ESTÉGANOS
INTERNATIONAL GROUP
Beyond the risk...

Seguridad en el desarrollo de SW

ESTÉGANOS
INTERNATIONAL GROUP
Beyond the risk...

ACIS
Jornada Nacional de Seguridad

Seguridad en el Desarrollo de SW

Fernando Ferrer Olivares
CISA, PMP, CCSA, CISM
Socio fundador Estéganos International Group

Agenda

- Introducción
- El ciclo de vida de desarrollo de SW
- Recursos
- Consideraciones de Seguridad en el SDLC NIST 800-64
- Conclusiones

Introducción

ESTÉGANOS INTERNATIONAL GROUP
Beyond the risk...

- Debilidades comunes en el SDLC que conllevan a código vulnerable, e inevitablemente, a deficiencias de seguridad
  - **No entendimiento de las consecuencias a largo plazo de un proceso de seguridad débil a través del SDLC**
    - **No realizar modelos de amenazas**
    - **No establecer ni seguir estándares de seguridad en SW**
  - **Conflicto de los objetivos de negocio con la seguridad durante cada fase**
    - **Aplicaciones ricas en funcionalidad vs. Aplicaciones seguras**
  - **Visualizar los requerimientos de seguridad en el contexto equivocado**
    - **Seguridad general vs. Seguridad específica**

