Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

La Interfaz de Seguridad en Métrica versión 3 y su implementación a través de la familia de normas ISO/IEC 27000. Un caso aplicado en una empresa certificada en CMMI

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

- Francisco Javier Valencia Duque
- PhD en Ingeniería, Industria y Organizaciones
- CISA/CRISC/CF/LA 27001
- Universidad Nacional de Colombia
- fjvalenciad@unal.edu.co

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

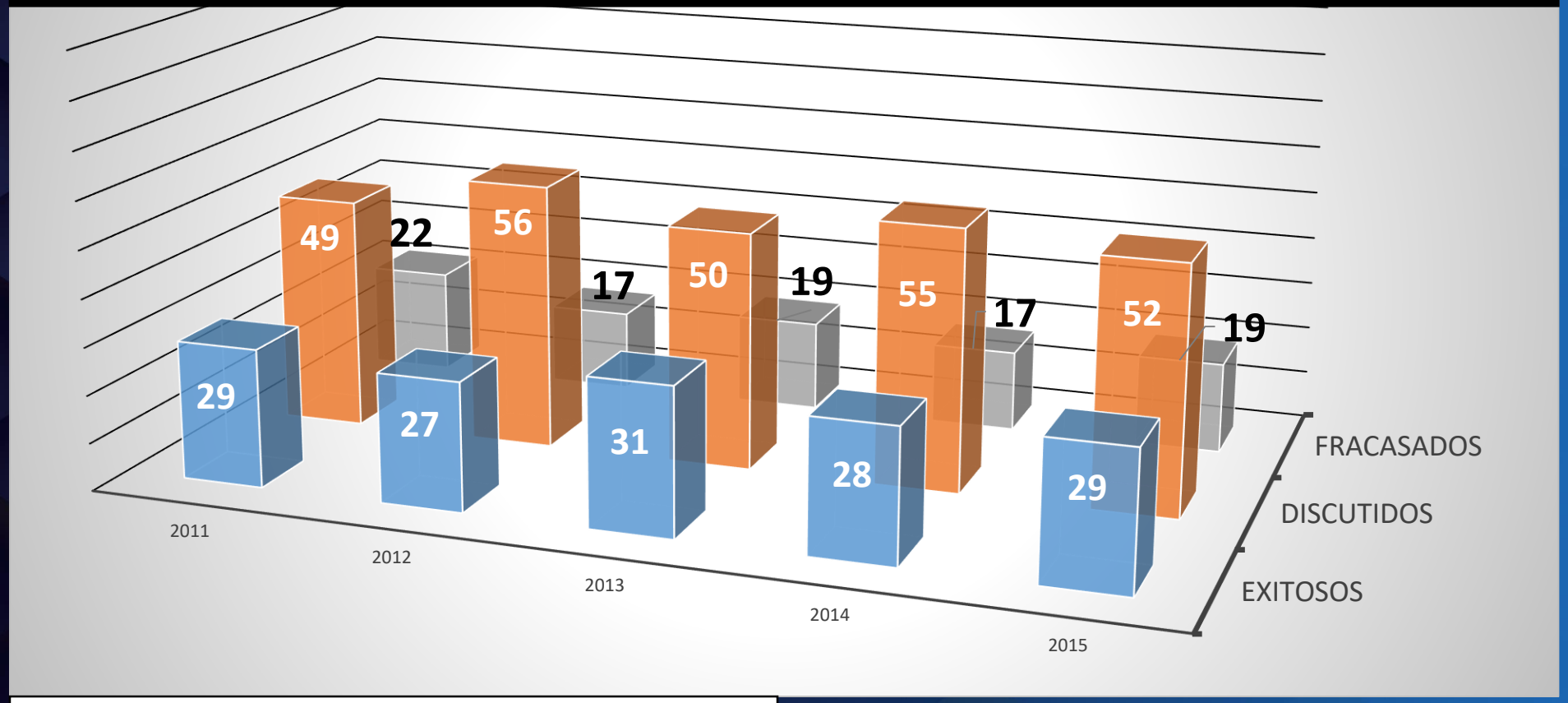
INTRODUCCIÓN

C.A Technologies advierte que el 77% de las apps que pasan a la fase de producción son vulnerables a ciberataques. Esto se debe a que, **con la premura de posicionar sus productos, muchas empresas dejan de lado la seguridad**. No obstante, ello es un error lamentable pues, más tarde, conduce a costosos errores y, finalmente, a que los clientes pierdan la confianza en las instituciones.

Fuente: https://www.widefense.com/devsecops-o-como-impulsar-el-desarrollo-de-aplicaciones-seguras/

INTRODUCCIÓN

Distribución porcentual del nivel de éxito obtenido en proyectos de software (Informe CHAOS 2015)



Fuente: elaborado a partir de (Navarro, 2018)

Instituto Superior Tecnológico del Azuay

CIDE Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia CET-BOLIVIA

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

- El software esta presente en las actividades cotidianas y por ello es considerado uno de los activos esenciales en la operación de las organizaciones, de allí el surgimiento de disciplinas como SAM

- SecDevOps o Secure DevOps

- Sistema de gestión de seguridad de la Información basado en la familia de normas ISO/IEC 27000

- “Los ingenieros de software deben conocer tanto las amenazas a la seguridad que enfrentan los sistemas, como las formas en las que es posible neutralizar tales amenazas”(SOMMERVILLE, 2011, p.367).

- Los proyectos de desarrollo de software son actividades de alto riesgo (Neves & Silva, 2016) y si no atacas activamente los riesgos, ellos te atacaran activamente (Khater, Mohamed, & Kamel, 2013)

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

CasaSegura

Análisis de riesgos

La escena: Oficina de Doug Miller antes de comenzar el proyecto de software CasaSegura.

Participantes: Doug Miller (gerente del equipo de ingeniería del software CasaSegura) y Vinod Raman, Jamie Lazar y otros miembros del equipo de ingeniería de software del producto.

