

Artículos HC Gestión

# CrowdStrike Falcon: Gestión De Riesgos y Continuidad

19-07-2024

*crisis*  
**CROWDSTRIKE**  
*global*



HC•Gestión

Riesgos | Finanzas | Estrategia



# CrowdStrike Falcon: Gestión de riesgos y continuidad

Por Esperanza Hernández Avendaño

*“Es un recordatorio contundente de la vulnerabilidad inherente en nuestras infraestructuras digitales interconectadas y la necesidad crítica de una gestión de riesgos más robusta.”*

*Leonardo Berro, Socio Director Security Advisor.*

En la madrugada del viernes 19 de julio de 2024, empresas de diferentes sectores, especialmente del sector aéreo, se vieron impactadas por la caída de sus sistemas vinculada a problemas en la actualización del software CrowdStrike que protege

a los sistemas informáticos de ciberataques, específicamente de la actualización de la herramienta Falcon Cloud Security que protege las operaciones en la nube.

En el momento en que esta herramienta presenta fallas los sistemas con Azure y Windows no pueden garantizar la seguridad del sistema y por lo tanto se bloquean para evitar daños. De lo informado por CrowdStrike se infiere que Azure no reconoció la actualización por errores en esta y por lo tanto, se desencadenaron las “pantallas azules de la muerte” (Blue Screen of Death) en los hosts de Windows. CrowdStrike ha asegurado que el incidente no se debió a un ataque cibernético, sino a un error en la actualización de Falcon Cloud Security.

En la mayoría de los casos resulta más sencillo como se dice popularmente “mirar los eventos con el espejo retrovisor y no con el panorámico” y por lo tanto a partir de la materialización del evento de riesgo pueden emitirse muchas opiniones de lo que se “debería haber hecho y no se hizo” y con mayor razón cuando el impacto de la materialización del evento de riesgo es global y produce no solamente grandes afectaciones económicas sino también reputacionales, de hecho, en el mismo día el valor de las acciones de CrowdStrike ya había descendido el 20%, arrastrando igualmente al valor de la acción de Microsoft con una caída del 2,9% (datos porcentuales del Diario La República, Colombia, 19 de julio de 2024).

Por lo descrito en el párrafo inmediatamente anterior, en este artículo me referiré específicamente a lo que podemos aportar como gestores integrales de riesgos y que nos sirve de enseñanzas “hacia adelante” para quienes estamos dedicados a la gestión de riesgos financieros, no financieros y emergentes.

En la gestión de riesgos es importante establecer el factor o causa del evento de riesgo de manera preventiva y no correctiva, luego para quienes gestionamos riesgos la primera enseñanza que surge con este caso, es la necesidad de llevar a cabo un análisis integral de los factores o causas de todos los riesgos a los que se encuentra expuesta la entidad y no de realizar un enfoque individual de únicamente uno de ellos. En una evaluación integral por ejemplo y en este caso específico, se revisan no solamente los factores del riesgo cibernético sino todos los factores o causas de los demás riesgos asociados, como lo son los riesgos operacionales derivados de las posibles caídas de sistemas o fallas tecnológicas del proveedor de servicios tecnológicos.

La segunda enseñanza es la necesidad de establecer como política en la gestión integral de riesgos la diversificación de proveedores o terceros, no solamente de servicios tecnológicos, que actúen como respaldo ante las posibles fallas y/o materialización de eventos de riesgos de parte de estos. En la gestión del riesgo operacional, especialmente de los riesgos tecnológicos, es fundamental la diversificación y la redun-

dancia como parte de la administración de la continuidad del negocio y de sus componentes como lo es el Plan de Recuperación de Desastres (DRP) de sistemas y tecnologías de la información.

Una tercera enseñanza, aplicable no solamente a las entidades o empresas usuarias sino también a los mismos proveedores de servicios tecnológicos es la necesidad de llevar a cabo pruebas rigurosas previas o anteriores a la implementación de actualizaciones y/o del lanzamiento de nuevos productos. Seguramente surgirán más enseñanzas de este y de otros casos que puedan presentarse, puesto que los riesgos no se pueden eliminar sino mitigar y por lo tanto, se reitera que la gestión de riesgos debe ser integral y que su posición en la cadena de valor y en la estructura organizacional de la entidad o de la empresa debe ser estratégica por el impacto que la materialización de los eventos representa en la rentabilidad y continuidad del negocio.

---

#### Fuentes:

(Páginas web de julio 19 de 2024)

- Diario La República, Colombia
- Forbes AR
- Infobae



HC•Gestión

Riesgos|Finanzas|Estrategia