Seguridad de la seguridad, un método empírico

I. Rossenbach – June 2017

***Abstract* – "Security of security, an empirical methodology" is a study which aims at developing a method to help make reliable decisions in the security field. It mainly focuses on how to avoid taking certain wrong decisions when dealing with crisis or major incidents.**

***Index Terms* – Business continuity, business process management, computer security, crisis management, data security, decision making, decision theory, human factors, incidents, organizational aspects, safety management, security management.**

***Resumen* – El presente estudio tiene por objeto el desarrollo de un método de ayuda a la toma de decisiones fiables en el ámbito de la seguridad, es decir, cómo evitar tomar ciertas malas decisiones, en particular en el dominio de la gestión de crisis o de incidentes mayores.**

***Palabras claves* – Aspectos organizacionales, continuidad en las operaciones, factores humanos, gestión de crisis, gestión de la seguridad, gestión de procesos, incidentes, seguridad, seguridad informática, seguridad de los datos, toma de decisiones, teoría de la decisión**

I. INTRODUCCION

Este estudio tiene por objeto establecer un método para tomar decisiones fiables en el ámbito de la seguridad. Empezaremos por definir los conceptos y las prácticas que analizaremos, y a continuación se hará hincapié en la importancia del azar y de lo inesperado en cuestión de riesgos, ya que implican una gran dificultad o imposibilidad para establecer métodos deterministas. Por otra parte, nuestras limitaciones humanas, individuales y colectivas, generan una gran incertidumbre en la toma de decisiones. En particular, debido a factores psicológicos, emocionales, y organizacionales. Para aumentar la fiabilidad de esos procesos, una analogía resultará particularmente útil: ¿cómo pueden evitar los programadores las vulnerabilidades más peligrosas y frecuentes? Elegiremos a continuación, un campo de aplicación: la toma de decisiones en situación de crisis. En esta área, mencionaremos problemas específicos observados en una gran organización. Luego enumeramos los factores de riesgos humanos típicos que pueden incidir desfavorablemente sobre la toma de decisiones de seguridad. Para cada uno de estos factores, deduciremos las preguntas operacionales que permitirán ponerlos de manifiesto. Por último, confrontaremos estas preguntas con la lista de los problemas observados a fin de verificar su pertinencia. Y veremos en consecuencia de qué manera el método propuesto es una eficaz herramienta de ayuda para evitar la toma de malas decisiones.

II. LA SEGURIDAD

Riesgos, amenazas y seguridad son conceptos polisémicos, altamente cargados simbólicamente. Designan una multitud de conceptos específicos y diferentes. Agreguemos a esto que cada época influencia el significado de las palabras y que el siglo XXI anhela seguridad, llevando esta temática a boca de todos y de cualquier manera. Ejemplo de cacofonía conceptual y de errancias absurdas de cierto tipo de pensamiento securitario es llamar a la seguridad "primera libertad" [1]. Es fundamental nombrar correctamente las cosas de las que vamos a hablar. Esto no reducirá las penas del mundo pero al menos nos ayudará a pensar mejor.

La seguridad es una situación objetiva que se caracteriza por la existencia de riesgos pero que están dominados. Puede referirse a riesgos accidentales (consecuencia posible de acciones humanas involuntarias), o a actos malintencionados.

Los riesgos en sí son contingencias adversas que pueden ser ciertas, potenciales o futuras. Derivan de la probabilidad de que una amenaza "utilice" intencionalmente o no, una vulnerabilidad.

Si convenimos con el filósofo Spinoza [2] en que cada cosa, individuo u organización, se esfuerza por perseverar en su ser, se deduce que procurarán minimizar las contingencias adversas. Es decir, tratarán de evolucionar en el espacio y en el tiempo, en estados en los cuales puedan dominar los riesgos que las amenazan.

Lo que vemos aquí es que la seguridad, elemento esencial de la vida, es el resultado de una dinámica de dominio. Para "ser", toda cosa trata de dominar los riesgos que pesan sobre ella, ya sean endógenos o exógenos.

Hay cuatro formas de abordar un riesgo: reducirlo, aceptarlo, rechazarlo o transferirlo. La reducción del riesgo consiste en disminuir la probabilidad de que una amenaza se materialice o, si esto sucede, en reducir su impacto y consecuencias. Aceptar el riesgo es considerar que su efecto indeseado, leve o letal, es aceptable teniendo en cuenta los objetivos, metas, intereses u obligaciones de la persona u organización en cuestión. Rechazar el riesgo significa modificar lo que somos o lo que hacemos a fin de evitar vulnerabilidades. Esto equivale a no realizar una acción o a eliminar una funcionalidad. Por último, transferir el riesgo es delegarlo a un tercero, con o sin su consentimiento.

También hay que señalar que la seguridad es siempre el resultado de una dinámica, incluso cuando el sistema es perfectamente estático y que no evoluciona. Por un lado, porque las amenazas externas pueden variar, y por otro lado, porque la reacción, la reducción de los impactos de un incidente necesariamente es siempre dinámica.

De esta característica dinámica se puede concluir que la seguridad siempre es un proceso, que involucra al individuo u organización, y nunca únicamente una metodología, un sistema, una competencia o un producto.

III. LO IMPREVISTO, FACTOR CLAVE DE LA SEGURIDAD

Estas consideraciones ponen de relieve un elemento esencial y constitutivo del riesgo y de la seguridad: lo inesperado. Por definición, las contingencias adversas, es decir los riesgos, no son deterministas. Si lo son, entonces, se trata de impedimentos (y no de riesgos). Es decir que en el núcleo de cualquier acción y cualquier reflexión acerca de la seguridad reside el futuro incierto, lo desconocido, el azar, la probabilidad. Términos que hablan de nuestra incapacidad fundamental para predecir el futuro.