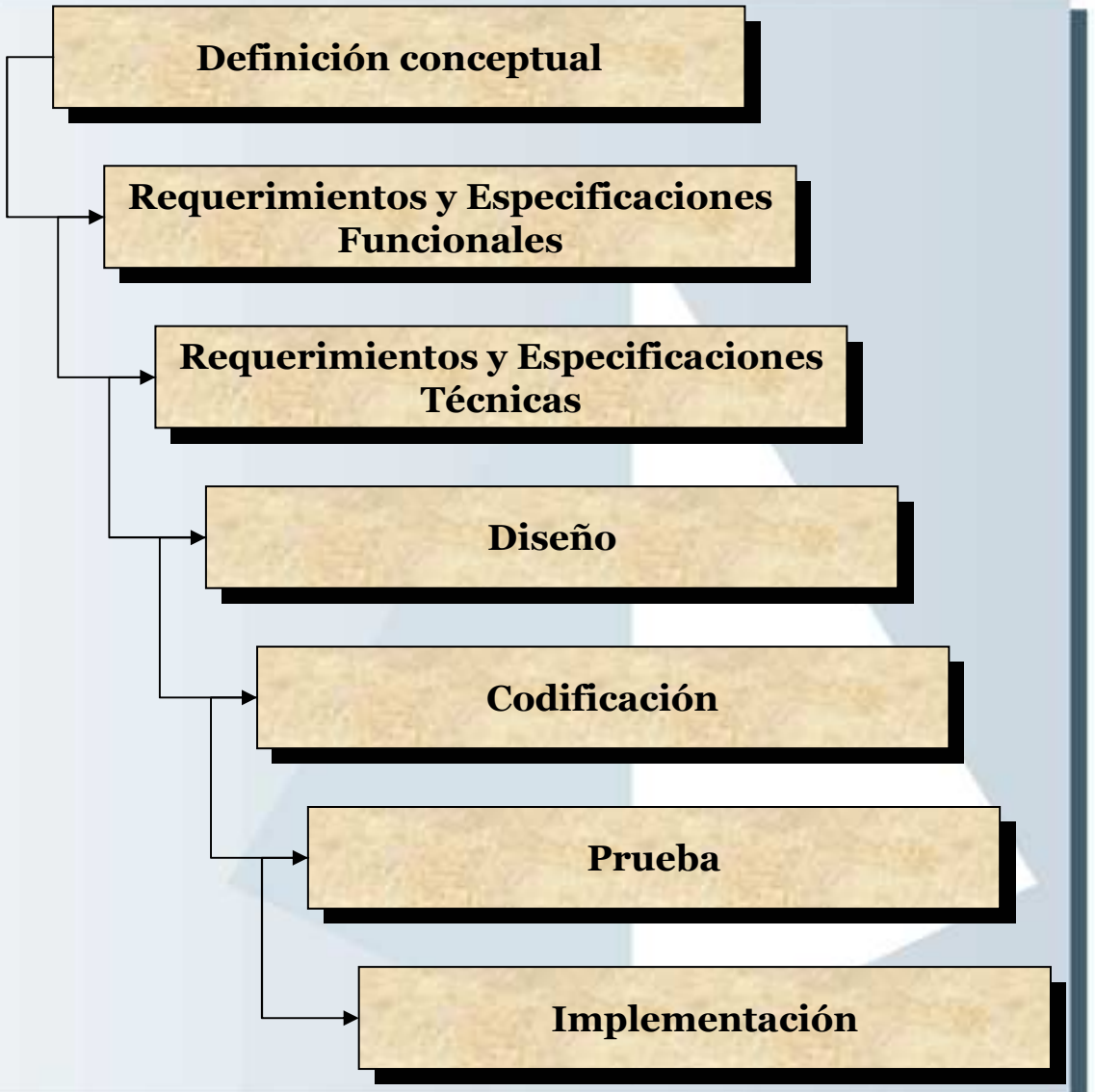
Introducción

- Debilidades comunes en el SDLC que conllevan a código vulnerable, e inevitablemente, a deficiencias de seguridad
  - **Desarrollar sin pensar en la seguridad**
    - **Dedicación a la codificación**
    - **Desconocimiento**
    - **Requerimientos no claros**
    - **Carencia de liderazgo de proyecto**
    - **Carencia de un SDLC que incluya las actividades de seguridad**
  - **Desarrollo de pruebas inadecuados**
    - **Pruebas de unidad vs. Pruebas de integración**
  - **Utilizar herramientas inapropiadas para descubrir debilidades del SW**

El ciclo de vida de desarrollo de SW (SDLC)

ESTÉGANOS INTERNATIONAL GROUP
Beyond the risk...

- Pasos que una organización sigue cuando desarrolla herramientas o aplicaciones de SW, incluyendo orden, responsables y productos generados
- Debe estar bien documentado
- Ciclo de mantenimiento



Recursos

- **Los siguientes artículos y estándares cubren tanto la seguridad de la información y la codificación segura y ofrecen principios, y procesos que usted puede integrar inmediatamente para mejorar la seguridad del SW:**
  - **NIST Special Publication 800-64—Security Considerations in the Information System Development Life Cycle**
  - **NIST Special Publication 800-27—Engineering Principles for Information Technology Security**
  - **NIST Special Publication 800-55—Security Metrics Guide for Information Technology Systems**
  - **ISO/IEC 12207:1995—Information technology—Software life cycle processes**
  - **ISO/IEC 17799:2005—Information technology—Security techniques—Code of practice for information security management**
  - **Microsoft's Trustworthy Computing Security Development Lifecycle paper**

Consideraciones de Seguridad en el SDLC NIST 800-64

ESTÉGANOS
INTERNATIONAL GROUP
Beyond the risk...

- Esta guía presenta un modelo de referencia (framework) para incorporar la seguridad en todas las fases del proceso SDLC, desde el inicio hasta la disposición
- Ayuda a identificar controles de seguridad efectivos en costo que pueden ser seleccionados y adquiridos
- Explica como incluir requerimientos de seguridad de la información en las fases apropiadas del SDLC

SDLC del NIST 800-64

ESTÉGANOS INTERNATIONAL GROUP
Beyond the risk...

	Initiation	Acquisition / Development	Implementation	Operations / Maintenance	Disposition
SDLC	- Needs Determination: • Perception of a Need • Linkage of Need to Mission and Performance Objectives • Assessment of Alternatives to Capital Assets • Preparing for investment review and budgeting	- Functional Statement of Need - Market Research - Feasibility Study - Requirements Analysis - Alternatives Analysis - Cost-Benefit Analysis - Software Conversion Study - Cost Analysis - Risk Management[7] Plan - Acquisition Planning	- Installation - Inspection - Acceptance testing - Initial user training - Documentation	- Performance measurement - Contract modifications - Operations - Maintenance	- Appropriateness of disposal - Exchange and sale - Internal organization screening - Transfer and donation - Contract closeout

Consideraciones de Seguridad NIST 800-64

ESTÉGANOS INTERNATIONAL GROUP
Beyond the risk...

	Initiation	Acquisition / Development	Implementation	Operations / Maintenance	Disposition
SECURITY CONSIDERATIONS	- Security Categorization - Preliminary Risk Assessment	- Risk Assessment - Security Functional Requirements Analysis - Security Assurance Requirements Analysis - Cost Considerations and Reporting - Security Planning - Security Control Development - Developmental Security Test and Evaluation - Other Planning Components	- Inspection and Acceptance - System Integration - Security Certification - Security Accreditation	- Configuration Management and Control - Continuous Monitoring	- Information Preservation - Media Sanitization - Hardware and Software Disposal

Consideraciones de Seguridad NIST 800-64

ESTÉGANOS INTERNATIONAL GROUP
Beyond the risk...

