Riesgo tecnológico y ciberhigiene

Dr Alexander Ressos, TEP
Attorney-at-Law (Switzerland and Germany),
Solicitor (England & Wales and Hong Kong)
Of Counsel, KGP Legal LLC
alexander.ressos@kgplegal.com.sg
www.ressos.com.sg

Los controles AML/CFT de un licenciatario de DPT funcionan sobre tecnología, y la MAS (Monetary Authority of Singapore, la autoridad monetaria y supervisora financiera) regula esa tecnología mediante dos notices y un conjunto de guidelines que en la práctica son inseparables del programa de prevención del blanqueo.

La MAS Notice PSN05 on Technology Risk Management impone requisitos jurídicamente vinculantes a los proveedores de servicios de pago. La entidad debe contar con un marco para identificar sus sistemas críticos. Cada sistema crítico no puede sufrir más de cuatro horas de inactividad no programada en cualquier periodo móvil de doce meses y debe tener un objetivo de tiempo de recuperación de cuatro horas. La MAS debe recibir notificación en el plazo de una hora desde el descubrimiento de un incidente relevante, y un informe sobre la causa raíz en los catorce días siguientes.[1] La MAS Notice PSN06 on Cyber Hygiene impone seis medidas básicas: proteger las cuentas de administrador, aplicar con prontitud los parches de seguridad, establecer un conjunto escrito de estándares de seguridad, implantar defensas perimetrales de red, desplegar protección contra malware y utilizar autenticación multifactor para el acceso administrativo y el acceso a la información de clientes.[2] Las Technology Risk Management Guidelines de enero de 2021 fijan el estándar, no vinculante pero sujeto a inspección, para todo lo demás.

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

Abarcan la gobernanza, el desarrollo de software, la gestión de terceros, la respuesta a incidentes, el control de accesos, la gestión de claves criptográficas y las pruebas de penetración.[3]

Para una entidad de DPT, el apartado de gestión de claves de las TRM Guidelines tiene un peso especial, porque las claves privadas de la entidad son los activos de sus clientes. La MAS espera ceremonias de generación de claves documentadas y módulos de seguridad de hardware (HSM) o equivalentes. Espera una segregación de funciones que impida que una sola persona pueda mover fondos de clientes, soluciones de almacenamiento en frío para el grueso de los activos y procedimientos de recuperación probados. Se trata también de requisitos de custodia conforme a la parte K, capítulo II, y la MAS los inspecciona como un único tema. Un hackeo es también un evento de prevención del blanqueo. Los tokens robados salen a través de los monederos de la entidad. La entidad debe poder rastrearlos, comunicarlos conforme a la PSN03 y a la sección 45 de la CDSA y cooperar con la policía y con otras plataformas de intercambio para congelarlos. Un plan de respuesta a incidentes que solo abarque la recuperación técnica, y no la comunicación regulatoria ni el rastreo on-chain, está incompleto. La parte Q, capítulo II contiene una lista de control para las primeras setenta y dos horas tras un hackeo.

Notas

1. MAS Notice PSN05, Technology Risk Management, dictada al amparo de la Payment Services Act 2019, párrafos sobre la identificación de sistemas críticos, el máximo de 4 horas de inactividad no programada, la notificación de incidentes en 1 hora y el informe sobre la causa raíz en 14 días. ↩
2. MAS Notice PSN06, Cyber Hygiene, dictada al amparo de la Payment Services Act 2019, párrs. 4–9, sobre los seis requisitos de ciberhigiene. ↩
3. MAS, Technology Risk Management Guidelines, 18 de enero de 2021, en particular la sección 10, sobre la gestión de claves criptográficas, y la sección 12, sobre el control de accesos. ↩

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

Disclaimer

This article is provided for general information only. It is based on publicly available sources as at its date of publication. These sources have not been independently verified against licences, regulatory registers or the records of the entities concerned. It is not legal, tax, financial or investment advice. Nor is it a recommendation to invest in, transact with or use the services of any entity mentioned. Law and regulation change frequently, so the content may be incomplete or outdated. To the fullest extent permitted by law, Dr Alexander Ressos and the publisher of SingaporeIQ exclude all liability for loss or damage arising from the use of or reliance on this article. Readers should obtain advice on their specific circumstances before acting or refraining from action.

Names and trademarks of the entities discussed belong to their owners and are used for identification only. Their mention implies no endorsement, affiliation or allegation of wrongdoing. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. Corrections and updates: contact@ressos.com.

© 2026 Dr Alexander Ressos. This article may be quoted with attribution to SingaporeIQ (SingaporeIQ.com). Reproduction in full and any commercial use require prior written consent. The Legal Terms at https://singaporeiq.com/legal-terms apply.

Author contact: Dr Alexander Ressos, TEP · contact@ressos.com