GUÍA Y LINEAMIENTOS PARA DESARROLLO SEGURO

Proceso: Gestión de Información y Soporte Tecnológico.

Versión 1
08/01/2016

Tabla de contenido

OBJETIVO

Brindar herramientas y lineamientos necesarios para tener en cuenta para el desarrollo de los Sistemas de Información del Ministerio de Ambiente y Desarrollo Sostenible en cuanto a Seguridad de la Información.

ALCANCE Y APLICABILIDAD DEL PRESENTE DOCUMENTO

Proveer los lineamientos y/o directrices referentes a la Seguridad de la Información que se requiere para con el fin de llevar a cabo la planeación, desarrollo, implementación, uso, operación y demás actividades necesarias para la adquisición o desarrollo de un Sistema de Información en el Ministerio de Ambiente y Desarrollo Sostenible.

POLÍTICA GENERAL

Para apoyar los procesos operativos y estratégicos el Ministerio de Ambiente y Desarrollo Sostenible usará y facilitará las Tecnologías de la Información y las Comunicaciones para el mejoramiento o implementación de nuevos procesos para en consecuencia cumplir con los objetivos y cubrir las necesidades de la entidad. Ahora bien, los Sistemas de Información a usar pueden ser adquiridos a través de terceras partes bien sea en desarrollos a la medida o mediante herramientas comerciales o no comerciales que satisfagan la necesidad que se pretende subsanar siempre y cuando estén cumplan con los lineamientos establecidos por la Oficina TIC y la Arquitectura Empresarial (acorde a los lineamientos de Gobierno en Línea). Igualmente, se pueden implementar y mantener Sistemas de Información desarrollados por personal del Ministerio.

Acorde a lo anterior y con el fin de adoptar de forma eficiente el desarrollo de Sistemas de Información, la Oficina de Tecnologías de la Información y Comunicación TICS y el Grupo de Sistemas deben elegir, elaborar, mantener y difundir el “Método de Desarrollo de Sistemas de Información” que considere apropiado o los requerimientos que apliquen, de acuerdo con los lineamientos aquí expuestos y a las funciones operativas y capacidades técnicas y de plataforma que existan al interior de MADS. Cuándo la necesidad de un Sistema de Información sea manifiesta se debe garantizar que éste incluya lineamientos, procesos, buenas prácticas, plantillas, soporte y demás obligaciones que sirvan para regular los desarrollos de Software internos, teniendo en cuenta la mitigación de riesgos

y el aseguramiento de la calidad definido, así mismo se deben identificar y gestionar los posibles riesgos referentes a Seguridad de la Información durante todo el ciclo de vida del Software.

En la medida de lo posible y según la legislación colombiana lo permita, los sistemas de información adquiridos a través de terceras partes deben siempre certificar el cumplimiento de estándares de calidad en el proceso de desarrollo.

REQUERIMIENTOS DE DESARROLLO

Se deben tener presente los siguientes ítems durante la fase de análisis de requerimientos de Sistemas de Información (Desarrollo):

- Se deben identificar riesgos del nuevo desarrollo.
- Se debe, en lo posible, solicitar garantía general acerca de bugs (Errores en la operación del Software) y flaws (Errores en el diseño y análisis de requerimientos de la aplicación).
- En caso de que el Software sea pre-elaborado, verificar que se cubren las necesidades tanto actuales como a corto plazo.
- Verificar que los requerimientos del Software y sus requerimientos funcionales cumplen con la legislación colombiana vigente.

a) Proceso de suministro: define las actividades del proveedor, organización que proporciona un sistema y el producto Software o servicio Software al adquiriente. Obligatoriamente la seguridad debe incluirse en el diseño de todas las capas de arquitectura (negocio, datos, aplicaciones y tecnología) equilibrando la necesidad de seguridad de información, con la necesidad de accesibilidad. Igualmente, la tecnología se debe analizar para determinar los riesgos para en cuanto a Seguridad, y el diseño se debería revisar contra patrones y definiciones conocidos (virus, ataques).

   - Dentro del proceso de suministro el proveedor debe entregar como mínimo un Manual de Usuario, que contenga adicionalmente las explicaciones funcionales para los usuarios finales), Manual Detallado del Sistema de Información, que incluya los requerimientos de instalación, la infraestructura, los pasos de instalación, la arquitectura de la base de datos y de la aplicación y los diagramas de componentes).
   - Todos los productos de Software que se adquieran e instalen en los equipos de cómputo del Ministerio deben contar con su respectiva licencia de uso. Se deben definir las características de licenciamiento (Comercial – vigencia, GNU, libre, por uso, por demanda).
   - Definir la entrega del Software (Se debe entregar instalador, y el Software debe quedar correctamente montado y configurado).
   - La aplicación debe ser modelada mínimamente con base en un Modelo de

entidad/relación, Estructura de Base de Datos, Diccionario de Datos, Casos de Uso, Casos de Abuso y Diagrama de Clases. [Verificar aplicabilidad dependiendo del caso de Software a adquirir]

b) Proceso de desarrollo (apartado 5.3): define las actividades del desarrollador, y como es requerido por parte de la organización, la definición y el desarrollo del producto de Software. Adicionalmente se debe tener presente los siguientes ítems:

- El Ministerio de acuerdo con su infraestructura y necesidades, puede exigir determinado lenguaje de programación previa evaluación interna de acuerdo a los lineamientos dados por Arquitectura Empresarial
- Se deben definir las necesidades de infraestructura y la segregación de capas que la aplicación requiera.
- Para la recepción de aplicaciones se debe revisar el listado de verificación llamado "Requisitos para la recepción de aplicaciones (Hand Over)".

c) Proceso de operación (apartado 5.4): define las actividades del operador y la organización esperada que proporciona el servicio de operar un sistema informático en su entorno real, para sus usuarios. Se deben realizar todas las pruebas necesarias para verificar su seguridad, tales como: casos de abuso, puertas traseras, recomendaciones y pruebas de seguridad de los navegadores (browser), pruebas de ethical hacking, y las demás pruebas derivadas de las metodologías y buenas prácticas anteriormente mencionadas. También se requiere la entrega de informes detallados de las pruebas realizadas y sugerencias. Adicionalmente se debe tener presente los siguientes ítems:

- Para la puesta en operación se debe realizar previamente una fase de prueba en un entorno diferente al de producción. Las pruebas deben incluir respuesta de operación y cumplimiento de funciones de acuerdo con lo planeado y pruebas de rendimiento (carga y stress).
- Las pruebas acerca de la operación y correcto funcionamiento se deben ejecutar con el usuario final y se debe documentar su aceptación o cambios.
- En caso de que se requieran pruebas con bases de datos e información del Ministerio, éstas deben contener información transformada, cambiada, alterada o entrecruzada procurando distorsionar la información, para que las pruebas sean lo más completas posibles

d) Proceso de mantenimiento: define las actividades del responsable de mantenimiento, y la organización que proporciona el servicio de mantenimiento del producto Software; esto es, la gestión de las modificaciones al producto Software para mantenerlo actualizado y operativo. De la misma forma, la información tratada por las aplicaciones aceptadas por el Ministerio, debe preservar la confiabilidad desde su ingreso, transformación y entrega a las aplicaciones

de la Entidad. Este proceso incluye la migración y retirada del producto Software. Adicionalmente se debe tener presente los siguientes ítems:

- Definir las características y necesidades del Software en caso de que una migración sea requerida.
- Se debe tener en cuenta el proceso de apagado o fin de servicio de la aplicación entre lo cual se debe definir claramente la entrega y almacenamiento de la información.

Las principales características de los Sistemas de Información, para el tema de Seguridad de la Información se describen a continuación. Se aclara que estas características son mandatorias para cualquier sistema que sea implementado al interior de MADS:

1. Control de acceso a la aplicación con autenticación simple, doble o triple dependiendo de la criticidad:

   - En caso de que se requiera contraseña, se debe garantizar un control por defecto que garantice el uso de contraseñas seguras (que contenga mayúsculas, minúsculas, números y al menos un carácter especial y su longitud no puede ser menor a 8 dígitos).
   - En lo posible se debe automatizar el requerimiento de cambio de clave periódico.
   - Debe tener un control ante fallo de autenticación (límite de intentos de validación, bloqueo/desbloqueo de inicio de sesión).

2. Gestión de usuarios y gestión de privilegios:

   - Se debe tener presente el “Principio del Mínimo Privilegio”, es decir, se debe habilitar a los usuarios lo que ineludiblemente requieran para cumplir las funciones del puesto que ocupan (Se debe poder configurar privilegios de lectura, escritura, borrado y edición).
   - Se debe incluir vigencia de activación de la cuenta de usuario (fecha de creación, periodos de suspensión y fecha de uso máximo automatizada).
   - Si aplica: No permitir sesiones simultaneas, bloqueo automático de sesión por inactividad, Historial de acceso (log in / log on).
   - Se debe incluir un botón siempre visible de cerrado de sesión.
   - Los indicadores de sesión no deben estar en las cabeceras de las “cookies”.