Initiation

- Needs Determination:
  - Perception of a Need
  - Linkage of Need to Mission and Performance Objectives
  - Assessment of Alternatives to Capital Assets
  - Preparing for investment review and budgeting

- Security Categorization
- Preliminary Risk Assessment

Categorización de la Seguridad

- La organización debe contar con un enfoque estándar para establecer categorías de seguridad para la información y los sistemas de información
- Las categorías deben basarse en el impacto potencial que ciertos eventos pueden causar sobre los sistemas de información requeridos para cumplir la misión, proteger los activos, cumplir las responsabilidades legales mantener la continuidad de las operaciones, y proteger a los individuos
  - Bajo, Moderado, Alto
- Las categorías, en conjunto con información de amenazas y vulnerabilidades, se utilizan para valorar el riesgo de operar el sistema
  - Pérdida de confidencialidad, Pérdida de integridad, Pérdida de disponibilidad
- Las categorías facilitan la selección apropiada de controles de seguridad para los sistemas de información
- FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems

Consideraciones de Seguridad NIST 800-64

ESTÉGANOS INTERNATIONAL GROUP
Beyond the risk...

Initiation

- Needs Determination:
  - Perception of a Need
  - Linkage of Need to Mission and Performance Objectives
  - Assessment of Alternatives to Capital Assets
  - Preparing for investment review and budgeting

- Security Categorization
- Preliminary Risk Assessment

Valoración preliminar del riesgo

- Describir las necesidades básicas de seguridad del sistema, en términos de integridad, disponibilidad, confidencialidad, accountability, no repudiación
- Definir el ambiente de amenazas en el cual operará el sistema
- Identificación inicial de los controles de seguridad requeridos
- NIST SP 800-30, *Risk Management Guide for Information Technology Systems*
- NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*

Consideraciones de Seguridad NIST 800-64

ESTÉGANOS INTERNATIONAL GROUP
Beyond the risk...

Acquisition / Development
- Functional Statement of Need
- Market Research
- Feasibility Study
- Requirements Analysis
- Alternatives Analysis
- Cost-Benefit Analysis
- Software Conversion Study
- Cost Analysis
- Risk Management[7] Plan
- Acquisition Planning
- Risk Assessment
- Security Functional Requirements Analysis
- Security Assurance Requirements Analysis
- Cost Considerations and Reporting
- Security Planning
- Security Control Development
- Developmental Security Test and Evaluation
- Other Planning Components

- **Valoración formal y periódica del riesgo**
  - Posibilita identificar los requerimientos de protección del sistema
  - Análisis más profundo y específico
  - Genera información esencial requerida para el Plan de Seguridad
  - Incluye:
    - Identificación de amenazas y vulnerabilidades en el sistema de información
    - El impacto o magnitud de daño potencial que una pérdida de confidencialidad, integridad, o disponibilidad podría causar sobre los activos u operaciones de la organización (incluyendo misión, funciones, imagen, reputación)
    - Debe considerar los controles existentes y su efectividad
    - La identificación y análisis de los controles de seguridad para el sistema
  - Debe realizarse antes de la aprobación de las especificaciones de diseño
  - Puede suministrar justificaciones para especificaciones
  - No será necesariamente un documento largo y complejo
  - Requerirá la participación de personal apropiado
  - La selección de tipos de salvaguardas o contramedidas debe considerar los resultados del análisis de requerimientos de aseguramiento
  - Puede identificar deficiencias en el análisis de requerimientos de integridad, confidencialidad y disponibilidad o en el análisis de requerimientos de aseguramiento de seguridad
  - El análisis debe repetirse hasta alcanzar consistencia
  - NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*

Consideraciones de Seguridad NIST 800-64

ESTÉGANOS INTERNATIONAL GROUP
Beyond the risk...

