|  |  |  |
| --- | --- | --- |
| **INFORMACIÓN DEL USUARIO** | | |
| **Nombre:** |  | **Cédula:** |
| **Sistema de información:** |  | **Fecha análisis línea base:**  **Fecha verificación de cumplimiento:** |
| **INSTRUCCIÓN DEL DILIGENCIAMIENTO** | | |
| De la siguiente lista, **marque con una X** de acuerdo con la siguiente instrucción:   1. Al finalizar las actividades de análisis y definición de requisitos de seguridad de la información, seleccione:  * **Aplica**: en caso de que el requisito se vaya a implementar en el desarrollo del sistema de información. * **No aplica**: en caso de que le jefe de la OTI haya autorizado la exclusión del requisito.  1. Al finalizar la actividad de implementación de requisitos de seguridad de la información, seleccione:  * **Cumple:** en caso de evidenciar que el requisito de seguridad fue correctamente implementado en el sistema de información. * **No cumple:** en caso de evidenciar que el requisito de seguridad de la información no fue implementado satisfactoriamente.   Igualmente, registre las observaciones que considere necesarias al final del formato. | | |

| **No.** | **Requisito de seguridad de la información** | **Tipo de requisito** | **Análisis línea base** | | **Verificación de cumplimiento** | |
| --- | --- | --- | --- | --- | --- | --- |
| **Aplica** | **No aplica** | **Cumple** | **No cumple** |
| 1 | Aplicar el principio de privilegio mínimo. | Acceso. |  |  |  |  |
| 2 | Verificar que los controles de acceso fallen de forma segura. | Manejo de excepciones. |  |  |  |  |
| 3 | Gestión de usuarios, grupos de usuarios, asignación de roles y perfiles. | Perfil de usuario. |  |  |  |  |
| 4 | Mostrar la última fecha y hora de ingreso. | Sesión de usuario. |  |  |  |  |
| 5 | Permitir a un usuario estar asociado a uno o más roles. | Privilegios de usuario. |  |  |  |  |
| 6 | Generar informe con los usuarios activos. | Gestión de usuarios. |  |  |  |  |
| 7 | Trazabilidad de las acciones realizadas por los usuarios. | Auditorías de usuarios. |  |  |  |  |
| 8 | Para usuario internos: integración con Active Directory.  Para usuarios externos: módulo de seguridad del sistema de información. | Acceso. |  |  |  |  |
| 9 | Protección y autorización de uso de datos personales. | Protección de datos personales. |  |  |  |  |
| 10 | Autenticación secreta de usuario. | Autenticación segura y secreta. |  |  |  |  |
| 11 | Controles de bloqueo de cuenta de usuario. | Bloqueo de usuarios. |  |  |  |  |
| 12 | Uso de técnicas de construcción seguras en el desarrollo de la aplicación. | Patrones de desarrollo. |  |  |  |  |
| 13 | Cerrar transacciones por inactividad. | Sesiones seguras. |  |  |  |  |
| 14 | El identificador de sesión nunca se revela. | Confidencialidad. |  |  |  |  |
| 15 | Toda nueva autenticación genera un nuevo identificador de sesión. | Sesiones seguras. |  |  |  |  |
| 16 | Los identificadores de sesión son largos, aleatorios y únicos. | Sesiones seguras. |  |  |  |  |
| 17 | Límite en el número de sesiones por usuario. | Sesiones únicas. |  |  |  |  |
| 18 | Visualización de sesiones activas. | Sesiones seguras. |  |  |  |  |
| 19 | Opción de terminar otras sesiones activas. | Sesiones únicas. |  |  |  |  |
| 20 | Las fallas de validación de entradas de datos son rechazadas y registradas. | Manejo de Logs. |  |  |  |  |
| 21 | Rutinas de validación de entradas de datos del lado del servidor. | Validación de datos de entrada en formularios. |  |  |  |  |
| 22 | Protección contra inyección de SQL. | Transacciones seguras. |  |  |  |  |
| 23 | Protección contra inyección LDAP. | LDAP seguro. |  |  |  |  |
| 24 | Protección contra Cross-Site Scripting (XSS). | Asegurar HTML. |  |  |  |  |
| 25 | Almacenamiento en caché desactivado. | No cache. |  |  |  |  |
| 26 | Información sensible es enviada al servidor en el cuerpo o cabeceras del mensaje HTTP. | Envío seguro de datos. |  |  |  |  |
| 27 | Los datos almacenados en el cliente no contienen información sensible. | Sesiones seguras. |  |  |  |  |
| 28 | Los archivos enviados a la aplicación no son utilizados por comandos de I/O (Entrada/Salida). | Escanear variables de entrada. |  |  |  |  |
| 29 | Los archivos cargados por el usuario son analizados por el antivirus. | Upload seguro. |  |  |  |  |
| 30 | Datos no confiables, no se utilizan en recursos de dominios compartidos. | Upload seguro. |  |  |  |  |
| 31 | Uso de certificados digitales internos, en sistemas consultados al interior de la entidad.  Uso de certificados digitales válidos públicamente, en sistemas expuestos a internet. | SSL en la aplicación. |  |  |  |  |
| 32 | Uso de autenticación de doble factor en aplicaciones core del negocio. | Autenticación segura. |  |  |  |  |
| 33 | Cifrado de los datos que se transportan entre capas. | Cifrado en interoperabilidad. |  |  |  |  |
| 34 | Métodos HTTP no utilizados (por ejemplo: TRACE, PUT y DELETE) se encuentran bloqueados. | Request seguro. |  |  |  |  |
| 35 | Uso de versiones de software más recientes. | Diseño y cumplimiento de SLA. |  |  |  |  |
| 36 | Aplicación desarrollada sobre el estándar IPv6 con compatibilidad para IPv4. | IPv6 / IPv4. |  |  |  |  |
| 37 | Verificar ataques comunes de XML | Entidades externas XML. |  |  |  |  |
| 38 | No aceptar objetos serializados de fuentes no confiables. | Deserialización insegura. |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Los siguientes requisitos son propuestos por el ***Grupo de Trabajo de Informática Forense y Seguridad Digital***, seleccione **aplica** o **no aplica**, según el resultado de la revisión y concertación con el grupo de trabajo responsable del desarrollo. | | | | | | | |
| **No**. | **Requisitos adicionales de seguridad de la información.** | **Tipo de requisito** | | **Análisis del requisito** | | **Verificación de cumplimiento** | |
| **Aplica** | **No aplica** | **Cumple** | **No cumple** |
| 1 |  |  | |  |  |  |  |
| 2 |  |  | |  |  |  |  |
| 3 |  |  | |  |  |  |  |
| 4 |  |  | |  |  |  |  |
| 5 |  |  | |  |  |  |  |
| **OBSERVACIONES** | | | | | | | |
|  | | | | | | | |
| **FIRMAS** | | | | | | | |
| **Nombre:**  **Firma:**  **Cargo:** Ingeniero desarrollador. | | | **Nombre:**  **Firma:**  **Cargo:** Supervisor o Coordinador del grupo de trabajo responsable del desarrollo. | | | | |
| **Nombre:**  **Firma:**  **Cargo: *Coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital*** | | | | | | | |