¿Por qué más es menos?: la paradoja de la insatisfacción en riesgos

La teoría de la homeóstasis del riesgo (RHT) nos recuerda la importancia del factor subjetivo del individuo en el proceso de toma de riesgos en sus actividades diarias. La comparación recurrente de los umbrales de actuación frente al riesgo y los beneficios o problemas que esto pueda acarrear, permiten modificar el comportamiento conductual hacia una tendencia arriesgada o precavida. Dependiendo de estos valores, el ingreso de nuevos controles orientados a minimizar el riesgo podrían ser anulados en el tiempo debido a la *confianza* que dicho control agrega a la ecuación, abriendo la puerta a actitudes arriesgadas que inicialmente no se tomarían.

David E. Acosta Rodríguez

Si usted es el responsable de seguridad de la información en una empresa, responsable de riesgos informáticos, administrador de tecnologías de seguridad o el responsable financiero, es posible que escenarios frustrantes como los siguientes le sean familiares:

• En el marco de un proyecto de mejora de la seguridad de la información en una organización, se implementa una solución de seguridad perimetral consistente en un cortafuegos y un sistema de detección de intrusos (IDS). Sin embargo, los intentos de acceso no autorizado, virus y explotación de vulnerabilidades no disminuyen. Debido a ello, el ROSI (retorno de inversión en seguridad de la información) estimado al principio del proyecto nunca se llegó a obtener…

• En una situación similar, una solución de antivirus se ha implementado en otra empresa. Como parte del análisis de desempeño de dicha solución en el corto plazo, se observa que los vectores de infección han cambiado y se registran en ubicaciones en las cuales antes no se habían presentado o se suponía que ya estaban controladas, obteniendo como resultado que el número total de infecciones mensuales se ha incrementado, contrariamente a lo esperado…

• Posterior a la revisión del plan de recuperación de desastres (Disaster Recovery Plan - DRP) se estableció un tiempo objetivo de recuperación (Recovery Time Objective - RTO) menor que el anterior, debido al ingreso de nuevos controles que garantizarían una disponibilidad mayor. Sin embargo, posterior a la prueba anual de dicho DRP se observa que los tiempos no concuerdan con lo planificado y que al contrario, no se nota el resultado de la inversión de los controles adicionales…

Lo que el sentido común nos indicaría es que con la implementación de nuevos controles el riesgo debería disminuir. Pero en algunos entornos se observa un comportamiento paradójico en la cual el ingreso de nuevos controles puede no tener los resultados esperados en el sistema base, e incluso llegar a aumentar el riesgo inicial, lo cual nos dirige a una pregunta sin salida: ¿hasta qué punto podemos llegar en inversión e implementación de controles para reducir el riesgo en la organización de forma satisfactoria sin tener una decepción al final?

La teoría de la homeóstasis del riesgo: una descripción inicial

La teoría de la homeóstasis del riesgo (*Risk Homeostasis Theory* (RHT) fue descrita por el profesor Gerald J.S. Wilde en su libro "*Target Risk: Dealing with the danger of death, disease and damage in everyday decisions*" [1] (primera edición publicada en 1994 y segunda edición en 2001). En dicho libro, se tomaban las bases del concepto de "compensación del riesgo" (*risk compensation*) [2] y a través de múltiples ejemplos y comparaciones se llegaba a la conclusión de que los individuos –de forma inconsciente, subjetiva y particular– definen unos "niveles de riesgo" que están dispuestos a asumir en cualquier actividad en su vida. En función de los controles de seguridad implementados, el comportamiento ante ese riesgo puede variar, permitiendo al individuo "confiar" en dichos controles y permitirse tomar riesgos que previos a la implementación de dichos controles no tomaría. Es precisamente este concepto del cual toma su nombre la teoría: "Homeóstasis" o la característica de un sistema que le permite modificar su ambiente interno para mantener una condición estable y constante con base en unos umbrales previamente definidos que darán paso a una regulación conductual. Estos umbrales –desde la perspectiva del riesgo– son:

• **Riesgo cero (R_0):** es un estado mental ideal en el cual el individuo no identifica ningún riesgo asociado a la situación a la cual se enfrenta, permitiéndose tomar cualquier acción sin ninguna restricción.

• **Riesgo percibido (R_P):** en el cual el individuo de forma subjetiva analiza las variables de riesgo en su entorno y define un "punto actual de riesgo". Este riesgo estimado es determinado por las experiencias anteriores del individuo ante la situación que se le presenta, el cálculo de potencial perjuicio, los controles presentes en el entorno y el grado de confianza que se tenga para comportarse de forma óptima ante la situación de riesgo. Con el tiempo, esta variable tenderá a R_0.

