GUÍA PARA LA ELABORACIÓN DE POLÍTICAS DE SEGURIDAD EN LA EMPRESA

Por Univ. Nac. de Colombia

Texto traducido y adaptado de "The Security Policy Life Cycle: Functions and Responsibilities", de Patrick D. Howard, Information Security Management Handbook, Edited by Tipton & Krause, CRC Press LLC, 2003.

Publicado en SecurityTechnology | Nov. – Dic. 2006

http://www.st-magazine.com/

Esta metodología es potencialmente útil para el desarrollo, implementación, mantenimiento y eliminación de un conjunto completo de políticas – tanto de seguridad como en otras áreas. Este documento presenta algunos puntos de que deben tenerse en cuenta al desarrollar algunA política de seguridad informática.

«Muchas políticas de seguridad informática suelen fallar ya que se desconoce lo que implica realmente desarrollarlas.»

Es frecuente que las personas involucradas con seguridad informática tengan una visión estrecha de lo que significa desarrollar las políticas de seguridad, pues no basta con escribirlas y pretender ponerlas en práctica. En ocasiones se incluye la asignación de responsables, se realizan actividades para dar a conocerlas y, quizá, se supervise su cumplimiento; pero esto tampoco basta. Muchas políticas de seguridad informática fallan ya que se desconoce lo que implica realmente desarrollarlas.

Es importante resaltar que una política de seguridad tiene un ciclo de vida completo mientras esta vigente. Este ciclo de vida incluye un esfuerzo de investigación, la labor de escribirla, lograr que las directivas de la organización la acepten, conseguir que sea aprobada, lograr que sea diseminada a través de la empresa, concienciar a los usuarios de la importancia de la política, conseguir que la acaten, hacerle seguimiento, garantizar que esté actualizada y, finalmente, suprimirla cuando haya perdido vigencia. Si no se tiene en cuenta este ciclo de vida se corre el riesgo de desarrollar políticas que sean poco tenidas en cuenta, incompletas, redundantes, sin apoyo pleno por parte de los usuarios y las directivas, superfluas o irrelevantes.

Este documento presenta algunos puntos de que deben tenerse en cuenta al desarrollar alguna política de seguridad informática.

¿Por qué tener políticas escritas?

Existen varias razones por las cuales es recomendable tener políticas escritas en una organización La siguiente es una lista de algunas de estas razones.

· Para cumplir con regulaciones legales o técnicas

· Como guía para el comportamiento profesional y personal

· Permite unificar la forma de trabajo de personas en diferentes lugares o momentos que tengan responsabilidades y tareas similares

· Permiten recoger comentarios y observaciones que buscan atender situaciones anormales en el trabajo

· Permite encontrar las mejores prácticas en el trabajo

· Permiten asociar la filosofía de una organización (lo abstracto) al trabajo (lo concreto)

Definición de política

Es importante aclarar el término política desde el comienzo. ¿Qué queremos dar a entender cuando decimos POLITICA o ESTÁNDAR o MEJOR PRÁCTICA o GUÍA o PROCEDIMIENTO?

Estos son términos utilizados en seguridad informática todos los días, pero algunas veces son utilizados correctamente, otras veces no.

Política. Declaración general de principios que presenta la posición de la administración para un área de control definida. Las políticas se elaboran con el fin de que tengan aplicación a largo plazo y guíen el desarrollo de reglas y criterios más específicos que aborden situaciones concretas. Las políticas son desplegadas y soportadas por estándares, mejores prácticas, procedimientos y guías. Las políticas deben ser pocas (es decir, un número pequeño), deben ser apoyadas y aprobadas por las directivas de la empresa, y deben ofrecer direccionamientos a toda la organización o a un conjunto importante de dependencias. Por definición, las políticas son obligatorias y la incapacidad o imposibilidad para cumplir una política exige que se apruebe una excepción.

Estándar. Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares sirven como especificaciones para la implemen tación de las políticas: son diseñados para promover la implementación de las políticas de alto nivel de la organización antes que crear nuevas políticas.

Mejor práctica. Es una regla de seguridad específica a una plataforma que es aceptada a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la organización.

