Published on *Revista .Seguridad* (http://revista.seguridad.unam.mx)


# POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA LAS NECESIDADES DEL USUARIO ACTUAL

Héctor Jesús Pérez Mancilla

Buenas prácticas

numero-27

Los equipos que alguna vez fueron máquinas superpotentes con millones de ciclos por minuto, ahora son sustituidos por pequeñas máquinas con $^{1}/_{16}$ de su tamaño original, con la capacidad de ser portátiles e incluso cuidar la salud del ser humano. Así también, Internet está marcando una tendencia hacia el cambio ubicuo que en la actualidad llamamos el Internet de las Cosas.

Por ello nos vemos en la necesidad de incrementar el nivel en la seguridad e implementar más opciones de cualquier política segura que conozcamos, ya que ahora no solamente se trata de salvaguardar la seguridad de la información, sino también la integridad del propio ser humano.

Es por eso que a las personas que se dedican a la seguridad informática de cualquier empresa u organización se les ha dado una nueva encomienda, una misión realzada en el ámbito de la seguridad informática que demanda un manejo de políticas más complejas, con mayor magnitud y con el fin de alcanzar el marco que nos garantice la seguridad de la información, siempre con un lenguaje asimilable para el usuario promedio y un entendimiento mínimo en la tendencia de la seguridad.

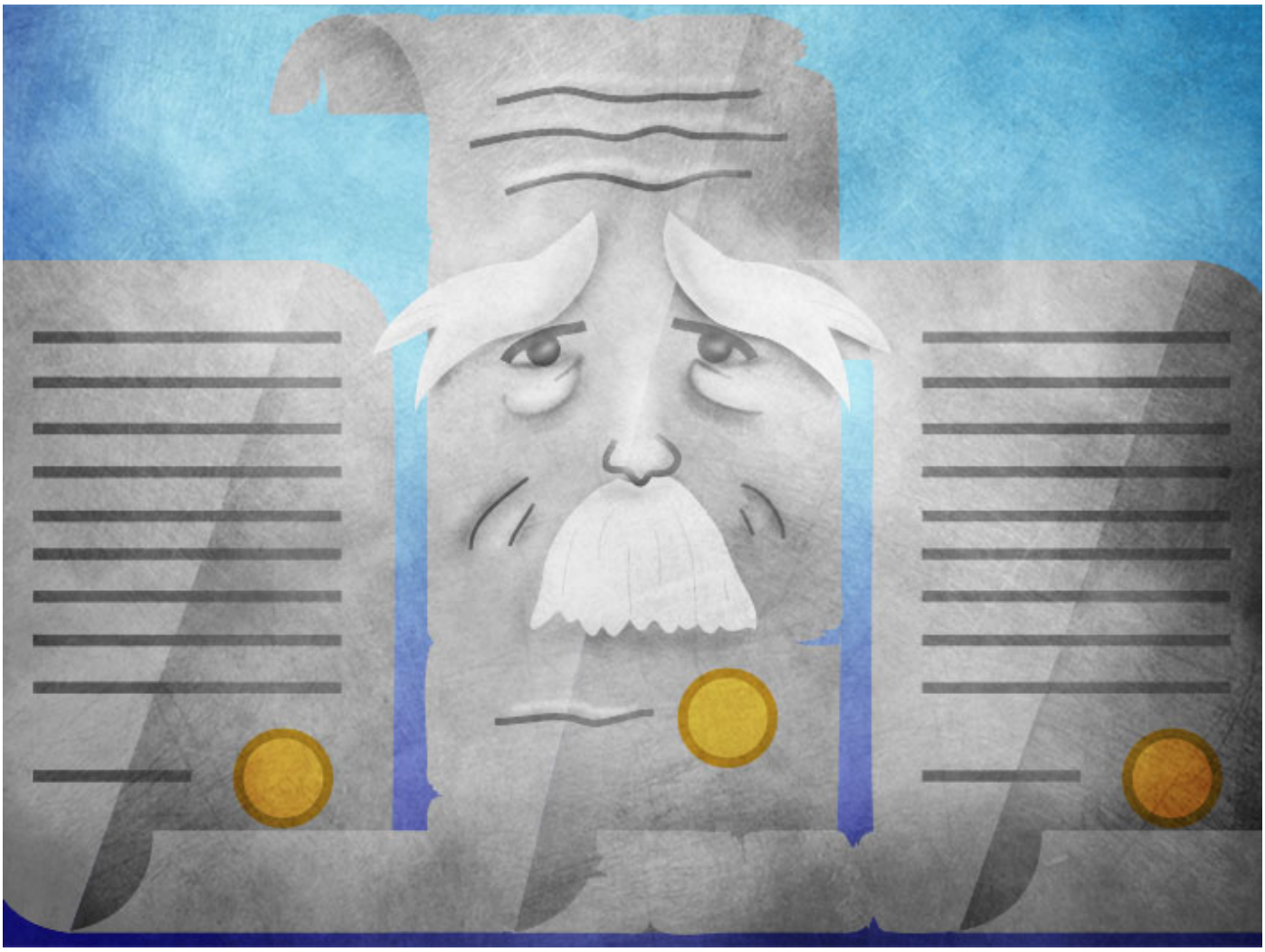
En este artículo se destacará la necesidad de tener buenas prácticas en las empresas sobre el manejo de la información y sus políticas de seguridad. En la mayoría de éstas el usuario promedio tiende a descuidar sus activos, ya sea personal o empresarial, con el fin de cumplir con su trabajo, lo cual provoca un incremento en los reportes de incidentes que se emiten en las organizaciones.

