Vulnerando la política de seguridad de la información por diversión y dinero

Uno de los componentes principales dentro de una estrategia de seguridad de la información en una organización es la Política de Seguridad. Este es un documento administrativo de alto nivel y de carácter obligatorio, en el cual se establecen los objetivos estratégicos y principios de seguridad de la información que deben ser seguidos en cualquier actividad que afecte el entorno de la organización y en donde se definen las responsabilidades y roles para todos los actores involucrados. Haciendo una comparación retórica, una política de seguridad de la información es a una organización lo que sería la constitución (o Carta Magna) para un país.

Sin embargo—y al igual que los activos físicos y lógicos—los componentes documentales y administrativos de una organización también tienen vulnerabilidades que pueden ser aprovechadas para impactar la seguridad y la operación. Lamentablemente, este tipo de vulnerabilidades no son tenidas en cuenta dentro de un análisis de riesgos "tradicional", dejando a la organización expuesta a potenciales ataques, como es el caso de una "huelga de celo", tal como se describirá a continuación.

La "huelga de celo" en el contexto sindical

Una "huelga de celo" o "trabajo a reglamento", es un tipo particular de huelga en la cual los trabajadores aprovechan los errores de contextualización y detalle de un procedimiento, aplicándolo de forma estricta, minuciosa y extremadamente al pie de la letra en su operación normal, causando demoras y alteraciones en la productividad de la organización. A diferencia de las huelgas tradicionales que implican una cesación temporal explícita del trabajo, en una "huelga de celo" las tareas asignadas al trabajador no son interrumpidas ni se incumplen las reglas fijadas, razón por la cual suelen ser más eficaces y más difíciles de contener y corregir. Muchas veces estas huelgas son desarrolladas de forma encubierta y sumamente organizada, dejando a la dirección sin herramientas para gestionar su impacto.

Uno de los sectores que más implementan este tipo de huelgas es el sector sanitario[1]. En ese ámbito, los procedimientos de higiene, manipulación de enfermos, muestras y medicamentos deben ser muy detallados para garantizar la idoneidad y seguridad tanto del paciente como del personal médico. Sin embargo, si estos protocolos no son redactados de forma específica y ajustada al entorno médico en el cual se aplican y no se contemplan las posibles excepciones, su implementación estricta puede dar paso a tardanzas injustificadas en la atención y a burocracia abusiva, poniendo en riesgo inclusive la vida humana. Aprovechando esa presión, los trabajadores en huelga pueden exigir el cumplimiento de sus peticiones. Adicionalmente, si la administración busca las potenciales causas de la huelga, se puede encontrar que el origen fue su misma incapacidad en la redacción de las normativas y sería contraproducente pedirle a los trabajadores que incumplan los procedimientos

David Eduardo Acosta R. CISA, CRISC, CISM, BS25999 LA, CCNA Security, CEH, CHFI Trainer, CISSP Instructor, PCI QSA, OPST
Es un consultor en seguridad de la información. Él pertenece al cuerpo de Oficiales Profesionales de Reserva del Ejército Nacional de Colombia como Teniente. Trabaja actualmente con Internet Security Auditors en Barcelona (España) y es el editor principal de PCI Hispano (www.pcihispano.com), portal especializado en los estándares del PCI SSC en español. Es miembro activo de IEEE. Puede ser contactado en dacosta@ieee.org.

fijados inicialmente, teniendo que asumir en su totalidad el impacto causado en la operación y quedando sin herramientas para aplicar acciones correctivas frente al personal que ha tomado parte en la huelga.

Vulnerando una política de seguridad de la información a través de una "huelga de celo"

Siguiendo el mismo concepto descrito anteriormente, vulnerar una política de seguridad de la información mal redactada puede ser bastante sencillo. Si tenemos en cuenta que la gran mayoría de estos documentos suelen estar basados en plantillas genéricas, son pocas veces revisados, no se ajustan a la realidad del negocio de la organización ni al estado actual del entorno informático y por lo general no incluyen procedimientos para la gestión de excepciones, el hecho de seguir estrictamente de tipo de normativas puede dar lugar a demoras en la operación y/o afectación a la integridad, confidencialidad o disponibilidad de la información. Adicionando el factor de obligatoriedad de cumplimiento por parte del personal involucrado, dichos fallos pueden ser amplificados mediante una "huelga de celo", causando una pérdida de productividad de la actividad empresarial, con sus consecuentes impactos tanto económicos como operativos (afectando acuerdos de nivel de servicio [ANS], por ejemplo).

