PBX: 3487800; Fax 3487804 SEDES: -Principal: Carrera 69 No. 25B - 44 -Atención al ciudadano: calle 26 No.57-41 Piso 15 y 16. Correo institucional: ssf@ssf.gov.co Portal institucional: www.ssf.gov.co



**POLÍTICA DE DESARROLLO SEGURO**

|  |  |  |
| --- | --- | --- |
|  | **MACROPROCESO DE GESTIÓN DE TECNOLOGÍA E INFORMACIÓN** | CODIGO: MAN-GSI-XXX |
| VERSION: 1 |
| **Política de desarrollo seguro** | FECHA: 12/Ago/2018 |

**Contenido**

[1. OBJETIVO 3](#_Toc522625210)

[2. ALCANCE 3](#_Toc522625211)

[3. DEFINICIONES 3](#_Toc522625212)

[4. GENERALIDADES 4](#_Toc522625213)

[5. INCUMPLIMIENTO 11](#_Toc522625214)

[6. RESPONSABILIDADES 11](#_Toc522625215)

1. OBJETIVO

Establecer las condiciones y vigilar que el desarrollo y mantenimiento llevado a cabo, tanto internamente como por proveedores externos de la Superintendencia de Subsidio Familiar (SSF), cumpla con buenas prácticas para el desarrollo seguro, además de establecer los criterios de seguridad que deben ser considerados en todas las etapas del desarrollo.

1. ALCANCE

Esta política se aplica a todo el software desarrollado para la Superintendencia de Subsidio Familiar (SSF). La política da cubrimiento a todo el personal de la SSF que haga parte de desarrollos, actualizaciones e instalaciones de software.

1. DEFINICIONES

**Desarrollador**: Persona que apoya el desarrollo de alguna de las fases del ciclo de vida del desarrollo de software para la SSF y que puede trabajar directamente para la SSF (planta, contratista, estudiante en práctica) o través de una empresa externa.

**Hash**: Es una función computable mediante un algoritmo, que tiene como entrada un conjunto de elementos, que suelen ser cadenas, y los convierte (mapea) en un rango de salida finito, normalmente cadenas de longitud fija.

**Lista blanca**: Es una lista o registro de entidades que, por una razón u otra, pueden obtener algún privilegio particular, servicio, movilidad, acceso o reconocimiento.

**Log**: es un registro oficial de eventos durante un rango de tiempo en particular. Se usa para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación.

**Personal**: Es aquella persona que tiene una relación laboral con la SSF directa o a través de un tercero, bajo cualquier tipo de vinculación: planta, contratistas, estudiantes en práctica, etc.

**Token**: Es un dispositivo que genera códigos de acceso que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación.

**URL (localizador de recursos uniforme)**: Es un identificador de recursos uniforme (Uniform Resource Identifier, URI) cuyos recursos referidos pueden cambiar, esto es, la dirección puede apuntar a recursos variables en el tiempo. Están formados por una secuencia de caracteres, de acuerdo a un formato modélico y estándar, que designa recursos en una red.

1. GENERALIDADES

La Oficina de TIC es la responsable de planificar, desarrollar y ejecutar las actividades relacionadas con el desarrollos, actualizaciones e instalaciones de software. Además, debe planificar la ejecución de pruebas funcionales y de seguridad de los sistemas nuevos o modificados antes de ejecutar la instalación en los servidores de producción.

**Normas de seguridad para todo el personal**

Se deberá estandarizar el ciclo de vida, criterios de seguridad y de calidad en el desarrollo de software.

Toda modificación de software crítico bien sea por actualizaciones o modificaciones, deberá ser analizada previamente en ambientes independientes de desarrollo y prueba, con el objetivo de identificar y analizar los riesgos de seguridad que acarrea dicha modificación.

Se deberán planificar detalladamente las etapas de paso a producción, incluyendo respaldos, recursos, conjunto de pruebas pre y pos-instalación, y criterios de aceptación del cambio.

Para propósitos de desarrollo y pruebas de software, se deberán generar datos de prueba distintos a los que se encuentran en el ambiente de producción.

Los desarrolladores de loa SSF y terceros, no deberán tener acceso a información de producción que contenga datos sensibles.

Se debe establecer un acuerdo previo con los terceros, que resguarde la propiedad intelectual y asegure los niveles de confidencialidad de la información manejada en el proyecto.

