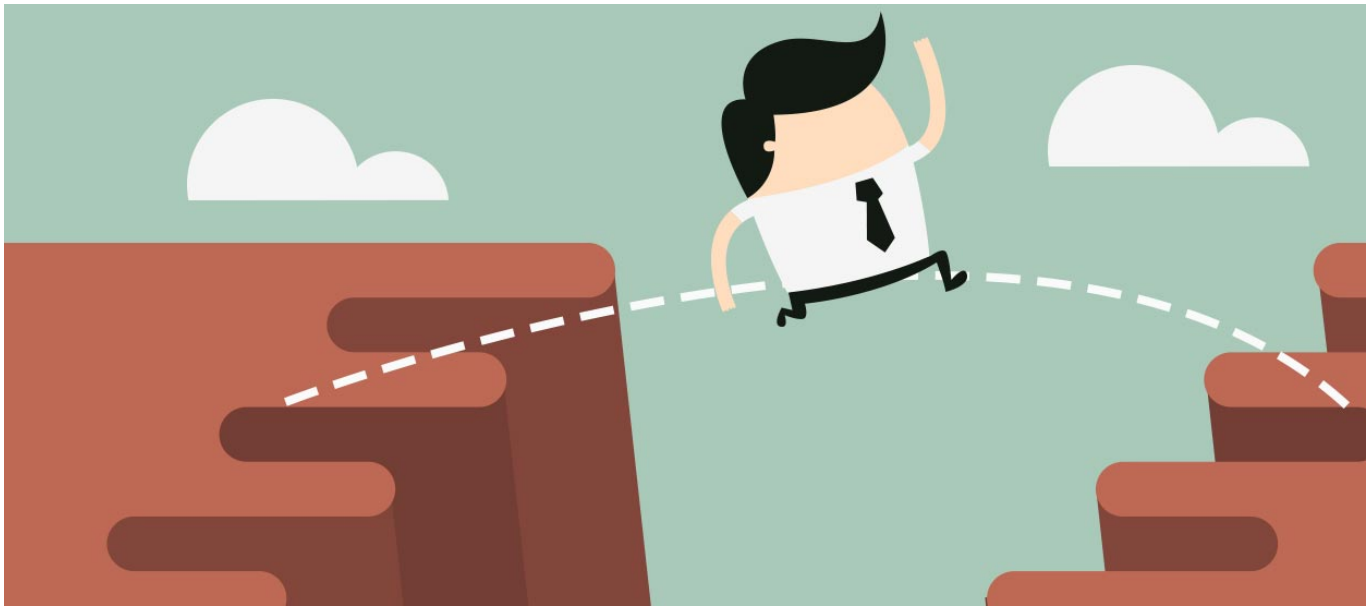
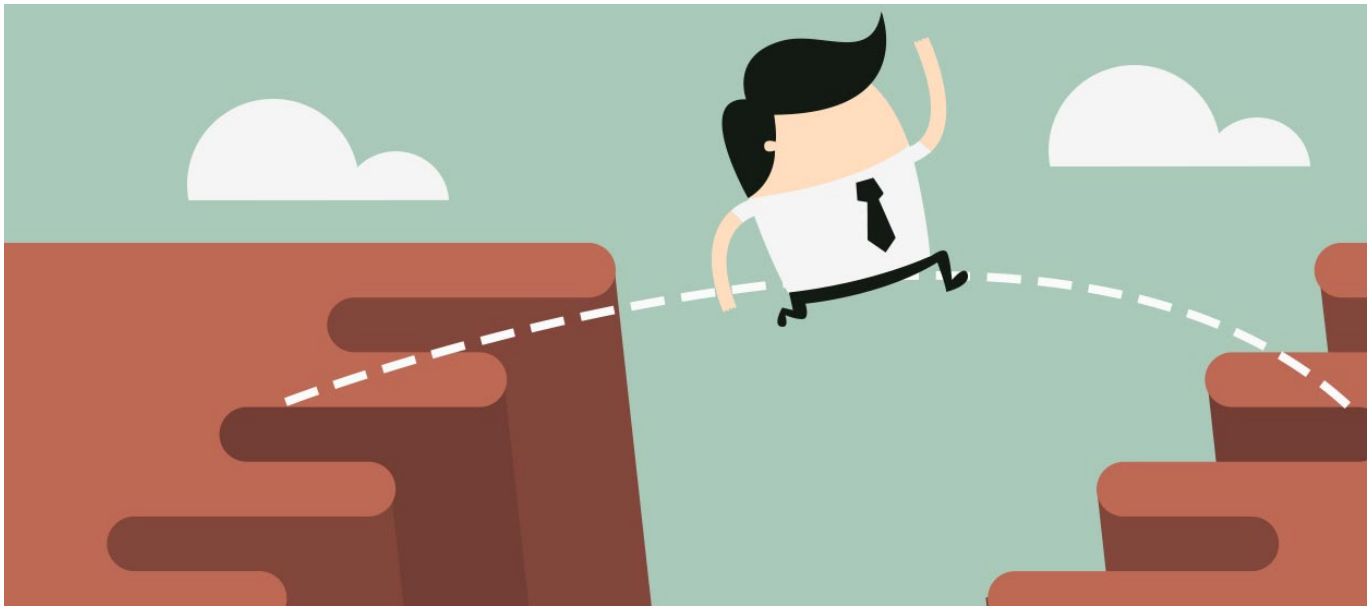
Blockchain y los Controles en los Riesgos (Parte 4/5)

Author : ibonreinoso

Categories : Auditoría, Certificación y Calidad de Sistemas Informáticos

Date : 29 noviembre, 2018





Buenas nuevamente! En esta entrada siguiendo con el post anterior (y a modo continuación), quisiera seguir desarrollando los riesgos que íbamos identificando. Esta vez, se han escogido los diez riesgos más relevantes (bajo mi criterio y discutibles). Después, se proponen soluciones con objetivo de minimizar los riesgos mediante controles; de tal manera que una vez

identificados el impacto y probabilidad de los riesgos se exponen cuestiones, ideas e iniciativas para saber cómo abordar el riesgo en cuestión.

