UNIVERSIDAD NACIONAL DE COLOMBIA
VICERRECTORIA GENERAL
DIRECCIÓN NACIONAL DE INFORMÁTICA Y COMUNICACIONES

Guía para elaboración de políticas de seguridad

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.

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 por parte de los usuarios y las directivas, superfluas o irrelevantes.

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

POR QUÉ TENER POLÍTICAS ESCRITAS

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

1. Para cumplir con regulaciones legales o técnicas
2. Como guía para el comportamiento profesional y personal
3. Permite unificar la forma de trabajo de personas en diferentes lugares o momentos que tengan responsabilidades y tareas similares
4. Permiten recoger comentarios y observaciones que buscan atender situaciones anormales en el trabajo
5. Permite encontrar las mejores prácticas en el trabajo
6. 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 POLÍTICA 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 universidad, 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 implementación 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 por el dueño del proceso o del sistema. Los procedimientos 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.

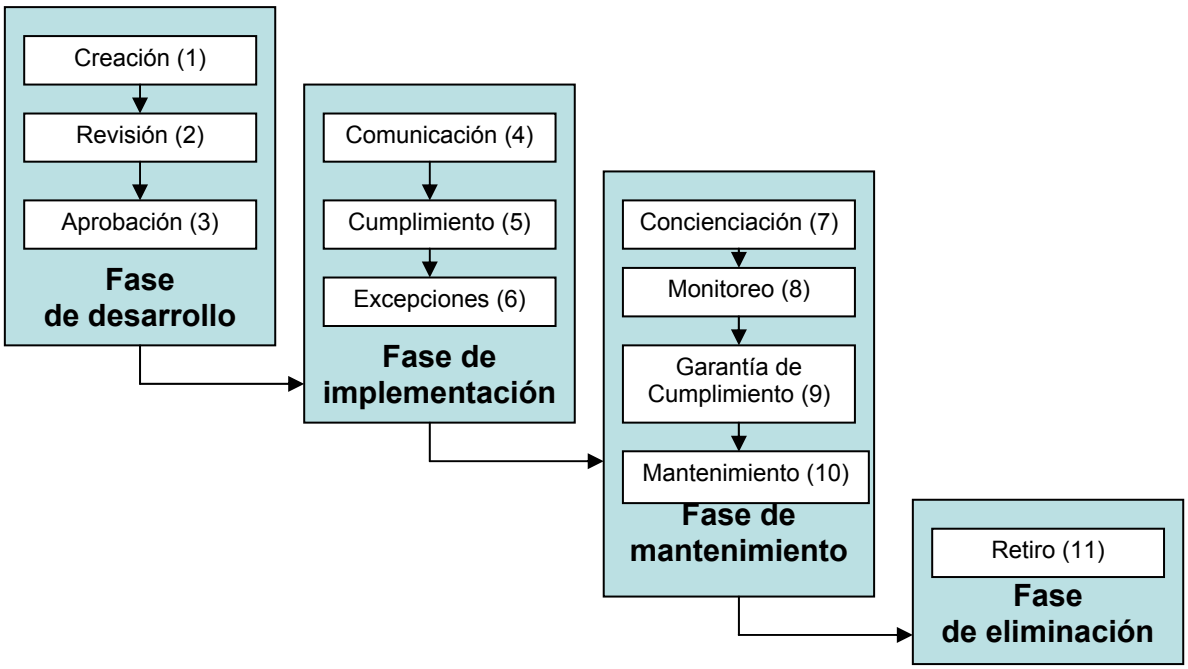
El cuadro anterior, además de presentar una definición de los términos utilizados en la enunciación e implementación de políticas, muestra una jerarquía entre las definiciones.

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 utilizando algún sistema de criptografía aprobado por la universidad 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 término "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.