De esto se desprende una diferencia estructural entre un procedimiento de seguridad y cualquier otro procedimiento: no podemos enraizarnos en ningún modelo determinista. Por supuesto, hay muchas áreas en las que los peligros pueden alterar los modelos teóricos utilizados. Tomemos por ejemplo el envío de una sonda a Marte. Muchos peligros pueden hacer fracasar una misión de este tipo. Sin embargo, la construcción y el envío de una sonda utilizan modelos deterministas. Es decir que, sin considerar los errores y la falta de información, y sin tener en cuenta la seguridad, la realización puede ser perfectamente dominada. En teoría, un modelo puede establecerse y su aplicación estricta puede ser perfectamente predecible. La situación es fundamentalmente diferente respecto a la seguridad. El conocimiento de las amenazas es necesariamente parcial; la evaluación de la probabilidad de los riesgos, es en el mejor de los casos estadística, en el peor cualitativa, pero nunca es cierta; la estimación del impacto de un incidente tiene una importante dimensión imprevisible, aleatoria.

Continuando con el ejemplo de la sonda hacia Marte: sabemos fabricar la sonda, dominamos las técnicas; sabemos cómo lanzar un cohete en órbita, y enviar la sonda hacia otro planeta; sabemos calcular su movimiento en el espacio; sabemos predecir dónde caerá, y como frenar su bajada en la atmósfera marciana. Por supuesto, existen riesgos, no dominamos perfectamente todos los parámetros y la sonda suele estrellarse en el suelo marciano. Pero teníamos un modelo para hacerla llegar a salvo. Por el contrario, si uno considera la seguridad de esta sonda, la modelización es muy difícil: para protegerla de los ataques en su lugar de fabricación, no se conocen bien las amenazas (¿sabotaje por un ingeniero depresivo? ¿Terrorismo? ¿Espionaje?). Para asegurar la puesta en órbita de la sonda, sólo podemos intentar evitar lo que en el pasado ha causado accidentes; para asegurar su *amartisaje*, tenemos poca experiencia, muchas hipótesis.

Como hemos mencionado, la frontera es porosa entre riesgos e impedimentos: un riesgo bien conocido, ya sea porque se modeló eficazmente o porque tenemos suficientes datos estadísticos fiables, puede dejar de ser un riesgo y convertirse en un impedimento, en un elemento conocido que se sabe manejar.

Pero concerniendo los riesgos que cada entidad intenta dominar, teniendo en cuenta que las contingencias adversas contienen una importante dimensión de imprevisto, no existen modelos deterministas.

Por lo tanto, muchos expertos y equipos de seguridad trabajan casi a ciegas, buscando en particular evitar el síndrome del "cisne negro" (cf. la "teoría del cisne negro", una metáfora que describe un acontecimiento imprevisible de muy escasa probabilidad pero teniendo, si se produce, consecuencias excepcionales [3]).

IV. PERMITIR *VERSUS* IMPEDIR

La mayoría de las acciones humanas tienen como objetivo permitir que ciertas cosas sean posibles, crear objetos que existen o procesos que tienen resultados predecibles. Administrar la seguridad es esencialmente diferente. Consiste en crear cosas e implementar procesos dedicados a impedir que ciertas cosas ocurran (la materialización de amenazas). Y si ocurren, que tengan el

más mínimo impacto. El conjunto de las posibilidades que permiten un acontecimiento es menor que el conjunto de las posibilidades que pueden impedir un acontecimiento. La seguridad trata de este segundo espectro de posibilidades.

Esto muestra que, debido a la importancia del factor de lo imprevisto que dificulta la modelización de la seguridad, y de la mayor cantidad de posibilidades desfavorables que de posibilidades favorables, una concepción mecanicista de la seguridad (es decir un conjunto determinado de causas y consecuencias) es necesariamente limitada.

En la mayoría de los casos, las decisiones de seguridad se apoyan sobre substitutos de leve fiabilidad: el asesoramiento de expertos, de proveedores de soluciones, o la evaluación comparativa, es decir, la comparación con otras organizaciones similares.

A partir de ahí, ¿cómo aumentar la fiabilidad de las decisiones?, ¿cómo evaluar los riesgos?, ¿cómo tomar decisiones acerca de los riesgos?, ¿cómo reducir los riesgos de un sistema complejo a un costo razonable?, ¿cómo decidir si se debe reducir o evitar los riesgos? y ¿cómo organizar la reacción a la materialización de un riesgo?

V. UNA PROBLEMATICA, LA DECISION

La imposibilidad o dificultad de establecer modelos deterministas para gestionar los riesgos tiene como consecuencia que esta actividad dependa mucho de las decisiones humanas.

Pero la racionalidad del pensamiento humano y de los comportamientos colectivos es limitada y no se puede modelizar. Sin embargo, la psicología, los estudios sobre el *management* y las organizaciones, el estudio de casos de incidentes, ataques, desastres y de la manera en que los humanos han reaccionado, produjo una importante cantidad de conocimiento (problemas típicos, problemas conocidos y comportamientos problemáticos, individuales o colectivos, han sido arduamente descriptos).

Nos encontramos en una situación en la que tenemos que hacer frente a fenómenos poco o nada modelizados, usando nuestros cerebros y nuestras organizaciones cuyos funcionamientos son a menudo erráticos. En pocas palabras: a menudo cometemos muchos errores al momento de decidir y determinar acerca de la seguridad y de los riesgos.

Como parte de este estudio, nos concentraremos en una dimensión: tomar decisiones acerca de los riesgos en situación de crisis, ya sea por individuos u organizaciones.

