Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

APLICAR EXITÓSAMENTE UN CICLO DE DESARROLLO SEGURO DE APLICACIONES

Congreso Internacional de DESARROLLO DE SOFTWARE

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

EXPOSITOR

- Carlos Gonzales Fung
- Ingeniero de Sistemas
- Universidad San Martín de Porres - Perú
- cgonzales@intelitech.com.pe

Congreso Internacional de DESARROLLO DE SOFTWARE

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

INTRODUCCIÓN

A lo largo de la historia de la evolución de las tecnologías de información, la seguridad casi siempre ha sido un aspecto rezagado. Es habitual que primero pensemos en la funcionalidad y luego, cuando alguna tecnología ya fue desplegada y tengamos evidencias de que hay vulnerabilidades, nos preocupemos de la seguridad. En el desarrollo de aplicaciones también ocurre: algo sucede en el desarrollo del software o aplicaciones, que termina finalmente en una vulnerabilidad y personas mal intencionadas (como algunos hackers) están al acecho para aprovecharse.

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

OBJETIVO DEL ESTUDIO

Presentar las principales prácticas, metodologías y estrategias que permitan producir aplicaciones seguras a través de la ejecución de un ciclo de desarrollo seguro. De esta manera, lograr que toda nueva aplicación o software desarrollado tenga un adecuado nivel de seguridad.

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

METODOLOGÍA DE LA INVESTIGACIÓN

Se abordará los temas siguientes presentando en cada uno de ellos su base de conocimiento, ejemplos y recomendaciones:

1. Principales Casos
2. La resistencia a aplicar la seguridad
3. Metodologías y prácticas aplicables al Ciclo de Desarrollo
4. Estrategias para aplicar las metodologías y prácticas. Factores de éxito.

Congreso Internacional de DESARROLLO DE SOFTWARE

Instituto Superior Tecnológico del Azuay

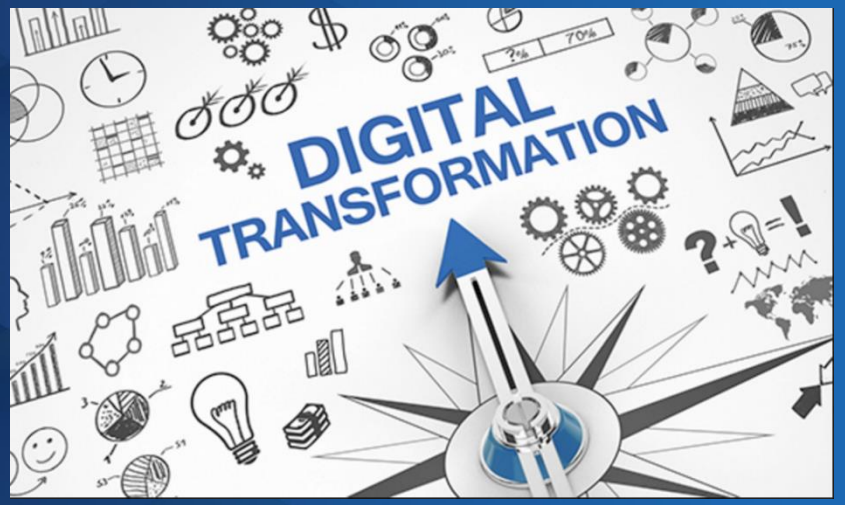
CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

METODOLOGÍA DE LA INVESTIGACIÓN

EL MUNDO DIGITAL DEL HOY (2000-2018)

- La tecnología es nuestro día a día. Es integrada.
- Crecimiento explosivo.
- Accesible para todos.
- Redes sociales.
- Las empresas se centran en lo que el cliente quiere y en cómo entregarle un producto o servicio.
- Alta capacidad de procesamiento.



