CONSEJO PROFESIONAL NACIONAL DE ARQUITECTURA Y SUS PROFESIONES AUXILIARES

POLÍTICA DE DESARROLLO SEGURO

Código	PA-GC-3
Versión	1
Tipo	Politica
Implementación	13/09/2017
Alcance	
Nivel de confidencialidad	

1. OBJETO

Definir los lineamientos generales para el desarrollo, mantenimiento y adquisición de software al interior de la Entidad, con el fin de determinar los controles de seguridad en el desarrollo de código fuente.

2. ALCANCE

Aplica a trabajadores o terceros que realicen actividades correspondientes al desarrollo, mantenimiento y adquisición de software para la Entidad. La Entidad determinará mediante sus procedimientos en que momento se considera viable autorizar las actividades de desarrollo de software con sus propios recursos. En todo caso la política de desarrollo seguro se aplicará a trabajadores o terceros a los que se les haya asignado actividades de desarrollo de software.

3. DEFINICIONES

CONFIDENCIALIDAD
DISPONIBILIDAD
INTEGRIDAD
INFORMACION PUBLICA
INFORMACION PUBLICA CLASIFICADA
INFORMACION PUBLICA RESERVADA
DATO PERSONAL
GESTION DE RIESGO
RIESGO DE SEGURIDAD
VULNERABILIDAD

4. CONDICIONES GENERALES

Para el desarrollo de software se debe realizar un proceso de planificación en donde se determine la respectiva metodología a utilizar; las etapas de desarrollo; la estructura de componentes a elaborar, los respectivos responsables, criterios de aceptación y las pruebas de funcionalidad y seguridad teniendo en cuenta los requerimientos y el cumplimiento de los objetivos de la Entidad. Las etapas deberán estar debidamente documentadas, con el objeto de generar registros de trazabilidad frente a los requerimientos, desarrollo y aceptación del software.

La identificación de las necesidades y requisitos de funcionalidad, calidad y seguridad, se documentan entre el área solicitante y la oficina administrativa y financiera. Los requerimientos del software se deben validar durante el proceso de aceptación del desarrollo de software.

Para el desarrollo y puesta de producción del software, se debe contar con tres ambientes separados: uno de desarrollo, uno pruebas y uno de producción, conformados por infraestructura y roles y responsabilidades claramente establecidas a fin de evitar modificaciones no autorizadas del código fuente del software.

Los cambios requeridos sobre el software se controlan través del Procedimiento de Control de Cambios, el cual permite que se documenten y establezcan los requerimientos y los niveles de aceptación del cambio. Dentro de los requerimientos de los cambios es necesario analizar los riesgos asociados a la seguridad de la información y la identificación de los controles a implementar para su adecuada gestión.
En los procesos de desarrollo de software se deben acordar cuando aplique, las condiciones para transferencia de los derechos de propiedad intelectual del código fuente del software.

Antes de iniciar el desarrollo de software, se debe acordar una metodología para hacer seguimiento al desarrollo del software, igualmente deben definir los requisitos y productos a entregar, responsabilidades, cronograma de desarrollo y requisitos de calidad y seguridad para el software. La metodología de desarrollo de software debe contemplar una etapa de gestión de riesgos, que permita tratar apropiadamente fallos que afecten la confidencialidad, integridad o disponibilidad de los sistemas de información y desarrollo.

CONSEJO PROFESIONAL NACIONAL DE ARQUITECTURA Y SUS PROFESIONES AUXILIARES

POLÍTICA DE DESARROLLO SEGURO

Código	PA-GC-3
Versión	1
Tipo	Politica
Implementación	13/09/2017
Alcance	
Nivel de confidencialidad	

La oficina administrativa y financiera debe validar los criterios técnicos del software para dar la aceptación formal: interoperabilidad, buenas prácticas de programación y seguridad. La aceptación de los criterios está determinada por los resultados de las pruebas propuestas sobre el software, las cuales tienen dentro de sus objetivos: determinar el correcto funcionamiento del software, detectar vulnerabilidades de seguridad y validar la facilidad de uso del software entre otros.

Los datos de pruebas con los que se verifique el software no deben utilizar datos reales de producción, se deben preparar conjunto de datos de prueba especiales que impidan la pérdida de confidencialidad de la información institucional.

En el desarrollo de software es necesario establecer controles que permitan conservar la seguridad y privacidad de la información; por lo tanto, es importante tener en cuenta los mecanismos de acceso a la información, autenticación, detección de intrusos, cifrado de datos, salvaguarda de confidencialidad, integridad, disponibilidad y protección de los datos personales.

DEFINICIÓN

CONFIDENCIALIDAD: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados
DATO PERSONAL: Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos personales pueden ser públicos, semiprivados o privados. Ley 1266/2008
DISPONIBILIDAD: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. (Norma ISO 27000:2014)
GESTION DE RIESGO: Actividades coordinadas para dirigir controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.
INFORMACION PUBLICA: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal, Ley 1712/2014.
INFORMACION PUBLICA CLASIFICADA: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712/2014
INFORMACION PUBLICA RESERVADA: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la ley 1712 de 2014
INTEGRIDAD: La propiedad de salvaguardar la exactitud y complejidad de la información. (Norma ISO27000:2014)
RIESGO DE SEGURIDAD: Toda posibilidad de ocurrencia de aquella situación que pueda afectar la confidencialidad, la integridad o la disponibilidad de la información.
VULNERABILIDAD: Debilidad de un activo o control que pueda ser explotado por una o más amenazas. (Norma ISO 27000:2014).

ELABORÓ	REVISÓ	APROBÓ
FELIX ALBERTO ROZO LARA **PROFESIONAL UNIVERSITARIO CODIGO 02 GRADO 03 - OFICINA ADMINISTRATIVA Y FINANCIERA** **Fecha de elaboración:** 09/08/2017	FELIX ALBERTO ROZO LARA **PROFESIONAL UNIVERSITARIO CODIGO 02 GRADO 03 - OFICINA ADMINISTRATIVA Y FINANCIERA** **Fecha de revisión:** 09/08/2017	DIANA FERNANDA ARRIOLA GOMEZ **DIRECTORA EJECUTIVA CODIGO 01 GRADO 03** **Fecha de aprobación:** 13/09/2017