En ausencia de modelo satisfactorio, y dada la inmensa dificultad – léase imposibilidad – de establecerlos, las analogías suelen ser el método más exitoso.

VI. UNA ANALOGIA FRUCTIFERA

En los últimos años el dominio de la informática ha visto crecer exponencialmente “aplicaciones” a las que acceden los usuarios, proveyendo servicios de tratamiento de la información. La interacción con sistemas físicos aumenta la presencia y multiplica los usos de tales aplicaciones.

Existen decenas de lenguajes de programación que permiten el desarrollo de aplicaciones, miles de configuraciones materiales, cientos de miles de personas en todo el mundo tienen las capacidades para programar. La seguridad de estas aplicaciones se ha convertido en una cuestión clave. Los resultados de tres años de *pentests* en un equipo que el suscripto dirigió, muestran que más del 60% de las vulnerabilidades que se descubren son aplicativas (en el contexto de la organización que se toma como sujeto). Existen métodos y herramientas de análisis de código que detectan errores de programación, lo que limita las posibles vulnerabilidades. Sin embargo, estos análisis de código son muy costosos y son deficientes para detectar errores funcionales (es decir, los errores de especificación).

En los primeros años del siglo nació una comunidad: *Open Web Application Security Project (OWASP)* cuyo trabajo es de libre acceso, y cuya misión es construir y proponer recomendaciones, métodos y herramientas para mejorar la seguridad de las aplicaciones web. El proyecto que ha alcanzado rápidamente un gran éxito y que es ahora una referencia es el “*OWASP Top Ten*” [4] (esta lista es referenciada por numerosas normas de seguridad, tales como *MITRE, PCI DSS, DISA, FTC,* etc.). Su objetivo es identificar y enumerar los diez riesgos más críticos para la seguridad de las aplicaciones web.

La característica especial de esta lista es que no es el resultado de “buenas prácticas” o la opinión de expertos (como las normas ISO), sino el resultado del análisis de cientos de miles de vulnerabilidades efectivamente descubiertas entre miles de clientes.

En el mismo sentido, el *Center for Internet Security* publica el *CIS Critical Security Controls for Effective Cyber Defense (CIS CSC)* [5]: una lista de veinte recomendaciones de seguridad. Si bien en este caso se trata de medidas preventivas que cubren todo el espectro de la seguridad informática, la concepción de esta lista y la priorización de sus artículos ha seguido el mismo principio: proviene de la observación de un panel de ataques reales.

En ambos casos, estas listas se materializan en *checklists*. El principio subyacente en ellas es que, dada la ausencia de modelos de seguridad deterministas, una clave para mejorar la seguridad de un sistema o de una aplicación es procurar que las vulnerabilidades más peligrosas y comunes sean evitadas.
Por analogía, intentaremos establecer una lista de errores comúnmente cometidos en la toma de decisiones, y a continuación la confrontaremos al dominio de la toma de decisiones en situación de crisis.

VII. DECIDIR EN TIEMPOS DE CRISIS

Una organización debe a veces gestionar la materialización de riesgos, es decir incidentes o crisis de seguridad. La empresa estudiada tiene procesos de gestión de crisis bien establecidos. Dependiendo de la gravedad de los incidentes, diferentes tipos de células de crisis pueden ser convocadas. Estas células tienen prioridad sobre todas las demás actividades y permiten reunir en una misma unidad espacial y temporal responsables y técnicos. Sus objetivos principales consisten en decidir acciones y medidas de salida de crisis y determinar la comunicación hacia el exterior. Las decisiones pueden tomarse rápidamente, fuera de los procedimientos estándar, para hacer frente a situaciones de emergencia. A través de los años, la organización observada también aprendió la importancia de comunicar correctamente con el fin de reducir la ansiedad de los empleados, clientes y usuarios. Sin embargo, disfuncionamientos en las gestiones de crisis son observados a menudo, sobre todo debido a la falta de experiencia (hay pocos ataques o incidentes de envergadura).

Los disfuncionamientos frecuentemente observados son:
– La organización prevista para gestionar las crisis no se aplica cuando ocurre una crisis, ello acarrea improvisaciones que retrasan el retorno a la normalidad.
– Dificultades de la jerarquía para distanciarse de las acciones técnicas, dificultades de los técnicos para despojarse de los reflejos diarios.
– Las lecciones de los incidentes están en general bien hechas, se deciden planes de acción, pero las lecciones sobre los problemas de la gestión de incidentes en sí se formalizan ocasionalmente.
– Las conclusiones de los reportes que formalizan las lecciones suelen ser diluidas al transmitirse a la alta jerarquía.
– Ciertas acciones deberían ser más discretas (como por ejemplo solicitar un servicio de seguridad para investigar sobre un caso), para no generar rumores que terminen sumándose al estrés colectivo.
– Ocurrió que se hayan decidido medidas técnicas que no tenían ninguna posibilidad de resolver los problemas (como reiniciar un servidor), sólo para que no se pueda criticar ulteriormente el hecho de no haberlo intentado.
– Ocurrió que medidas de seguridad hayan impedido reaccionar rápidamente a una crisis o incidente importante, y que no existiera alguna posibilidad de anularlas en caso de circunstancias excepcionales.
– A menudo, las células de crisis en las que participan responsables de la empresa, solicitan demasiado a los técnicos encargados de la resolución de la crisis. De esto resulta a menudo una tensión desfavorable en contra del trabajo eficiente. En algunos casos incluso, se observó una inversión de roles: las células de crisis comenzaron a ordenar acciones precisas, en lugar de elegir entre las opciones propuestas por los técnicos y los expertos.
– A veces, debido a la urgencia de una crisis o de un incidente mayor, se toman decisiones apoyándose sobre suposiciones falsas o erróneas que hubiesen sido fácilmente descalificadas (a menudo, un técnico podría haber alertado rápidamente sobre el error). Si bien es importante saber decidir sin tener toda la información necesaria, es igualmente vital poder confiar en algunas certezas.