Acquisition / Development
- Functional Statement of Need
- Market Research
- Feasibility Study
- Requirements Analysis
- Alternatives Analysis
- Cost-Benefit Analysis
- Software Conversion Study
- Cost Analysis
- Risk Management[7] Plan
- Acquisition Planning
- Risk Assessment
- Security Functional Requirements Analysis
- Security Assurance Requirements Analysis
- Cost Considerations and Reporting
- Security Planning
- Security Control Development
- Developmental Security Test and Evaluation
- Other Planning Components

- **Valoración formal y periódica del riesgo**
  - Adicional al sistema que se está desarrollando, debe considerarse la seguridad de los sistemas a los cuales éste está conectado directa o indirectamente
  - One way to incorporate the context is to have an enterprise security architecture. Without an enterprise perspective, the acquisition could be suboptimal, even to the extent of introducing vulnerabilities. If the enterprise context is not considered, there is a possibility that the system being acquired could compromise the other enterprise systems. The system being acquired may have a trust relationship with other enterprise systems, increasing the consequences of a compromise.
- Each enterprise system should address several enterprise-wide security objectives:
- A specific enterprise system should not create vulnerabilities or unintended interdependencies in other enterprise systems.
- A specific enterprise system should not decrease the availability of other enterprise systems.
- The security posture of the set of all the enterprise systems should not be decreased because of this specific enterprise system.
- External domains not under enterprise control should be considered potentially hostile entities. The systems connected to such external domains must analyze and attempt to counter hostile actions originating from these domains.
- Security specifications should be appropriate for the given state of the system environment.
- Security specifications should be stated clearly to convey the desired functions and assurances to the enterprise system product team and the developers.
- Implemented specifications should sufficiently reduce the risks to the enterprise system and to the enterprise mission that the system supports.

Consideraciones de Seguridad NIST 800-64

ESTÉGANOS INTERNATIONAL GROUP
Beyond the risk...

Acquisition / Development
- Functional Statement of Need
- Market Research
- Feasibility Study
- Requirements Analysis
- Alternatives Analysis
- Cost-Benefit Analysis
- Software Conversion Study
- Cost Analysis
- Risk Management[7] Plan
- Acquisition Planning
- Risk Assessment
- Security Functional Requirements Analysis
- Security Assurance Requirements Analysis
- Cost Considerations and Reporting
- Security Planning
- Security Control Development
- Developmental Security Test and Evaluation
- Other Planning Components

Análisis de requerimientos funcionales de seguridad

- Puede incluir las 2 fuentes de requerimientos de seguridad del sistema
  - Ambiente de seguridad del sistema (política de seguridad de la información de la empresa y arquitectura de seguridad de la empresa)
  - Requerimientos funcionales de seguridad
- Debe incluir un análisis de leyes y regulaciones que definan requerimientos de seguridad mínimos (baseline)
- Los requerimientos de seguridad legales, funcionales y de TI deben establecerse en términos específicos
- Para sistemas complejos, más de una iteración del análisis de requerimientos puede necesitarse
- Énfasis en integridad, disponibilidad y confidencialidad

Consideraciones de Seguridad NIST 800-64

ESTÉGANOS INTERNATIONAL GROUP
Beyond the risk...

Acquisition / Development
- Functional Statement of Need
- Market Research
- Feasibility Study
- Requirements Analysis
- Alternatives Analysis
- Cost-Benefit Analysis
- Software Conversion Study
- Cost Analysis
- Risk Management[7] Plan
- Acquisition Planning
- Risk Assessment
- Security Functional Requirements Analysis
- Security Assurance Requirements Analysis
- Cost Considerations and Reporting
- Security Planning
- Security Control Development
- Developmental Security Test and Evaluation
- Other Planning Components

- **Análisis de Requerimientos de Aseguramiento de la Seguridad**
  - Permite lograr confianza de que la organización alcanzará sus objetivos de seguridad – los controles operarán correctamente y serán efectivos en el ambiente operacional
  - Se basará en los requerimientos funcionales legales y de seguridad
  - Permitirá determinar cuánto y qué clase de aseguramiento, efectivo en costo, se requerirá para obtener la evidencia suficiente para producir el nivel de confianza deseado
  - *Common Criteria (CC) – Parte 3*
    - Evaluación de productos comerciales contra un conjunto de requerimientos y especificaciones del ISO/IEC 15408, Common Criteria for IT Security Evaluation.
  - Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules,* empleo de laboratorios de aseguramiento
  - Evaluaciones de terceras partes:
    - *Third-Party Evaluations*
    - *Accreditation of a System to Operate in a Similar Situation*
    - *Test and Evaluation Following a Formal Procedure*
    - *Test and Evaluation Under the Auspices and Review of an Independent Organization*
  - NIST SP 800-23, Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products.

