|  |
| --- |
| **INSTRUCCIÓN DEL DILIGENCIAMIENTO** |
| 1. Ítems de verificación: De la siguiente lista, marque con una **X** de acuerdo con la siguiente instrucción:  * **Si**: En caso de que este implementado en la plataforma tecnológica o sistema de información. * **No**: En caso de que no esté implementado en la plataforma tecnológica o sistema de información (en el campo de observaciones indicar porque no está implementado). * **N/A**: En caso de que la plataforma tecnológica o sistema de información no deba dar cumplimiento al ítem de verificación y con su respectiva observación.  1. Al Guía de hardening   Se debe aplicar la guía referencia de seguridad (NIST, CIS, SANS o incluso propias construidas por Fabricante), que apoyen las configuraciones de los elementos más importantes del sistema de información o plataforma tecnológica, tales como: sistemas operativos, servidores web, bases de datos, entre otros. |

|  |  |
| --- | --- |
| **INFORMACIÓN GENERAL** | |
| **Nombre:**  ***Profesional, Especialista*** | **Rol(s) o Cargo:**  ***dd/mm/aa*** |
| **Fecha: *dd/mm/aa*** | **Correo Electrónico:** |
| **Sistema de información o plataforma tecnológica:**  ***dd/mm/aa*** | **Grupo de trabajo responsable del sistema:**  ***dd/mm/aa*** |

| 1. **ÍTEMS DE VERIFICACIÓN** | **CUMPLIMIENTO** | | | **OBSERVACIONES** |
| --- | --- | --- | --- | --- |
| **SI** | **NO** | **N/A** |
| 1. **Arquitectura y continuidad** |  |  |  |  |
| ¿Se cuenta con una arquitectura hardware y software documentada del sistema de información, como el diagrama físico de base de datos, arquitectura del sistema, usuarios de servicio, entre otros? |  |  |  |  |
| ¿Los servidores están sincronizados con la hora legal colombiana? |  |  |  |  |
| ¿Se cuenta con arquitectura de alta disponibilidad del sistema de información o plataforma tecnológica? |  |  |  |  |
| ¿Se realiza backups y se tiene definido el tiempo de retención? |  |  |  |  |
| ¿Se cuenta con logs de auditoría a nivel de las plataformas tecnológicas, base de datos y sistema de información? |  |  |  |  |
| 1. **Ataques cibernéticos** |  |  |  |  |
| ¿Cuenta con protección del Firewall? |  |  |  |  |
| ¿Cuenta con protección del Antivirus? |  |  |  |  |
| ¿Cuenta con protección del IPS? |  |  |  |  |
| ¿Cuenta con protección ante ataques de denegación de servicio (DDOS)? |  |  |  |  |
| ¿Cuenta con protección del WAF? |  |  |  |  |
| ¿El sistema de información cuenta con separación de ambientes? |  |  |  |  |
| ¿Se han realizado pruebas de vulnerabilidad al sistema de información? |  |  |  |  |
| 1. **Integridad de las comunicaciones** |  |  |  |  |
| ¿Se utiliza controles de cifrado en el intercambio de información, por ejemplo, HTTPS, Tokens, SSH, ¿entre otros? |  |  |  |  |
| ¿Se utiliza certificados digitales? |  |  |  |  |
| 1. **Acuerdos con terceros** |  |  |  |  |
| ¿Se cuenta con acuerdos de nivel de servicio (ANS) y obligaciones de confidencialidad de la información con los proveedores que intervienen en el sistema de información? |  |  |  |  |
| 1. **Actualizaciones** |  |  |  |  |
| ¿Se aplican oportunamente los parches que libera el fabricante a nivel de base de datos y servidores? |  |  |  |  |
| 1. **Gestión de cambios** |  |  |  |  |
| ¿Los cambios sobre el sistema de información surten el procedimiento de cambios? |  |  |  |  |
| ¿Se maneja un control de las versiones del sistema de información? |  |  |  |  |
| 1. **Pruebas de carga** |  |  |  |  |
| ¿Se realiza una planificación de los recursos de hardware y software requeridos para el sistema de información? |  |  |  |  |
| ¿El sistema de información ha sido sometido a pruebas de carga y estrés? |  |  |  |  |
| ¿Se ha realizado un aseguramiento (Hardening) a los servidores y bases de datos que soportan el sistema de información o plataforma tecnológica? |  |  |  |  |
| 1. **Monitoreo** |  |  |  |  |
| ¿El normal funcionamiento del sistema de información o plataforma tecnológica se encuentra monitoreado? |  |  |  |  |
| ¿Se cuenta con un esquema proactivo para el monitoreo de eventos y alertas? |  |  |  |  |
| 1. **Autenticación** |  |  |  |  |
| ¿El sistema de información cumple con la política de seguridad para contraseñas de usuarios? |  |  |  |  |
| ¿Cómo se almacenan las contraseñas de los usuarios en la Base de Datos? ¿Cifradas? |  |  |  |  |
| ¿El sistema de información cuenta con controles para mantener la seguridad de la sesión del usuario? Por ejemplo, protección contra múltiples sesiones, tiempo límite de inactividad, manejo adecuado de cookies. |  |  |  |  |
| 1. **Segregación de funciones** |  |  |  |  |
| ¿Se cuenta con la asignación de roles y responsabilidades bien definidas para la administración del sistema de información? |  |  |  |  |
| ¿Se verifica periódicamente el listado de personas autorizadas dentro del sistema de información? |  |  |  |  |
| ¿Se cuenta con un procedimiento claro y bien definido para otorgar permisos de acceso al sistema? |  |  |  |  |