ETAPAS EN EL DESARROLLO DE UNA POLÍTICA



Hay 11 etapas que deben realizarse a través de "la vida" de una política. Estas 11 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 de 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 política también 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 universidad, 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 en el número de involucrados; aumento 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 universidad, 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 determinar 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 universidad, 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 implementación 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, cuando los casos lo ameriten, 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 continuada 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 cumplimiento. La tarea final es medir la concienciación de los miembros de la comunidad universitaria con la política y ajustar los esfuerzos de

acuerdo con los resultados de las actividades medidas.

Monitoreo: *Seguimiento y reporte del cumplimiento 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 de 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 cumplimiento en la etapa de concienciación.

Mantenimiento: *Asegurar que la política esté actualizada*

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 (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 re-visitadas, 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 universidad 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*.

ALGUNAS PRÁCTICAS RECOMENDADAS PARA ESCRIBIR UNA POLÍTICA

Sin importar que una política se enuncie formal o informalmente, esta debe incluir 12 tópicos:

1. La declaración de la política (cuál es la posición de la administración o qué es lo que se desea regular)
2. Nombre y cargo de quien autoriza o aprueba la política
3. Nombre de la dependencia, del grupo o de la persona que es el autor o el proponente de la política
4. Debe especificarse quién debe acatar la política (es decir, a quién está dirigida) y quién es el responsable de garantizar su cumplimiento
5. Indicadores para saber si se cumple o no la política
6. Referencias a otras políticas y regulaciones en las cuales se soporta o con las cuales tiene relación
7. Enunciar el proceso para solicitar excepciones
8. Describir los pasos para solicitar cambios o actualizaciones a la política
9. Explicar qué acciones se seguirán en caso de contravenir la política
10. Fecha a partir de la cual tiene vigencia la política
11. Fecha cuando se revisará la conveniencia y la obsolescencia de la política
12. Incluir la dirección de correo electrónico, la página web y el teléfono de la persona o personas que se pueden contactar en caso de preguntas o sugerencias

Otras prácticas que se recomiendan seguir son:

1. Uso de lenguaje sencillo (evitar lenguaje técnico hasta donde sea posible)
2. Escribir la política como si fuese a utilizarse siempre
3. Debe escribirse de tal forma que pueda leerlo cualquier miembro de la universidad
4. Se debe evitar describir técnicas o métodos particulares que definan una sola forma de hacer las cosas
5. Cuando se requiera, hacer referencia explicita y clara a otras dependencias de la organización
6. Utilizar la guía para la presentación de documentos escritos de la universidad

ASPECTOS IMPORTANTES PARA DEFINIR RESPONSABILIDADES EN EL DESARROLLO DE POLÍTICAS

En muchas ocasiones se asume que la función seguridad informática –ya sea un grupo o un individuo- sea la encargada de adelantar la gran mayoría de las etapas en el ciclo de vida de una política y que también actúe como el proponente para la mayoría de las políticas relacionadas con la

protección de los activos informáticos. Por diseño, la función seguridad informática tiene la responsabilidad a largo plazo y debe ejecutar las tareas diarias para asegurar los activos de información y por tanto, debe ser el dueño y debe ejercer control centralizado sobre las POLÍTICAS, ESTÁNDARES, MEJORES PRÁCTICAS, PROCEDIMIENTOS Y GUÍAS relacionados con seguridad informática.

Pero en ningún caso la función seguridad informática debe ser el proponente *de todas las políticas relacionadas con seguridad*, ni tampoco debe realizar todas las etapas de desarrollo en el ciclo de vida de la política. Por ejemplo, los dueños de los sistemas de información deben tener la responsabilidad para establecer los requerimientos necesarios para implementar las políticas de la universidad para sus propios sistemas. Cuando existan requerimientos de seguridad en cierta dependencia que deben cumplir con políticas de nivel superior, su proponente debe ser la dependencia que tiene interés en garantizar la efectividad de dicha política.

