Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente



SEGURIDAD DE LA

INFORMACIÓN

Este documento ha sido elaborado por Agesic (Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento).

El Marco de Ciberseguridad es un conjunto de requisitos (requisitos normativos y buenas prácticas) que se entienden necesarios para la mejora de la seguridad de la información y la ciberseguridad.

Usted es libre de copiar, distribuir, comunicar y difundir públicamente este documento, así como hacer obras derivadas, siempre y cuando tenga en cuenta citar la obra de forma específica.

Requerimientos de Seguridad de la información para adquisición de soluciones

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | 3.0 | **Categoría** | - |
| **Última actualización** | 19/11/2019 | **Estado** | Aprobado |

A continuación, se listan los requerimientos generales, los requisitos de firma electrónica y los requisitos operativos a contemplar en los pliegos de adquisición de soluciones.

**Requerimientos generales de seguridad**

|  |  |  |  |
| --- | --- | --- | --- |
| **Nro** | **Requerimiento** | **Contexto de aplicación** | **Justificación** |
| 1 | El sistema deberá cumplir con los protocolos de seguridad de la REDuy en los puntos de comunicación con la misma. | Todos los casos. | N/A |
| 2 | Integración con el sistema de seguridad de la PGE para la autenticación, autorización y auditoría de usuarios. Especialmente con sistema de uso de la cédula electrónica. | Todo sistema que realice autenticación de usuarios en el contexto de trámites ciudadanos | Uniformizar el acceso a las aplicaciones con una perspectiva orientada al ciudadano.  Habilitar la autenticación con el documento de identidad electrónica. |
| 3 | Utilización de canales de comunicación seguros entre módulos y/o componentes externos e internos. | Toda infraestructura o aplicación distribuida. | Se debe garantizar la confidencialidad e integridad en la transmisión de datos entre componentes. Decreto 92/014. |
| 4 | El sistema deberá utilizar un esquema de autorización basado en roles (RBAC) | Todos los casos. | Es el mecanismo recomendable para la gestión de usuarios y permisos. |
| 5 | Asignación de permisos a roles parametrizables (agregado del punto anterior) | Manejo detallado sobre permisos de los roles. | Este requerimiento puede ser deseable en la medida que se necesite establecer o adaptar los permisos asignados a los distintos roles que eventualmente cambian con el tiempo. |
| 6 | El sistema deberá contar con las herramientas de seguridad para garantizar la confidencialidad, integridad y autenticidad de los datos. El oferente deberá explicar cómo se implementan los aspectos antes mencionados a nivel de operación y a nivel de administración | Todos los casos. En particular aquellos de criticidad media y alta. | Conocer como el sistema almacena, transmite y manipula los datos garantizando la confidencialidad, integridad y autenticidad. |
| 7 | El sistema deberá contar con mecanismos de auditoría para todas las transacciones llevadas a cabo por el mismo. | Todos los casos. | En todos los casos se debe poder hacer una auditoría de las operaciones sobre el sistema. Esto garantiza transparencia y facilita las actividades de “investigación” ante un incidente de seguridad informática. |
| 8 | Se debe poder establecer las operaciones a auditar, e información a registrar para las mismas, incluyendo si fueron exitosas o fallidas. | Todos los casos. | Configurar conforme necesidades específicas los registros que se desean auditar. |
| 9 | Se debe poder establecer la marca de tiempo para los registros de auditoría de todas las operaciones. | Todos los casos. | Los registros de logs siempre deben tener marca de tiempo para poder correlacionar datos. |
| 10 | Se debe poder establecer para cada registro de auditoría la identificación unívoca del usuario que realiza las operaciones en los logs de auditoría; además la dirección IP y puerto de origen. | Todos los casos. | Poder identificar el usuario que efectuó la operación. |
| 11 | Poder establecer los tiempos de rotación y retención de los registros de auditoría. | Todos los casos. | Poder mantener el registro de eventos del sistema de una manera eficiente. |
| 12 | Poder establecer el envío de registros de auditoría por syslog (estándar) a un servidor externo. | Todos los casos. | Consolidación y correlación de logs. |
| 13 | El sistema deberá considerar las actividades de parametrización como operaciones a ser registradas. | Todos los casos. | Completitud en la traza de actividades. |
| 14 | El proveedor deberá indicar cuál es la seguridad implementada a nivel de logs de auditoría | Todos los casos. | Se debe saber que tanto se cuida la integridad de los logs, en particular para saber qué tan modificables son y si queda registro de dichas modificaciones. |
| 15 | Se debe cumplir con las buenas prácticas estipuladas en el top 10 de OWASP. | En particular sistemas web. | Es una buena práctica para asegurar el desarrollo de sistemas, en particular los web, y disminuir las vulnerabilidades inherentes a todas las aplicaciones. |
| 16 | Cifrado de información sensible que sea persistente en base de datos en forma independiente para diferentes usuarios u organismos (por ejemplo clave pública/privada). | Sistemas con información crítica y/o sensible. | Se debe poder garantizar la integridad y confidencialidad de la información sensible. |
| 17 | Ante incidentes de seguridad del producto y sus componentes se debe notificar a CERTuy | Ante incidentes de seguridad informática que sufran los sistemas de información que maneje el organismo, se debe solicitar su notificación inmediata por parte del proveedor al organismo. Quedando en manos del organismo la notificación al CERTuy. | Según lo establece decreto 451/009 |
| 18 | El proveedor deberá contar una contraparte especialista para consultas técnicas y de seguridad. | Todos los casos. | Tener una vía de comunicación identificada. |
| 19 | La aplicación deberá funcionar correctamente cuando ésta se encuentre  publicando servicios a través de un WAF (Web Application Firewall por  sus siglas en inglés) implementado típicamente sobre apache/mod\_security con las reglas de filtrando provistas por la comunidad OWASP (OWASP Core  Ruleset) y en modalidad bloqueante.  Si la aplicación no funcionase correctamente detrás del WAF, AGESIC podrá solicitar que se reprograme la aplicación o que el proveedor proporcione las excepciones a las reglas del WAF si lo considerase apropiado, dichas reglas deberán contar con la conformidad de AGESIC y/o el organismo. | Todo sistema web. Obligatorio para los vinculados a trámites en línea. | Proteger los sistemas expuestos a Internet. |
| 20 | La aplicación deberá permitir la autenticación con Usuario Gub.uy, o en su defecto la configuración de una política de usuarios y contraseñas. Dicha política debe poder soportar funciones básicas ABM y bloqueo de usuarios, así como caducidad, longitud y complejidad de contraseñas. Los usuarios deben poder cambiar sus contraseñas. | Todos los casos. |  |
| 21 | Cierre de sesión: Se deben suministrar opciones de desconexión o cierre de sesión (logout) que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación. | Todos los casos. |  |
| 22 | Manejo de información sensible propia del sistema: Se debe garantizar que el software desarrollado no divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.  No se debe mostrar información innecesaria, como por ejemplo, en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado. | Todos los casos. |  |
| 23 | Seguridad a nivel de ambiente: El software desarrollado no debe poder ejecutar comandos directamente en el sistema operativo. | Todos los casos. |  |
| 24 | Validación de datos: Las aplicaciones desarrolladas deben ser construidas de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación, en lo posible centralizadas y estandarizadas.  Se debe asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros. | Todos los casos. |  |