**Normas de seguridad para la gestión de Vulnerabilidades**

Se deberá establecer una gestión de vulnerabilidades técnicas orientada a analizar los problemas de seguridad (vulnerabilidades) que surgen en los productos de software, que sean publicadas por los proveedores de tecnología y las agencias especializadas (CVE, OWASP) o detectados por cualquier usuario y proponer las medidas de mitigación al riesgo definido.

Se deberá establecer un plan de actualización para el software que es desarrollado o se utiliza en la Entidad, asegurando que las últimas versiones y parches sean instalados lo antes posible, con el fin de evitar que alguna vulnerabilidad sea explotada.

**Normas de seguridad para la documentación del software**

El diccionario de datos, o repositorio de metadatos, deberá mantener una descripción actualizada de las definiciones de datos.

Si el desarrollador incluye comentarios en el programa fuente, estos no deben divulgar información de configuración innecesaria.

Todo sistema desarrollado por la SSF debe generar el protocolo de las condiciones de autenticación a la aplicación, el cual deberá ser revisado y aprobado por el equipo de seguridad de la información.

La documentación de los desarrollos deberá:

* Generarse durante el ciclo de vida de desarrollo y no postergarla hasta el final.
* Ser revisada por los usuarios finales del sistema en desarrollo.
* Actualizarse si el programa cambia alguna de sus funcionalidades.
* Almacenarse en un sitio centralizado (Servidor) administrado por la subdirección de desarrollo de aplicaciones.

**Normas de seguridad para proyectos de desarrollo**

Como parte de las actividades a realizar en esta fase de un proyecto de desarrollo, se deberán describir los requerimientos de seguridad que deben ser cubiertos por el nuevo sistema.

**Normas de seguridad para la especificación detallada de requerimientos**

En el análisis de factibilidad de los requerimientos, se deberá considerar el nivel de criticidad del sistema, además del nivel de protección de seguridad que requerirán los datos y las aplicaciones que lo compongan.

Los requerimientos de seguridad deberán ser compatibles con lo que se establece en las demás políticas de seguridad de la información de la SSF.

**Normas de seguridad para el diseño de Sistema**

El nivel de confidencialidad de todos los elementos que componga el software deberá ser definido teniendo en cuenta la criticidad de los datos.

Si se requiere el uso de cifrado de datos, este deberá ceñirse a los lineamientos descritos en la **política del uso de controles criptográficos.**

Si se utiliza un sistema gestor de bases de datos, se deberá emplear las herramientas de seguridad necesarias para garantizar el nivel de protección adecuado.

Todos los programas críticos deberán incluir la generación de registros de auditoría, considerando como mínimo la identidad del usuario que lee, borra, escribe, o actualiza, el tipo de evento y la fecha y hora del evento. Estos registros deben ser protegidos contra la manipulación no autorizada.

En la etapa de diseño se deberá proyectar el rendimiento esperado, con el objetivo de no sobre dimensionar los recursos necesarios para el funcionamiento del sistema (ancho de banda, RAM, recursos del servidor, etc.).

**Normas de seguridad para la codificación y pruebas**

No está permitido modificar programas sin que quede registrado o documentado el cambio. En caso de requerirse la implementación de un cambio, este deberá ceñirse a los lineamientos descritos en el **procedimiento de control de cambios**.

No está permitido escribir o modificar código auto-copiante o cualquier otro tipo de código malicioso (virus y gusanos), así como funciones u operaciones no documentadas o no autorizadas en los programas.

En lo posible, las pruebas del sistema deberán incluir: instalación, volumen, stress, rendimiento, almacenamiento, configuración, funcionalidad, seguridad y recuperación ante errores.

En lo posible, las pruebas deberán ser realizadas en forma automática, almacenando criterios y datos de pruebas en archivos, para permitir la verificación rápida y repetitiva.

Se deberán tener las siguientes consideraciones con relación a los datos de entrada y salida de los sistemas de información:

* Realizar las validaciones de datos de entrada y salida en un sistema confiable (por ejemplo: un servidor).
* Construir los aplicativos para que validen los datos de entrada y generen los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.
* Validar la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como tipos de datos, rangos válidos y longitud, entre otros.
* Validar las entradas de datos con una lista “blanca” que contenga un directorio de caracteres aceptados.
* Validar el intento de ingreso de bytes nulos, caracteres de nueva línea o caracteres de alteración de rutas.
* Limpiar las salidas de datos no confiables hacia consultas SQL, XML y LDAP o hacia comandos del sistema operativo.

Se deberán establecer los siguientes controles para la autenticación en los sistemas de información:

* Realizar los controles de autenticación en un sistema confiable (por ejemplo, un servidor).
* Si la aplicación administra un almacenamiento de credenciales, asegurar que únicamente se almacena el hash de las contraseñas.
* Validar los datos de autenticación, luego de haber completado todos los datos de entrada.