VIII. FACTORES DE RIESGOS HUMANOS

Si nos referimos a los estudios en el dominio del *management*, de la psicología, de las organizaciones, a las descripciones documentadas de crisis e incidentes mayores, así como a la propia experiencia del autor, podemos establecer una lista de factores que pueden causar la toma de malas decisiones en el campo de la seguridad.
Es probable que esta lista pueda aplicarse a muchas otras áreas, pero nos centraremos en la seguridad.

Racionalidad limitada
Los individuos y los grupos tienen la intención de ser racionales, pero debido a sus capacidades cognitivas limitadas, lo logran parcialmente.
Para compensar esta debilidad, las organizaciones a menudo piensan racionalizar sus decisiones mediante el uso de números [6].

Sesgo de confirmación
Tendencia a favorecer la información y las ideas conocidas o aceptadas, ignorando, rechazando o desvalorizando aquellos datos que las contradicen. Buscamos confirmar nuestras ideas, en lugar de cuestionarlas [7].

Sesgo de enacción
Mediante nuestras creencias y acciones, construimos la representación de nuestro entorno. Lo "ponemos en escena" y tendemos a considerar como "real" lo que parece "funcionar" en nuestra representación del mundo ("veo lo que creo"). Pero lo que "funciona" puede ser falso o sólo parcialmente cierto [8].

Historias versus estadísticas
Preferimos la consistencia de una historia, de una narración, a la realidad de las estadísticas (subrayemos, sin embargo que no hay nada peor que estadísticas mal interpretadas) [9] [10].

Rol del azar
Somos deficientes para evaluar el rol de la casualidad en la ocurrencia de eventos.

Falsedad de los recuerdos
Nuestros recuerdos son muy a menudo falsos o reconstruidos. Nunca son objetivos y siempre son el resultado de nuestra visión del mundo, pasada y presente.

Falta de apertura respecto a la información
Los grupos humanos tienden sólo a tener en cuenta y sólo a procesar la información reconocida y aceptada por todos los miembros.

Sesgo de conformidad
Los individuos tienden a adoptar la visión percibida como dominante en el grupo [11].

Groupthink
Fenómeno de grupo mediante el cual el deseo de armonía y de conformidad perturba o quita racionalidad a los procesos de decisión. Los miembros del grupo tratan de minimizar los conflictos y llegan rápidamente a decisiones por consenso sin un análisis crítico de las alternativas, y aislándose de las influencias externas.
Condiciones que favorecen al g*roupthink*: cohesión del grupo / aislamiento del grupo / preferencia del líder para una alternativa en particular / ausencia de procedimientos formalizados / homogeneidad socio-laboral e ideológica / estrés significativo debido a presiones externas / debilitamiento de la autoestima en relación con dificultades recientes.
Efectos sobre la decisión: examen incompleto de las alternativas / examen incompleto de los objetivos / ausencia de consideración de los riesgos asociados a la opción preferida / ausencia de reevaluación de alternativas inicialmente descartadas / búsqueda de información limitada / sesgo de selección de las informaciones / ausencia de planes alternativos [12].

Falso consenso
Falta de divulgación de las divergencias dentro de un grupo. El proceso de toma de decisión es muy rápido, pero la calidad de las decisiones es mala [13].

Hubris
El narcisismo y la excesiva confianza en sí mismo conduce a una sobreestimación de las propias capacidades [14].

Sesgo de compromiso
Vínculo afectivo entre un individuo u organización y su acción, resultado de varios tipos de factores psicológicos: cálculo estratégico, obligación de justificarse ante sus propios ojos, obligación de justificarse ante los demás. El compromiso, si no se quiebra, lleva a la escalada: tendencia a continuar una acción ineficaz y / o costosa y / o demasiado arriesgada [15].

Estandarización del peligro
Situación en la que individuos u organizaciones viven riesgos inicialmente considerados demasiado importantes durante un tiempo suficiente como para convertirlos en algo común y corriente (dejando de considerarlos como excepcionales).

Órdenes contradictorias
Un individuo o grupo está en presencia de órdenes contradictorias cuando tiene que cumplir con expectativas o directivas imposibles de llevarse conjuntamente adelante. A veces ciertas obligaciones que el individuo o grupo debe cumplir son conscientes, y otras, inconscientes (por ejemplo cuando entran en juego manipulaciones de incentivos como el honor, el respeto, la amistad, la esperanza, etc.), lo cual permite obtener de estos individuos acciones que no "quieren" hacer. Ejemplos de estas directivas contradictorias: Por un lado aumentar el *reporting* y por el otro exigir autonomía; exigir reactividad y al mismo tiempo pedir anticipación; exigir el desarrollo de nuevas actividades y a su vez un control de costos; aumentar la seguridad y la libertad a la vez [16].

Soluciones preferidas
Ciertas opciones son preferidas por los individuos u organizaciones. Se trata de aquéllas que son o parecen:
– Obvias, de "sentido común" (entendido como la expresión de la ideología dominante);
– Irresistibles, a causa del *hubris*, o porque son soluciones dominantes o prometen beneficios o éxitos excepcionales;
– Prácticas, es decir, que evitan considerar otras;
– Disponibles, validadas o experimentadas por otros;
– Fáciles de justificar.