La conversación:

Doug: Me gustaría usar algo de tiempo en una lluvia de ideas para el proyecto CasaSegura.

Jamie: ¿Acerca de que puede salir mal?

Doug: Sip. Aquí hay algunas categorías donde las cosas pueden salir mal. [Muestra a todos las categorías anotadas en la introducción a la sección 28.3.]

Vinod: Hmmm... quieres que sólo las mencionemos o...

Doug: No. Esto es lo que creo que debemos hacer. Todo mundo haga una lista de riesgos... ahora...

[Transcurren diez minutos, todos escriben].

Doug: Muy bien, deténganse.

Jamie: ¡Pero no he terminado!

Doug: Está bien. Revisaremos la lista de nuevo. Ahora, para cada ítem en su lista, asignen un porcentaje de probabilidad de que ocurrirá el riesgo. Luego, asignen un impacto al proyecto sobre una escala de 1 (menor) a 5 (catastrófico).

Vinod: Si creo que el riesgo es un volado, especifico una probabilidad de 50 por ciento y, si creo que tendrá un impacto de proyecto moderado, especifico un 3, ¿cierto?

Doug: Exactamente.

[Transcurren cinco minutos, todos escriben].

Doug: Muy bien, deténganse. Ahora haremos una lista grupal en el pizarrón. Yo escribiré; cada uno de ustedes dirá una entrada de su lista.

[Transcurren quince minutos; crean la lista].

Jamie (apunta hacia el pizarrón y ríe): Vinod, ese riesgo (apunta hacia una entrada en el pizarrón) es ridículo. Hay una mayor probabilidad de que a todos nos caiga un rayo. Debemos removerlo.

Doug: No, dejémoslo por ahora. Consideremos todos los riesgos, sin importar cuán locos parezcan. Más tarde filtraremos la lista.

Jamie: Pero ya tenemos más de 40 riesgos... ¿cómo vamos a manejarlos todos?

Doug: No podemos. Es por eso por lo que definiremos un corte después de ordenarlos. Yo haré ese corte y nos reuniremos de nuevo mañana. Por ahora, regresen a trabajar... y en su tiempo libre piensen en cualquier riesgo que hayan olvidado.

Pressman, R. (2013). *Ingenieria de Software*.

Instituto Superior Tecnológico del Azuay

Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia CET-BOLIVIA

MARCOS DE REFERENCIA DE RIESGOS Y SEGURIDAD DE APLICACIONES

ISO/IEC 27034 Seguridad de aplicaciones

- **ISO/IEC 27034-1:2011 — Information technology — Security techniques — Application security — Overview and concepts**
- **ISO/IEC 27034-2:2015 — Information technology — Security techniques — Application security — Organization normative framework**
- **ISO/IEC 27034-3:2018 — Information technology — Security techniques — Application security — Application security management process**
- **ISO/IEC 27034-4 — Information technology — Security techniques — Application security — Application security validation (draft)**
- **ISO/IEC 27034-5:2017 — Information technology — Security techniques — Application security — Protocols and application security control data structure**
- **ISO/IEC TR 27034-5-1:2018 — Information technology — Security techniques — Application security — Protocols and application security control data structure, XML schemas**
- **ISO/IEC 27034-6:2016 — Information technology — Security techniques — Application security — Case studies**
- **ISO/IEC 27034-7:2018 — Information technology — Security techniques — Application security — Assurance prediction framework**

MARCOS DE REFERENCIA DE RIESGOS Y SEGURIDAD DE APLICACIONES

Instituto Superior Tecnológico del Azuay

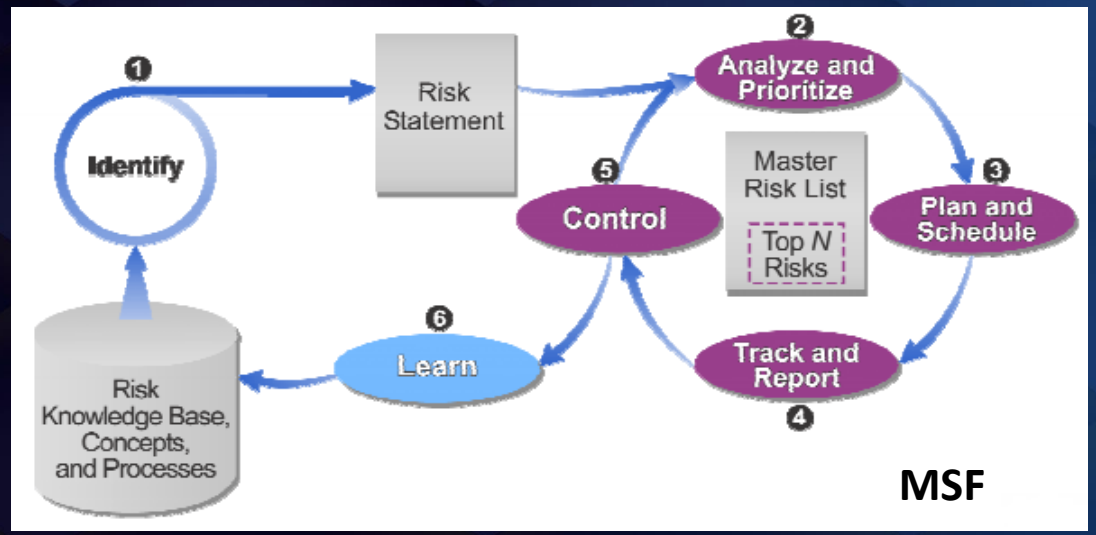
CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

Microsoft® Security Development Lifecycle

Software Assurance Maturity Model
A guide to building security into software development
Version 1.5

BSIMM
Building Security in Maturity Model (BSIMM) Version 9



MSF

La gestión de riesgos (RSKM) es un proceso que hace parte del nivel 3 (Definido) de CMMI

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

PROYECTO DE IMPLEMENTACIÓN DEL SGSI BASADO EN ISO/IEC 27001:2013 EN SIGMA INGENIERÍA

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

OBJETIVO DEL PROYECTO

Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) para cumplir con los requerimientos establecidos en la ISO/IEC 27001:2013 y los requerimientos impuestos por los clientes de la empresa.