Aunque el proponente o dueño de una política tiene una responsabilidad continúa sobre el ciclo de vida completo de la política, hay varios factores que influyen sobre la determinación y la decisión de quién o qué dependencia tienen responsabilidad directa para realizar etapas específicas del ciclo de vida de la política en una organización. Entre estos factores se incluyen:

1. **Separación de tareas**. El principio de separación de tareas debe ser aplicado para determinar la responsabilidad de una etapa en particular para garantizar que los chequeos y ajustes necesarios sean aplicados. Para proveer una perspectiva más amplia y diferente, un directivo, o un grupo que sea independiente del proponente, debe revisar la política y una directiva, superior al proponente, debe encargarse de aprobar la política. O, para disminuir los posibles conflictos de intereses, la función auditoria (o control interno), como oficina independiente dentro de la organización, debe ser encargada del monitoreo del cumplimiento de la política, en tanto que grupos u organizaciones de auditoria externos deben ser invitados a realizar una evaluación independiente del cumplimiento de las políticas para ser consistentes con el principio de separación de tareas.

2. **Eficiencia**. Adicionalmente, por razones de eficiencia, dependencias diferentes a la proponente deben tener alguna responsabilidad para la realización de ciertas etapas del ciclo de vida del desarrollo de una política. Por ejemplo, la difusión y la comunicación de la política sería mejor realizada si se encomendara a la dependencia encargada de estas funciones dentro de la organización (por ejemplo, la Secretaría General, las Secretarías de las sedes o UNIMEDIOS). Por otra parte, basados en la eficiencia, los esfuerzos de concienciación serían asignados a la función capacitación de la universidad (en este momento se encuentra en la Dirección Nacional de Personal y las oficinas de personal de las sedes) -aún cuando puede ocurrir que el personal de capacitación no esté entrenado específicamente en la labor de la concienciación de la política de seguridad-. En este último caso, sería mejor que la desarrollara la función de seguridad informática.

3. **Alcance del control**. Límites en el alcance del control que la dependencia proponente puede ejercer tiene impacto sobre quién debe ser el ponente de una política específica. Normalmente, el proponente sólo puede jugar un papel limitado en el monitoreo y en la garantía del cumplimiento de la política debido a que él no puede estar en todos lo sitios, en todo momento, donde ésta debe ser implementada. Los vicerrectores, decanos, directores de departamento, jefes de oficinas, de dependencias, de divisiones o de secciones, por su ubicación jerárquica, están cerca de las personas (docentes, estudiantes o empleados) a quienes afecta la política de seguridad y por tanto están en una mejor posición para monitorear de manera efectiva y garantizar el cumplimiento de la política. Por tanto deben

asumir la responsabilidad de estas etapas. Estos funcionarios pueden garantizar que la política está siendo seguida y que las contravenciones se manejan de manera adecuada.

4. **Autoridad**. Límites en la autoridad que un individuo o una dependencia ejerce, puede determinar la habilidad para desarrollar exitosamente una etapa del ciclo de vida de una política. La efectividad de una política, a menudo, puede ser juzgada por su visibilidad y el énfasis que la administración de la universidad coloquen. La efectividad de una política, en muchos casos, depende de la autoridad en la cual la política se soporta. Para que una política tenga un soporte en toda la organización, el directivo que la aprueba debe tener un reconocido grado de autoridad sobre una gran parte de la universidad. Normalmente, la función de seguridad informática de la organización no goza del nivel de reconocimiento ideal a través de toda la organización y requiere el soporte de directivas de nivel superior para cumplir con su misión. En consecuencia, la aceptación y el cumplimiento de las políticas de seguridad informática tienen mayor probabilidad de darse cuando la autoridad que la aprueba es de nivel superior.