Guía. Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares y buenas prácticas. Las guías son, esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

Procedimiento. Los procedimientos definen específicamente cómo las políticas, estándares, mejores prácticas y guías serán implementados en una situación dada. Los procedimientos son dependientes de la tecnología o de los procesos y se refieren a plataformas, aplicaciones o procesos específicos.

Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada a dicho proceso o sistema específico.

Generalmente los procedimientos son desarrollados, implementados y supervisados o del sistema. Los procedimientos por el dueño del proceso seguirán las políticas de la organización, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro de la dependencia donde ellos se aplican.

El cuadro anterior, además de presentar una definición de los términos utilizados en la enunciación e implementación de políticas, muestra una jerarquía entre las definiciones.

Un ejemplo de los requerimientos de seguridad interrelacionados podría ser:

1. En el nivel más alto, se puede elaborar una POLÍTICA, para toda la organización, que obligue a "garantizar seguridad en el correo electrónico cuyo contenido sea información confidencial"

2. Esta POLÍTICA podría ser soportada por varios ESTÁNDARES, incluyendo por ejemplo, que los mensajes de este tipo sean enviados utilicriptografía zando algún sistema de aprobado por la empresa y que sean borrados de manera segura después de su envío.

3. Una MEJOR PRÁCTICA, en este ejemplo, podría estar relacionada sobre la manera de configurar el correo sobre un tipo específico de sistema (Windows o Linux) con el fin de garantizar el cumplimiento de la POLÍTICA y del ESTÁNDAR.

4. Los PROCEDIMIENTOS podrían especificar requerimientos para que la POLÍTICA y los ESTÁNDARES que la soportan, sean aplicados en una dependencia específica, por ejemplo la Oficina de Control Interno.

5. Finalmente, las GUÍAS podrían incluir información sobre técnicas, configuraciones y secuencias de comandos recomendadas que deben seguir los usuarios para asegurar la información confidencial enviada y recibida a través del servicio de correo electrónico.

Nótese que, en muchas ocasiones, el trémino "política" es utilizado en un sentido genérico para aplicarlo a cualquiera de los tipos de requerimientos de seguridad expuestos. En este documento se llamará política, de manera genérica, a todos los requerimientos de seguridad mencionados antes y POLÍTICA (en mayúsculas) a las políticas propiamente dichas.

Hay varias etapas que deben realizarse a través de "la vida" de una política. Estas etapas pueden ser agrupadas en 4 fases.

1. Fase de desarrollo: durante esta fase la política es creada, revisada y aprobada.

2. Fase de implementación: en esta fase la política es comunicada y acatada (o no cumplida por alguna excepción).

3. Fase de mantenimiento: los usuarios deben ser concientes de la importancia de la política, su cumplimiento debe ser monitoreado, se debe garantizar su cumplimiento y se le debe dar mantenimiento (actualizarla)

4. Fase de eliminación: La política se retira cuando no se requiera más.

Creación, Planificación, investigación, documentación, y coordinación desde la política

El primer paso en la fase de desarrollo de una política es la planificación, la investigación y la redacción de la política o, tomado todo junto, la creación. La creación de una política implica identificar por qué se necesita la política (por ejemplo, requerimientos legales, regulaciones técnicas, contractuales u operacionales); determinar el alcance y la aplicabilidad de la política, los roles y las responsabilidades inherentes a la aplicación de la política y garantizar la factibilidad de su implementación. La creación de una políticatambién incluye la investigación para determinar los requerimientos organizacionales para desarrollar las políticas (es decir, que autoridades deben aprobarla, con quién se debe coordinar el desarrollo y estándares del formato de redacción), y la investigación de las mejores prácticas en la industria para su aplicabilidad a las necesidades organizacionales actuales.

De esta etapa se tendrá como resultado la documentación de la política de acuerdo con los procedimientos y estándares de la empresa, al igual que la coordinación con entidades internas y externas que la política afectará, para obtener información y su aceptación. En general, la creación de una política es la función más fácil de entender en el ciclo de vida de desarrollo de una política.

