Information Security Management Maturity Model V2.1

Bogotá, VIII Jornadas de Seguridad de la Información,

Juan Carlos Reyes Muñoz, Junio - 2008

Presentación Original en Inglés, preparada por Vicente Aceituno © ISM³ Consortium

http://www.ism3.com

Consorcio ISM³

1. Estándares de Seguridad
2. Enfoque del Negocio
3. Mejoramiento Contínuo
4. Orientación a Procesos
5. Niveles de Responsabilidad
6. Retorno de inversión
7. Metodología de Análisis de Riesgos
8. Visión General
9. Metricas
10. Ventajas
11. Resumen

AGENDA

1. **Estándares de Seguridad**
2. Enfoque del Negocio
3. Mejoramiento Contínuo
4. Orientación a Procesos
5. Niveles de Responsabilidad
6. Retorno de inversión
7. Metodología de Análisis de Riesgos
8. Visión General
9. Metricas
10. Ventajas
11. Resumen

AGENDA

Certificate and Certificate Revocation Lists Management - PKIX / X.509 and matching RFCs.
Symmetric Encryption Algorithms - DES, AES, RC2, IDEA.
Assymmetric Encryption Algorithms – PKCS, Diffie-Hellman.
Time Stamping – TSP.
One-Way Hash Functions - SHA-x, MD5.
Digital Signature Algorithms - PKCS, DSA, MAC, HMAC.
Pseudo Random Number Generation - X9.82.
Intellectual property protection - FairPlayTM, Microsoft® DRM.
Environment Hardening - CIS, NSA.
Secure Channel Formats - SSL, TLS, IPSEC, Ipv6.
Software Development Lifecycle Control - SSE-CMM, OWASP, SPSMM
Formats - S/MIME, XML, PKCS formats, OpenPGP.
Application Programming Interfaces - RFC2078 GSS-API, WSS.
Directories - LDAP, X.500, DNSSEC.
Authentication – SAML, Sender ID, Kerberos, RADIUS.
Authorization - RFC 2904 AAA Authorization Framework.
Deletion standards - Gutmann, DoD 5220.22.
Time keeping standards – SNTP.

Estándares de Seguridad

Management:

800-14 GAASP by National Institute of Standards and Technology.

Standard of Good Practice for Information Security from ISF.

SysTrust by AICPA.

ISO 17799 based on BS 7799 of the British Standards Institute.

ISO/IEC TR 13335-4 by ISO/IEC Joint Technical Committee 1.

Cobit by ISACA.

IT Baseline Protection by BSI

Risk Management

Magerit by Ministerio de Administraciones Públicas (Spain).

OCTAVE by Software Engineering Institute.

Alerts Monitoting – SVRRP by Organization for Internet Safety.

Handling of incidents and near-incidents - ISO18044.

Vulnerability Assessment – OSSTMM from ISECOM.

Products and Systems Engineering:

SSE-CMM (ISO/IEC 21827: 2002)

ISO15408 Common Criteria

Trusted Platform Module (TPM)

Trusted Network Connect (TNC)

Estándares de Seguridad

Pedalear no debería cansar, debería llevar a alguna parte!

1. Estándares de Seguridad
2. **Enfoque del Negocio**
3. Mejoramiento Contínuo
4. Orientación a Procesos
5. Niveles de Responsabilidad
6. Retorno de inversión
7. Metodología de Análisis de Riesgos
8. Visión General
9. Metricas
10. Ventajas
11. Resumen

AGENDA

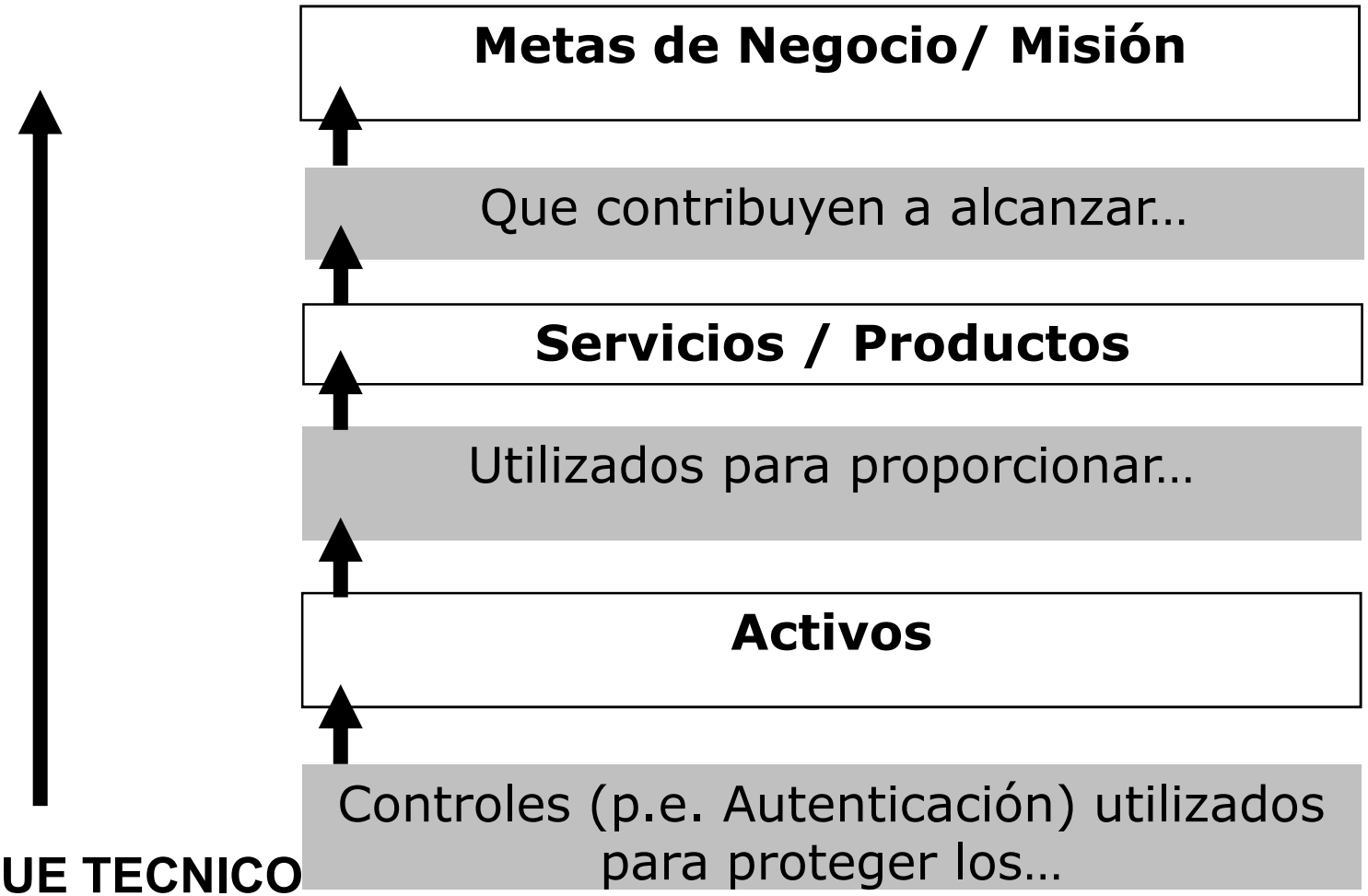
- **“Prevenir que nos ataquen”.** Lo que significa que para estar seguro hay que ser ***invulnerable***.

- Un incidente es cualquier pérdida de confidencialidad, integridad o disponibilidad.

- Cuando analizas información, te preguntas: **Es confidencial, tiene integridad, está disponible?**

El Enfoque Clásico de Negocio

ENFOQUE GERENCIAL



ENFOQUE TECNICO

El Enfoque Clásico de Negocio

- **"Garantizar que se cumplen las metas del negocio".** Lo que significa que para estar seguro, hay que **conseguir los objetivos de negocio a pesar de ataques, errores y accidentes.**

- Un incidente es el incumplimiento de un objetivo de negocio como resultado de un ataque, un error o un accidente.