Congreso Internacional de DESARROLLO DE SOFTWARE

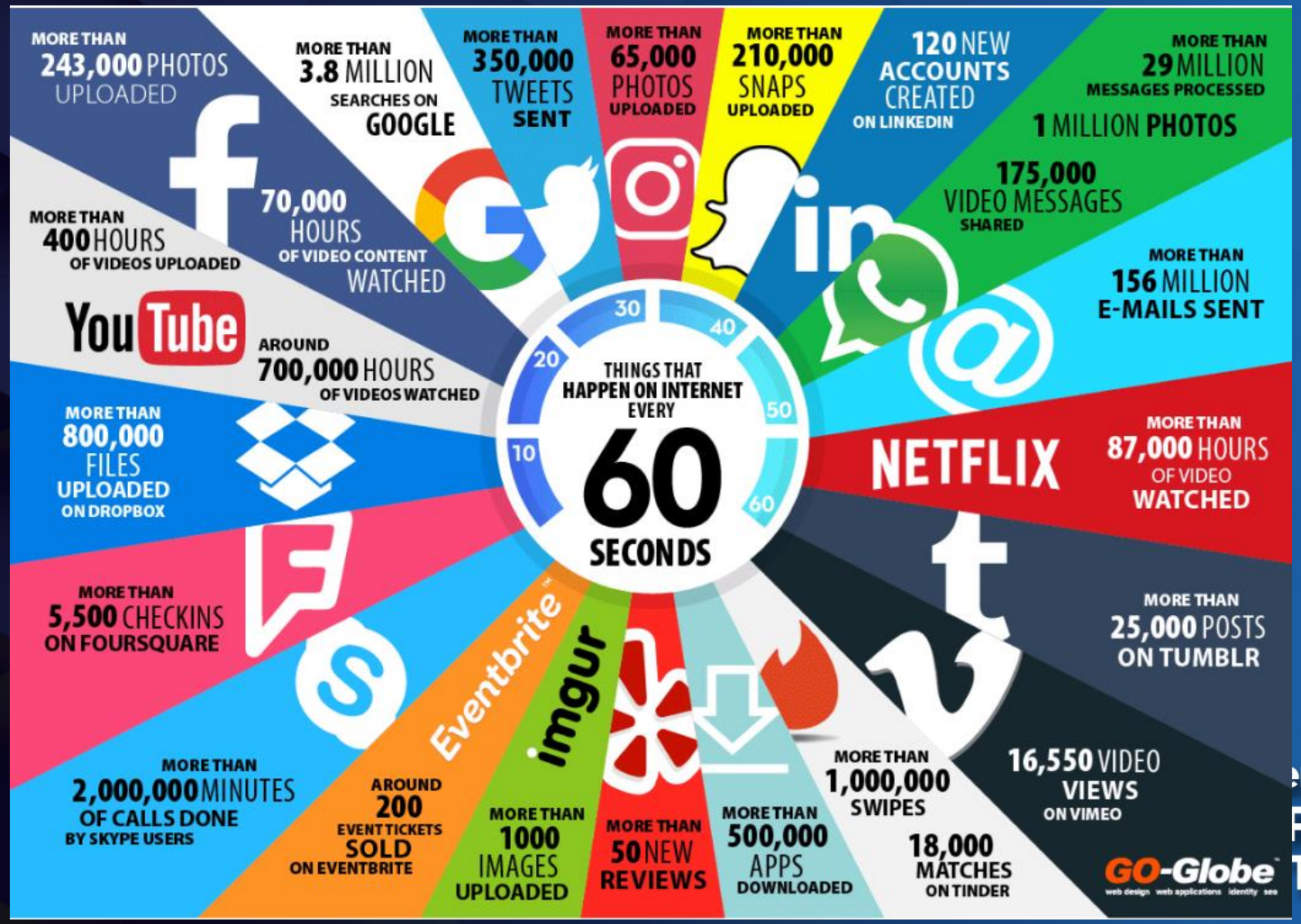
Instituto Superior Tecnológico del Azuay

Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia CET-BOLIVIA

METODOLOGÍA DE LA INVESTIGACIÓN

LO QUE SUCEDE EN CADA 60 SEGUNDOS (https://www.go-globe.com)



ernacional de
ROLLO
TWARE

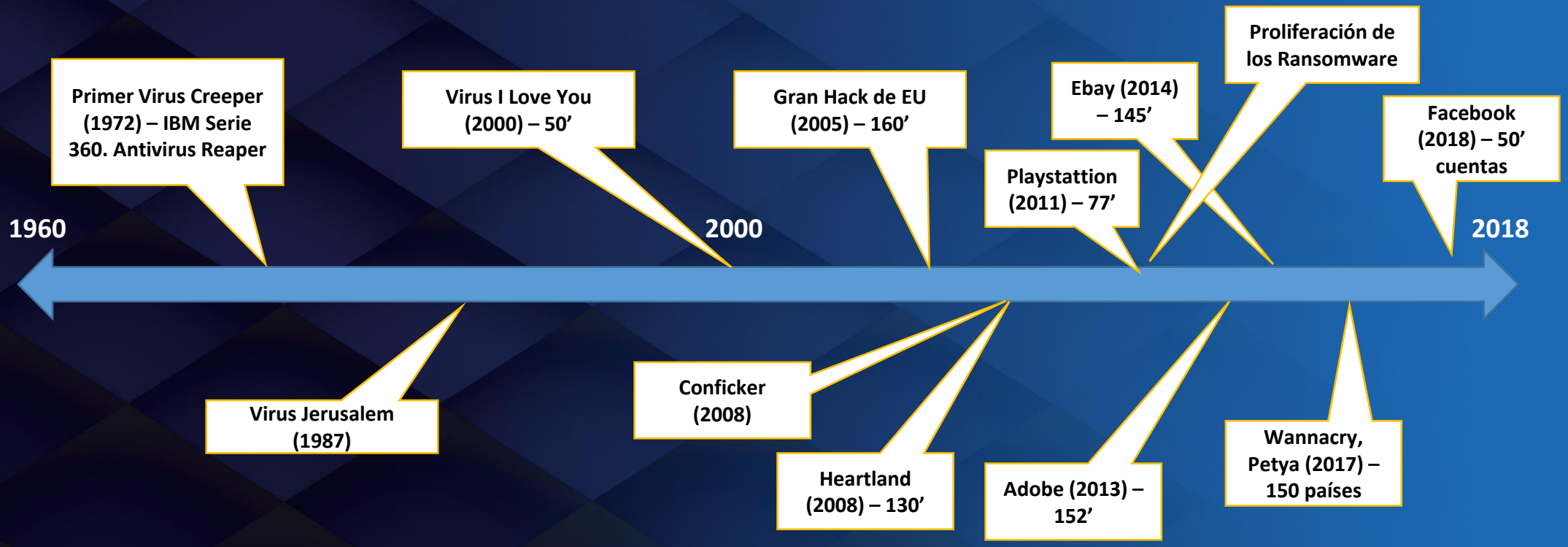
Instituto Superior Tecnológico del Azuay

Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia CET-BOLIVIA

METODOLOGÍA DE LA INVESTIGACIÓN

EVOLUCIÓN DE LA SEGURIDAD DE INFORMACIÓN



Congreso Internacional de DESARROLLO DE SOFTWARE

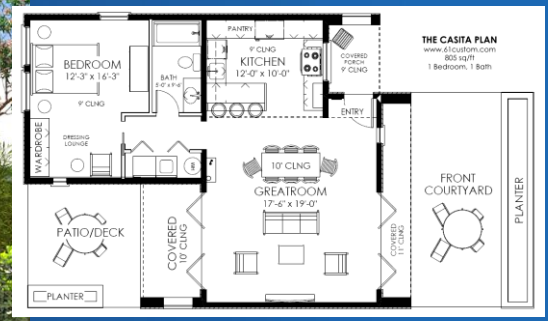
Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

METODOLOGÍA DE LA INVESTIGACIÓN

¿POR QUÉ ES NECESARIO?



Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

METODOLOGÍA DE LA INVESTIGACIÓN

- “La seguridad la vemos luego, ahora no es importante”
- “El líder usuario nos ha solicitado que la aplicación esté en producción mañana mismo”
- “No sabíamos que habían requisitos de seguridad que cumplir”
- “En la planificación se nos pasó considerar actividades de seguridad, no podemos cambiar el cronograma”
- “Nadie nos va a atacar, eso es muy difícil”
- “Así como está la situación, no creo que nos den más presupuesto. Menos para la seguridad”
- “Pasemos a producción como sea, ya luego regularizamos las vulnerabilidades de seguridad”

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

METODOLOGÍA DE LA INVESTIGACIÓN

PRINCIPALES RAZONES POR LAS QUE NO SE APLICA SEGURIDAD

- Falta de Capacitación y Concientización
- Desconocimiento de estándares y metodologías
- Falta de presupuesto
- Exigencias de la dirección y los líderes usuarios
- Falta de planificación
- Subestimación
- Falta de normativas que exijan cumplimiento de la seguridad o la falta de ejecución y seguimiento por las autoridades.

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

METODOLOGÍA DE LA INVESTIGACIÓN

Desarrollo Seguro de Aplicaciones

- Involucra no solo programar código seguro

También incluye:

- Arquitectura Segura de Aplicaciones
  - Diseño Seguro
  - Infraestructura Segura, así como trasmisión de datos y mecanismos de almacenamiento
- Un Ciclo de Vida de Desarrollo de Software Seguro
- Procedimientos de Análisis de Vulnerabilidades
- Gestión de Riesgos y Controles de Mitigación

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

METODOLOGÍA DE LA INVESTIGACIÓN

Externas:

- Hacktivistas
- Hackers

Internas:

- Empleados descontentos
- Proveedores
- Falta de uso de prácticas y procesos de seguridad

No necesariamente maliciosas:

- Un programador “Harcodea” una aplicación estableciendo un usuario y contraseña en el código de programa
- Un Gestor de Proyectos no incluye la actividad de revisión de código para no retrasar el proyecto.

Otras:

- Falta de entrenamiento
- Falta de soporte de los gerentes

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

METODOLOGÍA DE LA INVESTIGACIÓN

Beneficios de un Ciclo Seguro de Desarrollo de Aplicaciones

- Permite que las Partes Interesadas estén informados de los requerimientos de seguridad tan pronto como sea posible.
- Permite una mejor gestión del Presupuesto y Tiempo.
- Identifica vulnerabilidades y riesgos antes de la puesta en producción.
- Reduce los costos.

El CLIENTE implícitamente espera seguridad. La ORGANIZACIÓN al final es la responsable de asumir las consecuencias de incidentes de seguridad que pueden dañar su operación y/o su imagen.

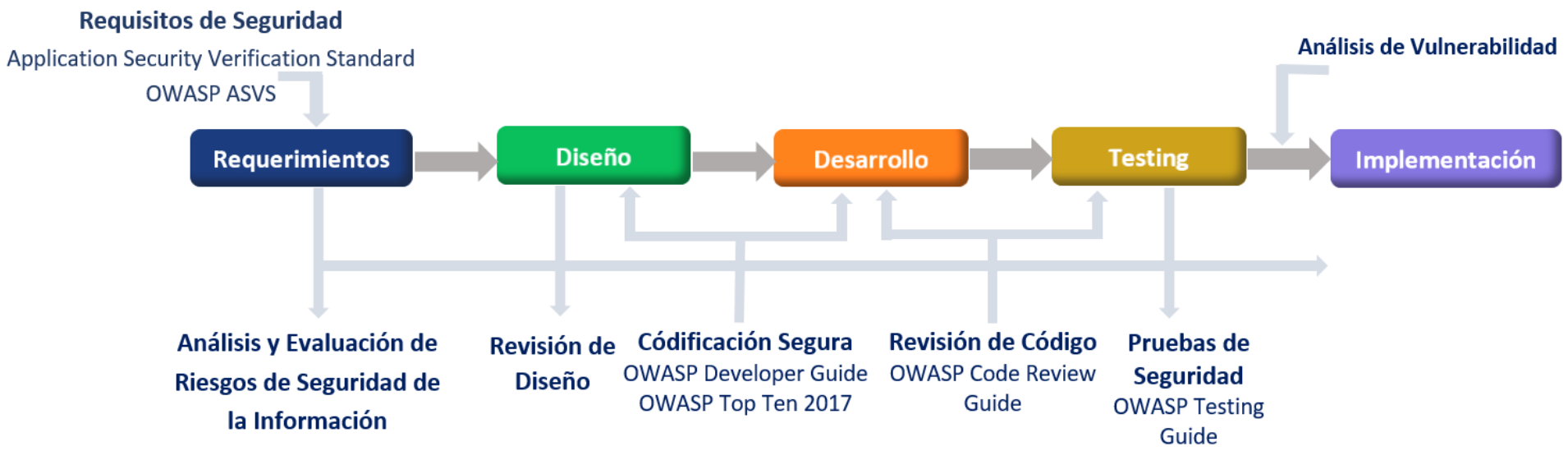
Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

