NORMATIVIDAD EN LAS ORGANIZACIONES: POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN - PARTE I

Miguel Ángel Mendoza López
Pablo Antonio Lorenzana Gutiérrez

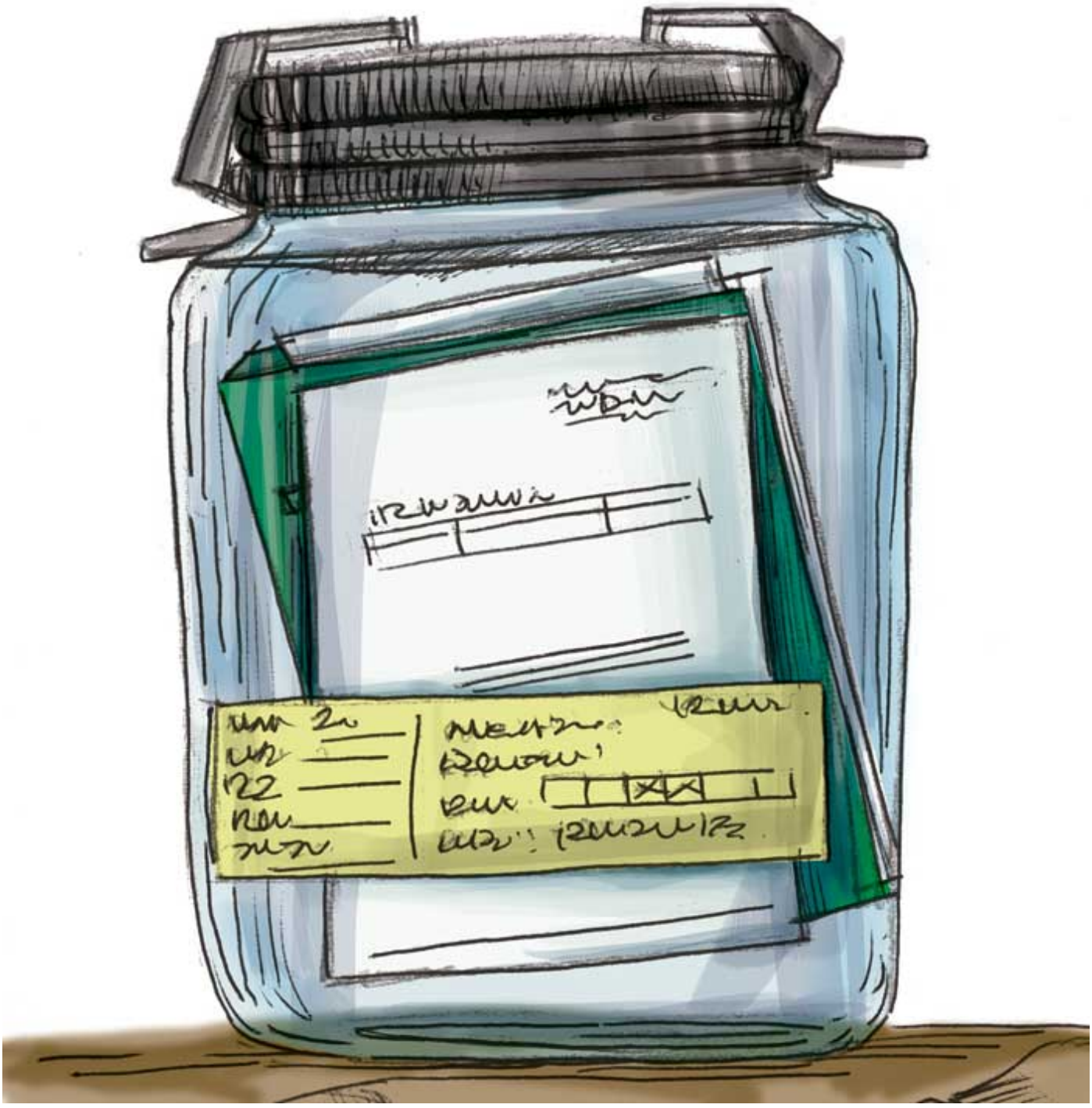
Gestión de seguridad

numero-16

En la actualidad, las organizaciones hacen uso de tecnologías de la información para su operación diaria. El logro de sus objetivos se debe en gran medida a su utilización. Sin embargo, existen riesgos inherentes a ellas, es decir, la posibilidad de que una debilidad sea aprovechada por una amenaza y sus consecuencias: divulgación, modificación, pérdida o interrupción de información sensible.