- Cuando analizas información usando ISM^3, te preguntas: **¿Que propiedades de esta información hay que proteger para que aporte valor para el negocio?**

El Enfoque ISM^3

ENFOQUE GERENCIAL

Metas de Negocio/ Misión

Depende de

Objetivos de Negocio

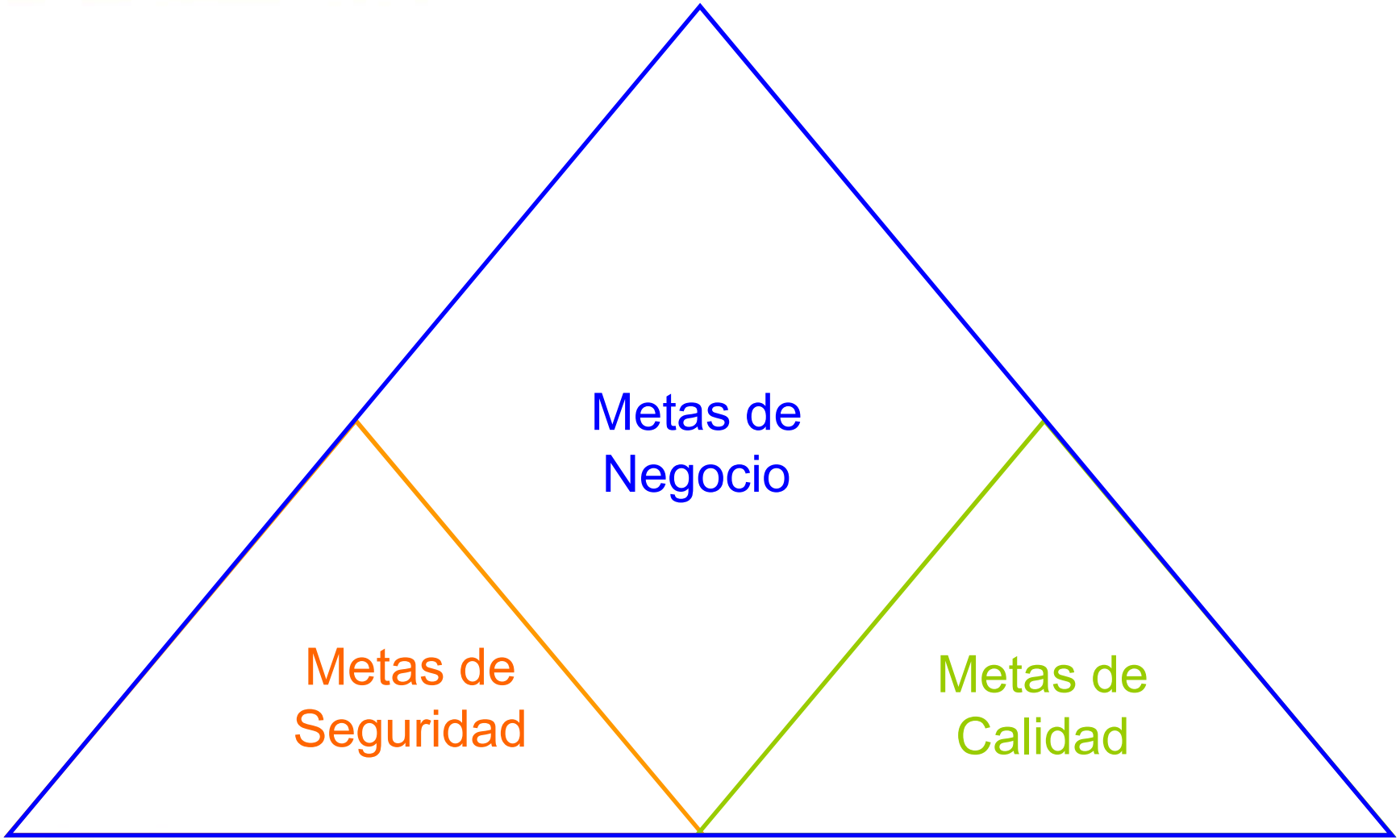
Cuyo alcance depende de

Objetivos de Seguridad

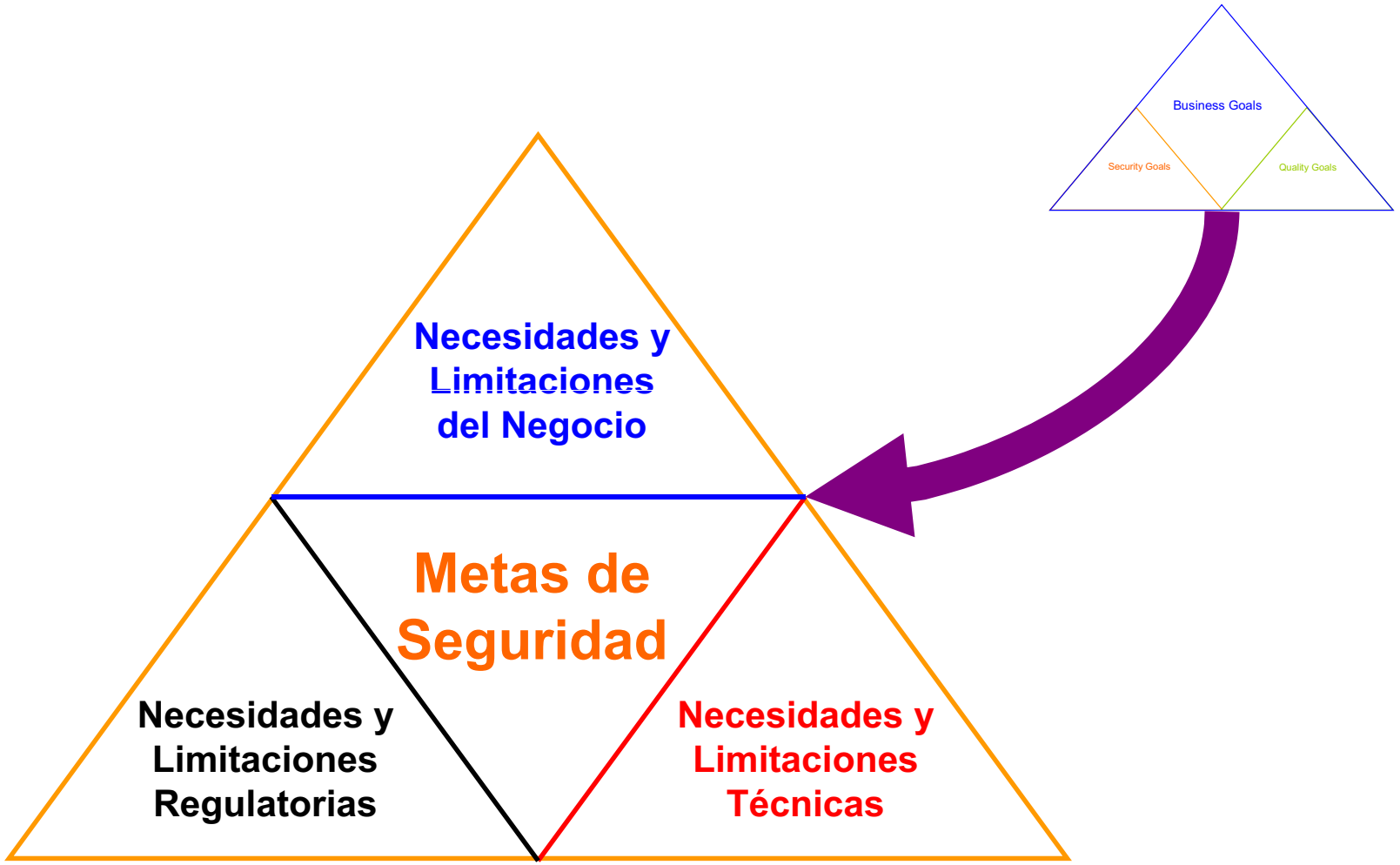
Logrados utilizando procesos de seguridad

ENFOQUE TECNICO

El Enfoque ISM³



El Enfoque ISM³



El Enfoque ISM³

Metas de negocio – Fundamentales para la existencia de la organización. Alcanzarlas depende de los objetivos de seguridad.

