POLÍTICA DE GESTIÓN DE VULNERABILIDADES Y BRECHAS

1. OBJETO

Esta política establece las directrices de SPACEROCK S.A.S. para la notificación, evaluación, gestión y respuesta ante vulnerabilidades o incidentes de seguridad de la información que puedan comprometer la confidencialidad, integridad o disponibilidad de los datos tratados por la compañía, conforme a la Ley 1581 de 2012, el Decreto 1074 de 2015 y las buenas prácticas internacionales.

2. DEFINICIONES

- Brecha de seguridad: Evento que implica el acceso no autorizado, pérdida, alteración o divulgación de información personal o confidencial.
- Vulnerabilidad: Falla o debilidad técnica o procedimental que puede ser aprovechada para comprometer un sistema o servicio.

3. ALCANCE

Esta política aplica a todos los sistemas, plataformas, aplicaciones, sitios web, equipos y recursos tecnológicos administrados o contratados por SPACEROCK S.A.S.

4. REPORTE DE INCIDENTES Y VULNERABILIDADES

Toda persona interna o externa que detecte o sospeche una vulnerabilidad o incidente de seguridad deberá notificar de inmediato al área responsable escribiendo a: info@spacerock.com.co

El reporte debe incluir la siguiente información (si se conoce):

- Fecha y hora del hallazgo o incidente
- Descripción técnica de la vulnerabilidad o brecha
- Sistema o aplicación afectada
- Datos comprometidos (si aplica)
- Método de detección

5. PROCEDIMIENTO DE RESPUESTA

Una vez recibida la notificación:

- Se activará el plan de respuesta y contención por parte del equipo de seguridad.
- Se evaluará la severidad del incidente según criterios como: tipo de información comprometida, número de afectados, nivel de exposición, posibilidad de daño y repercusiones legales o reputacionales.

- Se documentará y reportará el incidente a la autoridad competente si así lo exige la normatividad.
- Se implementarán medidas correctivas y preventivas para mitigar impactos y evitar recurrencias.

6. INTERACCIÓN CON INVESTIGADORES DE SEGURIDAD

SPACEROCK S.A.S. valora el trabajo ético de investigadores de ciberseguridad y promueve su colaboración bajo los siguientes lineamientos:

- Debe:
  - Detener pruebas al detectar una vulnerabilidad o exposición de datos no públicos.
  - Reportar inmediatamente a SPACEROCK y eliminar cualquier dato obtenido.
- Puede:
  - Visualizar o registrar datos únicamente para demostrar técnicamente la existencia de la vulnerabilidad, sin compartirlos ni difundirlos.

- No debe:
  - Realizar ingeniería social, pruebas físicas, ataques de denegación de servicio (DoS), envío de mensajes engañosos (“phishing”), instalación de software malicioso, ni acciones que afecten la operatividad o disponibilidad de los sistemas.
  - Exfiltrar, borrar, modificar o divulgar datos sin autorización expresa.
  - Exceder el alcance definido o simular accesos persistentes.

7. CONFIDENCIALIDAD Y TRATAMIENTO DE LOS REPORTE

Los reportes podrán ser anónimos, aunque se recomienda incluir un canal de contacto para aclaraciones técnicas. Toda la información será tratada bajo estricta confidencialidad y según la política de protección de datos personales vigente.

8. DISPOSICIONES FINALES

Cualquier hallazgo será gestionado con seriedad y transparencia. El cumplimiento de esta política será considerado como buena fe y SPACEROCK S.A.S. no tomará represalias legales contra quienes colaboren de forma responsable.

Fecha: 27 de agosto de 2024