Consideraciones de Seguridad NIST 800-64

ESTÉGANOS INTERNATIONAL GROUP
Beyond the risk...

Acquisition / Development

- Functional Statement of Need
- Market Research
- Feasibility Study
- Requirements Analysis
- Alternatives Analysis
- Cost-Benefit Analysis
- Software Conversion Study
- Cost Analysis
- Risk Management[7] Plan
- Acquisition Planning
- Risk Assessment
- Security Functional Requirements Analysis
- Security Assurance Requirements Analysis
- Cost Considerations and Reporting
- Security Planning
- Security Control Development
- Developmental Security Test and Evaluation
- Other Planning Components

Consideraciones y Reporte de Costos

- Determinar cuánto costará el desarrollo, incluyendo HW, SW, personal, entrenamiento y SEGURIDAD
- La identificación de costos asociados a la seguridad puede ser compleja. Posibles entradas:
  - Proceso de Administración de Riesgos, controles que mitigarán las vulnerabilidades identificadas
  - Mitigación del riesgo, que incluye un análisis costo-beneficio de los controles recomendados
- Incluir la seguridad como un ítem en los reportes presupuestales anuales o de adquisiciones mayores
  - En términos de valor o porcentuales
- El enfoque más efectivo en costo es incluir la seguridad al inicio del SDLC, debido a que:
  - Es más difícil adicionar funcionalidad en un sistema después de que ha sido construido
  - Es menos costoso incluir medidas preventivas que tratar con el costo de un incidente de seguridad
- OMB Memorandum 00-07, "Incorporating and Funding Security in Information Systems Investments."

Consideraciones de Seguridad NIST 800-64

ESTÉGANOS INTERNATIONAL GROUP
Beyond the risk...

Acquisition / Development
- Functional Statement of Need
- Market Research
- Feasibility Study
- Requirements Analysis
- Alternatives Analysis
- Cost-Benefit Analysis
- Software Conversion Study
- Cost Analysis
- Risk Management[7] Plan
- Acquisition Planning
- Risk Assessment
- Security Functional Requirements Analysis
- Security Assurance Requirements Analysis
- Cost Considerations and Reporting
- Security Planning
- Security Control Development
- Developmental Security Test and Evaluation
- Other Planning Components

Planeación de la Seguridad

- Asegurar que los controles de seguridad requeridos (planeados o existentes), para redes, facilidades, sistemas de información, estén totalmente documentados
- Provee una caracterización o descripción completa del sistema de información
- Pueden incluirse referencias a documentos claves del programa de seguridad de la información
  - Plan de administración de la Configuración
  - Plan de contingencia
  - Plan de respuesta a incidentes
  - Plan de concientización y entrenamiento en seguridad
  - Reglas de comportamiento
  - Valoración del riesgo
  - Resultados de pruebas y evaluaciones de seguridad
  - Acuerdos de interconexión de sistemas
  - Autorizaciones/acreditaciones de seguridad
- NIST Special Publication 800-18, *Guide for Developing Security Plans Information Technology Systems*
- NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*

Consideraciones de Seguridad NIST 800-64

ESTÉGANOS INTERNATIONAL GROUP
Beyond the risk...

Acquisition / Development
- Functional Statement of Need
- Market Research
- Feasibility Study
- Requirements Analysis
- Alternatives Analysis
- Cost-Benefit Analysis
- Software Conversion Study
- Cost Analysis
- Risk Management[7] Plan
- Acquisition Planning
- Risk Assessment
- Security Functional Requirements Analysis
- Security Assurance Requirements Analysis
- Cost Considerations and Reporting
- Security Planning
- Security Control Development
- Developmental Security Test and Evaluation
- Other Planning Components

- **Desarrollar controles de seguridad**
  - Diseñar, desarrollar, modifcar e implementar los controles, nuevos o adicionales, referenciados en el Plan de Seguridad

Consideraciones de Seguridad NIST 800-64

ESTÉGANOS INTERNATIONAL GROUP
Beyond the risk...

Acquisition / Development
- Functional Statement of Need
- Market Research
- Feasibility Study
- Requirements Analysis
- Alternatives Analysis
- Cost-Benefit Analysis
- Software Conversion Study
- Cost Analysis
- Risk Management[7] Plan
- Acquisition Planning
- Risk Assessment
- Security Functional Requirements Analysis
- Security Assurance Requirements Analysis
- Cost Considerations and Reporting
- Security Planning
- Security Control Development
- Developmental Security Test and Evaluation
- Other Planning Components

Prueba y Evaluación de la Seguridad desarrollada

- Probar, si es posible, que los controles trabajan apropiadamente y son efectivos, antes de colocarlos en producción
- Las pruebas deben basarse en un plan de evaluación y pruebas

Consideraciones de Seguridad NIST 800-64

ESTÉGANOS INTERNATIONAL GROUP
Beyond the risk...