Encuadre de la situación
El encuadre de una situación es la forma que tienen los individuos de abarcar e interpretar tal situación o problema. La manera de definir el encuadre a menudo depende de cómo se plantea el problema. Puede ser influenciada por el lenguaje, las circunstancias, las prioridades, la experiencia, la plausibilidad, las creencias... Un encuadre erróneo puede impedir ver "lo que es", o hacer ver "lo que no es" (o que ya no es). También revela una tendencia a evitar el riesgo ante la posibilidad de un beneficio (oportunidad) y buscar el riesgo frente a la posibilidad de una pérdida (una amenaza).

Disfuncionamiento de los equipos
Ciertos criterios pueden advertir sobre problemas de un equipo para tomar buenas decisiones:
– Fallos en el manejo de los factores humanos;
– Falta de preparación para manejar imprevistos;
– Abundante jerarquía en los equipos;
– Relaciones de sumisión nefastas a la cohesión del equipo;
– Fallas de comunicación;
– Cultura de la culpa (reprimendas por los errores) la cual neutraliza las iniciativas e impide un sano manejo de los errores;
– Dificultades para trabajar en un entorno heterogéneo;
– Exceso de confianza.

Comunicación defectuosa
Ciertos elementos son esenciales para establecer una buena comunicación con los terceros no implicados en el proceso de decisión:
– Asegurar la cohesión del discurso;
– Enunciar los cambios, explicarlos, darles significado;
– Explicar lo que está en juego;
– Promover los beneficios;
– Contestar las preguntas y reducir la incertidumbre;
– Crear las condiciones para que cada uno se implique y estimular la participación;
– Guiar la progresión (etapas, *plannings*, futuro previsible, etc.);
– No comunicar informaciones confidenciales o que provoquen inútilmente ansiedad.

Renunciamiento ético
Los individuos pueden renunciar a formular juicios éticos y morales sobre sus acciones o sobre aquéllas que los circundan, contentándose simplemente con obedecer a instrucciones o procedimientos. En tales casos, cesan de pensar, renuncian a ello, ya que se consideran sólo como una pieza más de un engranaje, y que no tiene nada que decir (cf. el concepto de banalidad del mal de Hannah Arendt [17]). Estas renuncias a pensar por uno mismo pueden constituir factores clave para la comisión de actos inmorales.

Olvido
La falta de memoria de una organización favorece la repetición de problemas que ya se produjeron y para los cuales ya habían sido estipuladas soluciones – buenas o malas.
El olvido provoca también, a menudo, una pérdida de seguimiento de las acciones y decisiones a través del tiempo.

Errores de razonamiento
Muchos errores de apreciación o de razonamiento pueden influir negativamente en las tomas de decisiones. Ejemplos de errores muy comunes:
– Si A, entonces B. B. Entonces A;
– Ilusión de causalidad, donde sólo hay correlación;
– Generalizaciones abusivas (generalizar una observación particular sin justificación);
– Enfoque inconsciente y arbitrario sobre ciertos aspectos, descuidando los demás.

Dilución de la responsabilidad
Las decisiones colectivas, asumidas por todo el grupo, conducen a mayores asunciones de riesgos que aquéllas asumidas de manera individual [18].

IX. ADAPTACION AL DOMINIO DE ESTUDIO

El objetivo de este estudio es obtener un método operativo. Por lo tanto, conviene ahora aplicar los factores anteriormente vistos al dominio de la toma de decisiones en situación de crisis.
Por otra parte, para que esto sea eficaz, cada tema será traducido en forma de una o más preguntas. El resultado será una lista de preguntas. Esta forma parece ser la más adecuado para realizar rápidamente un análisis sin interrumpir o dificultar el proceso observado.

X. LISTA DE PREGUNTAS

Ahora vamos a tratar de deducir preguntas para cada factor de riesgo identificado.
El objetivo de estas preguntas es revelar un problema potencial.

Racionalidad limitada
¿Estamos dispuestos y preparados para decidir sin contar con todas las informaciones (lo que equivale a asumir que las decisiones no serán del todo racionales)?

¿Elegimos la primer solución satisfactoria que se presenta en lugar de buscar la solución óptima? (lo que constituiría el enfoque más racional)
¿Se observan utilizaciones abusivas de números poco fiables o de interpretación ambigua para "racionalizar" opciones?

Sesgo de confirmación
¿Se han elegido opciones porque se han considerado como obvias o de "sentido común"?
¿Se han rechazado opciones sin análisis en base a un argumento único rápidamente considerado?

Sesgo de enacción
¿Se toma en cuenta en el proceso de decisión que "lo que funciona" en situaciones normales puede no funcionar en situación de crisis?
¿Cómo se empezó y como se llegó a considerar algo como "verdad" o certeza?

Historias frente a las estadísticas
¿Es posible referirse a estadísticas fiables, pertinentes y de definición clara?

Rol del azar
¿Se tiene en cuenta la intervención de la casualidad o de lo inesperado?

Falsedad de los recuerdos
¿Son las referencias al pasado factuales y significativas (recuerdos o datos)?

Falta de apertura respecto a la información
¿Hay informaciones consideradas importantes por parte de ciertos participantes, pero no tomadas en cuenta colectivamente?

Sesgo de conformidad
¿Tuvo cada uno la oportunidad de expresar su opinión en forma independiente (eventualmente anónima)?
¿Hay alguna información que pueda ser considerada pero que es rechazada por algunos?

Groupthink
¿Ha surgido un consenso rápidamente?
¿Existieron alternativas viables descartadas demasiado rápido?
¿Es el grupo muy homogéneo (funciones, experiencia, personalidad)?
¿La jerarquía o el líder expresan una fuerte preferencia hacia ciertas opciones?

Falso consenso
¿Los participantes piden aclaraciones sobre las opiniones de los demás?
¿Los participantes dan la bienvenida a las nuevas informaciones y discuten los datos ambiguos?
¿Los participantes reformulan sus propuestas incorporando las críticas recibidas en lugar de repetir los mismos argumentos?
¿Todos los participantes son activos en la discusión?
¿Los participantes pudieron expresar libremente su opinión (voto secreto si es necesario)?