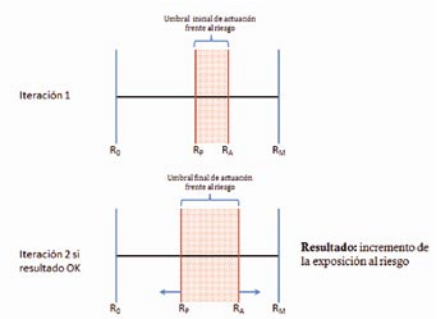
• **Riesgo máximo (R_M):** en el cual el individuo calcula el impacto máximo del riesgo en el escenario más pesimista.

• **Riesgo aceptado (R_A):** Comparando el riesgo percibido (R_P), el riesgo cero (R_0) y el riesgo máximo (R_M), el individuo procede a definir de forma subjetiva (en función de ventajas y desventajas) el nivel de riesgo que asumirá en la acción que realizará. También se denomina "riesgo objetivo". Con el tiempo, esta variable tenderá a R_M.

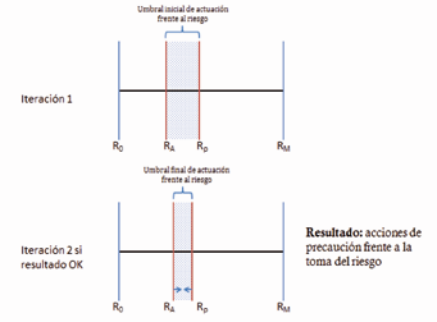
De estas actuaciones se puede concluir que la actividad de análisis de riesgos cuenta con un elevado número de componentes subjetivos y psicológicos, lo cual hace que el riesgo percibido (R_P) y el riesgo aceptado (R_A) varíe de un individuo a otro.

La actitud frente a dichos niveles es la siguiente:

– Cuando el individuo concluye que el nivel de riesgo percibido es menor que el riesgo aceptado, hay un umbral de riesgo adicional que el individuo puede "asumir" y "arriesgarse". En la siguiente actuación, si la respuesta fue satisfactoria el individuo minimizará el valor del riesgo percibido (por la experiencia) y maximizará el riesgo aceptado ampliando el margen de maniobra hasta que la respuesta sea errónea, en cuyo caso estabilizará R_P y R_A. Esta actuación se podría catalogar como "*riesgosa*".



– Cuando el individuo concluye que el nivel de riesgo percibido es mayor que el riesgo aceptado, la actitud cambia agregando mayores precauciones. Si el resultado de la actuación es satisfactorio, en una próxima acción se tratará de reducir la diferencia entre el riesgo percibido (R_P) y riesgo aceptado (R_A) hasta que la respuesta sea errónea, en cuyo caso estabilizarán los valores de R_P y R_A. Esta actuación se podría catalogar como "*precavida*".



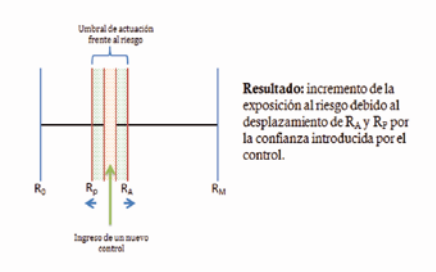
Estas decisiones se repiten de forma indefinida permitiendo ajustar las acciones al escenario en el cual el individuo se encuentre. El objetivo detrás de todo este comportamiento cíclico es encontrar unos valores fijos de R_P y R_A que se ajusten a las necesidades del individuo, para definir un patrón estable de riesgo en el tiempo.

Es de anotar que para que el sistema sea dinámico siempre debe existir un umbral de actuación (diferencial) entre R_P y R_A dado que todas las acciones tendrán un riesgo tácito. Cuando R_P y R_A son iguales, el individuo no tomará ninguna acción que le conlleve riesgo, optando por no hacer nada (lo cual es improductivo y va en contradicción a las actuaciones naturales).

Este comportamiento de regularización lo podemos simular con un sistema de control básico en el que con cada nueva salida tendremos una retroalimentación, que nos permitirá monitorizar los umbrales definidos en la nueva entrada con el fin de reducir las probabilidades de fallos y obtener los resultados buscados. En términos teóricos, el esquema presentado funciona sin problemas ante una entrada continua y homogénea. Pero, ¿qué sucede al insertar un nuevo control? La respuesta es que los controles nuevos agregarán una capa de "confianza" al sistema, lo cual se verá reflejado en un desplazamiento en partes iguales de R_P a R_0 y de R_A a R_M ampliando el diferencial del umbral de actuación, lo cual le facilitará al individuo tomar riesgos adicionales que antes no asumiría.