Partiendo de la tabla expuesta en la entrada anterior, a continuación se muestran diez riesgos en la tabla 1:

ID	Riesgo	Probabilidad	Impacto
R1	Vulnerabilidad de la plataforma	MUY ALTO	MUY ALTO
R2	Malware Dirigido	MUY ALTO	MUY ALTO
R3	Falta de Escalabilidad	MEDIO	MEDIO
R4	Responsabilidades poco definidas	MEDIO	MEDIO
R5	Fallo en cumplimiento tecnológico	MUY ALTO	MEDIO
R5	Pérdida de gobierno	MUY ALTO	MEDIO
R6	Implementación de claves	MUY ALTO	BAJO
R7	Compromiso de Claves	ALTO	BAJO
R8	Gestión de tiempos de espera	ALTO	NAJO
R9	Brecha de privacidad	MUY ALTO	MEDIO
R10	Retención de la información	BAJO	BAJO

A continuación, pasaremos a la explicación de los significados los riesgos, así como las medidas que se sugieren para controlar/mitigar el problema.

[R1] Vulnerabilidad de la plataforma: Al ser nueva tecnología, es posible que se diese la situación de que una vez en producción, se detectase una vulnerabilidad de tal manera que pusiese en jaque a toda la organización. Se propone primero invertir fondos para conocer las noticias y novedades desde este punto de vista y después establecer un plan de contingencia a modo preventivo.

[R2] Malware Dirigido: Si la organización fuese objetivo de ataque e intentan atacar de forma intencionada nuestro sistema operacional de Blockchain, hay que tener acciones previamente diseñadas para afrontar este riesgo. Primeramente, se deben establecer protocolos de acción para cada tipo de ataque conocido. Después, se deberían de comprobar periódicamente estas

pautas; de tal manera que garanticemos que el sistema es robusto y se defiende [1].

[R3] Falta de Escalabilidad: La escalabilidad está estrictamente vinculada a la velocidad de procesamiento de las transacciones que ocurren dentro de una blockchain específica. Las medidas que pueden tomarse son la medición de tiempos de espera y realizar periódicamente pruebas de carga, para ver si la infraestructura desarrollada sirve para el día a día dentro de la organización [1].

[R4] Responsabilidades poco definidas: Nuevamente, la organización deberá realizar un trabajo previo a la implementación para saber quien se debe responsabilizar de la administración y roles de la plataforma; quienes serán los incluidos y excluidos de la topología… es decir, será necesario realizar todo un análisis de responsabilidades donde se deberán acotar las funcionalidades para cada actor/rol identificado y dejarlo documentado.

[R5] Fallo en cumplimiento tecnológico: ¿Qué sucede si la tecnología deja de funcionar?¿En cuanto tiempo es posible reiniciar todo el sistema o, en su defecto, poner en marcha el respaldo correspondiente? Para ello, habrá que diseñar un plan de contingencia donde tengamos garantías de que este riesgo no va a suponer un problema. Los controles que se proponen son 1) tener un sistema respaldo en marcha (aunque de manera pasiva) y 2) someter a simulacros eventualmente para poder medir los tiempos de espera.

[R6] Implementación de claves: ¿Cada cuanto cambias las claves?¿Quién lo hace? Esas responsabilidades y periodos temporales en un documento. Además, se debería de gestionar periódicamente si ha habido vulnerabilidades de, por ejemplo, la metodología implementada.

[R7] Compromiso de Claves: Debemos asegurarnos de que las claves que preparamos y asignamos, efectivamente, se utilizan y se guardan de manera efectiva.

[R8] Gestión de tiempos de espera: ¿Qué sucede si el sistema tarda demasiado en responder, verificar y respaldar todo el proceso?

[R9] Brecha de privacidad: ¿Qué pasa si la clave se externaliza y se publica? Para ello

[R10] Retención de la información: ¿Cómo garantizamos que la información es efectivamente guardada sólo por nuestro sistema?¿Qué servicios pueden almacenar/acceder?

En resumen, hemos identificado y explorado muchos de los riesgos ya identificados en el post anterior. Sabemos que Blockchain tiene muchos quebraderos de cabeza iniciales, pero una vez desarrolladas estas cuestiones y sabiendo cómo mitigar los riesgos que tiene podremos gozar de los beneficios de esta tecnología (la posible exención de autoridad digital, la auditabilidad y trazabilidad entre otros [2]).

[1] https://www.iproup.com/blockchain/182-blockchain-bitcoin-ethereum-Los-tres-retos-de-la-tecnologia-Blockchain-escalabilidad-interoperabilidad-y-sustentabilidad

[2] https://oceano.biblioteca.deusto.es/primo-explore/fulldisplay?docid=TN_acm3225619&context=PC&vid=deusto&lang=en_US&search_scope=default_scope&adaptor=primo_central_multiple_fe&tab=default_tab&query=any,contains,blockchain&sortby=rank