Los objetivos de seguridad son derivados del negocio, cumplimiento y necesidades técnicas y limitaciones. Estas son las metas del Sistema de Gestión.

Las metas de seguridad miden los logros de los objetivos de seguridad en términos del negocio.

El Enfoque Clásico de Negocio

Ejemplos de Objetivos de Negocio:

- **Pagar impuestos cuando corresponde.**
- **Facturar todos los productos y servicios ofrecidos.**
- **Retener los registros necesarios para poder pasar cualquier auditoria.**

Objetivos de Seguridad.

Metas de Seguridad.

Qué hay que proteger?

Objetivos de Negocio.

Ejemplo de Objetivos de Seguridad:

- **Derivados de necesidades de negocio: “Los secretos deben ser accesibles solo por usuarios autorizados”**
- **Derivados de necesidades de cumplimiento: “La bases de datos con información financiera deben estar sujetas a reserva legal”**
- **Derivados de necesidades técnicas: “Los sistemas deben estar tan libres de vulnerabilidades como sea posible”**

Metas de Seguridad.

Qué hay que proteger?

Objetivos de Negocio.

Objetivos de Seguridad.

Ejemplos de Metas de Seguridad.

- **Metas de negocio: “Menos de dos secretos revelados al año, con un daño asociado inferior al 0.1% del valor contable de la compañía”**
- **Metas de cumplimiento: “Menos de un caso cada dos años de una base de datos no registrada mas de tres meses tras haberse creado”**
- **Metas técnicas: “Actualización de sistemas en la DMZ en promedio en menos de tres días”**

Qué hay que proteger?

Caso de Uso – Gestión sin ISM^3

Motivación: Eliminar los virus antes de que afecten la operación.

Objetivo: Ningún sistema debe contraer virus en algun momento

Actividad: Instalar antivirus en PC, servidores, servidores de correo, añadir las características antivirus de los firewalls, añadir antispyware, antitrojan, antirookit a la receta.

Política: prevenir que algun USB, DVD, toque los sistemas de la compañía sin haber pasado por chequeo de virus.

Criterios de Exito: Cuando ningun sistema contrae virus

Mejora Contínua: Añadir mas controles antimalware (Tripwire, CORE, etc)

Caso de Uso: Malware

Caso de Uso – Gestión estilo ISM^3

Motivación: lamentablemente los sistemas, especialmente Windows son propensos al malware. Debemos efectuar inversiones proporcionales al daño que éstos pueden hacer.

Meta: Los sistemas deben cumplir su rol de negocio con o sin malware.

Actividad: instalar antimalware en sistemas vulnerables. Medir la actividad, alcance, actualización y disponibilidad del antimalware. Considerar otras medidas, como utilizar sistemas menos propensos al malware.

Política: Utilizar en todos los sistemas la protección antimalware que le detectará y prevenir que el sistema deje de cumplir su rol de negocio.

Criterios de Exito: Cuando los sistemas protegidos continuan cumpliendo su rol de negocio sin verse interrumpidos o degradados.

Mejora Contínua: utilizar metricas para mejorar la protección antimalware y aplicarlas con mayor efectividad y ROI.

Caso de Uso: Malware

1. Estándares de Seguridad
2. Enfoque del Negocio
3. **Mejoramiento Contínuo**
4. Orientación a Procesos
5. Niveles de Responsabilidad
6. Retorno de inversión
7. Metodología de Análisis de Riesgos
8. Visión General
9. Metricas
10. Ventajas
11. Resumen

AGENDA

Lo que no puede medir, no lo puede gestionar.

Aquello que no puede gestionar no lo puede mejorar.

ISM3 usa PHVA por proceso & métricas para mejoramiento contínuo.

Mejoramiento Contínuo

Indefinido. El proceso puede ser utilizado pero no se encuentra definido.

Definido. El proceso es usado y se encuentra documentado.

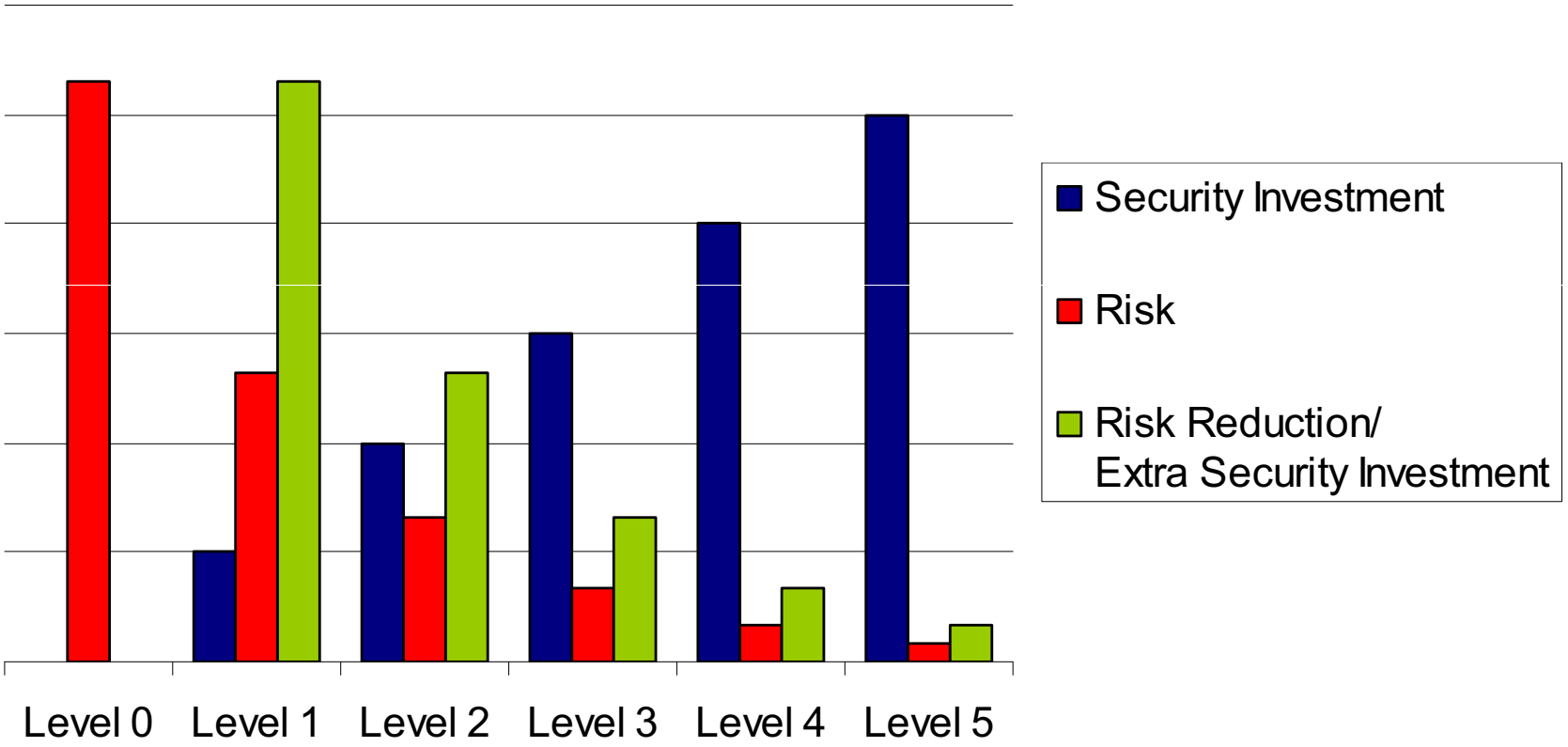
Gestionado. El proceso está definido y los resultados del mismo son usados para arreglarlo y mejorarlo.