Acquisition / Development

- Functional Statement of Need
- Market Research
- Feasibility Study
- Requirements Analysis
- Alternatives Analysis
- Cost-Benefit Analysis
- Software Conversion Study
- Cost Analysis
- Risk Management[7] Plan
- Acquisition Planning
- Risk Assessment
- Security Functional Requirements Analysis
- Security Assurance Requirements Analysis
- Cost Considerations and Reporting
- Security Planning
- Security Control Development
- Developmental Security Test and Evaluation
- Other Planning Components

Otros componentes de Planeación

- Tipo de Contrato
- Revisión de otros grupos funcionales
- Revisión por Certificador y Acreditador
- Naturaleza cíclica del proceso
- Evaluación y aceptación
- Desarrollo del RFP
- Especificaciones de Seguridad y Declaración del Desarrollo del Trabajo
  - Especificaciones generales
  - Especificaciones mandatorias
- Evaluación de Propuesta
- Desarrollo de un Plan de Evaluación
- Requerimientos contractuales especiales

Consideraciones de Seguridad NIST 800-64

ESTÉGANOS INTERNATIONAL GROUP
Beyond the risk...

Implementation

- Installation
- Inspection
- Acceptance testing
- Initial user training
- Documentation

- Inspection and Acceptance
- System Integration
- Security Certification
- Security Accreditation

Inspección y Aceptación

- Decisión de inspeccionar y luego aceptar y pagar por un entregable, para determinar que el sistema cumple las especificaciones
  - Pruebas por la organización
  - Validación y verificación por un contratista independiente
- Las pruebas, validaciones verificaciones deben incluir la seguridad del sistema
- Acreditación del sistema: aceptación y aprobación para autorizar el procesamiento
  - Es unas decisión separada basada en los riesgos y ventajas de instalar el sistema en el ambiente operacional
  - No es correcto incluir la autorización para colocar en funcionamiento el sistema como uno de los criterios de aceptación debido a que muchos factores están fuera del control del vendedor

Consideraciones de Seguridad NIST 800-64

ESTÉGANOS INTERNATIONAL GROUP
Beyond the risk...

Implementation

- Installation
- Inspection
- Acceptance testing
- Initial user training
- Documentation

- Inspection and Acceptance
- System Integration
- Security Certification
- Security Accreditation

Integración del sistema

- Ocurre en el sitio en donde el sistema será colocado en producción
- Pruebas de integración y aceptación ocurren después de la entrega e instalación del sistema
- Los controles de seguridad son establecidos e inicializados en concordancia con las instrucciones del fabricante y con las guías de implementación de seguridad disponibles

Consideraciones de Seguridad NIST 800-64

ESTÉGANOS INTERNATIONAL GROUP
Beyond the risk...

Implementation

- Installation
- Inspection
- Acceptance testing
- Initial user training
- Documentation

- Inspection and Acceptance
- System Integration
- Security Certification
- Security Accreditation

Certificación de Seguridad

- Antes de la puesta en funcionamiento del sistema, se debe asegurar que los controles de seguridad establecidos en respuesta a los requerimientos de seguridad fueron incluidos durante el proceso de desarrollo del sistema
- Pruebas y evaluaciones periódicas de los controles de seguridad deben realizarse en un sistema de información para asegurar que los controles están implementados efectivamente
- Aplicación de técnicas y procedimientos de verificación para obtener confianza de que salvaguardas y contramedidas apropiadas existen para proteger el sistema
- También describe las vulnerabilidades actuales del sistema
- NIST Special Publication 800-53A, *Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems*

Consideraciones de Seguridad NIST 800-64

ESTÉGANOS INTERNATIONAL GROUP
Beyond the risk...

Implementation

- Installation
- Inspection
- Acceptance testing
- Initial user training
- Documentation

- Inspection and Acceptance
- System Integration
- Security Certification
- Security Accreditation

Acreditación de Seguridad

- Autorización para que un sistema proceso, almacene o transmita información
- La decisión de acreditar está basada en el riesgo, que depende en gran parte, pero no exclusivamente, de los resultados de las pruebas y evaluaciones de seguridad durante el proceso de verificación de los controles de seguridad

Consideraciones de Seguridad NIST 800-64

ESTÉGANOS INTERNATIONAL GROUP
Beyond the risk...