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

ACERCA DE LA EMPRESA

SIGMA INGENIERIA

15 AÑOS

CMMI DEV /5

http://www.sigmaingenieria.com.co/

Sigma Ingeniería es líder en software de georreferenciación y SIG para la gestión pública en Colombia

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

ACERCA DE LA EMPRESA

GEOLUMINA®

Herramienta tecnológica que consolida y sistematiza a empresas y concesiones de alumbrado, permitiendo dar cumplimiento al reglamento técnico de iluminación y alumbrado público; Geolúmina es una plataforma tecnológica que optimiza el funcionamiento de su ejercicio organizacional ofreciendo información de calidad, actualizada y visible para la toma de decisiones a nivel gerencial y operativo.

Geoambiental®

Herramienta tecnológica que pretende ayudar en una adecuada y correcta intervención del medio ambiente; Geoambiental es una plataforma tecnológica basada en información geográfica que tiene como fin fortalecer los procesos y procedimientos de las Corporaciones Autónomas Regionales y demás organizaciones que gestionan el medio ambiente.

GeoAseo®

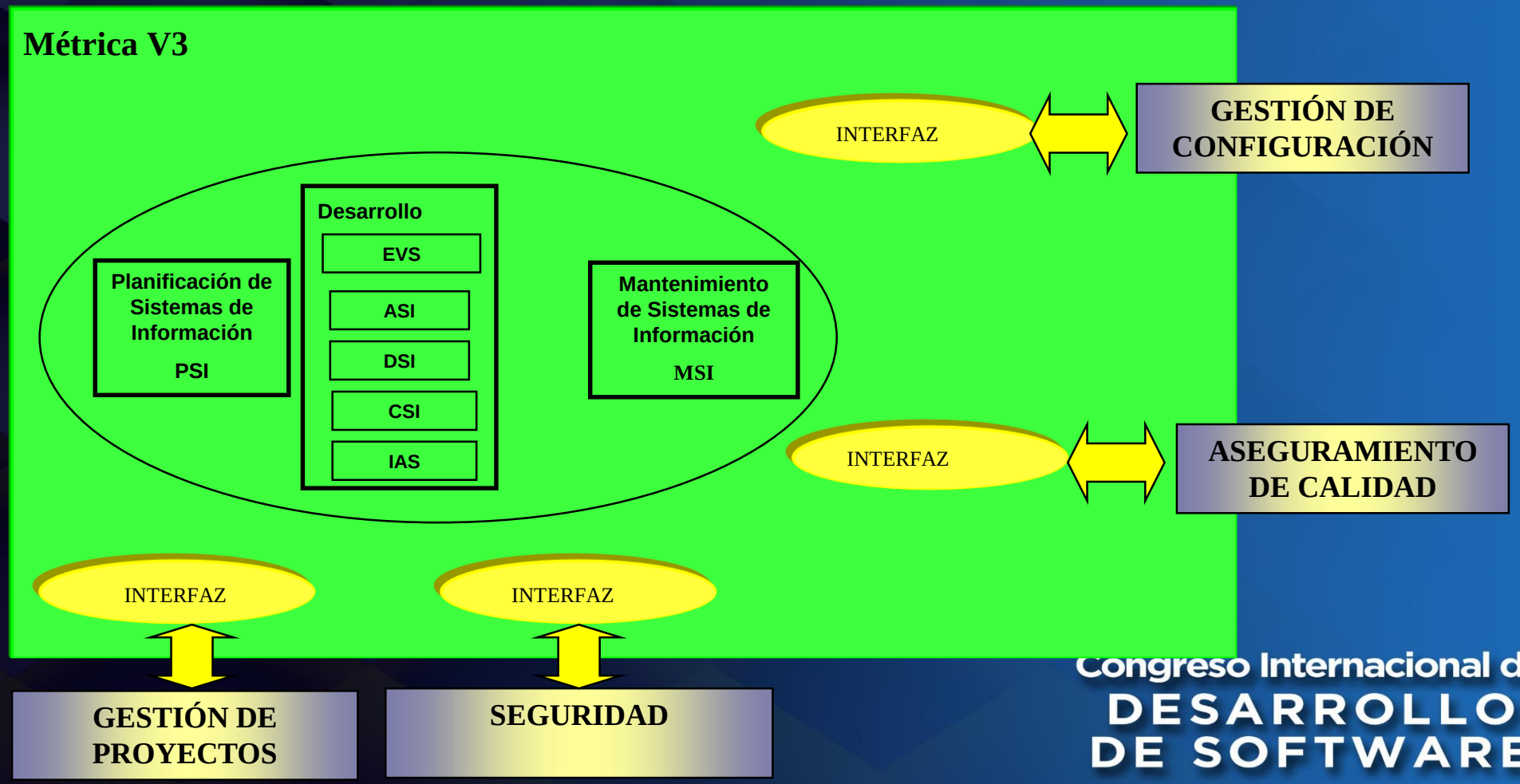
Herramienta tecnológica que logra optimizar el ejercicio de las empresas de aseo en operaciones como rutas, recolección, barrido, entre otras variables que se presentan en el proceso de aseo en las ciudades y municipios de un país. Sistema de información que ofrece indicadores de gestión, encaminados a mejorar calidad, eficacia, productividad y rentabilidad de su organización.