Controlado. El proceso está gestionado y sus hitos, así como la necesidad de recursos se puede predecir adecuadamente.

Optimizado. El proceso es controlado y el mejoramiento tiende a optimizar los recursos.

Niveles de Capacidad

Security Investment & Risk



Niveles de Madurez

1. Estándares de Seguridad
2. Enfoque del Negocio
3. Mejoramiento Contínuo
4. **Orientación a Procesos**
5. Niveles de Responsabilidad
6. Retorno de inversión
7. Metodología de Análisis de Riesgos
8. Visión General
9. Metricas
10. Ventajas
11. Resumen

AGENDA

Orientado a Procesos.

ISM^3 es compatible con ISO27001, Cobit, ITIL y ISO9001.

Las organizaciones no tienen que perder su inversión en el SGSI que manejen actualmente para adoptar ISM^3.

ISM^3 hace referencia a la buenas prácticas para cada uno de sus procesos.

Orientación a Procesos / Compatibilidad

Process	OSP-19 Internal Technical Audit
Description	This process validates: The effectiveness of vulnerability reduction measures. The effectiveness of access control measures. The effectiveness of user registration measures. The quality of the software developed in-house. It can be applied to all possible targets or a representative random sample. When performing emulated attacks from internal systems, it is commonly called internal "vulnerability" testing. When performing emulated attacks from external systems, is commonly known as penetration testing.
Rationale	Incidents arising from the exploitation of weaknesses in software and configuration weaknesses around the borders of an organization can be prevented by attacks emulation and subsequent software mending, environment hardening, investment and improved monitoring.
Documentation	**OSP-192-Attacks Emulation Procedure** **OSP-193-Attack Emulation Report Template** **OSP-194-Source Code Review Procedure** **OSP-195-Source Code Review Report Template** **OSP-196-User Registration and Access Control Review Procedure** **OSP-197- User Registration and Access Control Review Report Template** **GP-01C-Testing and Auditing Policy**
Inputs	Inventory of Assets (OSP-3).
Outputs	Attack Emulation Report (OSP-4) Source Code Review Report (OSP-8) User Registration and Access Control Review Report (OSP12, OSP-11) Metrics Report (TSP-4)
Activity	Number of Outputs submitted
Scope	Percentage of information systems that have been tested in the environment
Update	Time since last Outputs submission Mean time between Outputs submissions
Availability	Not Applicable
Responsibilities	Supervisor: TSP-14 Process Owner Process Owner: Information Security Management (Tester), or Independent Auditor

Ejemplo de Proceso

ISM^3 puede ser utilizado sólo o para mejorar una implantación de ISO27001.

Ejemplo para la actualización de Sistemas Críticos

A.12.5.2 Revisión Técnica de Aplicaciones luego de cambios al sistema operativo:

Cuando es modificado un sistema operativo, las aplicaciones críticas de negocio deben ser revisadas y probadas para garantizar que no hay un impacto adverso en la operación o en la seguridad.

ISM^3 e ISO27001

Process	**OSP-5 Environment Patching**
Description	This process covers the on-going update of services to prevent incidents related to known weaknesses.
Rationale	Patching prevents incidents arising from the exploitation of known weaknesses in services.
Documentation	OSP-051-Services Update Level Report Template, OSP-052-Services Patching Management Procedure
Inputs	Inventory of Assets, Alerts and Fixes Report
Work Products	*Up to date services in every environment,* Services Update Level Report.
Activity	Number of Work Products submitted, Number of patching updates in information systems
Scope	Percentage of information systems covered by the process
Update	Time since last Work Products submission Mean time between Work Products submissions Update level, calculated as follows: 1. Every information system update level is equal to the sum of the number of days old that are all the security patches pending to apply. 2. The environment update level is equal to the sum of the individual update levels, divided by the number of information systems. The lower this metric, the better. This metric allows checking of the progress of the patching process, and comparison of the update level of different environments.
Availability	Percentage of time the patching systems are available

Process	**OSP-5 Environment Patching**	**ID**
Description	This process covers the on-going update of services to prevent incidents related to known weaknesses.	**QUE**
Rationale	Patching prevents incidents arising from the exploitation of known weaknesses in services.	**PORQUE**
Documentation	OSP-051-Services Update Level Report Template, OSP-052-Services Patching Management Procedure	**DOCUMENTOS**
Inputs	Inventory of Assets, Alerts and Fixes Report	**ENTRADAS**
Work Products	*Up to date services in every environment,* Services Update Level Report.	**RESULTADOS**
Activity	Number of Work Products submitted, Number of patching updates in information systems	**METRICAS**
Scope	Percentage of information systems covered by the process	**METRICAS**
Update	Time since last Work Products submission Mean time between Work Products submissions Update level, calculated as follows: 1. Every information system update level is equal to the sum of the number of days old that are all the security patches pending to apply. 2. The environment update level is equal to the sum of the individual update levels, divided by the number of information systems. The lower this metric, the better. This metric allows checking of the progress of the patching process, and comparison of the update level of different environments.	**METRICAS**
Availability	Percentage of time the patching systems are available	**METRICAS**

Guía ISM³ (Explicación)

1. Estándares de Seguridad
2. Enfoque del Negocio
3. Mejoramiento Contínuo
4. Orientación a Procesos
5. **Niveles de Responsabilidad**
6. Retorno de inversión
7. Metodología de Análisis de Riesgos
8. Visión General
9. Metricas
10. Ventajas
11. Resumen

AGENDA

Transparencia: Las responsabilidades y los canales de reporte deben estar claramente definidos, documentados y divulgados.

Particionamiento: Todas las instancias de los procesos del SGSG deben tener uno y solo un propietario.

Supervisión: Todos lor procesos del SGSI deben tener al menos un supervisor.

Rotación: Todos los procesos críticos deben ser periodicamente transferidosa otro dueño de proceso.

Separación: Ningun dueño de proceso debe ser propietario de procesos incompatibles.

Guía para las responsabilidades

Strategic Practices

Manejo de metas estrategicas, coordinación y aprovisionamiento de recursos;