Hubris
¿Hay decisiones presentadas como "obvias"?
¿Se cuestiona de manera igual a todos los participantes, inclusive a los muy activos?
¿Se explicitan argumentos del tipo "tendremos éxito porque somos mejores que los demás"?

Sesgo de compromiso
¿Hay responsables que se involucran demasiado en los asuntos técnicos debido a sus antiguas funciones técnicas?
¿Hay algún responsable que parece demasiado involucrado emocionalmente en la gestión de crisis?

Estandarización de peligro
¿Después de un incidente de seguridad importante, es necesario modificar ciertas evaluaciones de riesgo previamente realizadas?
¿Después de la crisis, todas las *root cause* son identificadas y tratadas?

Órdenes contradictorias
Durante la gestión de la crisis, ¿hay pedidos u órdenes contradictorios (por ejemplo, exigir que los técnicos propongan soluciones y que a la vez tengan en cuenta las instrucciones técnicas de la jerarquía)?

Soluciones preferidas
¿Hay opciones para salir de la crisis que se consideran preferentemente porque parecen "obvias", "irresistibles", "prácticas", "disponibles" o "fácilmente justificables"?
¿Hay decisiones técnicas que sólo se deciden por miedo a que se critique posteriormente el no haberlas tomado?

Encuadre de la situación
¿Ha sido la descripción del contexto y de la situación de crisis objeto de un análisis contradictorio?
¿Serían las decisiones idénticas si, en vez de esperar un beneficio, se tratara de minimizar una pérdida (y a la inversa)?
¿Hay diferencias en el análisis del contexto causadas por elementos como el idioma o la cultura?

Disfuncionamiento de los equipos
¿Hay relaciones de subordinación o excesiva abundancia jerárquica nefastas para el funcionamiento de la célula de crisis?
¿Existen fallas en la comunicación interna en la célula de crisis?
¿Se observa una cultura de la culpa que pueda neutralizar las iniciativas (miedo al error)?
¿Parecen los equipos preparados para manejar lo inesperado?

Falla en las comunicaciones
Si hay comunicación de crisis (hacia el exterior), ¿se cumplen los siguientes criterios?: coherencia del discurso / explicación del cambio, darle sentido / explicar lo que está en juego / valorar los beneficios / respuesta a las preguntas y reducción de la incertidumbre / crear las condiciones para la participación y estimular la adhesión / guiar la progresión / no comunicar información confidencial o que genere innecesaria ansiedad.

Renunciamiento ético
¿Las decisiones o acciones de resolución de la crisis en la que estoy involucrado o que estoy presenciando, son éticamente legítimas?
¿Las decisiones o acciones de resolución de crisis pueden tener consecuencias éticamente inaceptables?

Olvido
¿Se ha constatado si ya han ocurrido crisis similares, y en caso positivo, cuáles han sido las decisiones adoptadas?
¿Las causas, circunstancias y acciones de resolución de la crisis o del incidente llevan a formalizar objetivamente las lecciones aprendidas?
¿Si se formalizaron las lecciones aprendidas, pero luego estas se "diluyen" a los fines de su comunicación (interna o externa), se conserva y utiliza no obstante una versión del documento que contenga todas las observaciones "en bruto"?
¿Las acciones de resolución de los problemas (*root cause*) se siguen aplicando correctamente en el transcurso del tiempo?
¿Se efectúa un balance y formalización de las lecciones aprendidas específicamente acerca de cómo la organización ha manejado la crisis o el incidente (para mejorar la gestión de crisis / incidentes)?

Errores de razonamiento
¿Hay errores lógicos básicos en el razonamiento?

Dilución de responsabilidad
¿Aquéllos que asumen los riesgos residuales son identificados personalmente (por su nombre individual y no por el de un comité o servicio)?

XI. SIMULACION DE APLICACION

Para comprobar la relevancia de nuestras preguntas, vamos a plantearlas frente a los problemas anteriormente identificados en el dominio de la toma de decisiones en situaciones de crisis.

El objetivo es determinar si nuestras preguntas permiten identificar la aparición o la presencia de estos problemas durante el proceso.

Problemas identificados / Preguntas que permiten identificarlos

La organización prevista para gestionar las crisis no se aplica cuando ocurre una crisis, ello acarrea improvisaciones que retrasan el retorno a la normalidad.
Aunque este es un problema de organización que nuestro cuestionario no aborda directamente, lo siguiente puede alertar sobre fallas patentes: ¿Parecen los equipos preparados para manejar lo inesperado?

Dificultades de la jerarquía para distanciarse de las acciones técnicas, dificultades de los técnicos para despojarse de los reflejos diarios.
Dos preguntas pueden revelar este tipo de problema:
– ¿La jerarquía o el líder expresan una fuerte preferencia hacia ciertas opciones?
– ¿Hay responsables que se involucran demasiado en los asuntos técnicos debido a sus antiguas funciones técnicas?

Las lecciones de los incidentes están en general bien hechas, se deciden planes de acción, pero las lecciones sobre los problemas de la gestión de incidentes en sí se formalizan ocasionalmente.
La pregunta "¿Se efectúa un balance y formalización de las lecciones aprendidas específicamente acerca de cómo la organización ha manejado la crisis o el incidente (para mejorar la gestión de crisis / incidentes)?" puede garantizar una mejoría continua en el procedimiento de gestión de la crisis / incidente.

