos específicos. Las normas cubren detalles como, por ejemplo, los pasos a seguir para lograr alguna implementación, los conceptos del diseño de los sistemas, las especificaciones de las interfaces del software, los algoritmos y otros. Las normas, por ejemplo, definirían la cantidad de bits de la llave secreta que se requieren en un algoritmo de cifrado. Por otro lado, las políticas simplemente definirían la necesidad de utilizar un proceso de cifrado autorizado cuando se envíe información confidencial a través de redes públicas, tales como Internet.

Las políticas están diseñadas para durar hasta cinco años, mientras que las normas sólo unos pocos. Las normas necesitan modificarse más a menudo debido al cambio incesante en los procedimientos manuales, en las estructuras organizacionales, en los procedimientos empresariales y en la tecnología de sistemas informáticos.

Las políticas generalmente van dirigidas a un público más amplio que las normas. Por ejemplo, una política que exija la utilización de paquetes antivirus se aplicaría a todos los usuarios de computadores personales, pero la norma que requiera el uso de certificados digitales de clave pública sólo podría ser dirigido al personal que realice operaciones a través de Internet.

Las políticas no sólo son distintas, sino que se encuentran a un nivel mucho más alto que los procedimientos. La declaración de una política describe los lineamientos generales que deben seguirse para atender un problema específico, mientras que los procedimientos dictan los pasos operativos específicos o los métodos manuales que los trabajadores deben emplear para lograr un objetivo dado. Por ejemplo, en muchos departamentos de tecnología informática existen procedimientos específicos para realizar los respaldos de los discos duros de los servidores. En este ejemplo, la política podría plantear o describir la necesidad de realizar respaldos, de tener almacenaje fuera de la sede y de salvaguardar los medios de respaldo. La norma podría definir el software a utilizar para hacer los respaldos y cómo configurar dicho software. El procedimiento podría describir cómo usar el software de respaldo, cómo y cuándo sincronizar dichos respaldos y otros detalles.

Por ejemplo, una política puede establecer el uso de aquel software antivirus autorizado por la gerencia de Seguridad Informática y ningún otro. El nombre del proveedor y el del producto pueden cambiar de mes a mes sin necesidad de cambiar la política. Esos detalles podrán aparecer en la norma, pero no en la política.

Algunas personas, particularmente los usuarios y personal del departamento de Tecnología de Información, frecuentemente dicen, "Cuando me digan algo, me ocupo de la Seguridad Informática". Esta actitud no es sorprendente cuando se aprecia en la mayoría de la gente una falta de conciencia sobre la magnitud de los riesgos que enfrentan en materia de Seguridad Informática, así como que tampoco tienen la disposición de tomarse un tiempo para analizar seriamente dichos riesgos. Aparte de

esto, por no contar con la pericia requerida, la mayoría de las personas no puede estimar la necesidad de establecer ciertas medidas de control.

Por ello, las políticas representan la manera más definitiva que la gerencia puede utilizar para demostrar la importancia de la Seguridad Informática, y que los trabajadores tienen la obligación de prestar atención a la Seguridad Informática. Las políticas pueden compensar aquellas influencias que, de otra manera, evitarían que se prestara suficiente protección a los recursos informáticos. Un ejemplo frecuente es el de los gerentes de mediano nivel que, en repetidas ocasiones, se niegan a asignar recursos en sus presupuestos a la Seguridad Informática. En este caso, la otra influencia es el bono que frecuentemente reciben como recompensa por mantener los costos bajos. Pero los gerentes de mediano nivel no pueden seguir negando las solicitudes de fondos para la Seguridad Informática si el apoyo es exigido por la alta gerencia.

La gerencia en toda organización tiene que aclarar sus intenciones con respecto a la operación de los computadores y las redes. Si la gerencia dedica tiempo a preparar una política de seguridad informática y su correspondiente documentación, entonces al presentarse el momento que sea necesaria la acción disciplinaria, la demanda o la litigación, la organización no estará sujeta a estos mismos problemas legales. Las políticas además representan para la gerencia una manera relativamente barata y directa de definir el comportamiento correcto.

Uno de los problemas más graves del campo de la seguridad informática tiene que ver con los esfuerzos fragmentados e inconsistentes que al respecto abundan. Demasiadas veces un departamento estará feliz de prestar su colaboración en materia de seguridad informática, mientras que otro de la misma organización se mostrará reacio. Dependiendo de los recursos computacionales que compartan estos departamentos, como la intranet, el departamento reacio crea peligros informáticos para el otro departamento. Esto podría suceder, por ejemplo, si un hacker obtuviera acceso a la intranet a través de un descuidado proceso de autenticación de usuario dentro del departamento reacio, y luego utilizara esta invasión para destruir información del departamento que sí presta atención a su seguridad. Aunque no es ni posible ni deseable que todas las personas de la organización estén familiarizadas con las complejidades de la seguridad informática, sí es importante que todos se suscriban a un nivel mínimo de protección. En términos de alto nivel, las políticas se utilizan para definir dicho nivel mínimo de protección, que algunos llaman línea de base.

Utilizar terceros, contratistas, consultores y personal temporal ya se ha convertido en una necesidad de las organizaciones, que a su vez deben establecer nexos empresariales cercanos con otras organizaciones, incluso cuando éstas representan competencia. La enorme cantidad de entes empresariales existentes ha dificultado el manejo de cosas como el control del acceso, la protección de la propiedad intelectual y todo lo relativo a la seguridad informática. Debido a que tanta gente está involucrada, existe la necesidad apremiante de coordinar consistentemente las actividades de los grupos internos y externos. Y allí es exactamente donde las políticas de seguridad informática pueden prestar gran ayuda. Por ejemplo, una política puede definir cuándo y dónde se requiere la firma de un acuerdo de confidencialidad, e igualmente definir cuándo no.

Supervisar directamente a toda esta gente no es práctico, necesitan aprender a auto-gestionarse, pero necesitan las instrucciones adecuadas para poder hacerlo bien. Así que la herramienta N° 1 para el manejo de la conducta de la gente en el área de seguridad

informática lo constituye el documento de políticas de seguridad informática.

José Torres (jtorres@scientech.com.ve)

Director de Tecnología e Información

Scientech de Venezuela

www.scientech.com.ve