Tactical Practices

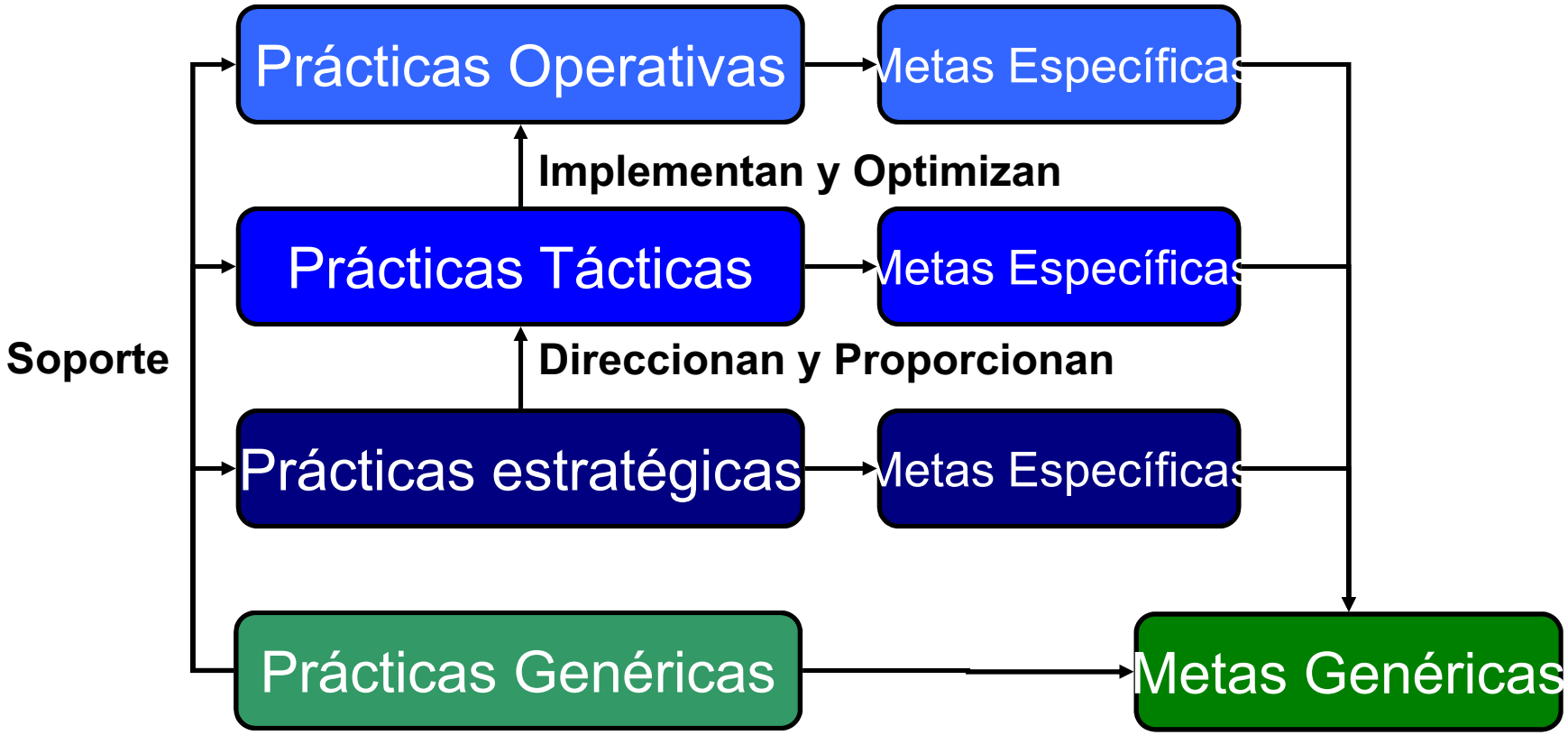
Maneja el diseño e implantación del SGSI, metas específicas y gestiona los recursos;

Operational Practices

Busca el logro de las metas definidas a partir de los procesos tecnológicos.

Responsabilidades: Gerencia

Responsabilidades: Jerarquía



Niveles de Responsabilidad

1. Estándares de Seguridad
2. Enfoque del Negocio
3. Mejoramiento Contínuo
4. Orientación a Procesos
5. Niveles de Responsabilidad
6. **Retorno de inversión**
7. Metodología de Análisis de Riesgos
8. Visión General
9. Metricas
10. Ventajas
11. Resumen

AGENDA

ISM^3 se adapta a organizaciones con diferentes contextos y misiones.

ISM^3 se adapta a organizaciones con diferentes recursos.

- La inversión en seguridad se lleva a cabo de acuerdo con las necesidades del negocio
- Algunas organizaciones pueden no tener un gran presupuesto para seguridad de la información (Regla 20 / 80).
- Los niveles de madurez reflejan diferentes niveles de sofisticación del SGSI.
- Las organizaciones pueden identificar sus procesos apropiados, escoger un nivel aplicable a ellos, y mostrar progreso en su implantación.

Flexibilidad

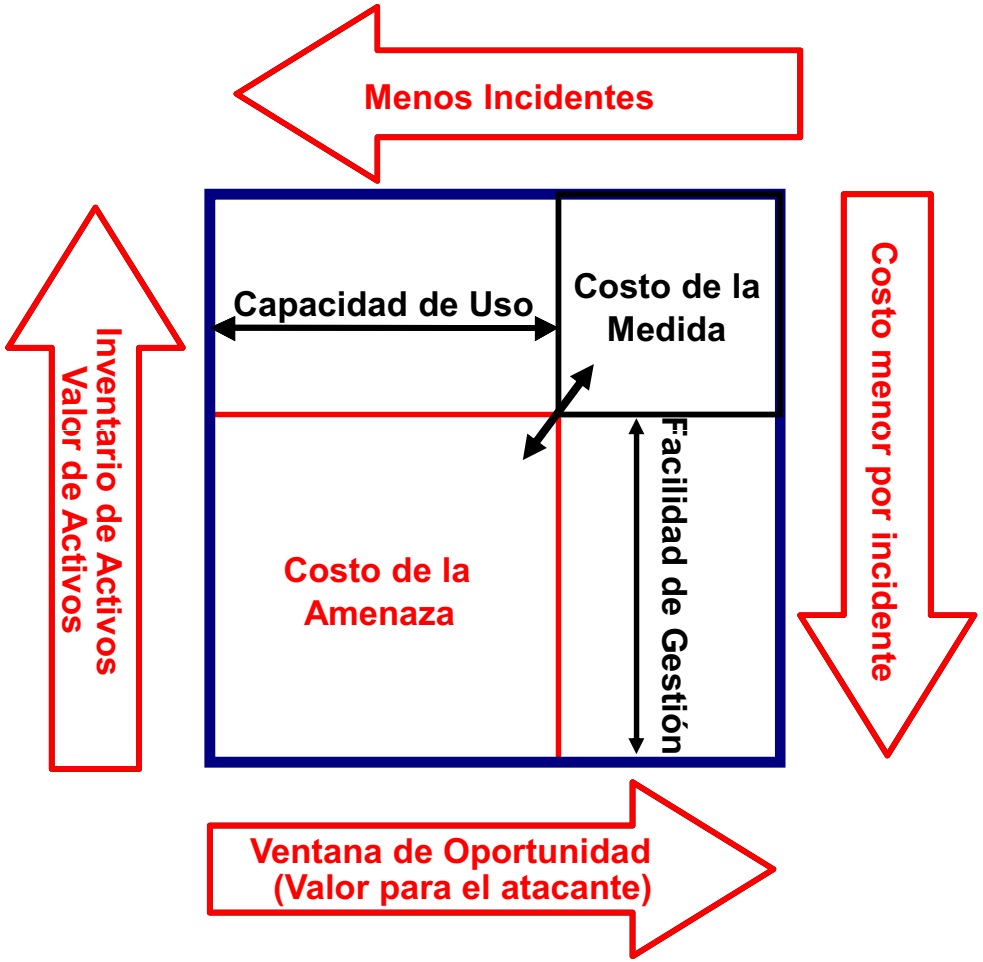
Paradoja de Mayfield

Costará una cantidad infinita de dinero dar acceso a un sistema a todo el mundo, y al mismo tiempo prevenir el acceso al mismo sistema a todo el mundo.

Estudio CERT :

Cuanto mayor sea la inversión, menor será la diferencia visible en seguridad de la información.

Inversión en Seguridad



Inversión en Seguridad

ISM3 Nivel 1 – Reducción significativa del riesgo proveniente de amenazas técnicas, para una inversión mínima en los procesos esenciales del SGSI.

Para organizaciones con bajos objetivos de seguridad, en ambientes de bajo riesgo.

ISM3 Nivel 3 – Alta Reducción del riesgo proveniente de amenazas técnicas, para una inversión significativa en los procesos esenciales del SGSI.

Para organizaciones con altos objetivos de seguridad, en ambientes de riesgo normal o alto.

ISM3 Nivel 5 - Alta Reducción del riesgo proveniente de amenazas técnicas, para una inversión alta y optimizada en los procesos esenciales del SGSI.

Para organizaciones con requerimientos específicos (como empresas de servicios publicos o instituciones financieras) con altos objetivos de seguridad en ambientes de riesgo normal o alto.

