SEGUIMIENTO A HALLAZGOS EN PRUEBAS DE VULNERABILIDAD

ÍNDICE

1. Objetivo

Establecer la metodología para identificar, clasificar y dar seguimiento a las vulnerabilidades encontradas en el escaneo a los activos de Controles volumétricos.

2. Alcance

De acuerdo a las vulnerabilidades encontradas con el software de escaneo utilizado en los activos localizados en las instalaciones de Pegasus Control, se obtiene su clasificación de acuerdo al nivel de gravedad y la frecuencia en la que se puede presentar para poder ejecutar las acciones que se mencionan a continuación.

3. Responsabilidades

Actividades	Responsable
Ejecutar escaneo de vulnerabilidades. Identificar y clasificar los hallazgos para presentarlos.	Sysadmin
Tomar los requerimientos, planificar las actividades y tiempo para contener o resolver los hallazgos encontrados.	Sysadmin
Ejecutar las acciones correctivas dentro del área de aplicativo.	Gerente de producto

Figura 1. Tabla de Responsabilidades

4. Definiciones

Nº	Término	Definición	Abreviación
1	Common Vulnerability Scoring System. (Sistema de puntuación de vulnerabilidades)	Sistema (métrica) de score con el que poder medir el impacto que una vulnerabilidad puede tener si es explotada.	CVSS
2	Common Vulnerabilities Exposures	Es una lista de entradas que contienen un No. de identificación, una descripción y al menos una referencia pública. Para el conocimiento público de las vulnerabilidades de la seguridad cibernética.	CVE
3	Nessus Attack Scripting Language	Lenguaje para crear pruebas de seguridad.	NASL

Figura 2. Tabla de Definiciones

5. Contenido

El software utilizado para el hallazgo de vulnerabilidades tiene cinco niveles de gravedad : Informativo, Riesgo Bajo, Riesgo Medio, Riesgo Alto, y Riesgo Crítico.

De los hallazgos, se determina la frecuencia con la que se puede replicar en el aplicativo, teniendo como parámetros: Baja, Media y Alta.

Teniendo ambos factores se clasifica la vulnerabilidad mediante la siguiente tabla para poder ejecutar las acciones correspondientes.

Gravedad / Frecuencia	Baja	Media	Alta
Informativo			
Bajo			
Medio			
Alto			
Crítico			

Figura 3. Matriz de impacto

Color	Descripción
	Vulnerabilidades que no afectan la operación del aplicativo, son consideradas de baja prioridad y su solución puede ser planificada en alguna versión de actualización y ejecutada en un plazo no mayor a 45 días.
	Vulnerabilidades que pueden afectar la operación del aplicativo, son consideradas de media prioridad y su solución debe de ser planificada y ejecutada en un plazo no mayor a 15 días.
	Vulnerabilidades que afectan totalmente y pueden detener la operación total del aplicativo, la solución debe de ser planificada y ejecutada en un plazo no mayor a 3 días.

Figura 4. Descripción de colores

De acuerdo al tipo de hallazgos en las vulnerabilidades son las acciones que se deben de realizar.

Tipo	Descripción	Acciones
Aplicaciones	Son todas aquellas aplicaciones que son necesarias para el funcionamiento del aplicativo, por ejemplo: ● PHP ● MySQL ● Python	● Actualizar las versiones de las aplicaciones. ● Configurar las aplicaciones para utilizar solo los puertos necesarios. ● En caso de requerir contraseñas, utilizar el estándar del documento **POL-004-TI Política de Uso de Contraseñas.**
Protocolos	Son todos los canales de comunicación utilizados por las plataformas para el traspaso de información, por ejemplo: ● HTML ● FTP ● SSH ● SOAP	● Abrir solo los puertos de comunicación de los protocolos utilizados. ● Actualizar la versión de los protocolos. ● En caso de requerir contraseñas, utilizar el estándar del documento **“POL-004-TI Política de Uso de Contraseñas”.**
Certificados	Son todas las credenciales y evidencia de que el sitio y la transferencia de información está cifrada y no puede ser vista un por tercero, por ejemplo: ● SSL ● HTTPS	● Validar que el sitio cuente con certificados. ● Validar que los certificados estén actualizados. ● En caso de filtración, revocar y generar un certificado nuevo.

Figura 5. Descripción de acciones conforme al tipo de vulnerabilidades

Las actualizaciones necesarias resultado del análisis de vulnerabilidades, se realizarán acorde al **PRT-017-TI PROCEDIMIENTO DE ACTUALIZACIONES.**

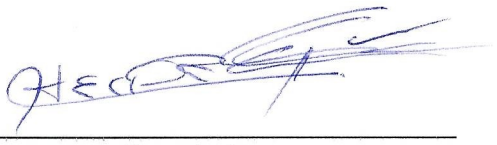
De acuerdo a la matriz de impacto de vulnerabilidades se asigna el tiempo de respuesta de cambio y de acuerdo al tipo de hallazgo, son las actividades que se tienen que planear.

6. Historial de Revisiones

Versión	Fecha	Cambios	Elaboró	Revisó	Aprobó
1.0	12/06/2020	Creación de documento	Silvestre García	Rubén Villafuerte	Rubén Villafuerte
1.1	12/10/2021	Actualización de firmas de actualización	Omar Aguilar	Rubén Villafuerte	Rubén Villafuerte
1.2	06/12/2022	Revisión de documentación	Omar Aguilar	Rubén Villafuerte	Rubén Villafuerte

7. Firmas de autorización

Gerente de Producto
Ruben Villafuerte



Sysadmin
Fabián Candelario