5. **Conocimiento**. La ubicación del proponente en la universidad puede inducir a deficiencias en el conocimiento del entorno en el cual la política será implementada, entorpeciendo su efectividad. El empleo de un comité que realice la evaluación de políticas puede ofrecer un entendimiento más amplio de las operaciones que afectará la política. Un organismo de este tipo puede ayudar a garantizar que la política sea escrita con el fin de promover su aceptación y su implementación exitosa y puede ser útil para prever problemas de implementación y para evaluar efectivamente situaciones donde las excepciones a la política pueden ser justificadas. De acuerdo con el alcance de la política, la labor de evaluación puede ser realizada por el comité nacional de informática o los comités de informática de las sedes.

6. **Aplicabilidad**. Finalmente, la aplicabilidad de la política también afecta la responsabilidad en las etapas de desarrollo del ciclo de vida de la política. ¿Qué áreas de la universidad son afectadas por la política? ¿La política aplica a una sola dependencia, sólo a los usuarios de una tecnología en particular o a toda la universidad? Si la aplicabilidad de una política está limitada a una sola dependencia, entonces la jefatura de la dependencia debe tener su propia política. Sin embargo, si la política es aplicable a toda la universidad, entonces una dependencia de alto nivel debe asumir la responsabilidad en relación con la política.

RESPONSABILIDADES EN EL MODELO DE CICLO DE VIDA DE LA POLÍTICA

Para garantizar que todas las etapas del ciclo de vida sean realizadas de manera apropiada y las responsabilidades para su ejecución sean asignadas adecuadamente, la universidad debe establecer un marco de referencia para facilitar el entendimiento, promover la aplicación consistente, establecer una estructura jerárquica para soportar mutuamente los distintos niveles de políticas, y acomodar efectivamente los frecuentes cambios tecnológicos y organizacionales.

Modelo de responsabilidad por etapa para cada tipo de política.

Responsabilidad				
Etapa	**Políticas**	**Estándares y buenas prácticas**	**Guías**	**Procedimientos**
Creación	Función seguridad informática	Función seguridad informática e ingenieros con conocimiento en el área	Función seguridad informática e ingenieros con conocimiento en el área	Dependencia que los propone
Revisión	Comité de evaluación de políticas	Comité de evaluación de políticas	Comité de evaluación de políticas	Función seguridad informática y director de dependencia
Aprobación	Rector general o vicerrector general	Rector general o vicerrector	Rector general o vicerrector	Directivo del área
Comunicación	Secretaría o UNIMEDIOS	Secretaría o UNIMEDIOS	Secretaría o UNIMEDIOS	Dependencia que los propone
Cumplimiento	Docentes, estudiantes, empleados y funcionarios con responsabilidades de supervisión en toda la universidad	Docentes, estudiantes, empleados y funcionarios con responsabilidades de supervisión en toda la universidad	Docentes, estudiantes, empleados y funcionarios con responsabilidades de supervisión en toda la universidad	Empleados y funcionarios con responsabilidades de supervisión de la dependencia
Excepciones	Comité de evaluación de políticas	Comité de evaluación de políticas	No aplica	Directivo del área
Concienciación	Función seguridad informática y función capacitación	Función seguridad informática y función capacitación	Función seguridad informática y función capacitación	Jefe de dependencia
Monitoreo	Funcionarios con responsabilidades de supervisión, función seguridad informática y función auditoria	Funcionarios con responsabilidades de supervisión, función seguridad informática y función auditoria	Funcionarios con responsabilidades de supervisión, función seguridad informática y función auditoria	Funcionarios con responsabilidades de supervisión y personas asignadas dentro de la dependencia, función seguridad informática y función auditoria
Garantizar cumplimiento	Funcionarios con responsabilidades de supervisión	Funcionarios con responsabilidades de supervisión	No aplica	Funcionarios con responsabilidades de supervisión asignados en la dependencia
Mantenimiento	Función seguridad informática	Función seguridad informática	Función seguridad informática	Dependencia que los propone
Retiro	Función seguridad informática	Función seguridad informática	Función seguridad informática	Dependencia que los propone