METODOLOGÍA DE LA INVESTIGACIÓN

CICLO DE DESARROLLO SEGURO DE APLICACIONES



Requisitos de Seguridad:	Propietario Aplicación (R), Gestor de la Aplicación, Seguridad de Información
Evaluación de Riesgos:	Propietario Aplicación (R), Gestor de la Aplicación, Seguridad de Información
Revisión de Diseño:	Seguridad de Información (R)
Desarrollo y Pruebas Unitarias:	Gestor de la Aplicación (R), Equipo de Desarrollo
Testing y Código Seguro:	Seguridad de Información (R)
Análisis de Vulnerabilidad:	Seguridad de Información (R)

Instituto Superior Tecnológico del Azuay

Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia CET-BOLIVIA

METODOLOGÍA DE LA INVESTIGACIÓN

OWASP

OWASP (Open Web Application Security Project)

- Sin fines de lucro.
- Objetivos:
  - ❑ Descubrir vulnerabilidades
  - ❑ Establecer mecanismos de defensa contra las causas de software no seguro
  - ❑ Educar en seguridad de aplicaciones.
- Libre.

En **OWASP** encontrará:

- Herramientas y estándares de seguridad en aplicaciones
- Libros completos de revisiones de seguridad en aplicaciones, desarrollo de código fuente seguro y revisiones de seguridad en código fuente
- Controles de seguridad estándar y librerías
- Investigaciones de vanguardia
- Extensas conferencias alrededor del mundo

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

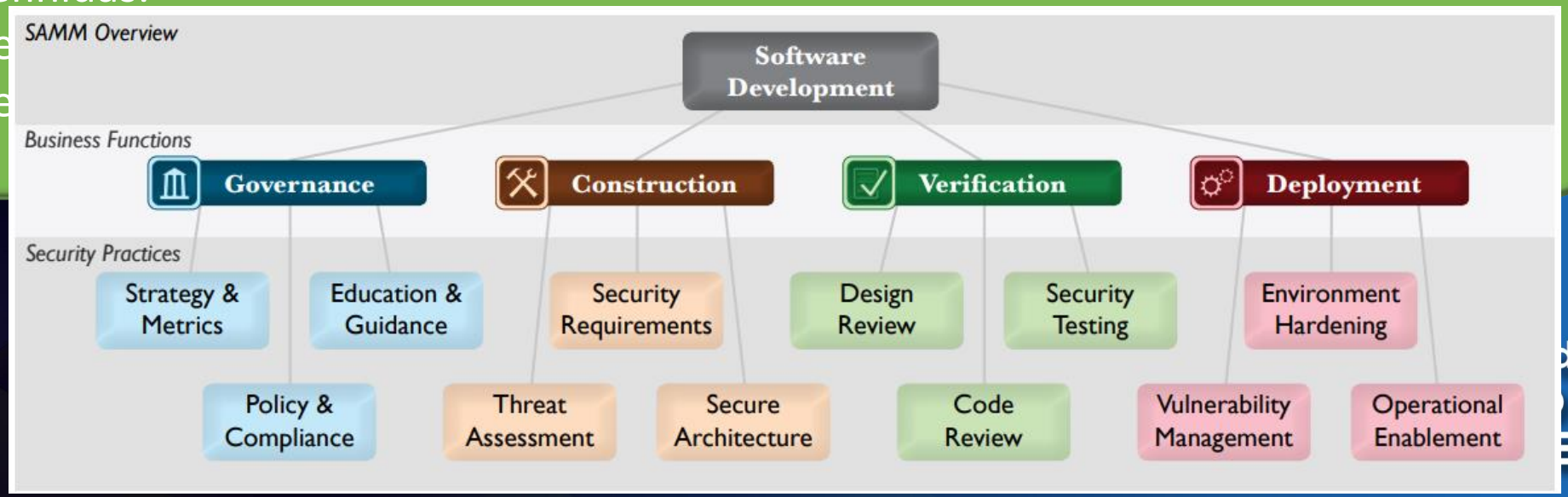
Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

METODOLOGÍA DE LA INVESTIGACIÓN

SAMM (Software Assurance Maturity Model)

Es un marco de referencia abierto cuyo objetivo es ayudar a las organizaciones a formular e implementar una estrategia para la seguridad de software. Estos recursos permiten:

- La evaluación de las prácticas de seguridad de aplicaciones existente.
- Implementar un programa de de seguridad software adecuado en iteraciones bien definidas.
- De
- De



Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

METODOLOGÍA DE LA INVESTIGACIÓN

El ASVS (Application Security Verification Standard) provee un base para controles de seguridad técnicos para testing de aplicaciones, así como controles de seguridad en el entorno, para proteger la aplicación de vulnerabilidades. Este estándar puede ser usado para establecer el nivel de confianza en la seguridad de aplicaciones WEB.

Su uso también puede aplicarse para contemplar los requisitos de seguridad de aplicaciones.