Se han encontrado empresas que carecen de políticas de seguridad informática o tienen algunas mal elaboradas o sin sentido, y otras que preservan políticas extremadamente ambiciosas y difíciles de cumplir. Un claro ejemplo es una entidad que basa la creación de sus políticas sin dimensionar el alcance de un modelo como ISO 27001 y sólo redacta el documento con el propósito de cumplir el

estándar, sin antes saber los retos tecnológicos que conlleva.

Podemos encontrar una empresa que, con el fin de tener un modelo de políticas, únicamente las elabora basándose en reglamentos, sin dar prioridad a la función principal: la protección de la información. Esto no sólo lleva a tener un régimen de políticas pobre, sino que carecen de continua revisión y cambio con el fin de cumplir los requisitos auditorías o procesos de evaluación empresarial.

También existen empresas que se proponen elaborar políticas extremadamente ambiciosas que no podrán cumplir ya que, por lo regular, no tienen los recursos necesarios en cuestiones económicas, tecnológicas o humanas. Normalmente el ciclo de vida de este documento provocará la desaparición y extinción de este de forma total o, en el mejor de los casos, su adecuación favorable.

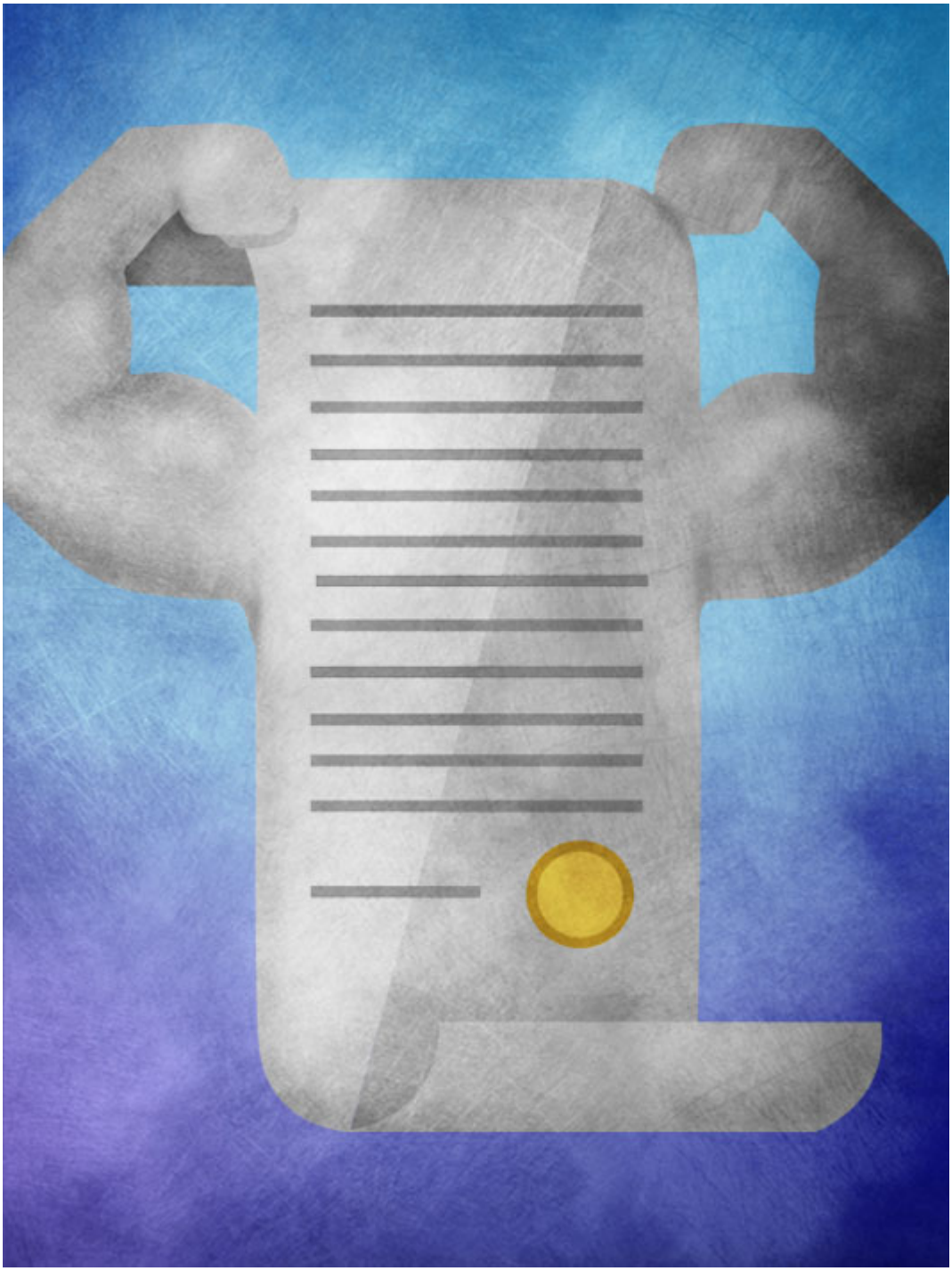


## ¿CÓMO ELABORAR UN DOCUMENTO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA Y DE SEGURIDAD DE LA INFORMACIÓN?

Dada la importancia de un documento de esta magnitud en cualquier empresa y en especial en las empresas TIC, al escribirlo deben contemplarse previamente los siguientes puntos:

1. Elaborar políticas claras. Cualquier usuario promedio podrá entenderlas, llevarlas a la práctica y cumplirlas en su totalidad.
2. Desarrollar políticas que la organización pueda realizar en función del usuario, ya que éste es quien logra que se lleven a cabo.
3. Establecer políticas que la alta dirección de la organización desee y pueda cumplir, no sólo elaborarlas para aprobar una auditoría o un proceso de evaluación.
4. Fijar políticas concretas. Deben mostrar tanto lo que se debe realizar como las limitantes de lo que se pretende proteger o no comprometer.
5. Toda política que se pretenda incluir en el documento se debe difundir; ningún usuario debe desconocerla.
6. El documento debe estar en un lugar de fácil acceso y consulta para que los usuarios de la compañía puedan leerla no a modo de complemento a sus labores, sino como una obligación expresa en su contrato.
7. Se debe dar una clasificación de protección de la información al documento, de eso dependerá su capacidad de difusión hacia los usuarios.
8. Es indispensable que los proveedores de servicios ajenos a la organización conozcan el documento para que se apeguen a ellas y apoyen en su cumplimiento.
9. Las políticas deben tener una campaña de difusión: Debe ser distinta pero no ajena a la campaña de concientización en materia de seguridad de la información, ya que de ésta dependerá que el documento sea analizado por todos los usuarios de la empresa y no sea olvidado.