Revisión: Evaluación independiente de la política

La revisión de la política es la segunda etapa en la fase de desarrollo del ciclo de vida. Una vez la documentación de la política ha sido creada y la coordinación inicial ha sido iniciada, esta debe ser remitida a un grupo (o un individuo) independiente para su evaluación antes de su aprobación final. Hay varios beneficios de la revisión independiente: una política más viable a través del escrutinio de individuos que tienen una perspectiva

diferente o más vasta que la persona que redactó la política; apoyo más amplio para la política a través de un incremento de involucrados; auento en el número de credibilidad en la política gracias a la información recibida de diferentes especialistas del grupo de revisión. Propio de esta etapa es la presentación de la política a los revisores, ya sea de manera formal o informal, exponiendo cualquier punto que puede ser importante para la revisión, explicando su objetivo, el contexto y los beneficios potenciales de la política y justificando por qué es necesaria. Como parte de esta función, se espera que el creador de la política recopile los comentarios y las recomendaciones para realizar cambios en la política y efectuar todos los ajustes y las

revisiones necesarias para obtener una versión final de la política lista para la aprobación por las directivas.

Aprobación: Obtener la aprobación de la política por parte de las directivas

El paso final en la fase de desarrollo de la política es la aprobación. El objetivo de esta etapa es obtener el apoyo de la administración

de la empresa, a través de la firma de una persona ubicada en una posición de autoridad.

La aprobación permite iniciar la implementación de la política. Requiere que el proponente de la política haga una selección adecuada de la autoridad de aprobación, que coordine con dicho funcionario, presente las recomendaciones emitidas durante la etapa de revisión y haga el esfuerzo para que sea aceptada por la administración. Puede ocurrir que por incertidumbre de la autoridad de aprobación sea necesaria una aprobación temporal.

Comunicación: Difundir la política

Una vez la política ha sido aprobada formalmente, se pasa a la fase de implementación.

La comunicación de la política es la primera etapa que se realiza en esta fase. La política debe ser inicialmente difundida a los miembros de la comunidad universitaria o a quienes sean afectados directamente por la política (contratistas, proveedores, usuarios de cierto servicio, etc.). Esta etapa implica determinar el alcance y el método inicial de distribución de la política (es posible que deban tenerse en cuenta factores como la ubicación geográfica, el idioma, la cultura y línea de mando que será utilizada para comunicar la política). Debe planificarse esta etapa con el fin de deterinmar los recursos necesarios y el enfoque que debe ser seguido para mejorar la visibilidad de la política.

Cumplimiento: Implementar la política

La etapa de cumplimiento incluye actividades relacionadas con la ejecución de la política. Implica trabajar con otras personas de la empresa, vicerrectores, decanos, directores de departamento y los jefes de dependencias (de división o de sección) para interpretar cuál es la mejor manera de implementar la política en diversas situaciones y oficinas; asegurando que la política es entendida por aquellos que requieren implementarla, monitorearla, hacerle seguimiento, reportar regularmente su cumplimiento y medir el impacto inmediato de la política en las actividades operativas.

Dentro de estas actividades está la elaboración de informes a la administración del estado de la implementación de la política.

Excepciones: Gestionar las situaciones donde la imimplementación no es posible

Debido a problemas de coordinación, falta de personal y otros requerimientos operacionales, no todas las políticas pueden ser cumplidas

de la manera que se pensó al comienzo. Por esto, es probable que se requieran excepciones a la política para permitir a ciertas oficinas o personas el no cumplimiento de la política. Debe establecerse un proceso para garantizar que las solicitudes de excepciones son registradas, seguidas, evaluadas, enviadas para aprobación o desaprobación, documentadas y vigiladas a través del periodo de tiempo establecido para la excepción. El proceso también debe permitir excepciones permanentes a la política al igual que la no aplicación temporal por circunstancias de corta duración.

Concienciación: Garantiza la concienciación de la política

La etapa de concienciación de la fase de mantenimiento comprende los esfuerzos continuos realizados para garantizar que las personas están concientes de la política y buscan facilitar su cumplimiento. Esto es hecho al definir las necesidades de concienciación de los diversos grupos de audiencia dentro de la organización (directivos, jefes de dependencias, usuarios, etc.); en relación con la adherencia a la política, determinar los métodos de concienciación más efectivos para cada grupo de audiencia (es decir, reuniones informativas, cursos de entrenamiento, mensajes de correo, etcétera); y desarrollo y difusión de material de concienciación (presentaciones, afiches, circulares, etc.). La etapa de concienciación también incluye esfuerzos para integrar el cumplimiento de la política y retroalimentación sobre el control realizado para su cumplimio.