**Requerimientos de firma electrónica**

Estos requerimientos aplican a cualquier sistema que necesite realizar una firma electrónica avanzada de persona física o jurídica.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nro** | **Requerimiento** | **Contexto de aplicación** | **Justificación** |  |
| 1 | El sistema deberá contar con los mecanismos para realizar firmas electrónicas basadas en certificados electrónicos X509v3. | Todos. | Es el estándar que utiliza firma electrónica avanzada. Garantiza compatibilidad. |
| 2 | En caso de tratarse de firmas de usuarios el mecanismo de firma deberá estar integrado a la transacción del usuario. | Todos. | Facilidad de uso para el usuario. |
| 3 | En caso de tratarse de firmas a nivel de servidor, se debe garantizar la adecuada protección de la clave privada. | Sistema que genere documentación de forma automática con la necesidad de firma. | Garantizar la integridad de las operaciones. |
| 4 | Deberá contar con mecanismos de validación de firmas y de certificados electrónicos. | Cualquier sistema que realice firmas de usuario o de servidor, o cualquier sistema que reciba documentación firmada. | Procesar firmas sin validar no tiene sentido en ningún contexto. |
| 5 | Deberá poder hacer uso de certificados electrónicos emitidos por cualquier prestador de servicio de certificación acreditados ante la UCE, siguiendo todos los lineamientos de dicha unidad. | Todo sistema que utilice certificados. | Todos los sistemas desarrollados para organismos del estado deben poder hacer uso de Firma Electrónica Avanzada (ley 18600) emitida por cualquier prestador acreditado. |
| 6 | Se debe soportar la autenticación de usuarios y firmas electrónicas de documentos utilizando la cédula digital. Evaluar la integración al servicio brindado por AGESIC. | Todos. | La cédula electrónica es un elemento de identificación de aplicación nacional. |
| 7 | Deberá soportar el uso de dispositivos criptográficos para la firma electrónica (tokens, smart cards, HSM, etc.) | Todos los casos de uso de firma. | El marco regulatorio exige que se utilicen dispositivos criptográficos para firma de personas físicas. |
| 8 | Se deberán utilizar estándares y protocolos seguros que no estén considerados obsoletos o vulnerables. | Todos los casos de uso de firma. | Vigencia tecnológica. |
| 9 | Se deberán utilizar los estándares de codificación de firmas propios de los tipos de documentos firmados (XADES, PDFSignature, etc.). | Todos los casos de uso de firma. | Utilizar estándares garantiza compatibilidad. |
| 10 | Cuando no exista un formato de firma para el documento, se deberá utilizar CMS-CAdES. | Todos los casos de uso de firma. | Utilizar estándares garantiza compatibilidad. |
| 11 | Validación de certificados a través de OCSP (Online Certificate Status Protocol), CRL (Certificate Revocation List) o equivalente. | Todos los casos de uso de firma. | Es parte de la operativa de firma. Lo importante es que el proveedor especifique como realiza la validación. |
| 12 | Debe ser compatible con el RFC 3161 para la solicitud de sellos de tiempo tanto sobre HTTP como sobre TCP, y debe poder realizar firmas electrónicas incluyendo sellos de tiempo (con el formato del RFC 3161). | Cuando se necesita dejar constancia de fecha y hora de la firma, o si se necesita firma longeva. | Es el estándar que debe utilizarse, ya que es el más utilizado a nivel mundial. Garantiza compatibilidad. |
| 13 | Deberá describir la solución diseñada para la firma de las transacciones. | Todos los casos de uso de firma, en particular con las transacciones críticas del sistema. | Poder validar la operativa. |