Congreso Internacional de
DESARROLLO
DE SOFTWARE

QUE ES MÉTRICA

Metodología de Planificación, Desarrollo y Mantenimiento de sistemas de información

ESTRUCTURA DE MÉTRICA



Instituto Superior Tecnológico del Azuay

CIDE Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia CET-BOLIVIA

Congreso Internacional de DESARROLLO DE SOFTWARE

Instituto Superior Tecnológico del Azuay

Centro de Investigación y Desarrollo Ecuador

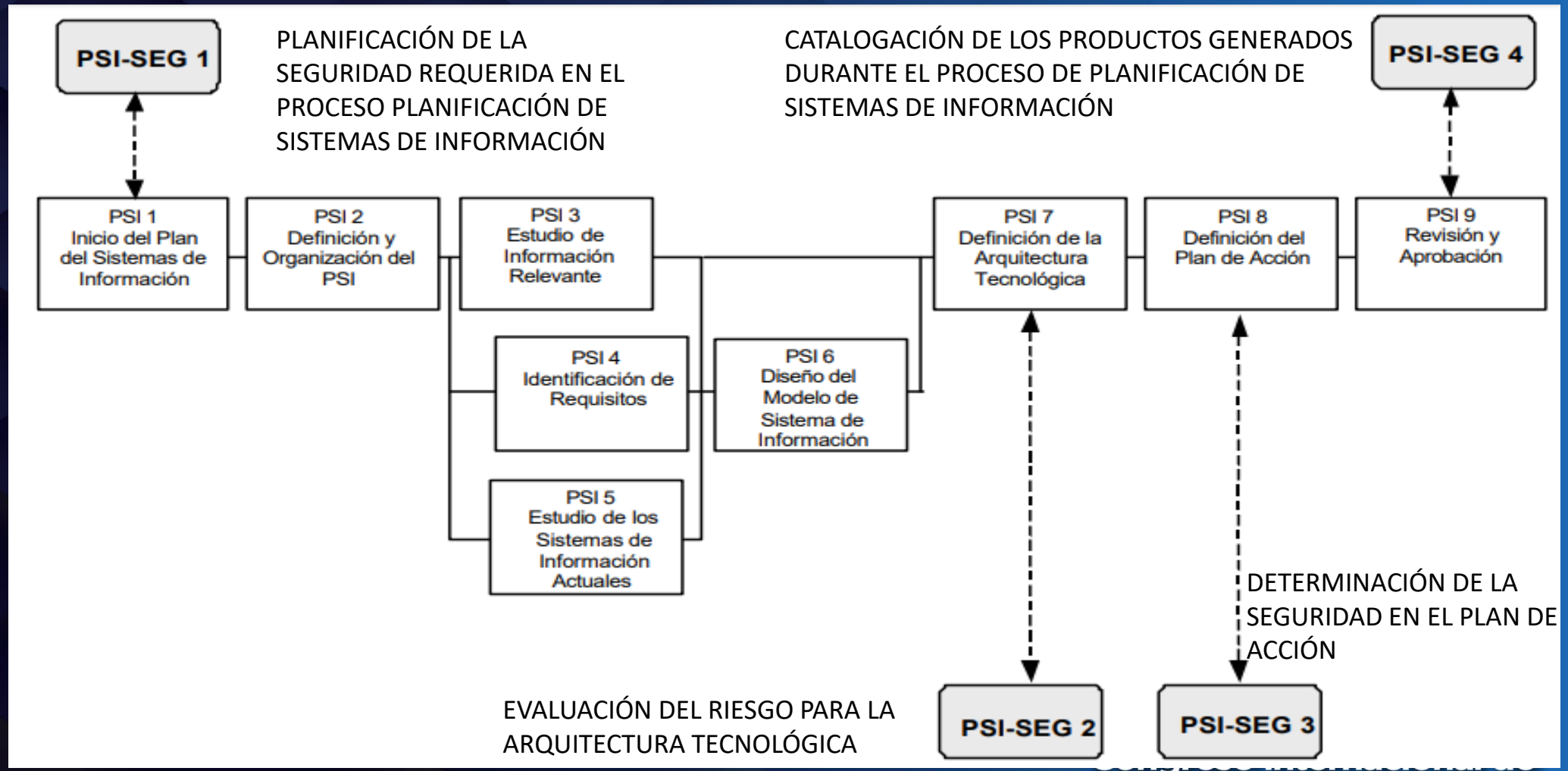
Centro de Estudios Transdisciplinarios Bolivia CET-BOLIVIA

INTERFAZ DE SEGURIDAD DE MÉTRICA

La interfaz de Seguridad hace posible incorporar durante la fase de desarrollo las funciones y mecanismos que refuerzan la seguridad del nuevo sistema y del propio proceso de desarrollo, asegurando su consistencia y seguridad, completando el plan de seguridad vigente en la organización o desarrollándolo desde el principio, utilizando MAGERIT como metodología de análisis y gestión de riesgos en el caso de que la organización no disponga de su propia metodología.

- Es considerado un requerimiento funcional
- El análisis de los riesgos constituye una pieza fundamental en el diseño y desarrollo de sistemas de información seguros