Versión vigente: 3.0.1 (2017)

DESARROLLO DE SOFTWARE

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

METODOLOGÍA DE LA INVESTIGACIÓN

REQUISITOS DE VERIFICACIÓN DETALLADA

- V1: Arquitectura, diseño y modelado de amenazas
- V2: Autenticación
- V3: Gestión de Sesiones
- V4: Control de Acceso
- V5: Manejo de Entrada de Datos Malicioso
- V7: Criptografía de almacenamiento
- V8: Gestión y registro de errores
- V9: Protección de Datos
- V10: Comunicaciones
- V11: Configuración de seguridad HTTP
- V13: Controles de código Malicioso
- V15: Lógica del Negocio
- V16: Archivos y Recursos
- V17: Móviles
- V18: Servicios Web
- V19: Configuración

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

METODOLOGÍA DE LA INVESTIGACIÓN

EJEMPLOS DE REQUISITOS DE ASVS

- Se debe definir una arquitectura de alto nivel para la aplicación. (Arquitectura)
- Todas las páginas y recursos de forma predeterminada deben requerir autenticación, excepto los destinados específicamente a ser públicos. (Autenticación)
- Las sesiones deben invalidarse después de un período de inactividad. (Sesiones)
- El acceso a los registros debe estar protegido, de tal manera que sólo los objetos o datos autorizados sean accesibles (Control de Acceso)
- Las rutinas de validación de entrada se deben aplicar en el lado del servidor. (Manejo de entrada)
- Verificar que la aplicación no emita mensajes de error o rastros de pilas que contengan datos sensibles que podrían ayudar a un atacante (Gestión de Errores).
- La aplicación para móviles no debe almacenar datos confidenciales en recursos compartidos potencialmente no cifrados en el dispositivo (Móvil).

Instituto Superior Tecnológico del Azuay

Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia CET-BOLIVIA

METODOLOGÍA DE LA INVESTIGACIÓN

GESTIÓN DE RIESGOS

METODOLOGÍA DE LA INVESTIGACIÓN

EJEMPLO GESTIÓN DE RIESGOS

Identificación	Nuestro proyecto de desarrollo involucra el tratamiento de información de datos personales. Hemos identificado que el usuario y equipo de desarrollo desconoce la normativa y los controles a aplicar. Identificamos el riesgo de realizar muchos reprocesos en el desarrollo para incorporar cambios referidos a requisitos de seguridad de la normativa, incumpliendo plazos.
Análisis	La probabilidad es alta y el impacto alto. El nivel de riesgo es alto.
Evaluación	Dado que el nivel de riesgo es alto. Nuestros criterios establecen que deben tratarse, y los riesgos altos en mayor prioridad.
Tratamiento	a) Capacitar al personal involucrado en la normativa de datos personales. b) Definir los requisitos de seguridad. c) Realizar auditoría post-implementación

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

METODOLOGÍA DE LA INVESTIGACIÓN

REVISIÓN DE DISEÑO

Identificar Vulnerabilidades en el Diseño propuesto a través de Identificación de Amenazas y Análisis de Riesgo de la Arquitectura

- **Verificar el Diseño de Arquitectura de seguridad Propuesto**, incluye la arquitectura de datos, arquitectura de la aplicación, arquitectura de infraestructura red y sistemas.

- Verificar que los requisitos de Seguridad (**OWASP Application Security Verification Standard)** han sido contemplados en las especificaciones de la solución.

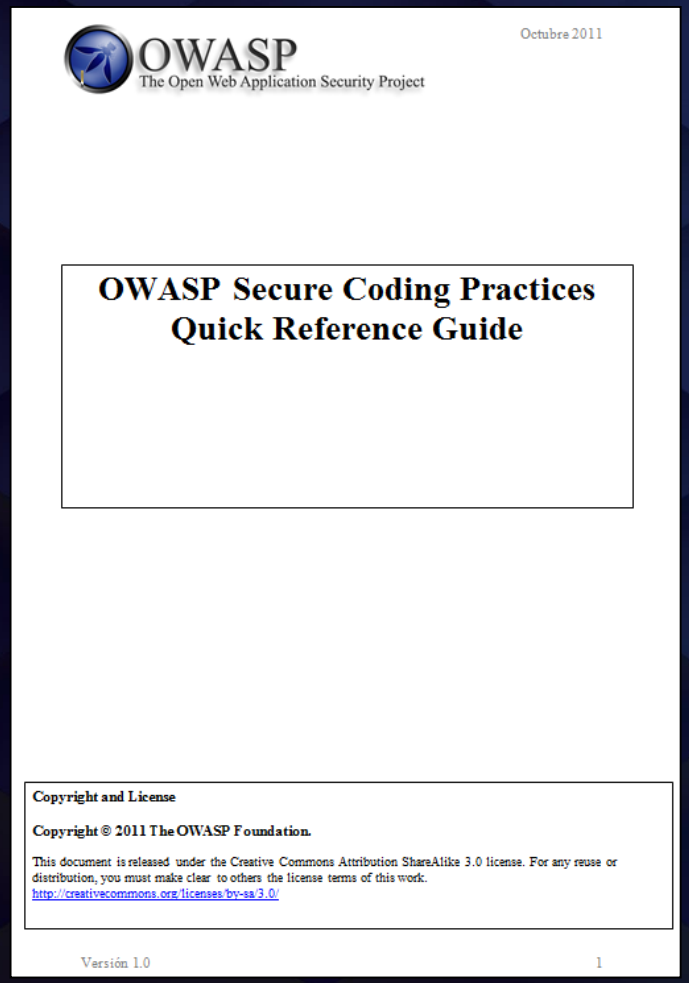
Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

METODOLOGÍA DE LA INVESTIGACIÓN

OWASP SECURE CODING PRACTICES


OWASP
The Open Web Application Security Project

Octubre 2011

OWASP Secure Coding Practices Quick Reference Guide

Conjunto de Prácticas comunes de codificación de software estructuradas a manera de Checklist. La implementación de estas prácticas mitiga las vulnerabilidades más comunes de software.