Las conclusiones de los reportes que formalizan las lecciones suelen ser diluidas para su transmisión a la alta jerarquía.
Las preguntas "¿Las causas, circunstancias y acciones de resolución de la crisis o del incidente llevan a

formalizar objetivamente las lecciones aprendidas?" y "¿Si se formalizaron las lecciones aprendidas, pero luego estas se "diluyen" a los fines de su comunicación (interna o externa), se conserva y utiliza no obstante una versión del documento que contenga todas las observaciones "en bruto"" asegura que una vuelta de experiencia útil será preparada y utilizada.

Ciertas acciones deberían ser más discretas (como por ejemplo solicitar un servicio de seguridad para investigar sobre un caso), para no generar rumores que terminen sumándose al estrés colectivo.
La siguiente pregunta sobre la comunicación, especialmente su último elemento puede evitar este tipo de error:
"Si hay comunicación de crisis (hacia el exterior), se cumplen los siguientes criterios?: coherencia del discurso / explicación del cambio, darle sentido / explicar lo que está en juego / valorar los beneficios / respuesta a las preguntas y reducción de la incertidumbre / crear las condiciones para la participación y estimular la adhesión / guiar la progresión / no comunicar información confidencial o que genere innecesaria ansiedad."

Ocurrió que se hayan decidido medidas técnicas que no tenían ninguna posibilidad de resolver los problemas (como reiniciar un servidor), sólo para que no se pueda criticar ulteriormente el hecho de no haberlo intentado.
La pregunta "¿Hay decisiones técnicas que sólo se deciden por miedo a que se critique posteriormente el no haberlas tomado?" revela específicamente este tipo de acciones innecesarias.

Ocurrió que medidas de seguridad hayan impedido reaccionar rápidamente a una crisis o incidente importante, y que no existiera posibilidad de anularlas en caso de circunstancias excepcionales.
Este problema, que se revela muy a menudo durante las crisis e incidentes mayores, se debería identificar al momento de definir las medidas de seguridad, por una pregunta específica como: "¿Es posible desactivar las medidas de seguridad en caso de emergencia (por ejemplo durante una crisis) y está previsto un entrenamiento para ese tipo de situaciones?"

A menudo, las células de crisis en las que participan responsables de la empresa, solicitan demasiado a los técnicos encargados de la resolución de la crisis. Esto genera con frecuencia una tensión desfavorable que perjudica la eficacia en el trabajo. En algunos casos incluso, se observó una inversión de roles: las células de crisis comenzaron a ordenar acciones precisas, en lugar de elegir entre las opciones propuestas por los técnicos y los expertos.
Tales acontecimientos negativos pueden detectarse usando las tres preguntas siguientes:
– Durante la gestión de la crisis, ¿hay pedidos u órdenes contradictorios (por ejemplo, exigir que los técnicos propongan soluciones y que a la vez tengan en cuenta las instrucciones técnicas de la jerarquía)?
– ¿La jerarquía o el líder expresan una fuerte preferencia hacia ciertas opciones?
– ¿Hay responsables que se involucran demasiado en los asuntos técnicos debido a sus antiguas funciones técnicas?

A veces, debido a la urgencia de una crisis o de un incidente mayor, se toman decisiones apoyándose sobre suposiciones falsas o erróneas que hubiesen sido fácilmente descalificadas (a menudo, un técnico podría haber alertado rápidamente sobre el error). Si bien es importante saber decidir sin tener toda la información necesaria, es igualmente vital poder confiar en algunas certezas.
La pregunta ¿Estamos dispuestos y preparados para decidir sin contar con todas las informaciones? (lo que equivale a asumir que las decisiones no serán del todo racionales) *subraya la importancia de este estado de espíritu en situación de crisis, mientras que la pregunta "*¿Cómo se empezó y como se llegó a considerar algo como "verdad" o certeza?*" debería alertar sobre la necesidad de controlar las informaciones que justifican acciones estructurantes.*

XII. METODOS DE USO

Esta metodología tiene como objetivo detectar problemas, no resolverlos.
La mayoría de las preguntas buscan detectar problemas de funcionamiento colectivo, es decir que sus lugares privilegiados de ejercicio son las reuniones, comités, grupos de trabajo, células de crisis.
Las preguntas deberían hacerse de manera continua (es decir, llegados al final de la lista, volver al principio) a lo largo de la gestión de la crisis o del incidente. La tarea requiere tomar distancia de las acciones de resolución. Suponiendo que una célula de crisis está encabezada por un director que toma las decisiones importantes en última instancia, que otra persona anima la reunión, coordina y toma notas, la tarea de desenrollar el cuestionario debe confiarse a una tercera persona que intervenga sólo cuando se detecta un problema en el transcurso de la gestión de crisis.

XIII. CONCLUSION

El ejercicio de confrontación de los problemas específicos observados con las preguntas identificadas sugiere cierta relevancia.

Sin embargo, este cuestionario no puede pretender ser exhaustivo. Como las metodologías OWASP o CIS CSC mencionadas anteriormente, hay que considerarlo como un tamiz. Y su eficacia para permitir identificar problemáticas comunes – aun si estas se manifiestan siempre de manera particular – dependerá de la precisión con que se formulen las preguntas y de la experiencia y competencia de quien las haga.

A su vez, y al igual que los métodos citados, la presente metodología irá aumentando su eficacia al ser pulida por la confrontación con la realidad. Practicarla permitirá afinar preguntas, descartar otras o añadir categorías importantes de riesgos humanos.

A fin también de aumentar la eficacia de este cuestionario, podrá ser útil agregar preguntas "positivas", es decir, no dedicadas a identificar problemas conocidos, sino a resaltar las diferencias con ciertas prácticas validadas por la experiencia.

Una profundización del método deberá detallar los aspectos temporales: ¿cómo determinar el momento adecuado para tomar una decisión de seguridad?, ¿cómo evitar que las precauciones tomadas – para evitar malas decisiones – no terminen retrasando demasiado el proceso de decisión?