INTERFAZ DE SEGURIDAD DE MÉTRICA



Instituto Superior Tecnológico del Azuay

Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia CET-BOLIVIA

DESARROLLO DEL PROYECTO

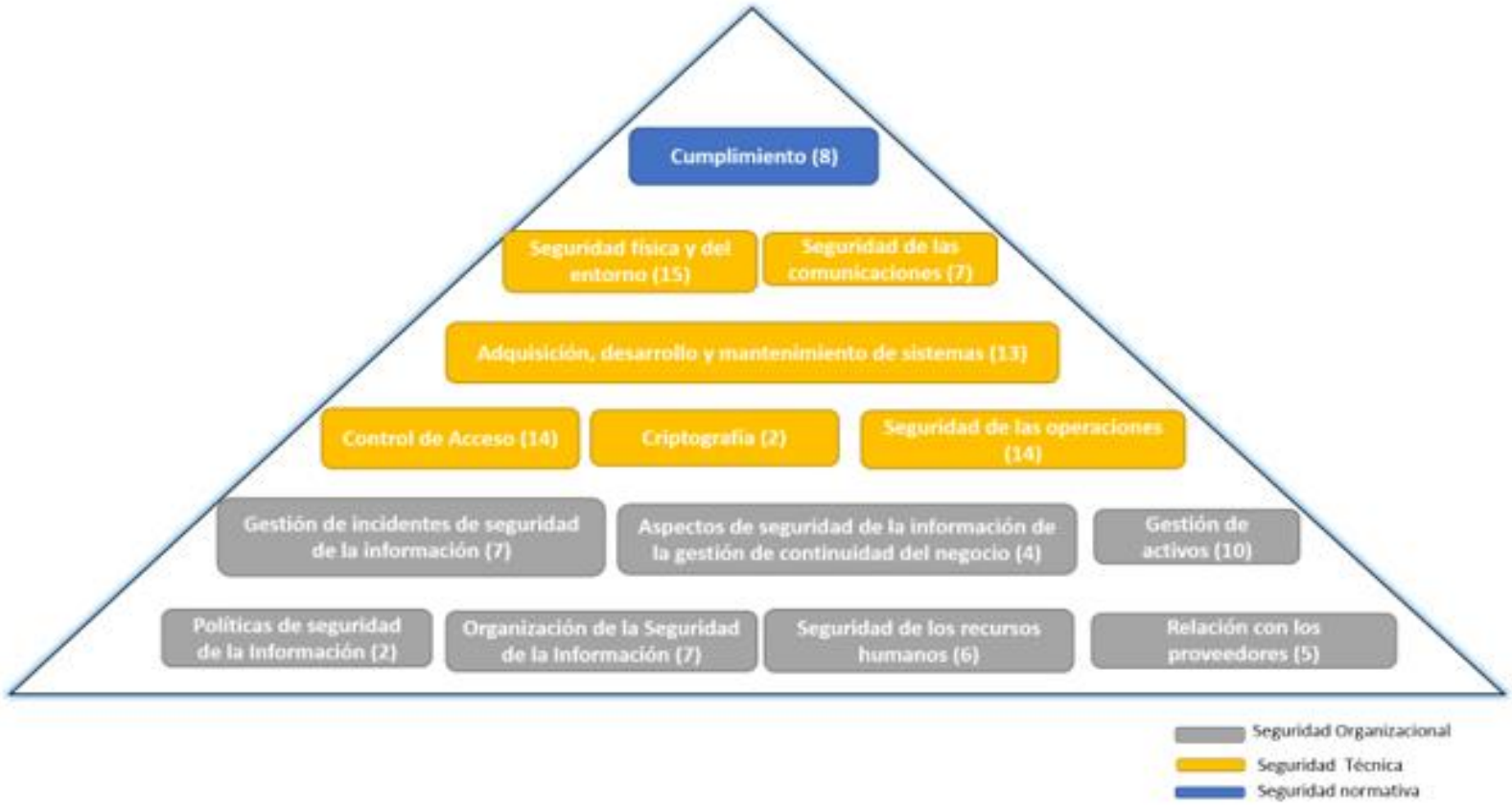
Fuente: (Valencia Duque & Orozco-alzate, 2017).

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

DESARROLLO DEL PROYECTO



Fuente: (Valencia Duque & Orozco-alzate, 2017)

ISO/IEC 27002:2013

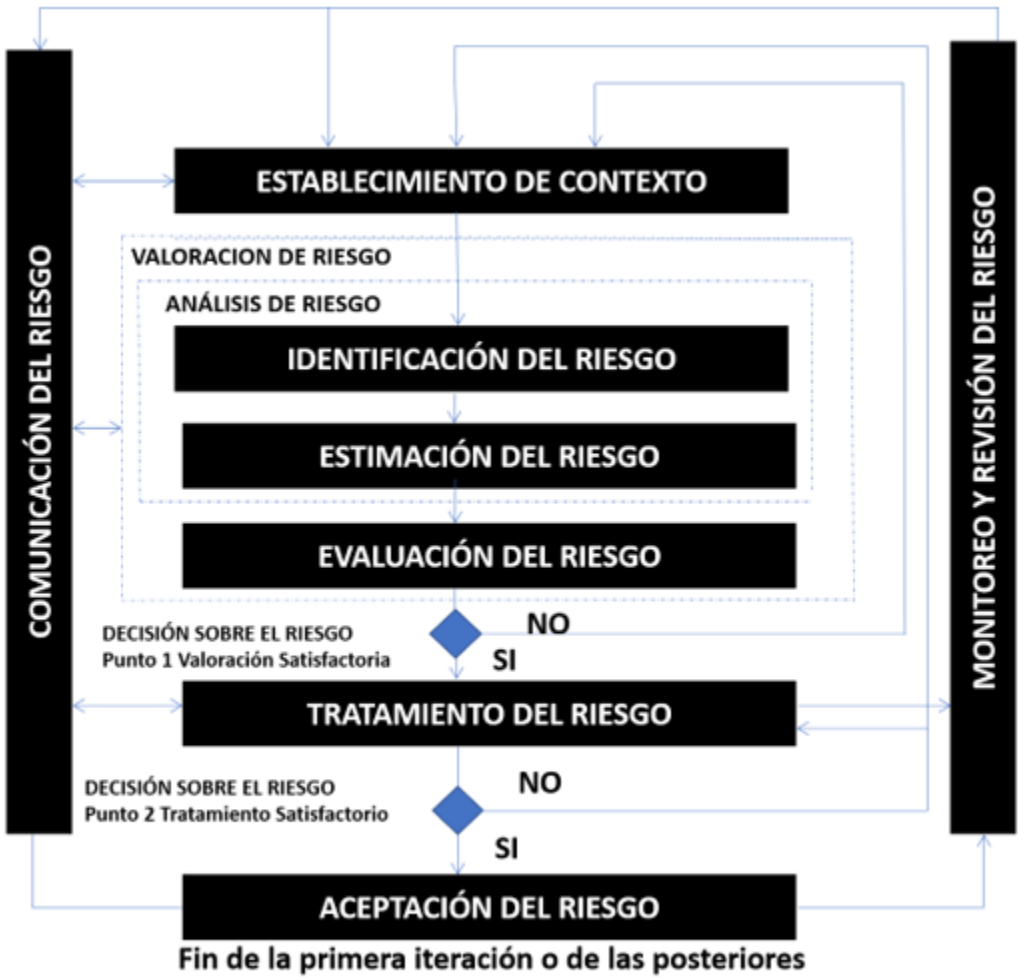
Congreso Internacional de DESARROLLO DE SOFTWARE