Versión 2011

Congreso Internacional de DESARROLLO DE SOFTWARE

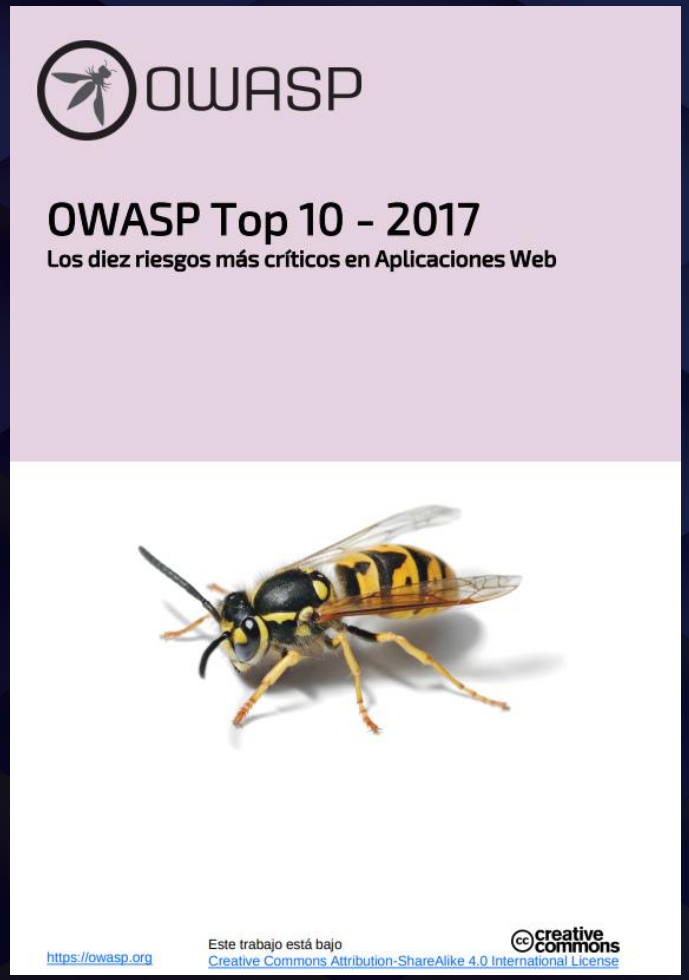
Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

METODOLOGÍA DE LA INVESTIGACIÓN

OWASP TOP TEN



El objetivo principal del Top 10 es educar a los desarrolladores, diseñadores, arquitectos, gerentes, y organizaciones; sobre las **consecuencias de las vulnerabilidades** de seguridad más importantes en aplicaciones web.

El Top 10 provee las **guías para identificar las vulnerabilidades y las recomendaciones técnicas básicas** sobre cómo protegerse en estas áreas de alto riesgo y también provee orientación sobre los pasos a seguir.

Congreso Internacional de DESARROLLO DE SOFTWARE

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

METODOLOGÍA DE LA INVESTIGACIÓN

OWASP CODE REVIEW GUIDE

Es un documento técnico dirigido al personal responsable de la revisión de código, a fin de que puedan realizar esa actividad usando las mejores prácticas en seguridad.
Versión Vigente: 2.0 (2017)

METODOLOGÍA DE LA INVESTIGACIÓN

OWASP CODE REVIEW GUIDE

Sample 7.7

```
1  HttpServletRequest request = ...;
2 String userName = request.getParameter("name");
3  Connection con  = ...
4   String query = "SELECT * FROM Users WHERE   name = '" + userName + "'";
5 con.execute(query);
```

An example of a vulnerable java code

The input parameter "name" is passed to the String query without any proper validation or verification. The query 'SELECT* FROM users where name" is equal to the string 'username' can be easily misused to bypass something different that just the 'name'. For example, the attacker can attempt to pass instead in this way accessing all user records and not only the one entitled to the specific user

```
'  OR  1=1.
```

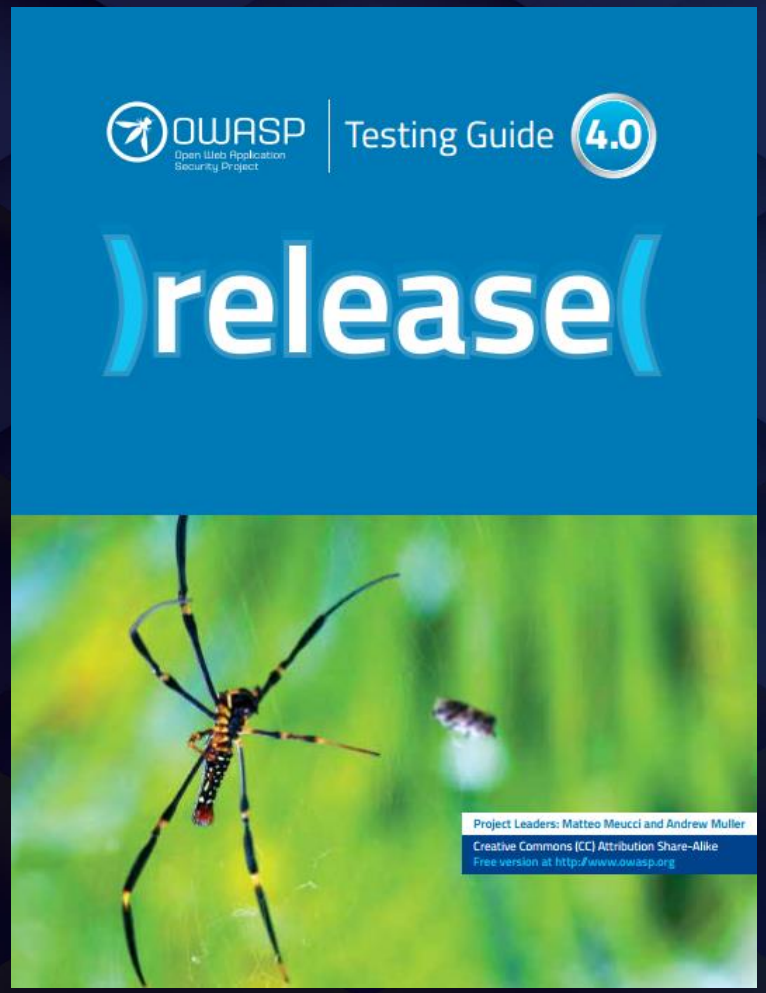
Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

