OBJETIVO

Presentar al equipo desarrollador los lineamientos y requerimientos de seguridad de la información en las actividades de desarrollo de aplicaciones para la Corporación.

ALCANCE

El alcance y enfoque de la política de desarrollo seguro incluye las actividades de desarrollo y mantenimiento de aplicaciones al servicio de la Corporación.

LINEAMIENTOS GENERALES

POLÍTICA DE ANÁLISIS Y ESPECIFICACIÓN DE REQUERIMIENTOS DE SEGURIDAD

- Previo a que un sistema de información sea desarrollado, mantenido o adquirido, el área de gestión tecnológica, deberá especificar los requerimientos o necesidades e seguridad básicos; por tanto se adjuntará un listado de las necesidades de seguridad asociadas para la etapa de análisis y desarrollo del requerimiento o implantación del software.

- La solicitud deberá ser evaluada con respecto a su viabilidad y conveniencia para analizar alternativas de desarrollo y la evaluación de los aspectos de seguridad necesarios en cumplimiento de los objetivos del requerimiento.

- Todo proyecto de desarrollo, mantenimiento o compra de software deberá cumplir los requisitos mínimos de seguridad y protección de la información de la Corporación, éste será un criterio fundamental para la aceptación del producto final.

- Las declaraciones de requerimientos de seguridad para nuevos sistemas (o mejoras a sistemas existentes) deben ser explícitamente definidos en su requerimiento, denotando el valor o importancia de la información ante un posible daño, divulgación o impactos que surja como resultado de fallas o por ausencia de la seguridad.

- Los módulos ejecutables nunca deberán ser trasladados directamente de las librerías de pruebas a las librerías de producción sin que previamente sean probados, revisados y recompilados.

- Toda aplicación o sistema de información deberá tener en cuenta aspectos de seguridad de la información asociados a los perfiles de usuario y accesos sobre los procesos y datos a nivel transaccional y demás.

- Las librerías de códigos fuentes de la Corporación deberán ser manejadas de manera centralizada y su acceso solo se realizará cuando se requiera una modificación o mantenimiento a una aplicación y mediante la puesta de una copia del código fuente a las librerías de ambiente de desarrollo.

- El paso a producción de cualquier aplicación, implica una verificación de las normas de seguridad asociadas al sistema de información.

Teniendo en cuenta que los objetivos de la seguridad de la información serán la confidencialidad e integridad, por lo tanto todo desarrollo y/o adquisición deberá tener en cuenta dichos propósitos:

VALIDACIÓN DE SEGURIDAD DE ACCESOS DE USUARIOS

- Se deberá asegurar que un usuario tenga los permisos necesarios para ejecutar su función y no se le concedan accesos y/o permisos a tareas que se excedan de su responsabilidad.

- Toda aplicación o sistema de información debe incluir el manejo interno de perfiles de usuario, accesos sobre tareas y los datos.

- En ambiente de pruebas, se deberá verificar que las cuentas de usuario asignadas, posean los accesos necesarios a las operaciones y a los datos, como actividad previa a implementación en ambiente de producción.

VALIDACIÓN DE DATOS DE ENTRADA

Se debe asegurar la validación de la información en su etapa de entrada en las aplicaciones para asegurar su integridad y minimización de la posibilidad de errores en la digitación para ingreso

- Datos estándar
- Doble digitación
- Tablas de referencia o lista de selección
- Control de Secuencia
- Control de rango de valores
- Control de Segregación de funciones

VALIDACION DE DATOS DE SALIDA

Se deberá exigir y asegurar a los desarrolladores las validaciones de los datos de salida de modo que se garantice las ejecuciones correctas de acuerdo a los requerimientos funcionales solicitados y por ende los resultados esperados.

VALIDACION DE PROCESAMIENTO DE DATOS

Se deberá validar la información procesada por los programas de aplicación e incorporar puntos de verificación o validación, para detectar posibles errores o problemas en los datos. Los controles específicos requeridos dependerán de la naturaleza de la aplicación y del impacto causado por la alteración de datos.

Se deberán considerar los siguientes controles:

- Verificar la detección de los siguientes errores:
  - Valores fuera de rango
  - Caracteres inválidos en campos
  - Datos incompletos
  - Exceso de los límites máximos o mínimos de volumen de datos.
- Revisiones periódicas del contenido de campos claves o archivos para confirmar su validez e integridad.
- Ejecutar los procedimientos apropiados para responder a la validación de errores.
- Definir las responsabilidades de todo el personal involucrado en el proceso de digitación y en lo posible automatizar al máximo mediante documentos electrónicos.

VALIDACION DE CIFRADO DE DATOS

Con el fin de proteger la confidencialidad e integridad de la información durante su transmisión a terceros o su almacenamiento, se deberá llevar a cabo una evaluación del riesgo de seguridad con el fin de identificar amenazas y controles de apropiados, dependiendo de la situación y/o de la criticidad de la información.

VALIDACION DE AUTENTICACIÓN DE MENSAJES

Se deberá considerar un sistema de autenticación de mensajes para aplicaciones que comprendan la transmisión de datos sensibles y donde sea vital la protección de la integridad del contenido. (ej. transferencia de fondos de manera electrónica u otros intercambios de información).

VALIDACION DE SEGURIDAD DE CODIGO FUENTE Y ARCHIVOS

- Nuevas aplicaciones en desarrollo y sus datos, deberán ser estrictamente alojados en ambiente diferente a producción; esta separación se llevará a cabo a través de la separación de los directorios y las librerías en ambientes de desarrollo con control de seguridad.

- En aquellas instancias donde el acceso al ambiente de producción es requerido para una modificación autorizada y/o para agregar una nueva aplicación, solo se concederán accesos de lectura y copiado a las personas que realizarán dicha actividad.

- Código fuente de aplicaciones deberá ser respaldado y protegido en un lugar externo.

- El uso de comandos del sistema operativo que pudiesen ser ejecutados a través de la aplicación, debe restringirse al máximo para los usuarios.

VALIDACION DE CONTROL DE CAMBIOS EN SISTEMAS DE INFORMACION
Todos los cambios significativos en aplicaciones, sistemas de información, o procedimientos críticos de producción, deberán ser solicitados formalmente a través del procedimiento de control de cambios se asegurará que sólo los cambios autorizados sean realizados y notificados al comité de cambios.

POLÍTICA DE CONTROL DE VERSIONES

- Antes de hacer uso de un nuevo aplicativo o con cambios sustanciales en ambiente de producción, deberá recibirse una aprobación escrita por parte de propietario de la información y/o responsable del área con la aprobación de su implementación en producción y para la asignación de la versión correspondiente.

- Las versiones del software deben ser protegidas para recuperación tanto por algún incidente o por requerimientos de información.

- Cada actualización a la versión software crítico de la Corporación deberá ser actualizada y depositada en custodia con el tercero elegido.

POLÍTICA DE DESARROLLO EXTERNO

Todo desarrollo de software por parte de proveedor del software deberá contar con la autorización virtual o física necesaria para efectuar las modificaciones necesarias.

Documentos relacionados

Metodología de Desarrollo.	
Instructivo de Gestión de Cambios	
Formato de Solicitud de cambio en sistemas de información y aplicaciones	
Manual de seguridad de la información – Cortolima	

FECHA	VERSIÓN	DESCRIPCIÓN
06-03-2017	00	