INFORME DE CASOS GENERADOS SEGURIDAD DIGITAL

INFRAESTRUCTURA ON -PRIMESE, 2022

A través de los monitoreos continuos realizados por el área de seguridad y privacidad de la información, se observa:

Los análisis generados desde el área de seguridad hacia los diferentes dominios y subdominios de cartagena.gov.co, se ha encontrado que mucho de ellos están publicados en el DNS público con acceso al exterior con erros de: carga de página o errores de consulta.

El área de seguridad y privacidad de la información registra los casos identificados que pueden contener alguna alerta de seguridad.

Se han reportado para que desde el ares de desarrollo revisen y notifiquen a infraestructura para corregir ciertos subdominios que puede que ya no se estén usando y así darles de baja del DNS público (cloudflare.com)

A continuación, se resumen el estado de reportes de seguridad internos en el mes de mayo de 2022.

SAUS		Herramienta utilizada			
Tecnico Asignado	Estado en SAUS	Nessus	Shodan	Terminal	Total general
Agente SAUS	Abierto	7	4		11
Total Agente SAUS		**7**	**4**		**11**
Sebastián Andres Zapateiro Núñez	Cerrada			2	2
	En curso (asignada)			32	32
Total Sebastián Andres Zapateiro Núñez				**34**	**34**
Total general		**7**	**4**	**34**	**45**

Se realizar seguimiento al análisis de vulnerabilidades tanto activos internos como los externos,
conexión a internet para el distrito de Cartagena, reportado en la plataforma saus Seguimiento de Vulnerabilidades de Activos (Nube Local, INTERNA -EXTERNA)

Conclusión:
Se recomienda revisar cada una de los 45 eventos reportados en SAUS, el cual contine descripción detallada de las vulnerabilidades de los servidores a nivel de sistemas operativos y aplicaciones, y se recomienda que sean actualizadas o parcheadas.