**Translation of Contents Generated by Orca-2-13b**

|  |  |  |
| --- | --- | --- |
| Question | **LLM Generated Content** | **Translation by GPT-4-Turbo** |
| 2 | ¿Puedes resumir los cambios realizados desde la versión 3.2.1 hasta la versión 4.0 de PCI DSS? | Can you summarize the changes made from version 3.2.1 to version 4.0 of PCI DSS? |
|  | Sí, puedo resumir los cambios realizados desde la versión 3.2.1 hasta la versión 4.0 de PCI DSS. Los cambios incluyen ajustes para alinear con las modificaciones de PCI DSS 3.2 a PCI DSS 3.2.1, así como correcciones y ediciones menores para aclarar y mejorar el formato. Luego, en la versión 4.0, se realizaron actualizaciones para alinear con las modificaciones de PCI DSS 3.2.1 a PCI DSS 4.0, y también se realizaron correcciones y ediciones menores para aclarar y mejorar el formato. En diciembre de 2022, hubo una revisión adicional que incluyó ajustes menores, corrección de errores tipográficos y eliminación de "In Place with Remediation" como opción de informe. | Yes, I can summarize the changes made from version 3.2.1 to version 4.0 of PCI DSS. The changes include adjustments to align with the modifications from PCI DSS 3.2 to PCI DSS 3.2.1, as well as minor corrections and edits to clarify and improve the format. Then, in version 4.0, updates were made to align with the modifications from PCI DSS 3.2.1 to PCI DSS 4.0, and there were also minor corrections and edits made to clarify and improve the format. In December 2022, there was an additional revision that included minor adjustments, correction of typographical errors, and the removal of "In Place with Remediation" as a reporting option. |
| 3 | ¿Cuáles son las nuevas requisitos para las evaluaciones de vulnerabilidades en la versión 4.0 de PCI DSS? | What are the new requirements for vulnerability assessments in PCI DSS version 4.0? |
|  | Las nuevas requisitos para las evaluaciones de vulnerabilidades en la versión 4.0 de PCI DSS incluyen resolver vulnerabilidades con una puntuación de 4.0 o más en el CVSS, realizar rescans cuando sea necesario, y tener un método de penetration testing definido, documentado e implementado que incluye enfoques aceptados por la industria y cobertura para el perímetro del SDE y los sistemas críticos. | The new requirements for vulnerability assessments in PCI DSS version 4.0 include resolving vulnerabilities with a CVSS score of 4.0 or higher, performing rescans when necessary, and having a defined, documented, and implemented penetration testing method that includes industry-accepted approaches and coverage for the CDE perimeter and critical systems. |
| 4 | ¿Puedes dar más detalles sobre las prácticas de prueba de penetración en PCI DSS? | Can you provide more details about penetration testing practices in PCI DSS? |
|  | Sí, puedo dar más detalles sobre las prácticas de prueba de penetración en PCI DSS. La PCI DSS requiere que se realice un penetration testing externo al menos una vez cada 12 meses y después de cualquier modificación o cambio significativo en la infraestructura o el software. El penetration testing debe ser realizado por un recurso interno calificado o un tercero de fuera de la organización calificado y debe cumplir con la metodología definida por la entidad. Además, las vulnerabilidades y debilidades de seguridad que se encuentren durante el penetration testing deben ser corregidas y verificadas mediante la repetición del testing. | Yes, I can provide more details about penetration testing practices in PCI DSS. The PCI DSS requires that external penetration testing be conducted at least once every 12 months and after any significant modification or change in the infrastructure or software. The penetration testing must be conducted by a qualified internal resource or a qualified third party from outside the organization and must comply with the methodology defined by the entity. Additionally, the security vulnerabilities and weaknesses that are found during the penetration testing must be corrected and verified by repeating the testing. |