Operations / Maintenance

- Performance measurement
- Contract modifications
- Operations
- Maintenance

- Configuration Management and Control
- Continuous Monitoring

Administración y control de la configuración

- Los sistemas de información están en constante estado de migración con actualizaciones al HW, SW, o firmware y posibles modificaciones al ambiente que roda al sistema
- Cambios a un sistema pueden tener impacto significativo en la seguridad del sistema
- Para mantener la acreditación del sistema, es necesario:
  - Documentar los cambios a los sistemas de información
  - Valorar continuamente el impacto potencial de los cambios sobre la seguridad del sistema

Consideraciones de Seguridad NIST 800-64

ESTÉGANOS INTERNATIONAL GROUP
Beyond the risk...

Operations / Maintenance

- Performance measurement
- Contract modifications
- Operations
- Maintenance

- Configuration Management and Control
- Continuous Monitoring

Monitoreo continuo

- Pruebas y evaluaciones periódicas y continuas de los controles de seguridad para asegurar su efectividad
  - Monitoreo de controles
  - Reportes del estado e la seguridad en el sistema a las instancias pertinentes
- Técnicas de monitoreo
  - Revisiones de seguridad
  - Auto-evaluaciones
  - Pruebas y evaluaciones
  - Auditorías
  - NIST Special Publication 800-53A, *Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems*

Consideraciones de Seguridad NIST 800-64

Disposition

- Appropriateness of disposal
- Exchange and sale
- Internal organization screening
- Transfer and donation
- Contract closeout

- Information Preservation
- Media Sanitization
- Hardware and Software Disposal

- **Preservación de la información**
  - **Identificar los métodos requeridos para recuperar la información en el futuro**
  - **Considerar los requerimientos legales para la retención de registros**

Consideraciones de Seguridad NIST 800-64

ESTÉGANOS INTERNATIONAL GROUP
Beyond the risk...

Disposition

- Appropriateness of disposal
- Exchange and sale
- Internal organization screening
- Transfer and donation
- Contract closeout

- Information Preservation
- Media Sanitization
- Hardware and Software Disposal

- **Saneamiento de medios**
  - **Evitar que los datos (información sensitiva) sean reconstruidos y accedidos por individuos no autorizados**
  - **Eliminación, borrado, o sobre escritura de medios magnéticos o eléctricos de almacenamiento**
  - **Borrado de memorias no volátiles**
  - **Formas de saneamiento:**
    - **Limpiar (no se puedan reconstruir datos haciendo un uso normal del sistema)**
    - **Purga – depuración (pueden reconstruirse datos a través de técnicas de laboratorio)**

Consideraciones de Seguridad NIST 800-64

ESTÉGANOS INTERNATIONAL GROUP
Beyond the risk...

