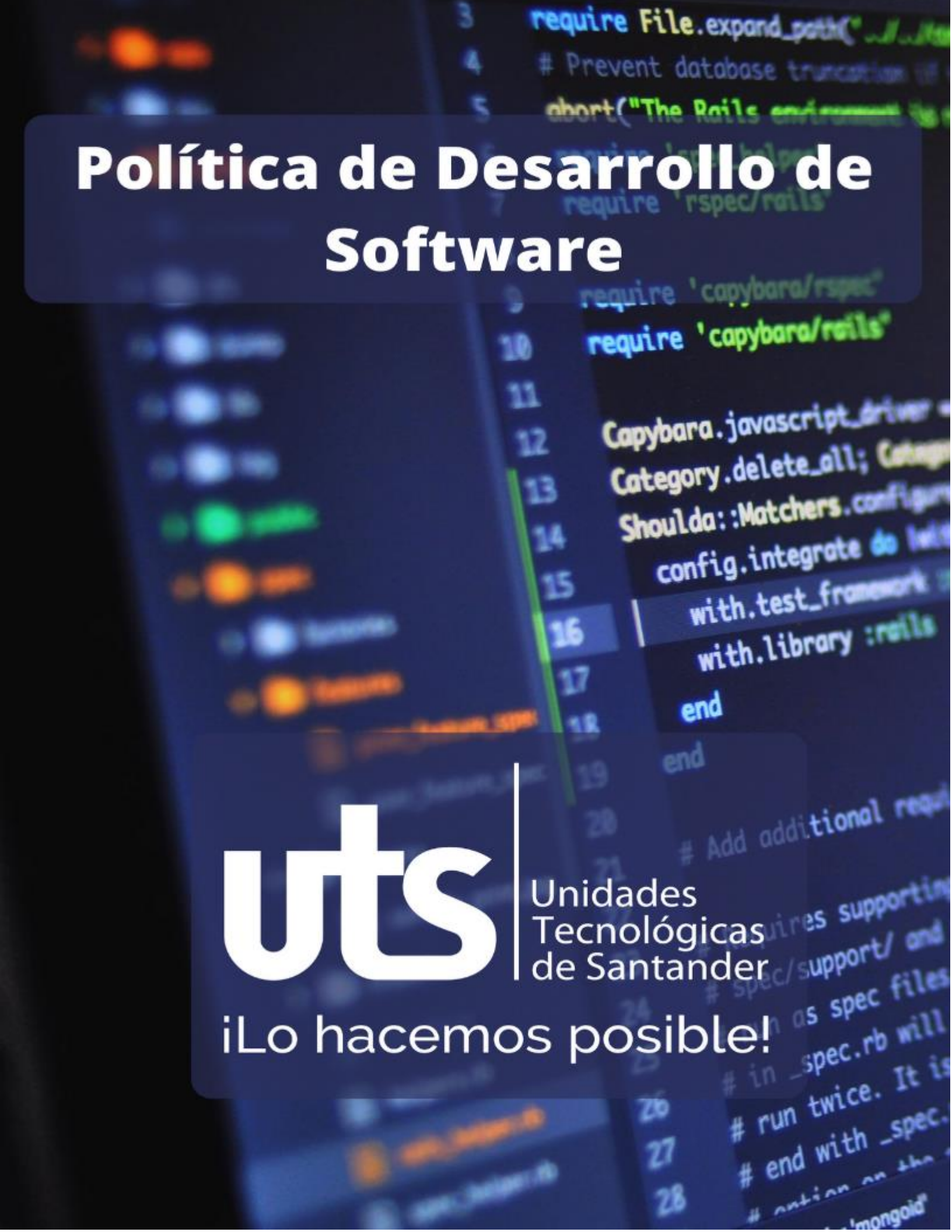
Política de Desarrollo de Software



Unidades Tecnológicas de Santander

¡Lo hacemos posible!

Contenido

1 OBJETIVO 3
2 ALCANCE 3
3 DEFINICIONES 3
4 GENERALIDADES 4
5 INCUMPLIMIENTO 9
6 RESPONSABILIDADES 9

1 OBJETIVO

Asegurar la calidad de desarrollo de software seguro con base en buenas practicas necesarias para preservar la seguridad de la información generando un valor agregado para la administración de software de las Unidades Tecnológicas de Santander.

2 ALCANCE

Esta política se aplica a todo el ciclo de vida de software desarrollado por las Unidades Tecnológicas de Santander, en colaboración con los diferentes procesos que para el caso se le asignen.

3 DEFINICIONES

Desarrollador: Funcionario, contratista o externo encargado de efectuar actividades en alguna o todas las fases del ciclo de vida del desarrollo de software para la UTS.