Monitoreo: Seguimiento y reporte del cumcumplimiento de la política

Durante la fase de mantenimiento, la etapa de monitoreo es realizada para seguir y reportar la efectividad de lo esfuerzos en el cumplimiento de la política. Esta información se obtiene de la observación de los docentes, estudiantes, empleados y los cargos de supervisión, mediante auditorias formales, evaluaciones, inspecciones, revisiones y análisis de los reportes de contravenciones y de las actividades realizadas en respuesta a los incidentes.

Esta etapa incluye actividades continuas para monitorear el cumplimiento o no de la política a través de métodos formales e informales y el reporte de las deficiencias encontradas a las autoridades apropiadas.

Garantía desde cumplimiento: Afrontar las contravenciones de la política

La etapa de garantía de cumplimiento de las políticas incluye las respuestas de la administración a actos u omisiones que tengan como resultado contravenciones de la política con el fin de prevenir que sigan ocurriendo. Esto significa que una vez una contravención sea identificada, la acción correctiva debe ser determinada y aplicada a los procesos (revisión del proceso y mejoramiento), a la tecnología (actualización) y a las personas (acción disciplinaria) involucrados en la contravención con el fin de reducir la probabilidad de que vuelva a ocurrir. Se recomienda incluir información

sobre las acciones correctivas adelantadas para garantizar el cumlimpiento en la etapa de concienciación.

Mantenimiento: Asegurar que la política esté actualizlizada

La etapa de mantenimiento esta relacionada con el proceso de garantizar la vigencia y la integridad de la política. Esto incluye hacer seguimiento a las tendencias de cambios en la tecnología, en los procesos, en las personas, en la organización, en el enfoque del negocio, etcétera, que puede afectar la política; recomendando y coordinando modificaciones resultado de estos cambios, documentándolos en la política y registrando las actividades de cambio. Esta etapa también garantiza la disponibilidad continuada de la política para todas las partes afectadas por ella, al igual que el mantenimiento de la integridad de la política a través de un control de versiones efectivo. Cuando se requieran cambios a la política, las etapas realizadas antes deben ser revisitadas, en particular las etapas de revisión, aprobación, comunicación y garantía de cumplimiento.

Retiro: Prescindir de la política cuando no se necesite más

Después que la política ha cumplido con su finalidad y no es necesaria (por ejemplo, la empresa cambió la tecnología a la cual aplicaba o se creó una nueva política que la reemplazó) entonces debe ser retirada. La etapa de retiro corresponde a la fase de eliminación del ciclo de vida de la política, y es la etapa final del ciclo. Esta función implica retirar una política superflua del inventario de políticas activas para evitar confusión, archivarla

para futuras referencias y documentar la información sobre la decisión de retirar la política (es decir, la justificación, quién autorizó, la fecha, etcétera).

Estas cuatro fases del ciclo de vida reúnen 11 etapas diferentes que deben seguirse durante el ciclo de vida de una política específica.

No importa como se agrupen, tampoco importa si estas etapas son abreviadas por necesidades de inmediatez, pero cada etapa debe ser realizada. Si en la fase de desarrollo la empresa intenta crear una política sin una revisión independiente, se tendrán políticas que no estarán bien concebidas ni serán bien recibidas por la comunidad universitaria.

En otras circunstancias, y por falta de visión, puede desearse omitir la etapa de excepciones de la fase de implementación, pensando equivocadamente que no existirán circunstancias para su no cumplimiento. También se podría descuidar la etapa de mantenimiento, olvidando la importancia de mantener la integridad y la vigencia de las políticas. Muchas veces se encuentran políticas inoficiosas en los documentos de importantes organizaciones, indicando que la etapa de retiro no está siendo realizada.

No sólo se requiere que las once etapas sean realizadas, algunas de ellas deben ser ejecutadas de manera cíclica, en particular mantenimiento, concienciación, monitoreo, y garantía de cumplimiento.