METODOLOGÍA DE LA INVESTIGACIÓN

OWASP TESTING GUIDE



La guía de pruebas tiene como objetivo cubrir los procedimientos y herramientas para realizar las pruebas de seguridad de las aplicaciones.

La mejor manera de usar esta guía es como parte de una verificación exhaustiva de la seguridad en aplicaciones.

Versión vigente: 4.0 (2015)

Congreso Internacional de DESARROLLO DE SOFTWARE

METODOLOGÍA DE LA INVESTIGACIÓN

OWASP TESTING GUIDE

PRUEBAS DE CAJA NEGRA Y EJEMPLO

Se tiene un servicio web que acepta la siguiente petición HTTP por el método GET:

```
https://www.ws.com/accountinfo?accountnumber=12039475&userId=asi9485jfuhe92
```

La respuesta debería ser similar a:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<Account="12039475">
<balance>€100</balance>
<body>Bank of Bannana account info</body>
</Account>
```

Comprobar la validación de datos en este servicio web REST es similar a las pruebas de una aplicación genérica:

Tratar ataques tales como:

```
https://www.ws.com/accountinfo?accountnumber=12039475' exec master..xp_cmdshell 'net user Vxr
pass /Add &userId=asi9485jfuhe92
```

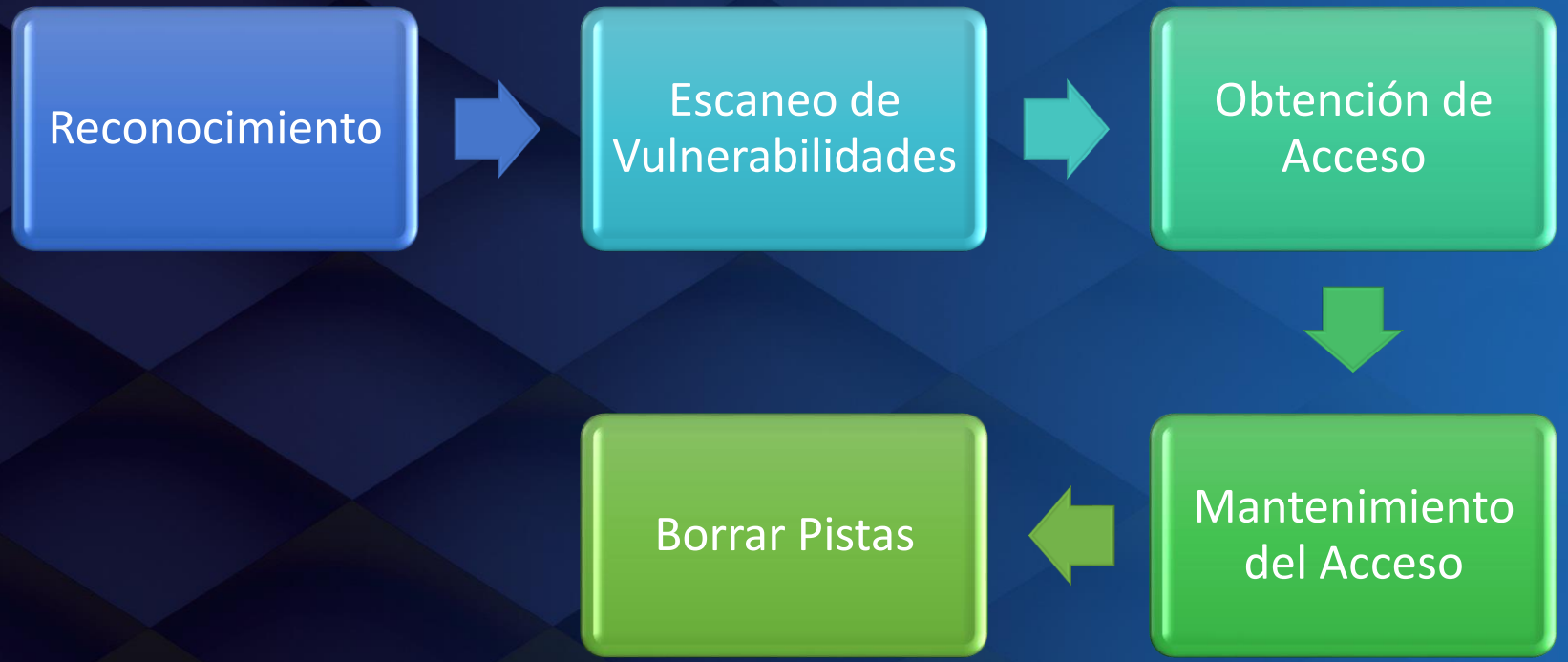
Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

METODOLOGÍA DE LA INVESTIGACIÓN

ANÁLISIS DE VULNERABILIDADES / TEST PENETRACIÓN



Congreso Internacional de DESARROLLO DE SOFTWARE

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

METODOLOGÍA DE LA INVESTIGACIÓN

ISO 27001:2013
A.14 Adquisición, desarrollo y mantenimiento de sistemas

A.14.1 Requisitos de Seguridad de los Sistemas de Información		
A.14.1.1	Análisis y especificación de requisitos de seguridad de información	Requisitos de seguridad en requisitos de nuevos sistemas o mejoras
A.14.1.2	Aseguramiento de servicios de aplicaciones sobre redes públicas	Debe ser protegida de actividad fraudulenta, divulgación no autorizada o modificación
A.14.1.3	Protección de transacciones en servicios de aplicación	Protegida de trasmisión incompleta, ruteo incorrecto, alteración o divulgación no autorizada

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

METODOLOGÍA DE LA INVESTIGACIÓN

ISO 27001:2013
A.14 Adquisición, desarrollo y mantenimiento de sistemas

A.14.2 Seguridad en los procesos de desarrollo y soporte	
A.14.2.1	Política de desarrollo seguro
A.14.2.2	Procedimientos de control de cambio
A.14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa

A.14.2 Seguridad en los procesos de desarrollo y soporte	
A.14.2.4	Restricciones sobre cambios a los paquetes (código fuente y librerías) de software
A.14.2.5	Principios de ingeniería de software seguros
A.14.2.6	Ambiente de desarrollo seguro

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

METODOLOGÍA DE LA INVESTIGACIÓN

ISO 27001:2013
A.14 Adquisición, desarrollo y mantenimiento de sistemas

A.14.2 Seguridad en los procesos de desarrollo y soporte	
A.14.2.7	Desarrollo contratado externamente (supervisar y monitorear)
A.14.2.8	Prueba de seguridad del sistema
A.14.2.9	Pruebas de aceptación del sistema

A.14.3 Datos de prueba	
A.14.3.1	Protección de datos de prueba

METODOLOGÍA DE LA INVESTIGACIÓN

OTROS MARCOS DE REFERENCIA O FUENTES

Marco / Certificación	Descripción
ISECOM OSSTMM 3 – The Open Source Security Testing Methodology Manual	Manual para las pruebas y análisis de seguridad.