Disposition

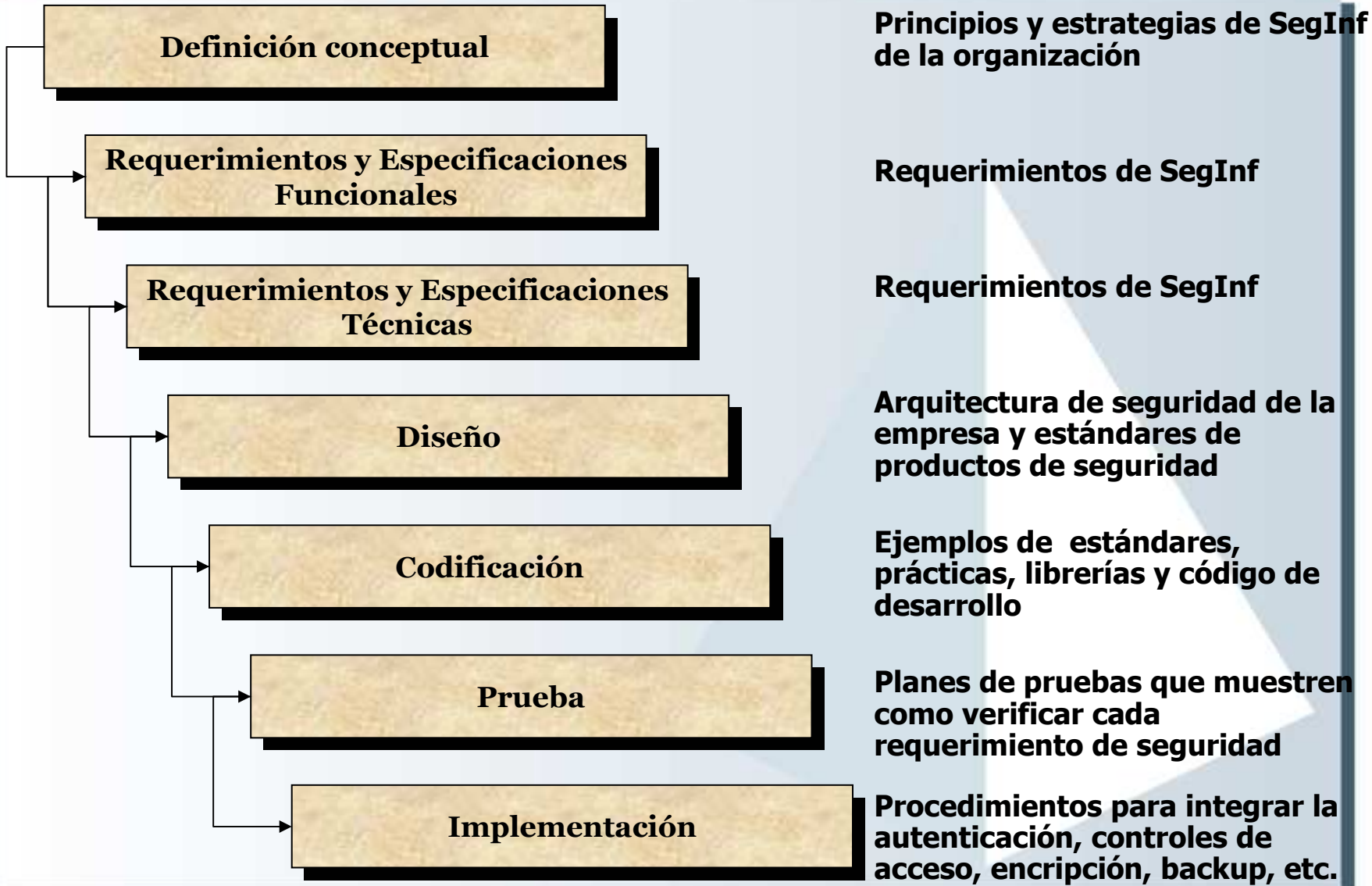
- Appropriateness of disposal
- Exchange and sale
- Internal organization screening
- Transfer and donation
- Contract closeout

- Information Preservation
- Media Sanitization
- Hardware and Software Disposal

Disposición de HW y SW

- Venta, dar de baja o descarte
- SW: Se deben cumplir los acuerdos de licencias y las regulaciones
- HW: Rara necesidad de destruirlo, excepto por algunos medios de almacenamiento que contienen información sensitiva y que no pueden ser saneados sin destrucción
  - Remoción o destrucción física de los medios, de forma tal que el HW remanente pueda ser vendido o dado de baja
  - Algunos sistemas pueden contener información sensitiva después de que el medio sea removido. Si existe duda de que información sensitiva permanezca en el sistema, El Oficial de Seguridad debe ser consultado antes de disponer del sistema

Información de seguridad en el SDLC



Conclusiones

- La inseguridad de las aplicaciones parte de un inadecuado proceso de desarrollo, un proceso que no considera la seguridad en todas sus fases
- Organizaciones que incorporan la seguridad en el SDLC se benefician de productos y aplicaciones que son seguras por diseño
- Incluyendo la seguridad desde el inicio del SDLC usualmente disminuirá costos y proporcionará una seguridad más efectiva que adicionarla cuando el sistema este operando
- Aquellas que no lo hacen pagarán su precio, tanto económico como en la interrupción del negocio

Bibliografía

- **Security in the software development life cycle,** Peter H. Gregory, CISSP, CISA
- **The Software Development Life Cycle: When to Secure Your Process,** Caleb Sima and Kevin Beaver
- **The Software Development Life Cycle: When to Secure Your Process, NIST 800-64**

ESTÉGANOS
INTERNATIONAL GROUP
Beyond the risk...

Gracias!

Fernando Ferrer Olivares, CISA, PMP, CCSA, CISM

fferrer@esteganos.com