PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES PARA LA RENOVACIÓN DEL ALOJAMIENTO Y MANTENIMIENTO DEL SISTEMA DE AUTOEVALUACIÓN DE CIBERSEGURIDAD DE ZIUR FUNDAZIOA (EXPTE. ZIUR2024-010)

1. ANTECEDENTES

Actualmente la sede de ZIUR Fundazioa dispone de la herramienta de Autoevaluación E-Qualify, que ha sido utilizada por ZIUR para disponer de un mecanismo de autoevaluación fiable y contrastado en el mercado, de una manera más rápida y eficiente que si tuviera que desarrollar dicho método desde cero.

Dado que su instalación inicial fue en 2019, es necesario renovar el alojamiento de la solución y el mantenimiento actualizado de los controles de seguridad para asegurar la continuidad del servicio.

2. OBJETO DEL CONTRATO

El objeto del presente Pliego de Prescripciones Técnicas es establecer las condiciones que regirán el contrato de renovación del alojamiento y mantenimiento de la solución de autoevaluación de ciberseguridad E-Qualify para los próximos dos (2) años.

3. DESCRIPCIÓN DE LAS PRESTACIONES DEL CONTRATO

Es necesario renovar el mantenimiento de E-Qualify, que incluye lo siguiente:

- **Alojamiento durante 24 meses en modelo SaaS**

- **Actualización de la versión de metodología**

  Desde la instalación inicial en 2019, se ha liberado una nueva versión de la metodología de calificación de LEET Security, en concreto en la actualidad está en vigor la versión 3.1. Esta nueva versión supone una adaptación de las medidas al estado actual de la tecnología, así como una mejora en la organización y estructura de los controles evaluados.

  En particular los cambios de la nueva metodología serían los siguientes:

  1. Mapeo de nuevos estándares y versiones actualizadas de los existentes. La aparición y/o relevancia de ciertos estándares ha recomendado su incorporación a la sección de mapeos.
  2. Redenominación de los términos utilizados:
  3. Traspaso de la sección '[SD.05] Gestión de Vulnerabilidades' al dominio "Operación de sistemas - SO".

4. Incorporación de diversos controles en las secciones correspondientes relacionados con el cumplimiento de las normativas de privacidad.
5. Introducción de las últimas tendencias en materia de autenticación.
6. Actualización del mecanismo de asignación del calificador adicional de privacidad (ahora denominado 'PRIV`).
7. Mejora del requerimiento sobre notificación de incidentes.
8. Se han mejorado los controles de la sección de 'Desarrollo seguro [SD]'
9. Reubicación de controles relacionados con la cadena de valor hacia clientes en el dominio de 'Cumplimiento - [CO]'
10. Mejora de las medidas relacionadas con el teletrabajo (SO.07)
11. Incorporación de prácticas relativas a la seguridad en containers en la sección '[SO.05]
12. Requerimientos de seguridad para los sistemas de información'
13. Introducción de medidas relacionadas con SDP - Software Defined Perimeter en la sección sobre controles de red (NC).
14. Consideración de los principios de confianza cero (zero trust) en la sección '[SO.05] - Requerimientos de seguridad para los sistemas de información'.
15. Incorporación de medidas relativas a la "procedencia" de los componentes de las soluciones en el dominio de terceras partes [TP].
16. Nuevo requisito relativo a la necesidad de contar con una ciber póliza para la cobertura de este tipo de riesgos en la sección [RE.06].
17. Nuevo requisito sobre la formación de los profesionales que participan en la gestión de la criptografía.
18. Adición de nuevas medidas avanzadas sobre seguridad física a modo de 'Tier 5' en los dominios de resiliencia (RE) y seguridad física (FS).
19. Nuevos requisitos relacionados con tecnologías SOAR (Security Orchestration, Automation and Response).
20. Incorporación de referencias a ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge).
21. Mención del estándar ASVS (Application Security Verification Standard) en el dominio de
22. 'Desarrollo Seguro - [SD]'
23. Adaptación de prácticas a entornos de Sistemas de Control Industrial.

Donostia-San Sebastián, a 15 de mayo de 2024.

DIRECTORA GENERAL DE ZIUR FUNDAZIOA

Maria Penilla Azcuenaga

Firmado digitalmente por MARIA PENILLA AZCUENAGA 20210051C el día