Para facilitar la práctica de este método en condiciones operacionales, se podrán hacer propuestas concretas para su uso. Una herramienta podrá también ser concebida.

Por último, cabe destacar que al inicio del desarrollo de este método teníamos en mente completarlo con recomendaciones que de alguna manera hubiesen venido a contestar las cuestiones planteadas. Después de algunos intentos, resulta que esto reduciría la utilidad del método. Si nuestro método incorporara recomendaciones, serían o demasiado genéricas y por lo tanto no muy útiles, o serían precisas, pero en tal caso inadaptadas a situaciones específicas. Además, las recomendaciones tendrían probablemente la desventaja de incitar a los usuarios del método a consultarlas directamente como "soluciones". El principal interés del método es plantear preguntas. Incentivar a la reflexión. Alentar dudas. Incumbe a aquéllos que lo utilizan la responsabilidad de imaginar respuestas apropiadas a su propio contexto. Así planteado, este método no es una herramienta de ayuda a la toma de buenas decisiones de seguridad, sino más bien una herramienta de ayuda para no tomar malas decisiones.

AGRADECIMIENTOS

El autor quiere agradecer a Yannick Meiller quien lo ayudó a desarrollar este trabajo en la ESCP Europe, a su amigo y colega Paul Frausto quien le dio aliento y con quien mantuvo innumerables e interesantes discusiones acerca de la seguridad y a su esposa Laura Vagnoni por su colaboración en la traducción al español, por su apoyo y amor.

REFERENCIAS

[1] François Hollande en un discurso en Ajaccio el 24 de marzo 2012 (à 25mn23s); Jacques Chirac en un discurso televisado en 1998 (à 7mn59).

[2] Baruch Spinoza, Éthique III, Proposition VI, 1677.

[3] Nassim Nicholas Taleb, Le hasard sauvage, 2001

[4] https://www.owasp.org/index.php/Category: OWASP_Top_Ten_Project

[5] https://www.cisecurity.org/controls/

[6] Herbert Simon, Administrative Behavior – A Study of Decision-Making in Administrative Organization, 1947.

[7] Raymond S. Nickerson, "Confirmation Bias: A Ubiquitous Phenomenon in Many Guises", Review of General Psychology vol. 2, no. 2, 175-220, 1998.

[8] Karl Weick, "The Social Psychology of Organizing", 1969.

[9] Reid Hastie, Robyn M. Dawes, Rational Choice in an Uncertain World: The Psychology of Judgment and Decision Making, 2001.

[10] Tversky, A. and Kahneman, D., "Judgments of and by representativeness". In D. Kahneman, P. Slovic & A. Tversky (Eds.), Judgment under uncertainty: Heuristics and biases, 1982.

[11] Solomon. E. Asch, "Effects of group pressure upon the modification and distortion of judgment. In H. Guetzkow (ed.) Groups, leadership and men, 1951.

[12] Irving Janis, Groupthink: Psychological Studies of Policy Decisions and Fiascoes, 1982.

[13] L. Ross, D. Greene, P. House, The "false consensus effect": An egocentric bias in social perception and attribution processes, 1977.

[14] P. Picone, G. Dagnino, A. Minà, The origin of failure: A multidisciplinary appraisal of the hubris hypothesis and proposed research agenda, 2014.

[15] Robert-Vincent Joule, Jean-Léon Beauvois, La soumission librement consentie : Comment amener les gens à faire librement ce qu'ils doivent faire ?, 1998.

[16] G. Bateson, Double bind, 1969. Steps to an ecology of the mind: A revolutionary approach to man's understanding of himself, 1972.

[17] H. Arendt, Eichmann à Jérusalem: Rapport sur la banalité du mal, 1963.

[18] M. A. Wallach, N. Kogan, D. J. Bem, Group influence on individual risk taking, 1962.
[19] http://www.patagonia2009.com
[20] I. S. Rossenbach, Une odyssée en Patagonie, La Découvrance, 2013.
El presente estudio también se basa en el material del curso "Seguridad / Seguridad y Gestión" de la ESCP Europa, impartido en 2016 por Yannick Meiller, Jean-Philippe Bouilloud Nathalie Prime, Florence Garrigues, Carla Mendoza y Hervé Laroche.

El AUTOR

I. Rossenbach es experto en seguridad *senior* y jefe de equipos de seguridad. Tras estudios de física, empezó a trabajar en ciberseguridad en 1998. Ha sido consultor en seguridad, jefe de proyectos de criptografía, instructor. Creó y dirigió un equipo de *pentests,* ha sido responsable de un equipo de seguridad operacional (SOC), realizó una expedición en kayak por la Patagonia [19] [20], y es actualmente responsable de un equipo de seguridad de una gran institución pública francesa. En febrero de 2017 integró por un año el equipo de seguridad informática de una organización internacional en Suiza, como experto y especialista en ciberseguridad. En términos de certificaciones, su doble interés por la técnica y el *management* podría enunciarse así: *2015 GIAC web Application Pentester* y *2016 Security/Safety management ESCP certified*. Ha sido conferencista en varios congresos, imparte cursos a nivel universitario (*Université Paris XIII* en 2016 por ejemplo). Le interesan todo tipo de riesgos, no sólo los riegos informáticos. Considera que no sólo es cuestión de actuar bien y rápido cuando se trata de seguridad, sino que también tenemos que pensar la seguridad. La seguridad no es buena por naturaleza. La seguridad no es un "derecho". La seguridad no sólo tiene que ver con reducir riesgos, sino que es una manera de manejarlos. Y tenemos que pensar como manejamos las cosas. www.cryptosec.org | iro@cryptosec.org | Twitter @secucrypt