El cuadro anterior proporciona una orientación para asignar responsabilidades a cada etapa de desarrollo de una política de acuerdo al nivel del requerimiento. En general, este modelo propone que la responsabilidad para las etapas relacionadas con las POLÍTICAS, ESTÁNDARES, MEJORES PRÁCTICAS y GUÍAS sean similares en muchos aspectos. Al existir una dependencia encargada de la gestión del programa de seguridad informática de toda la universidad, la función de seguridad informática debe servir como proponente para la mayoría de POLÍTICAS, ESTÁNDARES, MEJORES PRÁCTICAS Y GUÍAS relacionadas con la seguridad de los recursos de información de la universidad -en colaboración con los profesionales que tengan conocimientos en el área técnica específica-. Dentro de sus posibilidades, la función de seguridad informática debe realizar las etapas de creación, concienciación, mantenimiento y retiro para las políticas de seguridad de cada nivel. Sin embargo, hay excepciones a este principio general. Por ejemplo, aun

cuando tiene un impacto importante sobre la seguridad informática, es más eficiente que la dirección de personal sea quien proponga las políticas y los estándares, relacionados con seguridad informática, para contratar nuevos empleados. Las responsabilidades para las etapas relacionadas con el desarrollo de PROCEDIMIENTOS de seguridad son diferentes de las propuestas para las POLÍTICAS, ESTÁNDARES, MEJORES PRÁCTICAS y GUÍAS. El cuadro anterior muestra que los proponentes para los PROCEDIMIENTOS están por fuera de la función seguridad informática (un enfoque descentralizado), basados en la aplicabilidad limitada de dichos procedimientos a cierta dependencia. Aunque los PROCEDIMIENTOS se crean e implementan de manera descentralizada (en varias etapas), estos deben ser consistentes con las políticas de seguridad de mayor nivel; por tanto deben ser revisados por la función seguridad informática de la organización al igual que por el funcionario superior de la dependencia. Adicionalmente, las funciones de seguridad y de auditoria deben ofrecer retroalimentación al proponente sobre el cumplimiento de los PROCEDIMIENTOS cuando se estén conduciendo revisiones y auditorias.

La asignación de responsabilidades mostrada en el cuadro anterior se entiende mejor si se explora el modelo propuesto de acuerdo con las etapas del ciclo de vida:

- **Creación**. En la mayoría de las organizaciones la función seguridad informática debe servir como proponente de todas las políticas relacionadas con seguridad que engloban toda la organización y debe ser la responsable para crear estas POLÍTICAS, ESTÁNDARES, MEJORES PRÁCTICAS Y GUÍAS. Con el fin de garantizar la pertinencia de las políticas, es recomendable que en le universidad estas políticas sean elaboradas en conjunto con los profesionales conocedores del área técnica específica. Sin embargo, las actividades necesarias, para implementar GUÍAS y requerimientos de alto nivel deben ser realizadas por cada dependencia proponente para la cual los PROCEDIMIENTOS aplicarán ya que son específicos a la estructura y a la operación de la dependencia específica.

- **Revisión**. El establecimiento de un comité de evaluación de políticas proporciona un foro de amplio espectro para revisar y evaluar la viabilidad de POLÍTICAS, ESTÁNDARES, MEJORES PRÁCTICAS y GUÍAS que afectan a toda la organización. Aquí se propone que esta labor sea realizada por los comités de informática, que en principio están conformados por personas de diversas áreas organizacionales, interesadas en la seguridad informática. La responsabilidad del comité de evaluación es garantizar que las POLÍTICAS, ESTÁNDARES, MEJORES PRÁCTICAS y GUÍAS estén bien redactadas, sean comprensibles, estén coordinadas y sean viables en términos de las personas, procesos y tecnologías que afecta. Debido al volumen y el número de dependencias involucradas, es muy probable que un comité central de evaluación de políticas no pueda revisar todos los PROCEDIMIENTOS desarrollados por todas las dependencias proponentes. Sin embargo, los PROCEDIMIENTOS requieren una revisión similar y el proponente debe buscar un igual que los revise o diseñar un proceso de revisión por otras dependencias o, en último caso, solicitar una revisión por la función seguridad informática.