Adicionalmente, una política de seguridad de la información se soporta y complementa con documentos subalternos más focalizados a áreas/tópicos específicos, siendo clasificados de mayor a menor de acuerdo con el grado de obligatoriedad de cumplimiento. Es así como se encuentran las normas, los estándares, los procedimientos, las instrucciones técnicas, las guías, las recomendaciones, etc. La aplicación de una "huelga de celo" también sería posible en cualquiera de estos otros componentes del cuerpo normativo de la organización.

Algunos ejemplos ilustrativos de una "huelga de celo" sobre una política de seguridad de la información o de un documento subalterno vulnerable serían los siguientes:

- La política de seguridad de la información de una empresa obliga a que "todos los sistemas operativos susceptibles a malware tengan instalada una solución antivirus actualizada y en ejecución". Sin embargo, esta organización tiene dentro de su parque de ordenadores una serie de estaciones con hardware limitado que son usados como terminales de puntos de venta (TPV). Una "huelga de celo" se podría implementar en la instalación forzada de un antivirus sobre estas estaciones, con el consecuente impacto en el desempeño y la disponibilidad de las mismas, penalizando los tiempos de respuesta a clientes y la operación normal, así como la recepción de transacciones y las ventas diarias.
- La política de seguridad de la información indica la obligatoriedad en la aplicación de las actualizaciones de seguridad dentro del primer mes posterior a la publicación por parte del fabricante. La "huelga de celo" podría presentarse en la actualización de componentes críticos sin la debida planificación solamente para cubrir los plazos temporales indicados, pudiendo afectar la disponibilidad de los servicios de la empresa.
- En la gestión de contraseñas, la política indica que "el cambio de una contraseña en el caso de olvido se debe aplicar validando la identidad del usuario físicamente". Si el usuario no se encuentra en la ciudad o el país, el administrador encargado del cambio puede aplicar una "huelga de celo" en la implementación de este control, afectando los accesos de los usuarios.

Ejemplos adicionales se podrían encontrar en la implementación de políticas de gestión de cambios, gestión de usuarios, etc. en donde muchas veces las etapas de solicitud, aprobación e implementación suelen ser muy estrictas y se puede aprovechar la burocracia implícita dentro del procedimiento en la "huelga de celo", causando impacto en la operación normal de la empresa.

Lamentablemente—y al igual que en una "huelga de celo" normal—la organización afectada por este problema no se puede contradecir obligando al trabajador a que desobedezca los controles de la política de seguridad, ya que esto implicaría quitarle validez a la normativa y dejar a la empresa a merced del caos procedimental.

Cinco premisas básicas para blindar una política de seguridad contra un ataque de "huelga de celo"

Como se habrá podido concluir de las descripciones anteriores, las vulnerabilidades explotadas por la "huelga de celo" suelen estar relacionadas con errores en la redacción, problemas con la gestión de excepciones, desactualización y en el diseño de una política de seguridad o de sus documentos subalternos de forma desalineada con la realidad de la empresa e improcedentes en términos operativos. Este tipo de errores suelen tener su origen en la creencia que la documentación de seguridad solamente sirve para abultar los trámites burocráticos y que no será leída por nadie, fallos muy comunes en desarrolladores, operadores, administradores de sistemas y algunos responsables de seguridad despistados.

Para prevenir este riesgo, a continuación se enumeran una serie de premisas a tener en cuenta en el momento de la creación e implementación de una política de seguridad:

1. **Ejecute de forma periódica pruebas con escenarios hipotéticos para identificar fallos en la política que puedan ser aprovechados por usuarios malintencionados.** Con el fin de detectar debilidades en el cuerpo normativo antes de que puedan ser aprovechadas por empleados maliciosos, se puede hacer uso de ejercicios de aplicación de la política de seguridad de la información en situaciones simuladas en donde los participantes—personal de áreas clave dentro de la empresa por ejemplo (ej., legal, recursos humanos, relaciones públicas, seguridad física, continuidad del negocio)—puedan interactuar entre sí bajo un escenario hipotético. Este tipo de ejercicios son muy comunes en los planes de respuesta a incidentes y de continuidad del negocio, cuya metodología de pruebas puede ser también extrapolada a la política de seguridad de la información.