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

DESARROLLO DEL PROYECTO

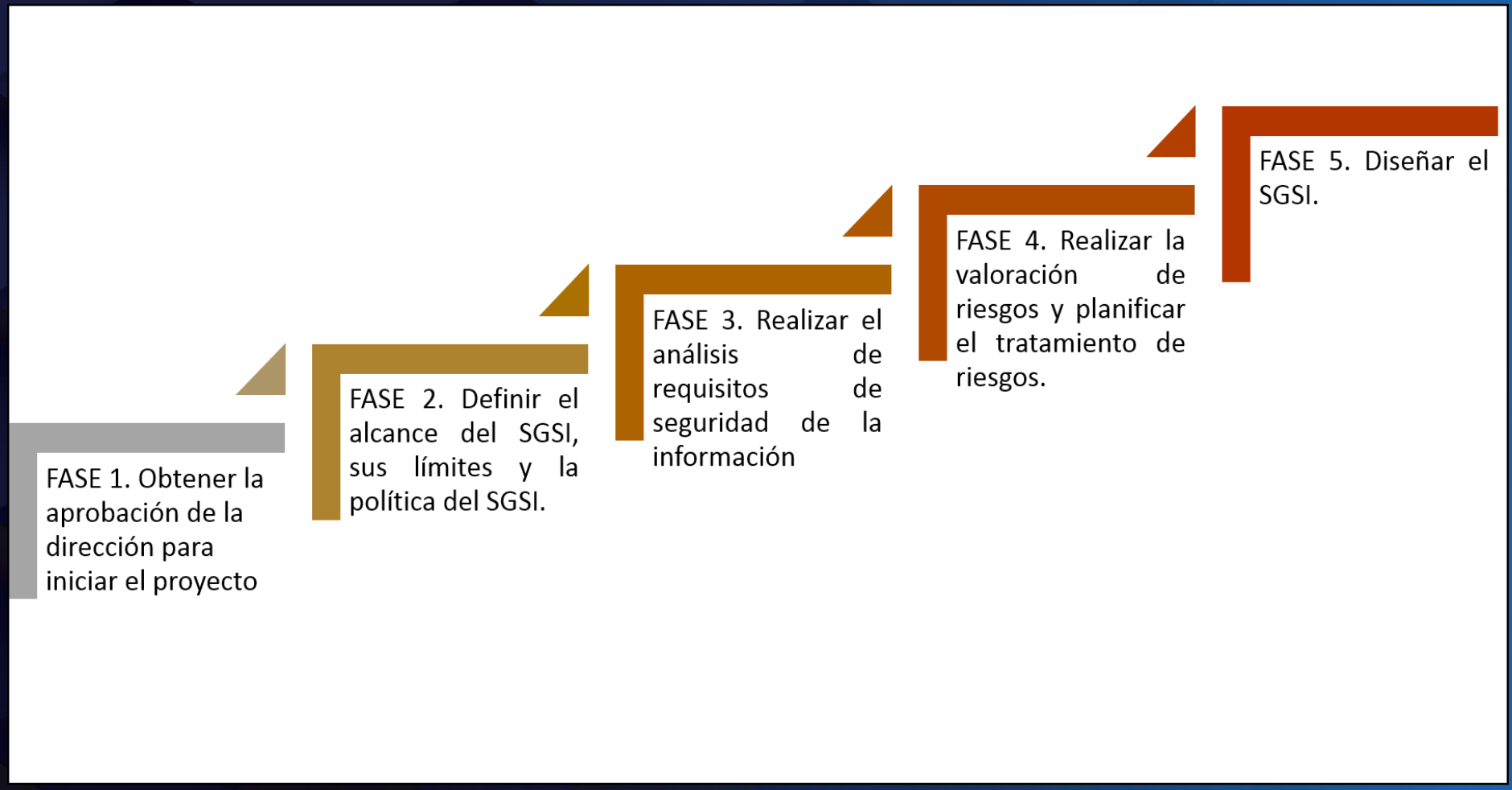


Fuente: (ICONTEC, 2009b)

ISO/IEC 27005:2008

Congreso Internacional de DESARROLLO DE SOFTWARE

DESARROLLO DEL PROYECTO



ISO/IEC 27003:2010

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

Congreso Internacional de DESARROLLO DE SOFTWARE

PARÁMETROS DE PROBABILIDAD

VALOR	NIVEL PROBABILIDAD	DESCRIPCIÓN	FRECUENCIA
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales. Probabilidad muy baja.	No se ha presentado en los últimos 5 años.
2	Improbable	El evento puede ocurrir en algún momento. Probabilidad baja.	Al menos 1 vez en los últimos 5 años.
3	Posible	El evento podría ocurrir en algún momento. Probabilidad media.	Al menos 1 vez en los últimos 2 años.
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias. Probabilidad alta.	Al menos 1 vez en el último año.
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias. Probabilidad muy alta.	Más de 1 vez al año.

