Requisitos mínimos de Seguridad para la construcción de Sistemas de Información

Oficina de Tecnologías de la Información

Versión 1.0

Objetivo:

Establecer los requisitos mínimos de seguridad para la construcción o adquisición de software por la Unidad para la Atención y Reparación Integral a las Víctimas.

Alcance:

Reconociendo la importancia de implementar elementos de seguridad en cada uno de los sistemas de información que la Unidad requiera construir o adquirir, se listan en este documento los requisitos mínimos de seguridad que deben tenerse en cuenta para cualquier desarrollo interno o externo de herramientas tecnológicas que, de una u otra manera, interactúen con información de la Unidad.

Los requisitos mínimos de seguridad que se encuentran en este documento, son estándar para cualquier desarrollo de software. Esto hace necesario que adicional a los requisitos aquí plasmados, para cada desarrollo en particular, se deben identificar los requisitos adicionales necesarios, dependiendo de la criticidad de la información que se maneje y los riesgos que se identifiquen sobre la misma.

Requisitos mínimos de Seguridad de la Información

Los requisitos mínimos de seguridad para sistemas de información, tomados en base a la publicación "FIPS PUB 200[1]", pretenden garantizar la confidencialidad, integridad y disponibilidad de la Información de la Unidad.

Los Sistemas de Información, desarrollados interna o externamente deben:

1. **Identificación, autenticación y control de acceso:**
    a. El Sistema de Información debe identificar y validar las credenciales de acceso presentadas por los usuarios, sistemas de información y/o servicios web que interactúen con la información de la Unidad.

        Indicadores de pruebas:
        - El 100% de los usuarios que accedan al sistema, deben contar con usuario y contraseña.
        - El 100% de los usuarios que tienen tres intentos fallidos de inicio de sesión, deben ser bloqueados.

    b. Exigir cambio de contraseña al personal registrado como usuario del Sistema de Información.

        Indicadores de pruebas:
        - El 100% de los usuarios deben ser creados por el administrador del Sistema de Información.
        - El 100% de los usuarios deben cambiar la contraseña en su primer ingreso.
        - El 100% de los usuarios deben cambiar la contraseña mensualmente (Actividad que debe exigir el sistema)

    c. Limitar el acceso a la información, para que solamente el personal, sistema de información y/o servicio web autorizado pueda interactuar con la información.
        - El 100% de los accesos a los diferentes módulos del sistema, deben tener autorización (Perfiles y Roles)

2. **Auditoría:**
    a. Crear, proteger y mantener registros de auditoría del Sistema de Información, que permitan el seguimiento, análisis e investigación de actividades ilegales, no autorizadas o inapropiadas sobre el Sistema de Información.

        Indicadores de pruebas:
        - El 100% de los registros de información (INSERT) en base de datos, debe generar registro de auditoría.

[1] Requisitos Mínimos de Seguridad para la Información Federal y Sistemas de Información. Estándares de procesamiento de Información Federal. Departamento de Comercio, Estados Unidos de América. Marzo 2006. http://csrc.nist.gov/publications/PubsFIPS.html

- El 100% de las modificaciones de información (UPDATE) en base de datos, debe generar registro de auditoría.
- El 100% de los intentos de registro de caracteres especiales en campos de texto, debe generar registro de auditoría.
- El 100% de los errores internos del Sistema de Información, deben generar registro de auditoría.

b. Garantizar que las acciones realizadas por los usuarios del Sistema de Información, puedan ser rastreadas para establecer responsabilidades

Indicadores de pruebas:

- El 100% de los registros de auditoría deben permitir evidenciar la asociación entre el usuario del sistema y las actividades realizadas.

3. Protección de la Información:

a. Garantizar que la información ingresada al sistema se encuentre depurada.
   - El 100% de la información que ingresa el usuario al Sistema debe validarse. (Los campos deben recibir la información que se espera. Ejemplo: El campo de correo electrónico debe recibir caracteres alfanuméricos y debe restringir caracteres especiales a excepción de: "@ y .")
   - El 100% de la información que el sistema recibe a través de servicios web, debe ser validada. (Verificar que la información recibida es la que se espera)

b. Garantizar que la información confidencial como contraseñas y respuestas de preguntas secretas (para recuperación de contraseñas) se encuentren protegidas.
   - El 100% de las contraseñas de los usuarios registrados, se deben almacenar cifradas.
   - El 100% de las respuestas secretas a preguntas para recuperación de contraseña, se deben almacenar cifradas.

c. Garantizar que la información se trasmita protegida.
   - El 100% de la información presentada al usuario y suministrada por el mismo, debe trasmitirse en protocolo SSL.
   - El 100% de la información intercambiada con otro sistema de información debe trasmitirse en protocolo SSL.