3. En caso de que la aplicación sea web, sin que los otros ítems de la presente guía sean excluyentes en cuánto apliquen, se debe considerar:

- EL uso de protocolo SSL – HttPS.
- Procurar que el uso de cookies sea mínimo y se usen solo si es necesario, en caso de que éstas se usen se recomienda que estén cifradas.
- Las URL deben ser limpias, es decir no exponer las variables del código en el enlace.
- Tener en cuenta el top10 de OWASP:
    I. Controles contra inyección de código: límite y validación de campos, codificación de caracteres especiales.
    II. Controles de gestión de sesión y autenticación: ver numeral dos y tres de esta guía.
    III. Controles para evitar el "Cross Side Scripting" (XSS): límite y validación de campos, codificación de caracteres especiales. Si se maneja información de alto nivel sensible o confidencial, es recomendable incluir en la validación de código HTML el uso de listas blancas (negar todo lo que no esté expresamente permitido)
    IV. Referencia Directa Insegura: verificar que a los objetos en referencia se tenga acceso solo por entidades/personas autorizadas para tal fin, además de implementar controles de autenticación si es necesario.
    V. Configuración de seguridad incorrecta: evitar configuraciones por defecto, realizar hardening a infraestructura, verificar que el entorno de pruebas y producción estén configurados idénticamente, pero tengan contraseñas diferentes, verificar parches y actualizaciones en todas las capas del modelo OSI de acuerdo con sus componentes, asegurando una arquitectura con una separación a nivel de Seguridad optima y eficiente para los componentes.
    VI. Exposición de datos sensibles: identificar y etiquetar la información de acuerdo con su sensibilidad y confidencialidad, cifrar el almacenamiento o la transmisión según corresponda en pro de proteger la información, eliminar información innecesaria y deshabilitar la función de autocompletar e inhabilitar cache en los formularios que manejen información sensible.
    VII. Control de acceso inexistente a funciones específicas: se deben eliminar accesos y funciones por defecto, así como también gestionar los accesos y autorizaciones para el uso, procesamiento, almacenamiento o lectura de información. Ver numeral 3 de la presente guía.
    VIII. Falsificación de peticiones en sitios cruzados (CSRF): para evitar que los usuarios sean víctimas de peticiones HTML no autorizadas o que se ejecuten funciones que afecten la integridad de la información, se pueden implementar controles como: captcha, token en url, o re confirmación de datos (ej: ¿Está seguro que desea enviar los datos del formulario? Sí|No).

IX. Uso de componentes con vulnerabilidades conocidas: deshabilitar funciones no actualizadas, realizar análisis periódico de vulnerabilidades y teniendo claro el uso de aplicaciones y sus versiones preparando y revisando la información del proveedor de acuerdo con las actualizaciones y soluciones presentadas, estos estudios se deben realizar antes durante y después de la implementación del Sistema de Información.

X. Redirecciones y reenvíos no validos: en lo posible evitar el uso de redirecciones o reenvíos de direcciones, si se usan verificar que no se expongan los parámetros o que estos no sean modificables.

4. Para el Uso de formularios, se debe considerar:

- Validación de campos y validación de datos de entrada.
- Límite del número de caracteres permitidos.
- Si existe interacción entre usuarios públicos (internet) y la aplicación y se requiere el envío de información y registro de correo electrónico se debe implementar control Captcha 2.0 o superior, con la validación de email habilitada, para evitar el almacenamiento en base de datos de “información borrador” o “información basura”.
- El envio de datos del formulario debe ser método post (oculto en el código).

5. Recomendaciones a nivel de estructuración de código:

- No se deben “quemar” (Dejar contraseñas escritas en el código) contraseñas y usuarios dentro del código. Al igual que direccionamiento IP interno, en el caso de páginas web.
- Tanto las rutas como las URL no deben ser canónicas.
- Evitar las saturaciones de buffer.
- Es recomendable eliminar las notificaciones de error que notifican sobre los servicios o tecnología usada. Se pueden realizar pruebas de inserción de errores para verificar la respuesta de la aplicación ante un error forzado.
- Se debe garantizar que la solución envíe o muestre mensajes relacionados con la propiedad intelectual, protección de datos personales, privacidad y transparencia, tanto a nivel de código como a nivel de despliegue de la aplicación.

6. Se deben establecer controles para cifrar la información que sea considerada sensible y evitar la posibilidad de repudio de una acción por parte de un usuario del sistema. Se deben asegurar los archivos del sistema y mantener un control adecuado de los cambios que puedan

presentarse. Si la aplicación maneja información confidencial, secreta o cubierta por la ley de protección de datos personales se deben evaluar posibles métodos de cifrado siempre y cuando no se afecte en un alto porcentaje el rendimiento del Sistema de Información. Se debe además documentar los roles y accesos que se autoricen a dicha información.

7. Auditoria y Logs

- La aplicación debe almacenar registros automáticos de los cambios y acciones realizadas por usuarios en la aplicación, estos logs deben ser gestionables y deben estar protegidos y en lo posible ser no editables.
- Se deben incluir cláusulas contractuales que informen que el Ministerio podrá realizar supervisar y hacer seguimiento de la actividad de desarrollo de la solución que el contratista o tercero realice a fin de verificar los procedimientos y estándares de desarrollo seguro. Si el desarrollo se realiza en una locación por fuera de las instalaciones, estás pueden llegar a ser objeto auditable por parte del Ministerio en pro de la verificación del trato y uso de la información suministrada.