PARÁMETROS DE IMPACTO

		CRITERIOS DE SEGURIDAD		
VALOR	NIVEL	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
5	CRÍTICO	Información de alto nivel de confidencialidad de los clientes y/o del negocio podría estar expuesta a terceros no autorizados	La generación de datos inexactos, incompletos o modificados sin autorización, causaría una grave afectación en la información y/o procesos del cliente y/o del negocio.	La información y/o los activos tecnológicos que soportan el negocio podrían estar fuera de servicio o no disponibles por más de 48 horas
4	ALTO	Información confidencial de los clientes y/o del negocio podría estar expuesta a terceros no autorizados	La generación de datos inexactos, incompletos o modificados sin autorización, causaría una afectación considerable en la información y/o procesos del cliente y/o del negocio.	La información y/o los activos tecnológicos que soportan el negocio podrían estar fuera de servicio o no disponibles entre 24 y 48 horas
3	INTERMEDIO	Información reservada de los clientes y/o del negocio podría estar expuesta a terceros no autorizados	La generación de datos inexactos, incompletos o modificados sin autorización, causaría una afectación importante en la información y/o procesos del cliente y/o del negocio.	La información y/o los activos tecnológicos que soportan el negocio podrían estar fuera de servicio o no disponibles entre 12 y 24 horas
2	MODERADO	Información importante de los clientes y/o del negocio podría estar expuesta a terceros no autorizados	La generación de datos inexactos, incompletos o modificados sin autorización, causaría una moderada afectación en la información y/o procesos del cliente y/o del negocio.	La información y/o los activos tecnológicos que soportan el negocio podrían estar fuera de servicio o no disponibles entre 6 y 12 horas
1	BAJO	Información considerada pública de los clientes y/o del negocio podría estar expuesta a terceros no autorizados	La generación de datos inexactos, incompletos o modificados sin autorización, causaría una baja afectación en la información y/o procesos del cliente y/o del negocio.	La información y/o los activos tecnológicos que soportan el negocio podrían estar fuera de servicio o no disponibles menos de 6 horas

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

CRITERIOS DE ACEPTABILIDAD

RIESGO/VULNERABILIDAD	CRITERIO	DESCRIPCIÒN	MONITOREO
1 a 5 /<=20%	ACEPTABLE	Se deben conservar las acciones y controles implementados para mantener el nivel de riesgo en este estado y monitorear constantemente su situación.	Realizar seguimiento mínimo cada 120 días
6 a 10 /21% AL 40%	TOLERABLE	Se requieren acciones que disminuyan la probabilidad o el impacto a un nivel aceptable.	Realizar seguimiento mínimo cada 90 días
11 a 15 /41 AL 60%	IMPORTANTE	Se hace indispensable desarrollar planes de acción y tomar medidas alternas que permitan gestionar el riesgo **en el corto plazo**, y evitar su impacto negativo en el logro de los objetivos.	Realizar seguimiento mínimo cada 60 días
16 a 20/61 AL 80%	INACEPTABLE	Se hace indispensable desarrollar planes de acción y tomar medidas alternas que permitan gestionar el riesgo **lo más pronto posible**, y evitar su impacto negativo en el logro de los objetivos.	Realizar seguimiento mínimo cada 30 días
21 a 25/> AL 80%	INADMISIBLE	Se hace indispensable desarrollar planes de acción y tomar medidas alternas que permitan gestionar el riesgo **de inmediato**, y evitar su impacto negativo en el logro de los objetivos.	Realizar seguimiento mínimo cada 15 días

ANÁLISIS DE BRECHA

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

Gap de la ISO/IEC 27002

CAPÍTULO DE LA NORMA	% AVANCE
4. CONTEXTO DE LA ORGANIZACIÓN	16%
5. LIDERAZGO	61%
6. PLANIFICACIÓN	8%
7. SOPORTE	46%
8. OPERACIÓN	0%
9. EVALUACIÓN DEL DESEMPEÑO	0%
10. MEJORA	0%
PROMEDIO GENERAL	19%

Categorias de control	Nivel de madurez	Aplican
5. Políticas de Seguridad de la Información	50,0%	2
6. Organización de la seguridad de la información	34,0%	7
7. Seguridad del recurso humano	57,0%	6
8. Gestión de activos	28,0%	10
9. Control de acceso	30,8%	14
10. Criptografia	0,0%	2
11. Seguridad física y del entorno	5,5%	11
12. Seguridad de las operaciones	30,4%	14
13. Seguridad de las comunicaciones	16,5%	7
14. Adquisición, desarrollo y mantenimiento de sistemas	37,7%	11
15. Relaciones con los proveedores	31,5%	4
16. Gestión de incidentes de seguridad de la información	21,0%	7
17. Aspectos de seguridad de la información de la gestión de continuidad del negocio	12,5%	4
18. Cumplimiento	17,5%	8
Promedio general	**26,6%**	**107**

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

ESTRUCTURA DE DESGLOSE DE ACTIVOS

1	PROCESOS DE NEGOCIO
2	SERVICIOS DE TI
3	DATOS/INFORMACIÓN/CONOCIMIENTO
4	SISTEMAS DE INFORMACIÓN TRANSACCIONALES
5	SISTEMAS DE INFORMACIÓN SOPORTE
6	MOTORES DE BASES DE DATOS
7	SISTEMAS OPERATIVOS
8	PC's DE ESCRITORIO E IMPRESORAS
9	SERVIDORES (Físicos, virtuales y en la nube)
10	CENTROS DE REDES Y CABLEADO
11	CENTROS DE COMPUTO
12	ENERGIA