10. Se debe tener como mínimo una revisión del documento con una periodicidad menor a los 180 días. Lo más importante que debemos analizar y tener claro es que ninguna política es perfecta. Los usuarios tratarán de encontrar fallos en las mismas para burlarlas o no ser sancionados. Por eso, ninguna política es perpetua ni ha sido “escrita en piedra”.

El marco de normatividad en el que nos basaremos para elaborar el documento deberá ser siempre aquel que nos acomode y sea acorde a nuestra organización (su giro, su capacidad tecnológica y su capacidad humana). No debemos ambicionar un marco normativo muy complejo si no lo vamos a cumplir ya que de esto también depende que sea exitoso al ponerlo en marcha dentro de la empresa.



Respecto al marco de elaboración en que se basa, deberá ser siempre en total y completo apoyo de la dirección general o alta dirección de la organización y contemplar que la persona o área encargada de generar el mutuo acuerdo de documentación de seguridad sea totalmente ajena al área de tecnología. De esta manera evitaremos que exista un error muy común cometido en las organizaciones: hacer juez y parte al área de tecnología.

Es preferible tener una persona o área de seguridad que no dependa de la tecnología y que esté siempre a la salvaguarda de la seguridad, verificando que se cumplan las políticas y que se gestionen correctamente los incidentes generados, con un seguimiento continuo de los mismos hasta su

remediación.

No se puede dejar fuera nunca la ayuda de los consultores externos quienes, a través de su perfil de consultoría en seguridad informática, han obtenido la certeza de verificar un documento de políticas en el marco de su normatividad hacia la organización. Siempre es válido utilizar a una de estas personas que no intervenga directamente en la organización, únicamente en su verificación de documentación y procedimientos de seguridad informática.

## ¿CÓMO SABER CUÁNDO NUESTRO DOCUMENTO DE POLÍTICAS ESTÁ TERMINADO?

Las características de nuestro documento al final de la redacción incluyen:

- Ser entendible.
- Ser fácil de asimilar.
- Que pueda ser cumplido por cualquier usuario de la organización.
- Ser factible para el área de tecnología.
- Estar disponible para cualquier miembro de la organización.
- Ser leído por los proveedores externos para que ayuden en su cumplimiento.
- Tener por completo el apoyo de la alta dirección de la organización.

Entonces podemos decir “misión cumplida” ya que así tendremos Políticas de Seguridad Informática y de Seguridad de la Información, y a partir de este momento comienza el cumplimiento del marco normativo en la organización del que serán partícipes los usuarios finales.

## SI QUIERES SABER MÁS CONSULTA:

- Gestión de seguridad de la información basado en MAAGTICSI
- Lo que no debes pasar por alto para gestionar la seguridad de la información
- Hablando correctamente de la seguridad de la información

---