   Para detectar problemas que puedan ser explotados por una "huelga de celo", se debe examinar una situación de aplicación de la política de seguridad (enunciado del simulacro) y seguir paso-a-paso las instrucciones descritas en el cuerpo normativo. Si se detectan tareas o directivas que puedan penalizar la operación normal o se identifican casos de posibles excepciones, revisarlas en detalle y aplicar los criterios descritos a continuación.

2. **Analice el contexto de seguridad de la información de la organización e intente equilibrar los controles de seguridad con la operación.** La política de seguridad debe estar diseñada para adaptarse al entorno que protege y no al contrario. Es por esta razón que se requiere conocer previamente y en detalle la necesidad de protección de la información y el entorno cultural en el que la organización trabaja con el fin de redactar procedimientos que contengan las siguientes características:

- **Lógico**—Los procedimientos deben ser lo más naturales posibles y alineados con la operación actual de la organización. Igualmente, deben cumplir con los criterios de coste/beneficio con base en las potenciales amenazas existentes. El implementar controles desalineados a la realidad de la empresa puede dar pie a controles sub-dimensionados o sobredimensionados que pueden desgastar sin necesidad a la organización. En este punto, muchas veces pueden servir como referencia la revisión de experiencias de otras organizaciones (benchmarking).
- **Preciso**—La política debe ser redactada de forma—que plasme con exactitud las necesidades de seguridad de la empresa y se focalice en ese punto en particular. Cualquier desviación puede ser la puerta para una potencial vulnerabilidad. La modularización puede convertirse en un elemento importante en este punto.
- **Conciso**—La redacción de la política debe ser realizada empleando las palabras estrictamente indispensables para declarar la idea. Se debe evitar el uso de palabras poco usuales, superfluas, demasiado técnicas o de relleno que puedan difuminar el concepto y permitir ambigüedades y malos entendidos. La brevedad es indispensable.
- **Oportuno**—La política debe estar actualizada en todo momento y describir el momento actual y las necesidades del entorno al que aplica. El desajuste entre los cambios y los controles puede dar como resultado una degradación del nivel de seguridad, permitiendo vulnerabilidades en la implementación de contramedidas y salvaguardas.
- **Claro**—En la redacción de la política se debe tener presente al público objetivo: los usuarios. Cualquier persona que lea el documento debe ser capaz de entenderlo sin necesidad de recurrir a referencias externas. Esto implica la minimización de términos técnicos a los estrictamente necesarios y al uso de lenguaje sencillo.
- **Completo**—La política de seguridad debe cumplir con la máxima de las cinco Ws (y una H)[2]:
  – Who? (¿Quién?)
  – What? (¿Qué?)
  – Where? (¿Dónde?)
  – When? (¿Cuándo?)
  – Why? (¿Por qué?)
  – How? (¿Cómo?)

  La ausencia de cualquiera de estos elementos en un control puede indicar que se trata de un control innecesario que se puede obviar ya que no contiene una justificación práctica.
- **Objetivo**—Finalmente, la política debe ser redactada en tercera persona, eliminando cualquier factor subjetivo que pueda indicar que la elección de un control se realizó por favoritismos o por preferencias de un individuo, una tecnología o área en particular.

  Al finalizar la tarea de redacción de la política (o en el momento de su revisión/re-evaluación), sus controles deben ser pasados por los anteriores filtros con el objetivo de identificar elementos innecesarios o vulnerables.