- **Aprobación**. La diferencia más importante entre las responsabilidades con las POLÍTICAS, con los ESTÁNDARES, con las MEJORES PRÁCTICAS o con las GUÍAS, es el nivel de aprobación requerido para cada uno y el alcance de su implementación. Las POLÍTICAS de seguridad que afectan toda la organización deben ser firmadas por el rector general (o el vicerrector general) para garantizar el nivel necesario de énfasis y visibilidad a estas (quizá el tipo más importante de políticas). Ya que los ESTÁNDARES, las MEJORES PRÁCTICAS y las GUÍAS son diseñadas para cumplir una política específica, estos deben ser aprobados con la firma de un directivo subordinado del rector general (o el vicerrector general), quien tendrá la responsabilidad de implementar la política. El director

de informática, normalmente, será el responsable de aprobar este tipo de políticas. Igualmente, los PROCEDIMIENTOS de seguridad deben ser aprobados por la directiva que tiene la responsabilidad administrativa directa de la dependencia para la cual aplican dichos procedimientos.

- **Comunicación**. Ya que la secretaría (general o de sede) o UNIMEDIOS cuentan con la infraestructura y la experiencia, deberían asumir la responsabilidad de la etapa de comunicación de las políticas que aplican a toda la universidad. Cuando sea una política que no cubra toda la universidad, el proponente debe asumir la responsabilidad de comunicar los procedimientos de seguridad, pero hasta donde sea posible debe buscar el apoyo de la secretaría o de UNIMEDIOS.

- **Cumplimiento**. Los mandos medios y empleados para quienes las políticas de seguridad son aplicables son los principales jugadores en la implementación y garantía inicial del cumplimiento de políticas que hayan sido publicadas recientemente. En el caso de las POLÍTICAS, ESTÁNDARES, MEJORES PRÁCTICAS y GUÍAS que afectan a toda la universidad, esta responsabilidad se extiende a todos los funcionarios con responsabilidades de supervisión, empleados, docentes y estudiantes a quien aplique. En relación con los PROCEDIMIENTOS de seguridad, esta responsabilidad estará limitada a los jefes y a los empleados de la dependencia donde apliquen los procedimientos

- **Excepciones**. En todos los niveles de una organización, habrá situaciones potenciales que impedirán el cumplimiento total de una política. Es importante que el proponente de la política o un individuo o grupo con una autoridad igual o superior revise las excepciones. El comité de evaluación de políticas puede ser efectivo en investigar las solicitudes de excepciones recibidas de las dependencias que no pueden cumplir con POLÍTICAS, ESTÁNDARES, Y MEJORES PRÁCTICAS. Ya que las GUÍAS son, por definición, recomendaciones o sugerencias y no son obligatorias, solicitudes formales de excepción en su aplicación no son necesarias (aunque es recomendable que existan argumentos documentados y aprobados para no seguirlas). En el caso de los PROCEDIMIENTOS de seguridad, el directivo que aprobó el procedimiento debe también servir como autoridad para aprobar las excepciones relacionadas.

- **Concienciación**. Para la mayoría de organizaciones, la función de seguridad informática está idealmente ubicada para administrar la etapa de concienciación en seguridad y debe por tanto tener la responsabilidad de esta etapa en el caso de las POLÍTICAS, ESTÁNDARES, MEJORES PRÁCTICAS Y GUÍAS que afectan a toda la universidad. Sin embargo, el equipo de seguridad informática debe realizar esta etapa en coordinación con el departamento de capacitación de la organización (Dirección Nacional de Personal u Oficina de Personal de sede) para garantizar unidad en el esfuerzo y en el óptimo uso de los recursos. El directivo o jefe de dependencia proponente de los PROCEDIMIENTOS debe responsabilizarse para concienciar los empleados de los procedimientos de seguridad que están a su cargo. Dentro de lo posible, esto debe ser realizado con el consejo y la asistencia de la función de seguridad informática.