Las herramientas y medios técnicos por sí mismos ya no garantizan un adecuado nivel de seguridad con relación al manejo de la información. En este contexto, las políticas de seguridad surgen como una herramienta para ayudar en el proceso de concientización de los miembros de una organización, sobre la importancia y sensibilidad de la información, además de ofrecer un marco normativo para el uso adecuado de la infraestructura de TI.

De acuerdo con la encuesta *The State of Network Security 2012*, realizada a más de 180 profesionales de seguridad de la información y TI, la mayoría de los incidentes de seguridad de la información que se producen en las organizaciones son ocasionados por los propios empleados, ya sea por descuido, desconocimiento o intencionalmente, debido a que no existen mecanismos de control que regulen su conducta. En otras palabras, no existen políticas de seguridad de la información. Si no existe una política, el empleado no dispone de normas, desconoce los límites y responsabilidades asociadas a las actividades que desempeña.



El desarrollo de políticas de seguridad puede verse como una labor complicada debido al bloqueo creativo del responsable durante la redacción y generación de su contenido, generalmente suelen ser víctimas del *síndrome de la hoja en blanco*. Para evitar esto, es recomendable responder las siguientes interrogantes:

- ¿Quién debe ser la persona responsable de crear las políticas?

- ¿En qué estándar o mejor práctica deben tener base?
- ¿Cuáles son los ámbitos de aplicación?
- ¿Qué estructura debe tener el documento?
- ¿Cómo redactar los enunciados?
- ¿Existen o deben crearse otros documentos que complementen a las políticas?
- ¿Cómo deben difundirse entre los empleados?

La respuesta a cada una de estas preguntas resulta complicada si no se cuenta con los elementos básicos para la elaboración de las políticas. Un elemento esencial es conocer el objetivo y las características que debe poseer un documento como este.

En el ámbito de la seguridad de la información, una política es un documento que describe los requisitos o reglas específicas que deben cumplirse en una organización. Presenta una declaración formal, breve y de alto nivel, que abarca las creencias generales de la organización, metas, objetivos y procedimientos aceptables para un área determinada. Entre otras características:

- Requiere cumplimiento (obligatorio).
- El incumplimiento deriva en una acción disciplinaria.
- Se enfoca en los resultados deseados y no en los medios de ejecución.
- Deben ser concisas y fáciles de entender.
- Deben mantener un balance entre la protección y la productividad.

Las políticas de seguridad de la información proveen un marco para que las mejores prácticas puedan ser seguidas por los empleados, permiten minimizar riesgos y responder a eventos indeseados e inesperados. También ayudan al personal de la organización a asegurar sus activos, definir la postura de la organización hacia la protección de la información frente a accesos no autorizados, modificación, divulgación o destrucción. De manera específica, las políticas permiten:

- Proteger activos (personas, información, infraestructura y sistemas).
- Definir reglas para la conducta esperada del personal y usuarios.
- Definir roles y responsabilidades del personal.
- Definir y autorizar sanciones en caso de una violación.
- Mitigar riesgos.
- Ayudar en el cumplimiento de leyes, regulaciones y contratos.
- Crear conciencia entre el personal sobre la importancia y protección de los activos, principalmente de la información.

Los beneficios que ofrecen las políticas pueden ser fácilmente descartados si no se definen de manera previa las personas a las cuales están dirigidas (audiencia), lo que determina el sentido de los enunciados escritos. Se pueden tener diversos intereses dentro de la organización, por lo que la audiencia de las políticas puede ser dividida en categorías. Todos los usuarios (lectores) se incluyen en al menos una categoría, por ejemplo:

- Personal administrativo (recursos humanos, contabilidad, etc.).
- Personal técnico (programadores, administradores de sistemas, administradores de red, etc.).
- Usuarios finales.

La audiencia determinará lo que se debe incluir en cada política. Por ejemplo, no siempre se incluirá

una descripción del *porqué* cierta acción es necesaria en una política. Si el lector es responsable de configurar un sistema, es posible que no requiera una explicación del enunciado de la política. Un miembro del personal administrativo conoce los principios y el contexto detrás de esas acciones en un lenguaje no técnico, por lo que tampoco requiere de la explicación. Sin embargo, si el lector es un usuario final, sería útil incorporar una descripción del *porqué* un control de seguridad es necesario, esto contribuye en el entendimiento y cumplimiento de la política.

La estructura jerárquica también juega un rol importante para el cumplimiento. Es recomendable contar con una política rectora de carácter gerencial, soportada por otro grupo de políticas de carácter técnico, de las cuales pueden derivar guías y/o procedimientos.

- **Política rectora**. Es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información, establece la importancia de los activos, el *qué* y *porqué* una organización planea protegerlos. Debe ser enriquecida con otras políticas dependientes, guías y

  organizaciones,seguridad,información,politicas

  procedimientos.