Se deberá realizar una gestión de las sesiones, que tenga en cuenta los siguientes aspectos:

* Realizar la creación de identificadores de sesión en un sistema en cual se confíe (por ejemplo: el servidor).
* Garantizar la existencia de opciones de desconexión o cierre de sesión de los aplicativos (logout) que permita terminar completamente con la conexión asociada.
* No exponer los identificadores de sesión en URL, mensajes de error ni logs, y no transmitirlos como parámetros.
* Asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.
* Asegurar que la sesión expire después de cierto tiempo.
* No permitir la apertura de sesiones simultaneas con el mismo usuario.

Se deberá asegurar el manejo de operaciones sensibles en los aplicativos desarrollados, permitiendo el uso de dispositivos adicionales como tokens o el ingreso de parámetros adicionales de verificación.

Todas las funciones de criptografía de las aplicaciones desarrolladas deben ser implementadas en sistemas confiables (por ejemplo: el servidor).

Se deben considerar los siguientes aspectos en el manejo de errores:

* Garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios. Los mensajes de error deben ser genéricos.
* Liberar espacio en memoria cuando ocurra una condición de error.

Para el manejo de archivos se deberán acatar las siguientes consideraciones:

* Remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.
* Prevenir la revelación de la estructura de directorios de los sistemas construidos.

Para el establecimiento de conexión a las bases de datos se deberán considerar los siguientes aspectos:

* No incluir las cadenas de conexión a las bases de datos en el código de los aplicativos.
* Cerrar la conexión a las bases de datos desde los aplicativos, tan pronto como estas no sean requeridas.

Se deberá remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.

Se deberán desarrollar los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y garantizar que dichos archivos solo tengan privilegios de lectura.

No se deberá incluir en parámetros, nombres de directorios o rutas de archivos. En su lugar, se deben utilizar índices que internamente se asocien a directorios o rutas pre-definidas.

Se deberá liberar la memoria previa a la salida de una función y de todos los puntos de finalización de la aplicación.

Se deberá garantizar la protección del código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.

No se deberá permitir que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

Se deberán utilizar funciones de control de integridad (hash) para verificar la integridad del código interpretado, bibliotecas, ejecutables y archivos de configuración previo a su utilización.

**Normas de seguridad para la Implementación**

Se deberá velar por la implementación de los controles de seguridad al mismo tiempo que la implementación de los componentes, funciones o módulos a los cuales controla.

Se deberá efectuar sintonía o ajuste (tuning) de los controles establecidos en la fase de diseño.

Las aplicaciones deberán contar con un sistema de autenticación de usuario, que mínimo exija nombre de usuario y contraseña. Además, en los casos que la aplicación esté expuesta a internet, debe implementarse la validación de captcha.

Las aplicaciones deberán contar con manejo de diferentes roles con permisos de acceso y operaciones asociados a estos.

**Normas de seguridad para la post implementación**

Se deberá revisar y auditar la existencia de los controles de seguridad definidos en la etapa de diseño.

Al menos una vez cada año, se debe realizar un escaneo de las aplicaciones más recientes puestas en producción, en busca de vulnerabilidades, manteniendo un registro de los resultados y las acciones correctivas tomadas.

1. INCUMPLIMIENTO

El incumplimiento de esta política de seguridad y privacidad de la información traerá consigo las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno Nacional y Territorial en cuanto a seguridad y privacidad de la información se refiere.

1. RESPONSABILIDADES

**Equipo de Seguridad de la Información:** Velar por el cumplimiento de la presente política.

**Oficina de las TIC:** Recibir, canalizar y gestionar cualquier aviso de problema o incidente en la operación de los sistemas de información, además de disponer de medidas de protección adecuadas para el desarrollo y mantenimiento correcto y seguro de los sistemas de información.

**Desarrolladores:** Cumplir con las disposiciones definidas en esta política y documentar el sistema y sus modificaciones.

**Personal:** Acatar los lineamientos descritos en la presente política para el desarrollo, instalación y actualización de software.

|  |  |  |
| --- | --- | --- |
| **ELABORO** | **REVISO** | **APROBO** |
| **Nombre:** | Alinatech (Roger Ortiz) | **Nombre:** |  | **Nombre:** |  |
| **Cargo:** | Consultor | **Cargo:** |  | **Cargo:** |  |
| **Fecha:** | 08/08/2018 | **Fecha:** |  | **Fecha:** |  |