3. **Establezca controles compensatorios y medidas de excepción.** La flexibilidad de adaptación a los cambios inevitables en la tecnología y a las nuevas amenazas debe ser un factor clave en la política de seguridad para garantizar su vigencia y subsistencia. Adicional a los controles directivos (dentro de los cuales se encuentra la propia política), disuasivos, preventivos, detectivos, correctivos y de recuperación que conforman el arsenal básico de protección, se deben incluir los controles compensatorios. Un control compensatorio se define como un control alternativo que se puede implementar cuando existe una

limitación administrativa o técnica justificada (excepción) que no permita el uso de un control establecido inicialmente. Este tipo de controles se caracterizan por proporcionar un nivel de seguridad igual o superior al control original.

Por otro lado, es imprescindible el establecimiento de medidas extraordinarias en el caso de emergencias. Estas medidas se conocen como "medidas de excepción" y le permiten a la política adaptarse a situaciones imprevistas, sirviendo como contramedida en el caso de fallo de un control o respuesta a actuaciones imprevistas, como en el caso de una "huelga de celo".

4. **Defina mecanismos de comunicación para obtener retroalimentación por parte de los usuarios de la política.** La definición de canales de comunicación bidireccional le permitirá a la dirección obtener información de primera mano de los usuarios de la política para así adaptarla con base en las experiencias provenientes de la operación del día a día. Los formularios de contacto, los buzones de sugerencias, los chats online u otras herramientas de redes sociales pueden convertirse en canales válidos para la obtención de esta retroalimentación que permitirá la detección temprana de errores y su corrección proactiva.

   El uso de incentivos puede ser implementado como herramienta de persuasión para que el personal se involucre en este tipo de iniciativas.

5. **Establezca cronogramas de revisión periódica de la política de seguridad y actualizaciones cuando se presenten cambios significativos en el entorno.** La responsabilidad en la revisión de los documentos, los umbrales temporales y los escenarios que activen estas revisiones se deben dejar establecidos dentro de la propia política, incluyendo cambios de tecnologías, ingreso o retiro de terceros, delegación de tareas en empresas externas (outsourcing), adquisiciones/fusiones, etc. que sean catalogados como cambios significativos del entorno.

   Adicionalmente, es indispensable que el responsable de seguridad mantenga alineados los controles de la política de seguridad con las amenazas del entorno. De esta manera se garantiza que la aplicabilidad de este documento es válida y alineada con la realidad de la empresa, evitando controles obsoletos o innecesarios.

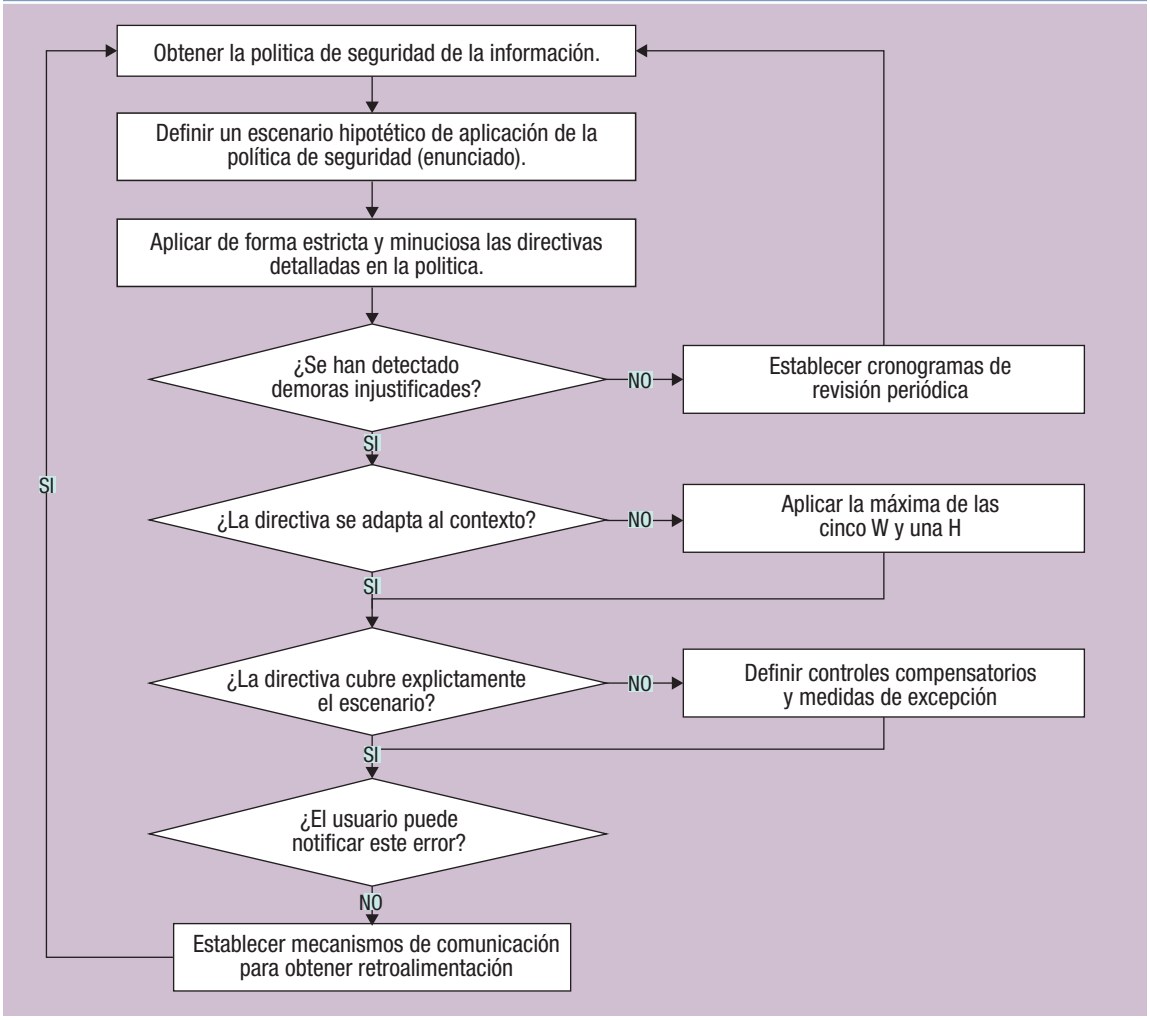
   En términos generales, el flujo de validación quedaría de la siguiente manera (**figura 1**):

