Política de divulgación de vulnerabilidades

ÚLTIMA ACTUALIZACIÓN: 29 de septiembre de 2025

BriskHeat está comprometido con la protección de nuestros clientes, datos y sistemas. Agradecemos el papel de la comunidad de seguridad en ayudarnos a mantener un entorno seguro y protegido.

Esta política describe nuestro enfoque para gestionar informes no solicitados de vulnerabilidades. Aunque no solicitamos activamente comentarios ni operamos un programa formal de recompensas por errores, tomamos todos los informes válidos con seriedad y los investigamos a fondo.

Reporte de Problemas de Seguridad

Si considera que ha encontrado una vulnerabilidad de seguridad en un sistema o activo de BriskHeat, por favor repórtelo enviándonos un correo electrónico a website.security@briskheat.com.

Al reportar, por favor:

- Respete la privacidad: si accede a los datos de otra persona (por ejemplo, nombres de usuario, contraseñas o información personal), deténgase inmediatamente y repórtelo. No guarde, comparta ni transmita estos datos.
- Actúe de buena fe – Envíe su reporte sin condiciones ni exigencias.
- Colabore de manera responsable – Reporte sus hallazgos de inmediato. Deje de realizar pruebas tras identificar el primer problema y solicite permiso antes de continuar. Permítanos un tiempo razonable para investigar y resolver el problema antes de cualquier divulgación pública.

Por favor, no:

- Exfiltre datos. Utilice una prueba de concepto para demostrar el problema.
- Aproveche la vulnerabilidad para desactivar o eludir los controles de seguridad.
- Participe en ingeniería social (por ejemplo, phishing o suplantación de identidad).
- Utilice herramientas automatizadas o escáneres sin autorización previa.

Proceso Posterior al Reporte

Una vez que recibamos un informe, BriskHeat:

1. Mantendrá la confidencialidad – Solicitamos que todas las comunicaciones relacionadas con la vulnerabilidad permanezcan privadas.
2. Verificará el problema – Investigaremos y confirmaremos la validez del informe.
3. Remediará – Si se confirma, abordaremos la vulnerabilidad e implementaremos una solución o mitigación.
4. Comunicará – Confirmaremos la recepción de su informe en un plazo de 10 días hábiles y proporcionaremos actualizaciones de estado según corresponda.
5. Después de la resolución, BriskHeat podrá, a su entera discreción, optar por reconocer públicamente la contribución del informante. Esta decisión se toma tras una revisión interna y se basa en factores tales como, pero no limitados a, la naturaleza de la vulnerabilidad, su impacto y la alineación con nuestras políticas internas.

Tenga en cuenta: BriskHeat no opera un programa formal de recompensas. Cualquier reconocimiento es discrecional y se determina caso por caso, en función de factores como la gravedad, el impacto y la alineación con los criterios internos.

Nota Importante

Esta política está diseñada para alinearse con las mejores prácticas de seguridad actuales. Sin embargo, BriskHeat no solicita activamente informes de vulnerabilidades a través de plataformas públicas o divulgación. Cualquier tiempo, esfuerzo o recurso invertido en la evaluación de nuestros sistemas se realiza a la entera discreción del informante.

Agradecemos los esfuerzos de quienes deciden reportar de manera responsable y ayudarnos a mejorar nuestra postura de seguridad.

Actualizaciones de la Política

BriskHeat se reserva el derecho de modificar o actualizar esta Política de Divulgación de Vulnerabilidades en cualquier momento sin previo aviso. Recomendamos a los informantes e investigadores revisar la política periódicamente para mantenerse informados de cualquier cambio.