Táctica	Aplicabilidad en seguridad de la información
Táctica A: Incrementar el beneficio percibido de conductas cautelosas	Creación de objetivos de seguridad global y premiación a la superación de dichos objetivos, bonos económicos o prestaciones por lograr certificaciones, participación en formación o cumplimiento de estándares, mejores puntajes en formación en seguridad, proactividad en seguridad, soporte a compañeros, etc.
Táctica B: Reducir el coste percibido de conductas cautelosas	Implementación de herramientas de seguridad que no penalicen el desempeño general del empleado y que se adapten al flujo operativo normal e integración de la seguridad en las labores del día a día y la cultura de la organización, con lo cual se verá una optimización en tiempos de respuesta en atención de incidentes, maximización de la disponibilidad, menor soporte en atención de problemas y aplicación de criterios de autodefensa en seguridad de la información mediante las herramientas y formación proporcionada por la empresa debido a que la seguridad se convierte en una acción "normal" y no en una "carga".
Táctica C: Incrementar el coste percibido de comportamientos riesgosos	Alertas y reporte de actuaciones riesgosas identificadas a usuarios y administradores, llamados de atención por parte de RRHH, etc.
Táctica D: Reducir el beneficio percibido de comportamientos riesgosos	Asistencia a formaciones de seguridad adicionales, pérdida de bonificaciones, etc.

Tabla 1

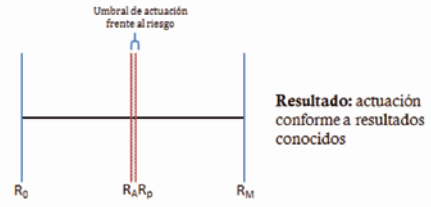


En iteraciones posteriores, nuevamente se empezará con la búsqueda de valores estáticos de R_P y R_A. Si se permite que dichos valores de referencia regresen a sus valores originales, paulatinamente se irá anulando de forma parcial o total la mejora introducida.

Incorporando la RHT en la solución de la paradoja

Dentro de la naturaleza de los sistemas es imposible frenar el cambio en el estado de las cosas y de los niveles de riesgo subjetivos definidos, dado que cualquier actuación comprende en cierta medida "asumir un riesgo".

Realizando un análisis de las diferentes alternativas y variables dentro de los niveles de riesgo enunciados, en general se podría concluir que la actitud más beneficiosa y que menos riesgos conllevaría es aquella actitud de precaución, en la cual el riesgo percibido es siempre mayor al riesgo aceptado y cuyo diferencial entre ambas variables es mínimo.

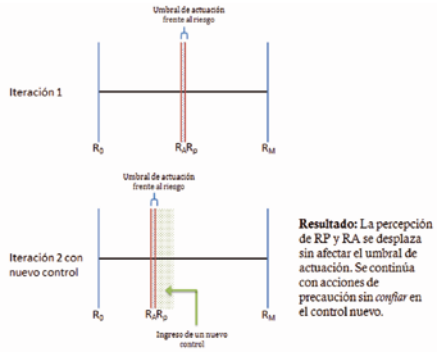


Para hacer que esta estrategia sea efectiva, el profesor Wilde presenta 4 tácticas orientadas a "manipular" los valores de riesgo estimado por el individuo:

- Táctica A: Incrementar el beneficio percibido de conductas cautelosas.
- Táctica B: Reducir el coste percibido de conductas cautelosas.
- Táctica C: Incrementar el coste percibido de comportamientos riesgosos.
- Táctica D: Reducir el beneficio percibido de comportamientos riesgosos.

Ahora bien, establecido un patrón estable de riesgo en el individuo que cumpla con las premisas anteriores, el ingreso de un nuevo control no debería modificar el diferencial establecido entre R_P y R_A. El objetivo que

se debe buscar con el ingreso de un nuevo control es *desplazar* de forma conjunta R_P y R_A hacia R_0. De esta forma, la adición de nuevos controles no supondrá riesgos adicionales ni cambios en las adaptaciones conductuales de los individuos ante las mismas situaciones.



RHT en la seguridad de la información

La teoría de la homeóstasis del riesgo es aplicable en cualquier situación en la cual exista un comportamiento ajustado a riesgos y toma de decisiones. Extrapolando dicha sentencia, su aplicabilidad se puede encontrar en cualquier comportamiento político, económico, social, de salud, etc. De hecho, las anotaciones iniciales del profesor Wilde se orientaron hacia el análisis del comportamiento en los accidentes de tráfico posterior al ingreso de controles de seguridad. De los campos nombrados anteriormente no podemos excluir la seguridad de la información, cuya relevancia en la sociedad actual cada día obtiene mayor notoriedad.

