



Escuela Tecnológica
Instituto Técnico Central

**PRINCIPIOS PARA LA
CONSTRUCCIÓN DE SISTEMAS
SEGUROS**

CÓDIGO:

VERSIÓN: 1

VIGENCIA:

PÁGINA:1 de 7

PRINCIPIOS PARA LA CONSTRUCCIÓN DE SISTEMAS SEGUROS



Escuela Tecnológica
Instituto Técnico Central

**PRINCIPIOS PARA LA
CONSTRUCCIÓN DE SISTEMAS
SEGUROS**

CÓDIGO:

VERSIÓN: 1

VIGENCIA:

PÁGINA:2 de 7

Tabla de Contenido

1.	Introducción	3
2.	Objetivo	4
3.	Principios para la Construcción de Sistemas Seguros	5
4.	Control de Cambios	7



Escuela Tecnológica
Instituto Técnico Central

PRINCIPIOS PARA LA CONSTRUCCIÓN DE SISTEMAS SEGUROS

CÓDIGO:

VERSIÓN: 1

VIGENCIA:

PÁGINA:3 de 7

1. Introducción

La seguridad en aplicaciones es el uso de principios y/o buenas prácticas de seguridad, durante el ciclo de vida del software. Estos principios tienen como fin garantizar la preservación de la confidencialidad, integridad y disponibilidad de los datos almacenados en los sistemas de información, evitando en todo momento, el acceso no autorizado a los mismos.

Adicional, la no implementación de los principios y/o buenas prácticas, durante el ciclo de vida del software, permite la materialización de la "Deuda Técnica".

La "Deuda Técnica" es un fenómeno muy común en nuestros tiempos, pues se asocia al impacto económico que deben asumir las empresas, debido a la mala calidad del software (re-trabajo, atrasos, etc)

El presente documento pretende proponer una serie de principios para la construcción de sistemas seguros, que ayudarán, en gran medida, a evitar la materialización de los riesgos relacionados con el desarrollo de aplicativos para la Escuela Tecnológica Instituto Técnico Central (ETITC)



Escuela Tecnológica
Instituto Técnico Central

PRINCIPIOS PARA LA CONSTRUCCIÓN DE SISTEMAS SEGUROS

CÓDIGO:

VERSIÓN: 1

VIGENCIA:

PÁGINA:4 de 7

2. Objetivo

Proponer los principios para la construcción de sistemas seguros, que permitan garantizar la preservación de la confidencialidad, integridad y disponibilidad de la información que se recolecta, procesa y custodia, en los aplicativos desarrollados o adquiridos por la ETITC.



Escuela Tecnológica
Instituto Técnico Central

PRINCIPIOS PARA LA CONSTRUCCIÓN DE SISTEMAS SEGUROS

CÓDIGO:

VERSIÓN: 1

VIGENCIA:

PÁGINA:5 de 7

3. Principios para la Construcción de Sistemas Seguros

- Utilizar herramientas licenciadas u Open Source para la actividad de desarrollo de aplicaciones.
- Deshabilitar las funcionalidades de completar automáticamente en las cajas de texto.
- Establecer el tiempo de duración de las sesiones activas en las aplicaciones.
- Evitar las conexiones concurrentes con el mismo usuario a las aplicaciones desarrolladas.
- Validar el tipo de dato de entrada
- Generar los datos de salida de manera confiable.
- Implementar mecanismos de seguridad para proteger el id de sesiones.
- Proporcionar la mínima información de la sesión establecida y almacenada en cookies.
- Cambiar el ID de sesión, cada vez que un usuario cambie su estado (apertura / cierre de sesión).
- Evitar que por medio de código los ID de sesiones puedan ser editados
- No divulgar, en respuestas de error, información relacionada con sistemas operativos, identificadores de sesión o información de las cuenta de usuario, versiones de bases de datos, número de error
- Remover todas las funcionalidades y archivos, que no sean necesarios para los aplicativos de la ETITC, previo a la puesta en producción.
- No publicar la estructura de directorios de los aplicativos (en mensajes de error o barra de navegación).
- Evitar incluir las cadenas de conexión a las bases de datos, en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independiente, los cuales se recomiendan estén cifrados.
- Proteger el código fuente de los aplicativos construidos, de tal forma, que no pueda ser descargado ni modificado por los usuarios.



Escuela Tecnológica
Instituto Técnico Central

PRINCIPIOS PARA LA CONSTRUCCIÓN DE SISTEMAS SEGUROS

CÓDIGO:

VERSIÓN: 1

VIGENCIA:

PÁGINA:6 de 7

- Garantizar una adecuada asignación de privilegios de acceso por usuario (lectura, lectura/escritura, etc)
- Garantizar que en los logs se registre la mayor cantidad de información del usuario en cuestión, incluyendo los usuarios con roles administrativos.
- Si se utiliza un lenguaje que no sea compilado, asegurarse de limpiar el código que se pone en producción, para que no contenga rutinas de pruebas, comentarios o cualquier tipo de mecanismo que pueda dar lugar a un acceso indebido.
- Propender para que las versiones de Sistemas operativos, motores de bases de datos, servidores de aplicaciones, y máquinas virtuales se encuentren para garantizar el soporte respectivo y disminuir la probabilidad de existencia de vulnerabilidades que pueden ser explotadas.
- Implementar certificados digitales que permitan preservar la confidencialidad e integridad de la información, mediante algoritmos de cifrados simétricos y/o asimétricos.
- Implementar mecanismos para garantizar que las contraseñas de acceso a las aplicaciones se cambien periódicamente y propender para que estas sean robustas.



Escuela Tecnológica
Instituto Técnico Central

**PRINCIPIOS PARA LA
CONSTRUCCIÓN DE SISTEMAS
SEGUROS**

CÓDIGO:

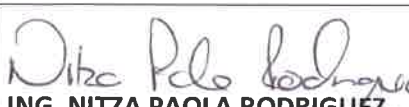
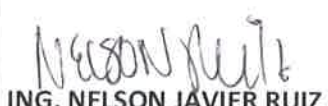
VERSIÓN: 1

VIGENCIA:

PÁGINA:7 de 7

4. Control de Cambios

FECHA	VERSIÓN	CAMBIOS
28/02/2018	1	Adopción del Documento.

ELABORÓ	REVISÓ	APROBÓ
 ING. NITZA PAOLA RODRIGUEZ. Sistemas de Información	 ING. NITZA PAOLA RODRIGUEZ. Sistemas de Información	 ING. DAVID LEONARDO TORRES. Profesional de Gestión de Informática y Comunicaciones.
 ING. NELSON JAVIER RUIZ Contratista	 ING. DAVID LEONARDO TORRES. Profesional de Gestión de Informática y Comunicaciones.	