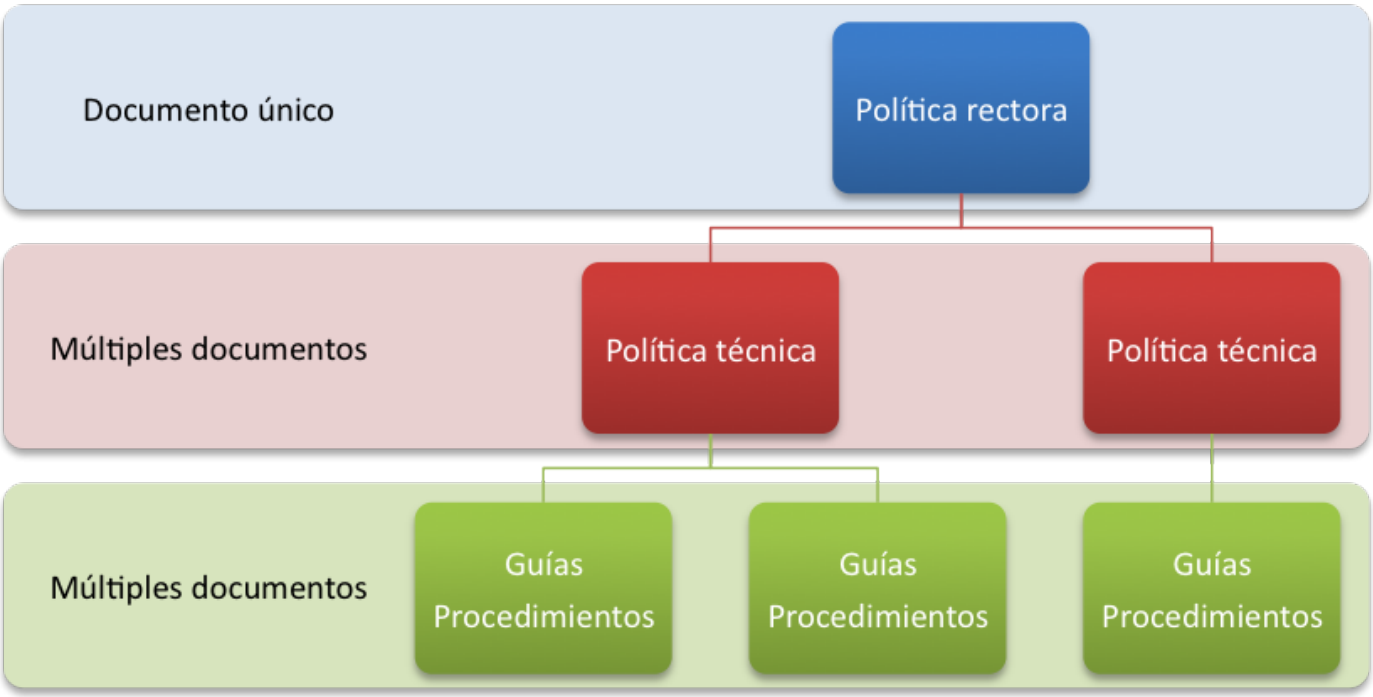
  Image not found or type unknown

- **Políticas técnicas**. Son más detalladas que la política rectora y definen los elementos necesarios para asegurar los activos. En términos de nivel de detalle, una política técnica establece el *qué* (a mayor detalle), *quién*, *cuándo* y *dónde*. Describe lo que se debe hacer, pero no la manera de llevarlo a cabo, esto está reservado para las guías y procedimientos. Los temas que pueden ser considerados son:

  - *Sistemas operativos*
  - *Aplicaciones*
  - *Red*
  - *Administración*
  - *Planes de negocio*
  - *Dispositivos de seguridad*
  - *Dispositivos periféricos*
  - *Dispositivos móviles*

- *Criptografía*
- *Seguridad física*

- **Guías y procedimientos**. Proporcionan los pasos a seguir para llevar a cabo los enunciados de las políticas técnicas. Son documentos adjuntos y están escritos en un siguiente nivel de granularidad, ya que describen *cómo* se deben hacer las cosas. Generalmente, están redactados en un lenguaje técnico avanzado debido a que está dirigido a personal operativo. Por ejemplo, se pueden incluir guías de *hardening* de sistemas operativos.



Por otro lado, el desarrollo de políticas requiere de la participación de miembros de la organización directamente relacionados con los procesos esenciales de la misma, por lo que es importante contar con un comité o equipo que se encargará de autorizar cambios y actualizaciones de los documentos relacionados (políticas, procedimientos, guías y formatos).