| 1. **GUÍA HARDENING** | |
| --- | --- |
| **Nombre Sistema Operativo o plataforma tecnológica:**  ***(Nombre del servidor, plataforma tecnológica y versión)***  **Versión:**  ***(versión)*** | **Tomado de:**  ***(Nombre de la guía que se usa para la configuración de seguridad y nardening ej.:*** ***CIS NGINX Benchmark v2.0.1 - 06-15-2023)*** |

|  |
| --- |
| **Nota**: Los siguientes campos se deben diligenciar de acuerdo con la cantidad de controles de la guía que se utilice para la configuración de seguridad de la información o hardening de la plataforma tecnológica o sistema de información. |
| **Control: *(Número de control aplicado y nombre del control)*** |
| **Descripción: *(Descripción del control)*** |
| **Razón fundamental:**  ***(Los principales beneficios de usar)*** |
| **Auditoría:**  ***(Validación para revisar que el control se está ejecutando/gestionado en la plataforma o sistema)*** |
| **Remediación:**  ***(Donde la guía indica cómo se cierra la brecha de seguridad)*** |
| **Referencias:**  ***(Sitios de donde se tomó la información o guía con la que se ejecutó el hardening).***  ***http://nginx.org/en/docs/install.html*** |
| **Información adicional:**  ***(Descripción de información adicional que se deba contemplar o exponer)*** |
| **Evidencias de la aplicación del control:**  ***(Pantalla o documento que muestre las evidencias de la aplicación del control)*** |
| **Control: *(Número de control aplicado y nombre del control)*** |
| **Descripción: *(Descripción del control)*** |
| **Razón fundamental:**  ***(Los principales beneficios de usar)*** |
| **Auditoría:**  ***(Validación para revisar que el control se está ejecutando/gestionado en la plataforma o sistema)*** |
| **Remediación:**  ***(Donde la guía indica cómo se cierra la brecha de seguridad)*** |
| **Referencias:**  ***(Sitios de donde se tomó la información o guía con la que se ejecutó el hardening).***  ***http://nginx.org/en/docs/install.html*** |
| **Información adicional:**  ***(Descripción de información adicional que se deba contemplar o exponer)*** |
| **Evidencias de la aplicación del control:**  ***(Pantalla o documento que muestre las evidencias de la aplicación del control)*** |