Dentro de esta área encontramos un análisis y una gestión intrínseca del riesgo, lo cual nos permite determinar qué controles se implementarán dentro del entorno para garantizar la confidencialidad, la integridad y la disponibilidad de la información y los niveles hasta los cuales la organización o el empleado están dispuestos a asumir un potencial riesgo. Tales criterios los podemos encontrar en conceptos tan diversos como los planes de continuidad del negocio, planes de recuperación de desastres, proyectos de certificación y estandarización, e implementación de controles físicos y lógicos.

Sin embargo, la misma frustración que se puede encontrar en un proyecto de implementación de controles en tránsito se puede encontrar en seguridad de la información, si los niveles de riesgo estimados y máximos del usuario y de la organización no son gestionados de forma óptima. Se puede presentar el caso de una organización que invierte recursos, tiempo y personal y en el largo plazo nunca ve su retorno de inversión en seguridad (ROSI), debido a una mala gestión de la percepción de riesgo y "confianza".

Con el fin de optimizar la gestión de riesgo en seguridad de la información incorporando los criterios revisados a lo largo de este artículo relacionados con la teoría de la homeóstasis, en la **Tabla 1** veremos algunos ejemplos de aplicabilidad de cada táctica orientado al ámbito de seguridad de la información.

Adicionalmente, el concepto de "motivación" es uno de los más relevantes para manipular los valores de riesgo estimado y riesgo máximo, teniendo en cuenta que el objetivo del programa es la modificación conductual del individuo conforme con los niveles de riesgo definidos por la empresa. Esto se logra a través de **programas de concienciación y formación** e involucra elementos psicológicos motivadores orientados a lograr que las personas se aseguren por sí mismas conforme a sus roles y responsabilidades y transmitan esta sensación de seguridad al resto del grupo (psicoprevención).

Complementando todas estas actuaciones, encontramos **la implementación de controles de forma transparente** hasta donde sea posible**,** limitando la proporción de información al individuo a los explícitamente necesarios para que él pueda optimizar su toma de riesgos. Durante la implementación de controles, es importante responder a la siguiente pregunta: ¿es necesario que los usuarios conozcan que en el entorno informático existe un sistema de seguridad en el cual "puedan confiar" o simplemente introducir el control sin interferir en las actividades diarias del usuario? Si optamos por la primera estrategia, muy probablemente el riesgo estimado del usuario cambie, lo cual puede dar pie a actuaciones riesgosas debido a excesos de confianza motivados por percepciones subestimadas del riesgo provenientes de la "seguridad" provista por el nuevo control. Si optamos por la segunda estrategia, en la cual los controles se incorporan al sistema de forma transparente, el usuario continuará con sus umbrales de riesgo exactamente iguales a los encontrados de forma previa a la implementación del control y los resultados se notarán de forma inmediata, permitiendo demostrar a la Dirección el ROSI.

Conclusión

La teoría de la homeóstasis del riesgo (RHT) nos recuerda la importancia del factor subjetivo del individuo en el proceso de toma de riesgos en sus actividades diarias. La comparación recurrente de los umbrales de actuación frente al riesgo y los beneficios o problemas que esto pueda acarrear, permiten modificar el comportamiento conductual hacia una tendencia riesgosa o precavida. Dependiendo de estos valores, el ingreso de nuevos controles orientados a minimizar el riesgo podrían ser anulados en el tiempo debido a la *confianza* que dicho control agrega a la ecuación, abriendo la puerta a actitudes riesgosas que inicialmente no se tomarían.

Incrementar el beneficio percibido de conductas cautelosas y minimizar su coste, así como incrementar el coste percibido de comportamientos riesgosos y reducir su potencial beneficio permiten controlar los umbrales de riesgo hacia acciones precavidas. Soportando esta estrategia con un programa de concienciación e implementación transparente de controles, se puede obtener un retorno de inversión (ROI) óptimo.

Debido a que estos criterios se aplican en cualquier actuación humana, el uso de las mismas tácticas y estrategias a nivel de seguridad de la información permitirá que aquellos controles para garantizar la confidencialidad, integridad y disponibilidad de la información cumplan con el cometido con el que fueron definidos bajo los criterios de aceptación de riesgo de la organización, teniendo en cuenta siempre el factor humano y evitando la tecnocracia. ■

David E. Acosta Rodríguez
Consultor Senior en Seguridad
Dpto. de Consultoría
INTERNET SECURITY AUDITORS
deacosta@isecauditors.com

Referencias

[1] Target Risk: Dealing with the danger of death, disease and damage in everyday decisions. http://psyc.queensu.ca/target/index.html. Abril 2011.

[2] Risk Compensation: http://en.wikipedia.org/wiki/Risk_compensation. Abril 2011