MILE2 - Certified Secure Web Application Engineer	Certificación de MILE2 para formar profesionales para desarrollo seguro de aplicaciones. Cuenta con material muy desarrollado para tal fin.
EC-Council Certified Ethical Hacking (CEH)	La más completa certificación para realizar hackeo ético, análisis de vulnerabilidades, test de prenetración. Cuenta con una sección para Hacking de Aplicaciones Web.

METODOLOGÍA DE LA INVESTIGACIÓN

MARCOS NORMATIVOS

Sistema de Gestión de Seguridad de Información

- Uso de la Norma "ISO/IEC 27001:2013 Sistemas de Gestión de Seguridad de la Información".

Datos Personales

- Ley de Protección de Datos Personales. Reglamento. Directiva de Seguridad.

Otros

- Ley y Reglamento de Firmas y Certificados Digitales.
- Uso de la Norma "ISO/IEC 12207:2017 Ingeniería de Software y Sistemas. Procesos del ciclo de vida del software".
- Transición al Protocolo IP V6.

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

RESULTADO Y DISCUSIONES

¿CÓMO VENCER LA RESISTENCIA A APLICAR SEGURIDAD EN LAS APLICACIONES?

- Capacitación y Concientización
- Capacitación y Concientización
- Capacitación y Concientización
- ….

Otros importantes:

- Liderazgo
- Controles, Seguimiento, Monitoreo

Congreso Internacional de DESARROLLO DE SOFTWARE

RESULTADO Y DISCUSIONES

RETOS DE LA SEGURIDAD

Es importante que los desarrolladores conozcan todos los vectores de ataque y aspectos de seguridad. El desarrollador debe trabajar para asegurar que todos los puntos de entrada potenciales están cubiertos.

La seguridad puede comprometer la funcionalidad. El uso de nuevas tecnologías puede agregar complejidad a un diseño de software seguro.

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

RESULTADO Y DISCUSIONES

ESTRATEGIAS PARA LA IMPLEMENTACIÓN

Establezca procedimientos y controles claros, difúndalos y asegúrese que su equipo lo entiende

Haga una implementación gradual, mientras su equipo va creando hábitos de desarrollo seguro

Disponga de uno o más especialistas en seguridad de aplicaciones, de manera que no se quede sin soporte

Si trabaja con proveedores para el desarrollo, establezca claramente los procedimientos y estándares a cumplir, en cláusulas contractuales

Conforme vaya obteniendo resultados preséntelos a la dirección, para que mantenga su liderazgo y apoyo

ernacional de
ROLLO
DE SOFTWARE

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

CONCLUSIONES

1. La aplicación de un Ciclo de Desarrollo Seguro permite que las aplicaciones sean liberadas en entornos productivos con un adecuado nivel de seguridad.

2. Implementar y mantener un Ciclo de Desarrollo Seguro implica un esfuerzo permanente de la organización. A lo largo de los años, retribuye en menores costos de desarrollo y mantenimiento.

3. En la medida que el equipo de desarrollo conozca más sobre aspectos de seguridad, tendrá mejor oportunidad de aplicar las medidas que eviten que la aplicación sea vulnerable.

4. Existen marcos de referencia que ya definen y facilitan la implementación de un Ciclo de Desarrollo Seguro. Para empezar no hay que “reinventar la rueda”.

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

- Ingresa a:
- www.cidecuador.com
- Al finalizar este evento podrás encontrar esta presentación en su respectiva página web.

Congreso Internacional de
DESARROLLO DE SOFTWARE