Niveles de Madurez

1. Estándares de Seguridad
2. Enfoque del Negocio
3. Mejoramiento Contínuo
4. Orientación a Procesos
5. Niveles de Responsabilidad
6. Retorno de inversión
7. **Metodología de Análisis de Riesgos**
8. Visión General
9. Metricas
10. Ventajas
11. Resumen

AGENDA

- Existen muchos métodos de Análisis de Riesgo. Tenga en cuenta:
  - El alcance (que incluir, que excluir)
  - La profundidad (mantenga presentes los procesos de negocio)
  - La manera en quemodela las partes/objetos de la organización, sus relaciones, y los estados de sus ciclos de vida.
  - Su taxonomía de amenazas (no hay una unica aceptada en todos los niveles de profundidad)
  - La manera en la que calcula el impacto sobre sus activos (dinero, alto medio bajo o escalas de confidencialidad, integridad o disponibilidad asi como sus expansiones o combinaciones)
  - Taxonomía de los controles (no hay una unica aceptada en todos los niveles de profundidad. Muchos usan la lista de ISO17799)
  - Como combina las amenazas, su probabilidad, controles, su calidad e impacto para alcanzar un escenario de riesgo.

Análisis de Riesgo

- El análisis de riesgo de ISM3 es simple y significativo para la gerencia:
  - El alcance- Toda la organización, La profundidad – nivel de gestión, Modelo de negocio – funciones de negocio:
    - Governance.
    - Investigación.
    - Publicidad.
    - Inteligencia de negocio.
    - Recursos humanos.
    - Tecnologías de Información.
    - Legal.
    - Relaciones.
    - Administracion.
    - Financiera
    - Infrastructura.
    - Logistias.
    - Mantenimiento.
    - Aprovisionamiento.
    - Produccion.
    - ventas.

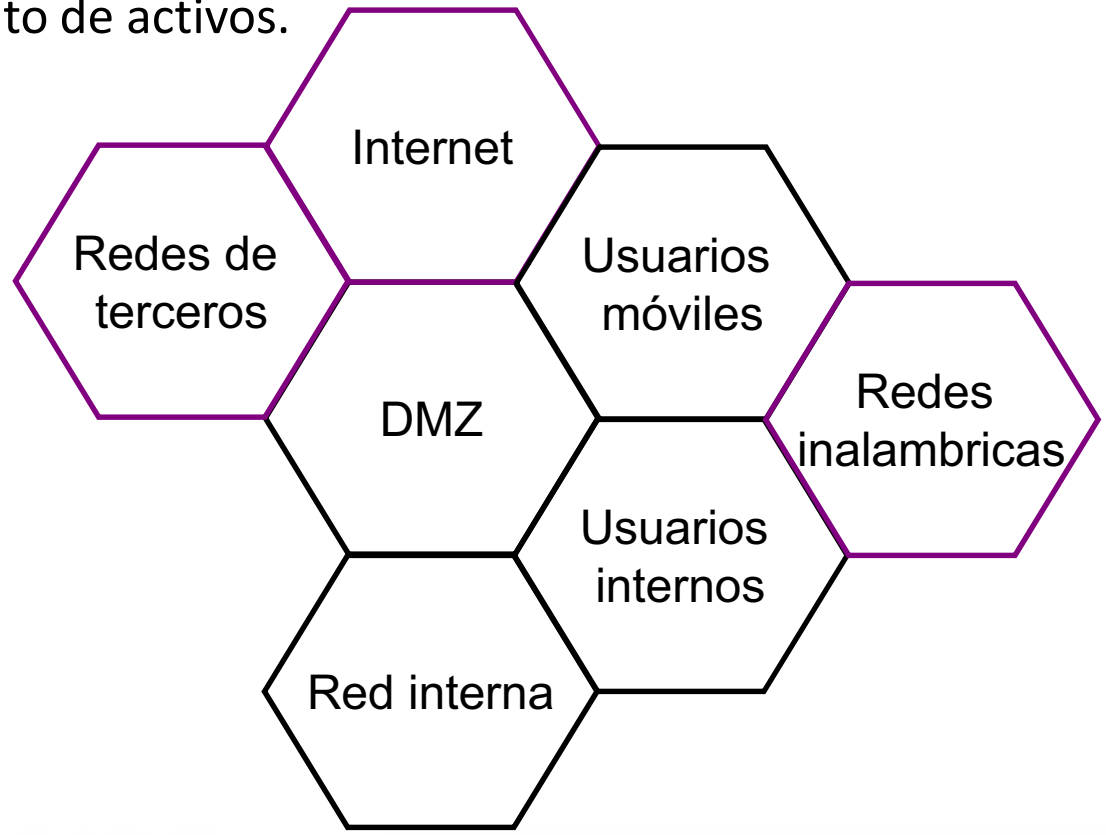
Análisis de Riesgo

Análisis de Riesgo

- El análisis de riesgo de ISM3 es simple y significativo para la gerencia:
  - Taxonomía de Amenazas:
    - Destrucción, corrupción o pérdida de información en los sistemas
    - Fallas en la destrucción de información expirada o sistemas & falla para detener los sistemas a discresión
    - Uso o acceso inapropiado de sistemas
    - Registro inapropiado de acceso a los sistemas
    - Uso no autorizado, espionaje o difusión de información clasificada
    - Baja en el rendimiento o falla total de sistemas & falla en el acceso autorizado.
    - Vencimiento de la información & Sistemas desactualizados
  - Taxonomia de controles – procesos ISM3 o ISO27001.
  - Los ambientes o escenarios de riesgo se propagan de acuerdo con las funciones de negocio que tienen que ver con ellos.

- Los sistemas de gestión son modelados por la gerencia.

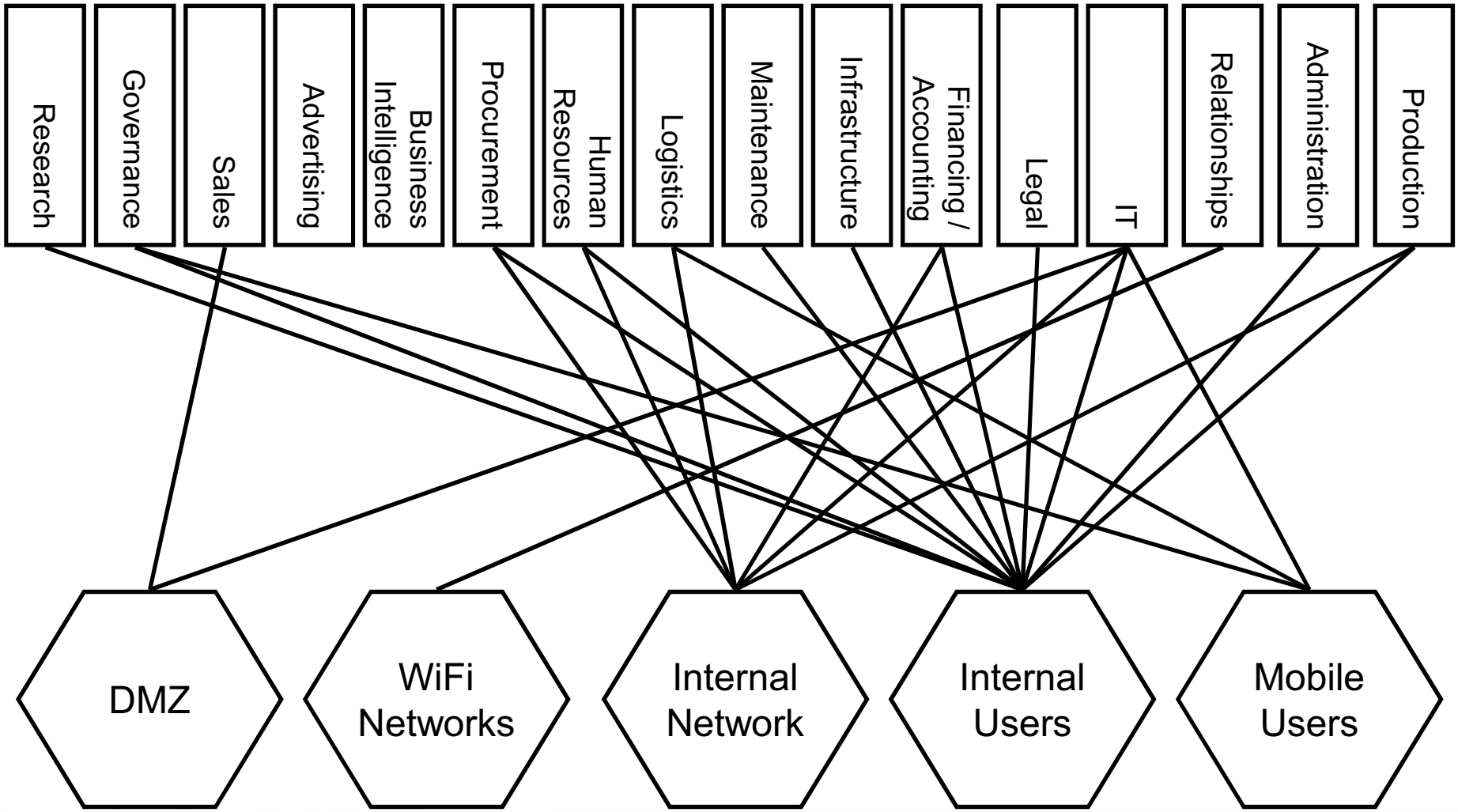
- Si usted modela un tigre como un conjunto de celdas, usted pierde la vision del animal. No se puede modelar una organización como un conjunto de activos.