**Requerimientos** **operativos**

Pautas de seguridad mínimas que deberá seguir el proveedor en el desarrollo del proyecto.

|  |  |  |  |
| --- | --- | --- | --- |
| **Nro** | **Requerimientos** | **Contexto de aplicación** | **Justificación** |
| 1 | Separación de ambientes | Todos los casos | En organizaciones donde se desarrollan o modifican sistemas es crucial la aplicación de actividades de control a fin de minimizar los riesgos derivados de incidentes accidentales o deliberados en los sistemas en producción, que pueden impactar negativamente en el desempeño de los mismos o en la información que procesan.  Estos controles administrativos deberán estar apoyados por herramientas de hardware y software que permitan la creación de ambientes que garanticen que cualquier cambio a un sistema o software sea realizado en el contexto adecuado, sea suficientemente probado y validado y se instale en producción en forma correcta.  Es por eso que se deberán crear al menos tres ambientes definidos e independientes: Desarrollo, Testing y Producción, así como la definición de los procedimientos y controles administrativos que permitan que el pasaje de un ambiente a otro se haga de manera adecuada y controlada. |
| 2 | Segregación de roles. | Todos los casos. | Un aspecto fundamental en la separación de ambientes de desarrollo de sistemas es la segregación de funciones. Esta consiste en distribuir adecuadamente las funciones y tareas, de tal manera de generar control por oposición, de forma que una persona no tenga la posibilidad de cometer u ocultar errores o fraudes en el transcurso normal de su trabajo. Existen tareas que no son compatibles para que la realice una sola persona, como ser las tareas de autorización, ejecución, registro, custodia de los activos, etc. Específicamente en lo que se refiere a desarrollo de sistemas, es importante segregar las actividades de los desarrolladores de la de los testers y administradores de sistemas. |
| 3 | Gestión de cambios. | Todos los casos. | Se debe tener en cuenta también, que aunque se hayan agotado todas las instancias para reducir el riesgo de que un cambio impacte negativamente en el sistema de producción, puede darse que esto ocurra, por lo que el proceso de gestión de cambios debe prever un mecanismo de vuelta a atrás (rollback) en caso de ser necesario.  Estos mecanismos deben ser probados en el ambiente de testing en todos los casos. |
| 4 | Acceso administrativo a través de una VPN | Únicamente en los casos que se justifique un acceso administrativo remoto. | El acceso administrativo necesario para mantener y operar la infraestructura no debe estar disponible desde Internet. Para aquellos casos en los que se requiera administración remota deberá implementarse dicho acceso a través de una VPN administrativa configurada para tal fin. En el mismo sentido, el acceso a estas interfaces debería estar restringido al mínimo de ubicaciones (o direcciones origen) necesario. En condiciones ideales debería preverse una red administrativa y habilitarse el acceso a estas interfaces solamente desde dicha red. En caso de no ser posible esta arquitectura de red, debería limitarse al mínimo el número de direcciones habilitadas para acceso administrativo. |