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

ESTADO DE AVANCE DOCUMENTAL DEL PROYECTO

Numeral ISO/IEC 27001:2013		Documentación
4.3	Determinación del alcance del SGSI	El alcance debe estar disponible como información documentada
5.2	Política de seguridad	e) La política de seguridad debe estar disponible como información documentada
6.1.2.	Valoración de riesgos de seguridad de la información	Información documentada acerca del proceso de valoración de riesgos de la seguridad de la información
6.1.3	Tratamiento de riesgos de seguridad de la información	Información documentada acerca del proceso de tratamiento de los riesgos de seguridad de la información
6.1.3	Declaración de aplicabilidad	d) Declaración de aplicabilidad
6.2.	Objetivos de seguridad de la información y planes para lograrlos	Objetivos de la seguridad de la información
7.2	Competencia	Evidencia de la competencia de las personas relacionadas con la seguridad de la información
7.5.	Información documentada	b) La que la empresa ha determinado que es necesaria para la eficacia del SGSI
7.5.3	Control de la información documentada	La información documentada de origen externo
8.1	Planificación y control operacional	Información documentada para tener confianza de que los procesos se han llevado a cabo de acuerdo a lo planificado
8.2.	Valoración de la seguridad de la información	Resultados de las valoraciones de riesgos de la seguridad de la información
8.3	Tratamiento de riesgos de seguridad de la información	Resultados de los tratamientos de riesgos de la seguridad de la información
9.1	Seguimiento, medición, análisis y evaluación	Evidencia de los resultados del monitoreo y de la medición
9.2	Auditoría interna	g) conservar la información documentada como evidencia de la implementación del programa de auditoría y de los resultados de ésta.
9.3	Revisión por la dirección	Evidencia de los resultados de la revisión por la Dirección
10.1	No conformidades y acciones correctivas	Naturaleza de las no conformidades y cualquier acción posterior tomada
10.1	No conformidades y acciones correctivas	Resultados de cualquier acción correctiva

DESARROLLO DE SOFTWARE

TAXONOMIA DE RIESGOS DE SOFTWARE

triangulo de hierro (también llamado triángulo mágico, triángulo de la dirección de proyectos

El reporte técnico CMU/SEI-93-TR-06 denominado identificación de riesgos basados en taxonomía estableció tres clases de riesgos de software:

Ingeniería del producto: los aspectos técnicos del trabajo a ser desarrollado

Ambiente de desarrollo: los métodos, procedimientos y herramientas usadas para producir el producto.

Limitaciones del programa: los factores contractuales, organizacionales y operacionales dentro del cual el software es desarrollado, pero que por lo general esta por fuera del control directo de la administración.

ALGUNOS EJEMPLOS DE TAXONOMIAS

Clase	Categoría	Riesgo	Nro de veces
Ingeniería de producto	Requerimientos	Requisitos de clientes poco claros	29
		"Síndrome del lavadero" *	27
		Requerimientos incumplibles	9
	Código y prueba unitaria	Falta de habilidades técnicas	14
		Técnicas complejas	10
	Integración y prueba	Bajo rendimiento del software	11
Ambiente de desarrollo	Proceso de desarrollo	Capacidad de equipo ineficiente	16
		Procesos de desarrollo inapropiado	8
	Desarrollo de sistema	Problemas con las nuevas tecnologías	13
		Inadecuada infraestructura	8
	Proceso administrativo	Programación de actividades poco realista	17
		Planeación de recursos optimista	16
		Falta de participación del nivel ejecutivo	12
	Ambiente de trabajo	Brechas de comunicación	21
		Conflictos entre los miembros del equipo	11
Restricción del programa	Recurso	Rotación del personal	17
		Presupuesto irrealista	15
		Recursos insuficientes	9
	Entorno del programa	Resistencia al cambio por parte de los usuarios	21
		Inadecuada aplicación de la ley	9

Fuente: (Sonchan & Ramingwong, 2014)

ALGUNOS EJEMPLOS DE TAXONOMIAS

FASE	Nro	Factor de riesgo
A nivel de usuario	1	Usuario irresponsable
	2	Bajo involucramiento del usuario
	3	No esta listo para aceptar nueva tecnología
	4	Incapacidad de transmitir ideas al diseñador
	5	Conflictos entre diferentes usuarios
Levantamiento de requerimientos	1	Malentendido en la recopilación de requerimientos
	2	Los requerimientos no son entregados
	3	Requerimientos incompletos
Planeación	1	Programación y presupuestos irrealistas.
	2	Metas poco realistas
	3	Personal inapropiado
	4	Falta de liderazgo y compromiso
	5	Pobre planeación
	6	Falta de metodologías apropiadas para la gestión de proyectos de software
	7	Cambios en la administración durante el desarrollo del proyecto
	8	Baja comunicación entre el equipo del proyecto de software y el equipo gerencial.
	9	Ausencia de datos históricos
Análisis	1	Cambios poco claros, erróneos y rápidos en los requisitos.
	2	Análisis de requisitos parciales
	3	Ausencia de habilidades del gestor de TI.
	4	Requerimientos no identificados.
	5	Ausencia de conocimiento acerca de herramientas y tecnologías de programación
	6	Falta de confidencialidad y precisión del software planeado.
	7	Cambios mayores en requerimientos después de la fase de planeación
	8	Cambios en las especificaciones de proyectos de software.

Fuente: (Pasha et al., 2018)

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

IMPACTOS DE LOS RIESGOS DE PROYECTOS DE SOFTWARE

Consecuencia	2015	2016	2017
Renegociación de tiempos	80 %	80 %	83,2 %
Renegociación del alcance del proyecto	59 %	65 %	60,4 %
Refuerzo del equipo del proyecto	55 %	62 %	55,5%
Renegociación del costo del proyecto	46 %	41 %	53,5 %
Cambio de gerente del proyecto	26 %	17 %	16,8 %
Liquidar y terminar el proyecto	3 %	4%	n.d.
Iniciar procesos jurídicos formales	4 %	2%	n.d.

Fuente:(ACIS, 2016; ACIS, 2017;ACIS, 2018)

Instituto Superior Tecnológico del Azuay

CIDE
Centro de Investigación y Desarrollo Ecuador

Centro de Estudios Transdisciplinarios Bolivia
CET-BOLIVIA

Muchas Gracias

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

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

Congreso Internacional de
DESARROLLO DE SOFTWARE