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 que se presentan durante el desarrollo de un software, este puede contener, fecha, autor, actividad, afectación dirección IP, unidades afectadas entre otra información.

Personal: Es aquella persona que tiene una relación laboral con la UTS 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.

Desarrollo: Creación o mejora de un producto software a partir de especificaciones ceñidas a los requerimientos de la Institución.

Confidencialidad: propiedad de que la información no esté disponible o revelada a personas no autorizadas, entidades o procesos. [ISO/IEC 27000: 2016].

Disponibilidad: propiedad de ser accesible y utilizable a la demanda por una entidad autorizada. [ISO/IEC 27000: 2016].

Integridad: propiedad de exactitud y completitud. [ISO/IEC 27000:2016].

Política: intenciones y direcciones de una organización como se expresan formalmente por la Alta Dirección. [ISO/IEC 27000: 2016].

4 GENERALIDADES

El grupo de recursos informáticos es la responsable de liderar, planificar, controlar, desarrollar y ejecutar las actividades relacionadas con el desarrollo de software, así como efectuar las actualizaciones e instalaciones de software. Además, este grupo lidera y ejecuta la planificación de pruebas funcionales y de seguridad de los sistemas nuevos o modificados situación que ser presenta antes ejecutar la instalación en los servidores de producción.

POLÍTICAS DE DESARROLLO DE SOFTWARE SEGURO

La presente política establece controles para garantizar que la seguridad de la información sea un requisito para el desarrollo de nuevos sistemas o la mejora a los existentes.

En caso de que el desarrollo sea llevado a cabo por el personal de la Institución, deben incluirse los requisitos de seguridad de la información en los nuevos sistemas de información o la mejora de los actuales.

Estos requisitos deben ser identificados mediante herramientas como: obtención de requisitos de cumplimiento a partir de políticas y reglamentación, revisiones de incidentes e identificación de vulnerabilidades.

Esta identificación debe ser documentada y revisada por las partes interesadas. En caso de que estos desarrollos sean producidos por terceros, debe seguirse un proceso formal de adquisición, que incluya los requisitos de seguridad de la información de la Institución.

De igual manera, el nivel de protección de la información que se encuentra en un ambiente de protección no puede ser disminuido utilizándolo en procesos de desarrollo y pruebas.

Debe evitarse que los datos de producción sean utilizados para el desarrollo, y en caso de ser necesarios, estos datos deben permanecer en estos ambientes tan poco como sea posible y estar bajo monitoreo permanente.

El proceso TI de la institución debe implementar los controles necesarios para asegurar que las migraciones entre ambientes de desarrollo, pruebas y producción sean aprobadas de acuerdo al procedimiento de control de cambios.

También, debe certificar que cualquier tipo de desarrollo que vaya a ser pasado a producción cumple con los requerimientos de seguridad establecidos antes de realizar este proceso.

Esta validación se realiza con metodologías ya establecidas o creadas por el proceso TI para tal fin, documentando todas las pruebas realizadas. Es responsabilidad del proceso de recursos informáticos, además, que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén adecuadamente actualizados o parchados.

Todo desarrollo, que haya sido creado interna o externamente, debe contar con un proceso de soporte. En caso de ser creado de manera interna, el (los) desarrollador(es) deben proporcionar un nivel adecuado de soporte y de documentación, en caso de no ser posible proveer el primero.

De manera externa, debe exigirse durante la contratación que se cuente con un proceso de soporte para los errores que puedan presentar las aplicaciones. Respecto a las aplicaciones, los desarrolladores, internos o externos, deben asegurar que:

- Antes de la puesta en producción, todas las características que no sean estrictamente esenciales deben ser removidas de la aplicación.
- Las conexiones a la base de datos son cerradas desde las aplicaciones tan pronto no sean requeridas.
- No se debe poder ejecutar comandos en el sistema operativo del servidor que las aloja.
- Debe prevenirse revelar la estructura de directorios de los sistemas de información de la Institución.
- Los valores para conexión a base de datos no deben estar insertados en el código sino en archivos independientes que permanecen por fuera del control de cambios, y que, de ser posible, se encuentren cifrados.

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 realizado por el personal y/o desarrollador, bien sea por actualizaciones o modificaciones, debe ser analizada en ambientes independientes de prueba, con el objetivo de identificar y analizar los riesgos de seguridad que acarrea dicha modificación de manera que no afecte el ambiente de producción.

Se debe realizar una planeación en detalle de todas 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.

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 de acuerdo a la política de protección de datos de la ley 1581 de 2012.

Normas de seguridad para la gestión de Vulnerabilidades

Se establecerá una gestión centralizada de vulnerabilidades la cual se debe orientar a analizar los problemas de seguridad que surgen en el ciclo de vida del desarrollo y de los productos de software.