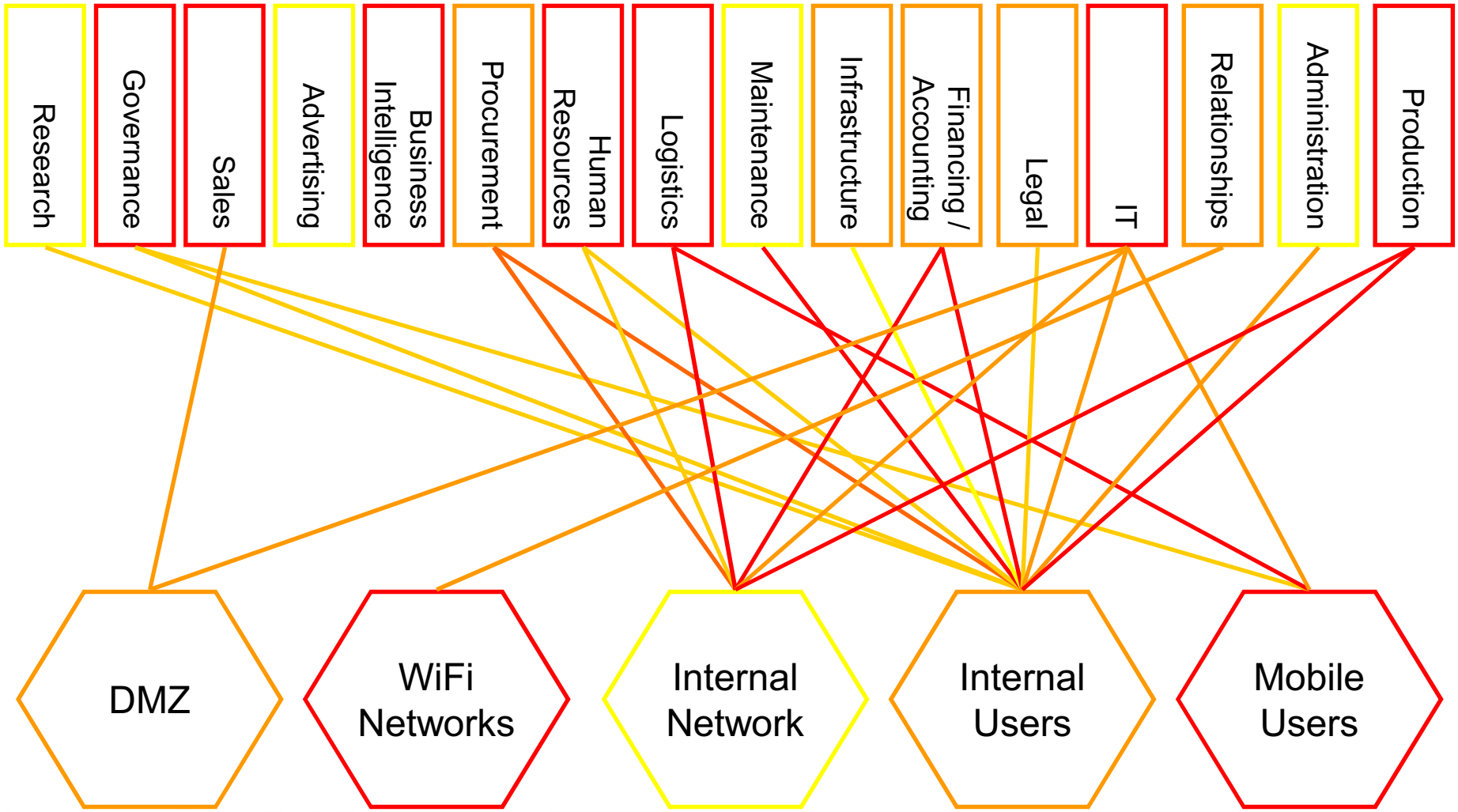
Ambientes de Riesgo

- El negocio se modela a nivel de gerencia.
- Cada funcion de negocio existente tiene una importancia diferente en cada organización

Ambientes de Riesgo



Ambientes de Riesgo



Ambientes de Riesgo

1. Estándares de Seguridad
2. Enfoque del Negocio
3. Mejoramiento Contínuo
4. Orientación a Procesos
5. Niveles de Responsabilidad
6. Retorno de inversión
7. Metodología de Análisis de Riesgos
8. **Visión General**
9. Metricas
10. Ventajas
11. Resumen

AGENDA

- Prevenir y mitigar incidentes que podrían poner en peligro los bienes de la organización, los productos o servicios que dependen de sistemas de información.
- Optimizar el uso de información, dinero, personal, tiempo e infraestructura.

- Los resultados del SGSI son:
  - Prevención de incidentes.
  - Incidentes paliados.
- Los resultados intangibles del SGSI son:
  - Reducción del riesgo;
  - Confianza.

Objetivos Generales

Visión General de ISM^3

- Liderar y coordinar:
  - **Seguridad de la Información;**
  - **Seguridad Física;**
  - **Seguridad e Higiene en el trabajo;**
  - **Interacción entre unidades de negocio;**
- Revisa y mejora el SGSI
- Proporciona recursos para seguridad de la información
- Define las relaciones con otras organizaciones.
- Define Objetivos de Seguridad consistentes con los objetivos de negocio, protegiendo los intereses de los accionistas;
- Define la distribución de responsabilidades.

Objetivos Estrategicos

Visión General de ISM^3

- Reportar a los gestores Estratégicos
- Definir el entorno de gestión operativa.
- Definir las metas de seguridad.
- Definir los entornos y sus ciclos de vida.
- Seleccionar los procesos de seguridad necesarios para cumplir con las metas de seguridad.
- Gestionar el presupuesto, el personal y otros recursos dedicados a seguridad de la información.

Objetivos Tacticos

Visión General de ISM^3

- Reportar a los gestores Tácticos, incluidos informes de incidentes;
- Identificar y proteger los sistemas.
- Proteger y apoyar el ciclo de vida de los sistemas;
- Gestionar el ciclo de vida de las medidas de seguridad;
- Utilizar los recursos eficaz y eficientemente;
- Llevar a cabo los procesos para la prevención, detección y mitigación de incidentes, tanto en tiempo real como tras el incidente.