El comité puede estar integrado por personal clave en la operación de la organización, que tenga el conocimiento y dominio de los procesos operativos. Por ejemplo, los jefes de departamento, dueños o custodios de activos, etc. Dentro de sus responsabilidades con relación a las políticas, se debe agregar:

- Aprobar nuevas políticas, iniciativas y actividades.
- Crear, revisar, aprobar y difundir.
- Sancionar violaciones.

- Realizar reuniones periódicas para la revisión, adecuación y cumplimiento.
- Establecer roles y responsabilidades para asegurar que las actividades se realizan en tiempo y forma.

El desarrollo de las políticas inicia con la priorización de los temas que deben abordarse, la identificación del personal al cual van dirigidas y los activos a proteger. Para ello, se pueden realizar las siguientes actividades:

- Seleccionar las áreas que utilicen información que deba ser protegida por alguna ley (nacional, estatal o local).
- Identificar información utilizada para la toma de decisiones críticas dentro de la organización.
- Identificar información crítica para la continuidad de las operaciones.
- Definir la sensibilidad de la información.
- Especificar un esquema de clasificación de información.

Una vez que se han realizado las actividades anteriores, el equipo de desarrollo de políticas debe comenzar la redacción de los documentos y seguir su ciclo de vida, el cual se basa en un proceso de mejora continua. La identificación de incumplimientos, inconsistencias y la retroalimentación de las partes involucradas permite realizar adecuaciones en los documentos. El ciclo se conforma de cinco fases:

- **Escritura.** La redacción debe emplear un lenguaje conciso y fácil de comprender, los responsables definen el sentido de la política, evitando el uso de negaciones directas en los enunciados. Por ejemplo, "El usuario debe bloquear su equipo al ausentarse de su lugar de trabajo", es una política que indica lo que está permitido, o "Se prohíbe que el usuario deje un equipo desatendido sin bloquear la sesión", es una política que indica lo que está prohibido. Ambas redacciones son aceptables siguiendo un enfoque permisivo o prohibitivo respectivamente, pero "El usuario no debe dejar su equipo desatendido sin bloquear la sesión" es una redacción de carácter negativo que debe evitarse.
- **Revisión.** Permite definir el contenido de las políticas de acuerdo a los intereses de la organización, el sentido de la redacción y la funcionalidad de lo descrito en los enunciados, sin afectar las operaciones cotidianas, es decir, mantener un equilibrio entre la funcionalidad y la operatividad.
- **Aprobación.** Una vez que hayan sido revisadas y se considere que el contenido es apropiado, las políticas deben ser ratificadas por el comité para su publicación. Se debe incluir la fecha de aprobación.
- **Difusión.** Una actividad primordial consiste en dar a conocer las políticas y su entrada en vigor, el crear las políticas y no difundirlas resulta un gran esfuerzo desperdiciado. Por tal motivo, el comité debe idear mecanismos para dar a conocerlas entre las audiencias, a través de actividades como la creación de carteles, trípticos, sesiones informativas y otras.
- **Actualización.** La aplicación de políticas es una actividad permanente y de mejora continua, por lo que pueden realizarse reajustes. La presencia recurrente de la violación de una política, una sugerencia de las partes involucradas, el uso de nueva tecnología o cambios en la estructura organizacional son algunas de las razones por las cuales se actualiza una política.

Con los puntos antes descritos, se pretende dar respuesta a algunas de las interrogantes plasmadas en este artículo, en la segunda entrega se abordará la estructura de los documentos y su alineación a una mejor práctica o estándar.

Los responsables de la creación de políticas deben considerar las operaciones cotidianas, los hábitos y la cultura organizacional, para instar a las audiencias en su aceptación y cumplimiento, basados en el principio de que las políticas no representan restricciones o cargas laborales, sino elementos que permiten proteger los activos al tiempo que madura la operación. De esta manera las organizaciones podrán gozar del beneficio que ofrecen.

Participaron como coautores de este artículo: Ing. Sandra Atonal Jiménez, Ing. Rubén Aquino Luna

Referencias

- **International Organization for Standardization.** ISO/IEC 27001:2005.
- **SANS Institute.** Information Security Policy - A Development Guide for Large and Small Companies.
- **SANS Institute.** Security Policy Roadmap - Process for Creating Security Policies.

- **SANS Institute.** A Short Primer for Developing Security Policies.
- **The State of Network Security 2012.** AlgoSec Survey Insights.

Si quieres saber más, visita:

- Riesgo tecnológico y su impacto
- Conferencia DISC 2012- Políticas de Seguridad
- Buenas prácticas, estándares y normas

Rrirr

Rkfdj