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, esta gestión iniciar se debe realizar en un ambiente controlado de pruebas de manera que no afecte el software en producción.

Se deben establecer monitoreos en los sistemas de información que contemple, entre otras, las siguientes acciones: escaneo de archivos infectados, escaneo de vulnerabilidades, análisis de

patrones para detectar acciones sospechosas, verificación contra listas negras, monitoreo del tráfico para detectar ataques de denegación de servicios entre otros.

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 el personal/desarrollador en las UTS, debe tener implícito el protocolo de las condiciones de autenticación a través de controles de acceso fuerte que incluyan contraseñas robustas para el acceso a las aplicaciones, el cual deberá ser revisado y aprobado por el personal designado por el Grupo de Recursos Informáticos.

Como buena práctica toda documentación de desarrollo debe tener:

- Crearse durante el desarrollo del software y no postergarse hasta el final.
- Actualizarse cuando en razón al desarrollo de software se presenten cambios.
- Almacenarse en un sitio destinado para guardar la documentación autorizado por el grupo de recursos informáticos.

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

Ante el análisis de factibilidad al momento de realizar los requerimientos, se debe 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 deben alinearse con las políticas de seguridad de la información de definidas en el MSPI de las UTS.

Normas de seguridad para el diseño de Sistema

Si se requiere el uso de cifrado de datos, este debe ceñirse a los lineamientos de desarrollo de software con referencia a los controles criptográficos.

Si el software desarrollado utiliza algún sistema gestor de bases de datos, este debe hacer uso de las herramientas de seguridad necesarias para garantizar el nivel de protección adecuado, de manera que no afecte la disponibilidad, integridad y confidencialidad de la información.

Todos los sistemas de información desarrollados y adquiridos por las UTS deben incluir la generación de registros de auditoría, el cual debe considerar la identidad del usuario que lee, borra, escribe, o actualiza, el tipo de evento y la fecha y hora del evento, además del origen.

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.

Al momento de realizar las pruebas es importante incluir: instalación, volumen, stress, rendimiento, almacenamiento, configuración, funcionalidad, seguridad y recuperación ante errores.

Se deben 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.
- 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.
- Validar que estén deshabilitados los métodos HTTP peligrosos como put, delete, trace y tenga restricción la administración remota.
- Validar que se protege la integridad del código, mediante: (i) la validación exhaustiva de: inputs, variables post y get (no enviar parámetros sensibles a través del método get), Cookies (habilitar atributos de seguridad como Secure y HttpOnly), y, cabeceras HTTP; (ii) la sanitización de los parámetros de entrada: es decir, que cuando se reciba la información de dichas variables especiales que comúnmente conforman un script, además de la restricción de formatos y tamaños de subidas de archivos; (iii) la sanitización y escape de variables en el código; (iv) verificación estándar de las Políticas de Origen de las cabeceras; y (v) la verificación y comprobación del token de CSRF (cuando aplique).
- Validar que los sistemas de información desarrollados restrinjan el uso de login contra ataques de fuerza bruta, implementando, entre otros: mecanismos de captcha accesibles o auto detectable, y/o limitar la tasa de intentos de login.

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

- Realizar los controles de autenticación en un sistema confiable.
- Validar que el almacenamiento de credenciales, guarden únicamente el hash de las contraseñas.
- Validar los datos de autenticación, luego de haber completado todos los datos de entrada.
- Controlar el escalamiento de privilegios en los Sistemas Operativos, servidor web y Bases de datos que hacen parte de la infraestructura del portal web.

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

- Se debe 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 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.

Validar que los mensajes de error generado por los sistemas de información, no revelen información sensible como: tecnología usada, excepciones o parámetros que dispararon el error específico, entre otros. El mensaje de error debe ser genérico.

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.

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.

Garantizar conexiones seguras a través de uso de certificados, SSL (HTTPS para la confianza de usuarios) y cifrado en la estructura de las peticiones para portales transaccionales, para evitar la manipulación de parámetros en las peticiones.

Se deben implementar acciones de seguridad con el fin de que los controles en los servidores (hardware o software) implemente acciones para la protección de acceso y de ataques como Cross-site scripting, SQL injection o Denial-of-service, entre otros.

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 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.

5 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 Institución, incluyendo lo establecido en las normas que competen al Gobierno Nacional y Territorial en cuanto a seguridad y privacidad de la información se refiere.

6 RESPONSABILIDADES

Grupo de Recursos Informáticos: 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.

7 HISTORIAL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN	NUMERO DE SOLICITUD DE CAMBIO	FECHA
01	Emisión inicial	N/A	Abril de 2021