|  |
| --- |
| **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.

**Nota**: Igualmente, registre las observaciones que considere necesarias al final del formato. Esto teniendo en cuenta que, “…cualquier exclusión de requisitos de la línea base, es comunicada, justificada y aprobada…” (Ver documento del Procedimiento Requisitos y Pruebas de seguridad en el desarrollo de sistemas de información GS03-P05). |

| **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 | Generar informe con los usuarios activos. | Gestión de usuarios. |  |  |  |  |
| 6 | Trazabilidad de las acciones realizadas por los usuarios. | Auditorías de usuarios. |   |  |   |   |
| 7 | Para usuario internos: integración con Active Directory. Para usuarios externos: módulo de seguridad del sistema de información.  | Acceso. |   |  |   |   |
| 8 | Protección y autorización de uso de datos personales. | Protección de datos personales. |   |  |   |   |
| 9 | Autenticación secreta de usuario.  | Autenticación segura y secreta. |   |  |   |   |
| 10 | Controles de bloqueo de cuenta de usuario. | Bloqueo de usuarios. |   |  |   |   |
| *11* | *Implementar un captcha como requisito de ingreso.* | *Captcha.* |  |  |  |  |
| 12 | Cerrar transacciones por inactividad. | Sesiones seguras. |   |  |   |   |
| 13 | El identificador de sesión nunca se revela. | *Sesiones seguras.* |  |  |  |  |
| 14 | Toda nueva autenticación genera un nuevo identificador de sesión. | Sesiones seguras. |  |  |  |  |
| 15 | Los identificadores de sesión son largos, aleatorios y únicos. | Sesiones seguras. |  |  |  |  |
| 16 | Límite en el número de sesiones por usuario. | Sesiones únicas. |  |  |  |  |
| 17 | Visualización de sesiones activas. | Sesiones seguras. |  |  |  |  |
| 18 | Opción de terminar otras sesiones activas. | Sesiones únicas. |  |  |  |  |
| 19 | Validación de entradas de datos. Todas las fallas son rechazadas y registradas. | Manejo de Logs. |  |  |  |  |
| 20 | *Validación de datos de entrada en formularios* | Validación de datos de entrada en formularios. |  |  |  |  |
| 21 | Protección contra inyección de SQL. | Transacciones seguras. |  |  |  |  |
| 22 | Protección contra Cross-Site Scripting (XSS). | Asegurar HTML. |  |  |  |  |
| 23 | *Headers y cookies seguros configurados.* | headers |  |  |  |  |
| 24 | Información sensible es enviada al servidor en el cuerpo o cabeceras del mensaje HTTP. | Envío seguro de datos. |  |  |  |  |
| 25 | Limitar tipos de archivos que pueden ser enviados a la aplicación. | Escanear variables de entrada. |  |  |  |  |
| 26 | 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. |  |  |  |  |
| 27 | Métodos HTTP no utilizados (por ejemplo: TRACE, PUT y DELETE) se encuentran bloqueados. | Request seguro. |  |  |  |  |
| 28 | Uso de versiones de software más recientes. | *Versiones actualizadas* |  |  |  |  |
| 29 | Aplicación desarrollada sobre el estándar IPv6 con compatibilidad para IPv4. | IPv6 / IPv4. |  |  |  |  |

|  |
| --- |
| 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*** |