CONTENIDO

1. OBJETIVO

El objetivo del presente documento es establecer reglas para garantizar la gestión en el desarrollo seguros de los sistemas informáticos del Hospital Departamental San Antonio de Pitalito.

2. ALCANCE

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir a todos los sistemas informáticos, tanto desarrollos propios o de terceros, y a todos los Sistemas Operativos y/o Software de Base.

3. USUARIOS

Los usuarios de este documento son todos los desarrolladores internos y externos, sistemas de información y áreas a fines delHospital Departamental San Antonio de Pitalito.

4. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001, capítulos A.14.1.2, A.14.1.3, A.14.2.1, A.14.2.2, A.14.2.5, A.14.2.6, A.14.2.7, A.14.2.8, A.14.2.9, A.14.3.1.

- Procedimiento de adquisición, desarrollo y mantenimiento de sistemas informáticos

5. DESCRIPCION DEL PROCEDIMIENTO

El Hospital departamental san Antonio de Pitalitoasegurará que el software adquirido y desarrollado tanto al interior del instituto, como por terceras partes, cumplirá con los requisitos de seguridad y calidad establecidos por él. Las áreas propietarias de sistemas de información, el área de sistemas de información, incluirán requisitos de seguridad en la definición de requerimientos y, posteriormente se asegurarán que

estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido.

5.1 Normas para el establecimiento de requisitos de seguridad

Normas dirigidas aEL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PITALITO, SISTEMAS DE INFORMACIÓN.

- Todos los sistemas de información o desarrollos de software deben tener un área propietaria dentro del instituto formalmente asignada.
- La área sistemas de información del HDSAP debe establecer metodologías para el desarrollo de software, que incluyan la definición de requerimientos de seguridad y las buenas prácticas de desarrollo seguro, con el fin de proporcionar a los desarrolladores una visión clara de lo que se espera.
- Las áreas propietarias de los sistemas de información, en acompañamiento con sistemas de información deben establecer las especificaciones de adquisición o desarrollo de sistemas de información, considerando requerimientos de seguridad de la información.
- Las áreas propietarias de los sistemas de información deben definir qué información sensible puede ser eliminada de sus sistemas y solicitar que estos soporten la eliminación de dicha información, como es el caso de los datos personales o financieros, cuando estos ya no son requeridos.

Normas dirigidas a: DESARROLLADORES (INTERNOS O EXTERNOS)

- Los desarrolladores deben documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada sistema de información que se quiera desarrollar, de acuerdo con los requerimientos de seguridad y los controles deseados.

- Los desarrolladores deben certificar que todo sistema de información adquirido o desarrollado utilice herramientas de desarrollo licenciadas y reconocidas en el mercado.
- Los desarrolladores deben deshabilitar las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible.
- Los desarrolladores deben establecer el tiempo de duración de las sesiones activas de las aplicaciones, terminándolas una vez se cumpla este tiempo.
- Los desarrolladores deben asegurar que no se permitan conexiones recurrentes a los sistemas de información construidos con el mismo usuario.
- Los desarrolladores deben utilizar usar los protocolos sugeridos por el área de sistemas de información, en los aplicativos desarrollados.
- Los desarrolladores deben certificar la transmisión de información relacionada con pagos o transacciones en línea a los operadores encargados, por medio de canales seguros.

5.2 POLÍTICA DE DESARROLLO SEGURO, REALIZACION DE PRUEBAS Y SOPORTE DE LOS SISTEMAS

El Hospital Departamental San Antonio de Pitalito velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se asegurará que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido por la institución.

Normas de desarrollo seguro, realización de pruebas y soporte de los sistemas

Normas dirigidas a: EL HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PITALITO

- El Hospital Departamental San Antonio de Pitalito es el responsables de realizar las pruebas para asegurar que cumplen con los requerimientos de seguridad establecidos antes del paso a producción de los sistemas, utilizando metodologías establecidas para este fin, documentado las pruebas realizadas y aprobando los pasos a producción. Estas pruebas deben realizarse por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica en la cual funcionan los aplicativos.
- El Hospital Departamental San Antonio de Pitalito debe aprobar las migraciones entre los ambientes de desarrollo, pruebas y producción de sistemas de información nuevos y/o de cambios o nuevas funcionalidades.

Normas dirigidas a: SISTEMAS DE INFORMACION

- sistemas de información debe implantar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.
- sistemas de información debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información del HDSAP.
- sistemas de información debe asegurase que los sistemas de información adquiridos o desarrollados por terceros, cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.
- sistemas de información debe generar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.
- sistemas de información, a través de sus funcionarios, se debe asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.

- sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.

Normas dirigidas a: DESARROLLADORES (INTERNOS O EXTERNOS)

- Los desarrolladores de los sistemas de información deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha.
- Los desarrolladores deben proporcionar un nivel adecuado de soporte para solucionar los problemas que se presenten en el software aplicativo del HDSAP.
- Los desarrolladores deben 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.
- Los desarrolladores deben suministrar opciones de desconexión o cierre de sesión de los aplicativos (logout) que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.
- debe incluir dentro del procedimiento y los controles de gestión de cambios el manejo de los cambios en el software aplicativo y los sistemas de información de la institución.
- Los desarrolladores deben 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; así mismo, deben implementar mensajes de error genéricos.
- Los desarrolladores deben remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.

- Los desarrolladores deben remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.

- Los desarrolladores deben certificar el cierre de la conexión a las bases de datos desde los aplicativos tan pronto como estas no sean requeridas.
- Los desarrolladores deben 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 asegurar que dichos archivos solo tengan privilegios de lectura.
- Los desarrolladores deben proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.
- Los desarrolladores deben asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

6. VALIDEZ Y GESTIÓN DE DOCUMENTOS

Este documento es válido hasta el31 de diciembre de 2017.

El propietario de este documento es el Hospital Departamental San Antonio de Pitalitoque debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

7. NORMATIVIDAD APLICABLE AL PROCEDIMIENTO.

No.	Descripción	Interna	Externa
1	Decreto 1599 de 2005 – MECI 1000:2005		**X**
2	Ley 1273 de 2009		**X**
3	Resolución 527 de 1999		**X**
4	Decreto 1011 del 2006		**X**

8. CONTROL DE CUMPLIMIENTO Y SANCIONES

En caso de existir incumplimiento de las Políticas de Seguridad de la Información de la E.S.E. y de los Procedimientos descritos en el presente Manual, por parte de un trabajador de la Institución, se comunicará al líder del proceso de Gestión de Talento Humano para que tomen las medidas de sanción respectivas por la inobservancia de la normatividad vigente (interna y externa), además de las responsabilidades civiles y penales a que hubiere lugar.