- **Monitoreo**. La responsabilidad para monitorear el cumplimiento de las POLÍTICAS, ESTÁNDARES, MEJORES PRÁCTICAS y GUÍAS que son aplicables a toda la organización es compartida entre los docentes, estudiantes, empleados, directivos, decanos, jefes de dependencia (oficina, división o sección), la función de auditoria (control interno) y la función de seguridad informática. Cada empleado que esta sujeto a los requerimientos de seguridad debe ayudar en el monitoreo del cumplimiento reportando las desviaciones que

observe. Aunque no deberían estar involucrados en la garantía de cumplimiento de las políticas, la función seguridad informática y la función auditoria (control interno) pueden jugar un importante papel en el cumplimiento del monitoreo. Incluye el cumplimiento del monitoreo de PROCEDIMIENTOS propios de dependencias mediante reportes de las contravenciones dirigidos al proponente con el fin de que se adelante la acción apropiada.

- **Garantía de cumplimiento**. La responsabilidad de garantizar el cumplimiento de los requerimientos de seguridad está en los funcionarios con responsabilidades de supervisión sobre los docentes, estudiantes y empleados afectados por la política. Por supuesto, esto no aplica para las GUÍAS, que por diseño no son obligatorias. Los jefes responsables de las dependencias en las cuales aplican los PROCEDIMIENTOS de seguridad son los garantes de su cumplimiento. La regla general es que cada persona que tenga autoridad para supervisar otras personas debe ser el funcionario que garantice el cumplimiento de la política de seguridad. Por tanto, en ningún caso la función de seguridad informática ni la función de auditoria debe asignársele autoridad "en lugar de" o "en adición a" el jefe. Aunque la función de seguridad informática no debe estar involucrada directamente en las acciones de garantía de cumplimiento, es importante que esté enterada, para reportar las acciones correctivas de tal forma que esta información pueda ser integrada en los esfuerzos de la etapa de concienciación.

- **Mantenimiento**. Debido a su responsabilidad en el programa de seguridad informática de la organización, la función seguridad informática es la que mejor está posicionada para dar manteniendo a las POLÍTICAS, ESTÁNDARES, MEJORES PRÁCTICAS Y GUÍAS que tengan aplicabilidad en toda la organización para garantizar que estén actualizadas y disponibles a todos los afectados. En los niveles inferiores de la organización, la dependencia proponente, como dueña de los PROCEDIMIENTOS de seguridad, debe realizar el mantenimiento de los procedimientos que ellos desarrollaron.

- **Retiro**. Cuando una POLITICA, ESTÁNDAR, MEJOR PRÁCTICA o GUÍA no se necesita más, debe ser retirada. El proponente del requerimiento debe tener la responsabilidad de retirarlo. Normalmente el equipo de seguridad informática realizará esta función con las políticas de seguridad que afectan toda la organización, en tanto la dependencia que es la dueña de los PROCEDIMIENTOS de seguridad debe tener la responsabilidad de retirar el procedimiento.

REFERENCIAS

Fites, Philip and Martin P.J. Kratz. *Information Systems Security: A Practitioner's Reference,* London: International Thomson Computer Press, 1996.
Hutt, Arthur E., Seymour Bosworth, and Douglas B. Hoyt. *Computer Security Handbook, 3rd ed.,* John Wiley & Sons, New York, 1995.
National Institute of Standards and Technology, *An Introduction to Computer Security: The NIST Handbook* , Special Publication 800-12, October 1995.
Peltier, Thomas R., *Information Security Policies and Procedures: A Practitioner's Reference*, Auerbach Publications, New York, 1999.
Tudor, Jan Killmeyer, *Information Security Architecture: An Integrated Approach to Security in the Organization,*Auerbach Publications, New York, 2001.

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.