|  |  |
| --- | --- |
| **Fecha:** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **RESPONSABLE DE LA INSPECCIÓN** | | | |
| **Nombre:** |  | **Cédula:** |  |
| **Cargo:** |  | | |

|  |  |
| --- | --- |
| **INFORMACIÓN DEL ALCANCE** | |
| **Sistema de información o elementos de la plataforma tecnológica** | **Grupo de trabajo responsable del sistema:** |
|  |  |
| **Colaboradores asignados:** | |
|  | |

| **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 un esquema de contingencia de las diferentes capas del sistema de información? |  |  |  |  |
| ¿Se realiza backups y se tiene definido el tiempo de retención? |  |  |  |  |
| * ¿Se cuenta con backup de las personas claves para la operación del sistema de información? |  |  |  |  |
| * Backup de Servidores. |  |  |  |  |
| * Backup de Base de Datos. |  |  |  |  |
| ¿Se cuenta con logs de auditoría a nivel de base de datos y de aplicación? |  |  |  |  |
| 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? |  |  |  |  |
| ¿Se aplican los parches a un intervalo planificado? |  |  |  |  |
| 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? |  |  |  |  |
| 1. **Monitoreo** |  |  |  |  |
| ¿El normal funcionamiento de la aplicación 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 protección contra ataques de fuerza bruta en su diseño? |  |  |  |  |
| ¿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? |  |  |  |  |