Conclusión

Con base en la información gestionada por la organización, en la política de seguridad se deben definir los requisitos y controles para la protección de los diferentes activos de acuerdo con su criticidad. Y es precisamente en ese punto en el cual la redacción de una política es un factor clave, ya que dependiendo de la forma como se expresen dichos controles puede tener fallos por ser "demasiado laxa" o "demasiado restrictiva". Dichas vulnerabilidades pueden ser objetivo de burocracia abusiva por parte de personal malicioso a través de una "huelga de celo", en donde se sigue de forma estricta lo descrito en los procedimientos. Si la política no está actualizada, no está alineada con la realidad operativa de la organización y no permite la gestión de excepciones, el impacto de este tipo de huelgas o acciones de sabotaje puede tener graves efectos en la gestión de la seguridad de la información en la empresa.

Para evitar y gestionar este problema es necesaria la aplicación metodológica de canales de comunicación bidireccional con el personal involucrado, la realización de pruebas periódicas en busca de potenciales incongruencias en el documento, la revisión recurrente del cuerpo normativo, el uso de controles compensatorios y medidas de excepción y el análisis continuo del contexto organizacional y la definición coste/beneficio de controles, tareas que en conjunto permitirán que la política no se convierta en un documento obsoleto y anticuado que tarde o temprano se transforme en una amenaza para la propia empresa.

Figura 1—Diagrama de flujo para evitar una "huelga de celo" en la política de seguridad de la información



Source: David Eduardo Acosta R. Reprinted with permission.

Referencias

1 ABC España; "Los enfermeros convocan una huelga de celo por el decreto que les impide prescribir medicamentos", 22 de octubre de 2015, *www.abc.es/sociedad/abci-enfermeros-convocan-huelga-celo-decreto-impide-prescribir-medicamentos-201510281549_noticia.html*

2 Spencer-Thomas, Owen; "Writing a Press Release", 20 de marzo de 2012, *www.owenspencer-thomas.com/journalism/media-tips/writing-a-press-release*

3 Williams, B.; "The Art of the Compensating Control" marzo de 2009, *https://www.brandenwilliams.com/brwpubs/TheArtoftheCompensatingControl.pdf*