Objetivos Operativos

Visión General de ISM^3

- GP-1 Document Management – Todos
- GP-2 ISM System Audit – AM, Auditores Externos
- GP-3 ISM Design and Evolution – Dpto Seguridad

Prácticas Generales

Visión General de ISM^3

- SSP-1 Report to Stakeholders – Dirección
- SSP-2 Coordination – Organización / MAN
- SSP-3 Strategic vision – MAN
- SSP-4 Define Division of Duties rules – Auditoria
- SSP-6 Allocate resources for information security – Organización

Prácticas Estrategicas

Visión General de ISM^3

- TSP-1 Report to strategic management - MAN
- TSP-2 Manage allocated resources - MAN
- TSP-3 Define Security Targets and Security Objectives -X
- TSP-4 Service Level Management – Dpto Seguridad
- TSP-6 Define environments and life-cycles - X
- TSP-7 Background Checks – Recursos Humanos
- TSP-8 Personnel Security –Recursos Humanos+Dpto Seguridad
- TSP-9 Security Personnel Training – Recursos Humanos
- TSP-10 Disciplinary Process – Recursos Humanos+Dpto Seguridad
- TSP-11 Security Awareness – Dpto Seguridad
- TSP-13 Insurance Management - X

Prácticas Tácticas

Visión General de ISM^3

- OSP-1 Report to tactical management
- OSP-2 Security Procurement
- OSP-3 Inventory Management
- OSP-4 Information Systems Environment Change Control
- OSP-5 Environment Patching
- OSP-6 Environment Clearing
- OSP-7 Environment Hardening
- OSP-8 Software Development Life-cycle Control
- OSP-9 Security Measures Change Control
- OSP-10 Backup & Redundancy Management

Prácticas Operativas

Visión General de ISM^3

- OSP-11 Access control
- OSP-12 User Registration
- OSP-14 Physical Environment Protection Management
- OSP-15 Operations Continuity Management
- OSP-16 Segmentation and Filtering Management
- OSP-17 Malware Protection Management
- OSP-19 Internal Technical Audit
- OSP-20 Incident Emulation
- OSP-21 Information Quality Probing
- OSP-26 Enhanced Reliability and Availability Management

Prácticas Operativas

Visión General de ISM^3

- OSP-22 Alerts Monitoring
- OSP-23 Events Detection and Analysis
- OSP-24 Handling of incidents and near-incidents
- OSP-25 Forensics
- OSP-27 Archiving Management
- OSP-21 Information Quality and Compliance Probing

Prácticas Operativas

Visión General de ISM^3

1. Estándares de Seguridad
2. Enfoque del Negocio
3. Mejoramiento Contínuo
4. Orientación a Procesos
5. Niveles de Responsabilidad
6. Retorno de inversión
7. Metodología de Análisis de Riesgos
8. Visión General
9. **Metricas**
10. Ventajas
11. Resumen

AGENDA

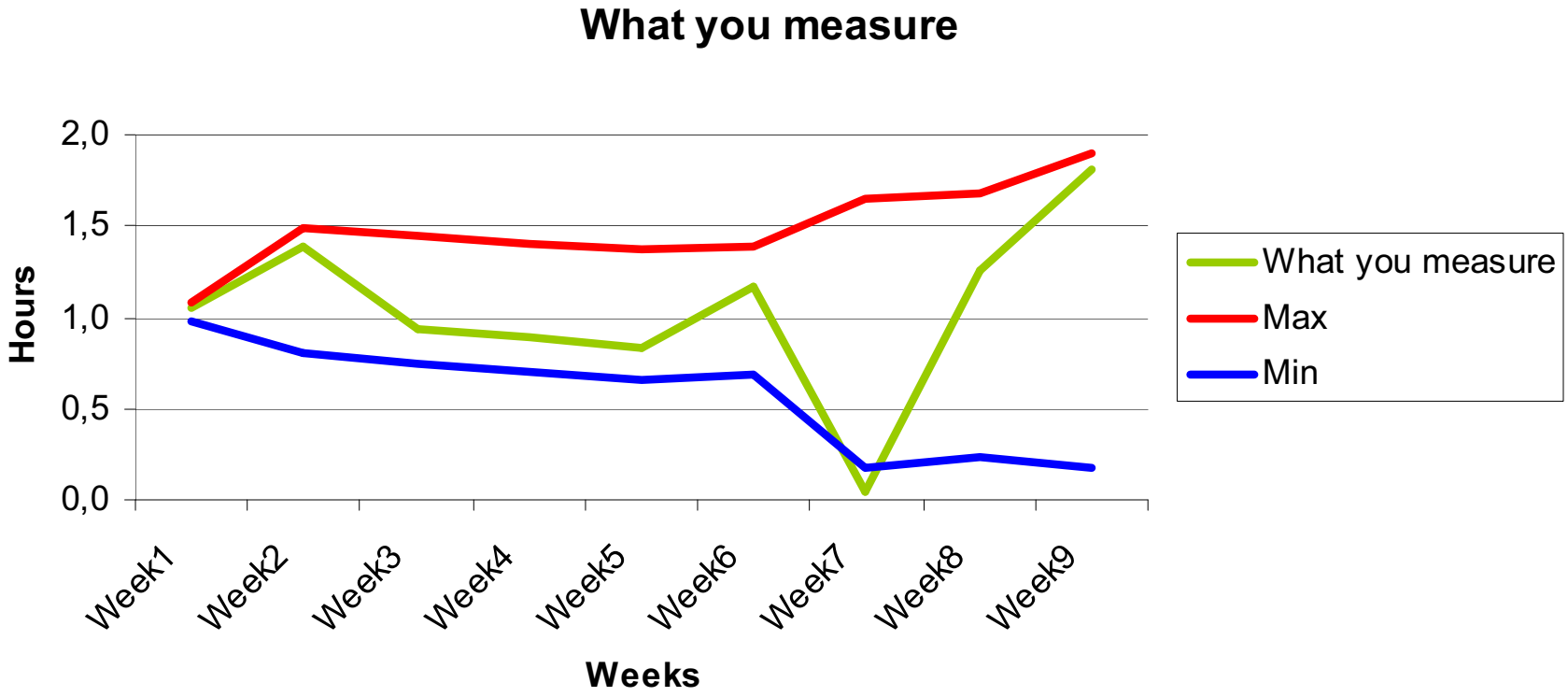
- Actividad: El numero de resultados producidos en un periodo.
- Alcance: La proporción del entorno que esta protegido. Por ejemplo, el antivirus podría estar instalado en el 50% de los PCs.
- Actualización: Lo recientes que son los resultados producidos en el periodo.
- Disponibilidad: La proporción del periodo que el proceso a funcionado, la frecuencia y la duración de las interrupciones.
- Otras métricas:
  - Retorno de Inversión / Eficiencia: La proporción de pérdidas evitadas comparada con el costo del proceso.
  - Eficacia: Proporción de resultados producidos comparados con el máximo posible. Esto implica la comparación con un valor conocido.

Tipos de Métricas

- Especificación de las métricas:
  - **Nombre.**
  - **Descripción de lo que se mide.**
  - **Como se mide la métrica.**
  - **Con que frecuencia se toma la medida**
  - **Como se calculan los umbrales.**
  - **Valores actuales de los umbrales**
  - **Mejor valor de la métrica**
  - **Unidades de medida.**

Métricas

- La métricas deben servir para:
  - Diferenciar lo normal de lo anormal
  - Saber si se mejora o se empeora
  - Saber si se tiene éxito o no.
  - Ahorrar esfuerzos; Se entiende que el proceso funciona si la métrica es normal, sólo se investiga si es anormal.


What you measure
2,0
1,5
1,0
0,5
0,0
Hours
Week1
Week2
Week3
Week4
Week5
Week6
Week7
Week8
Week9
Weeks
What you measure
Max
Min

Métricas

- El diagnóstico a partir de métricas sirve para detectar problemas :
  - Falta de recursos, por lo que habría que aumentar los recursos o relajar las metas de seguridad.
  - Metas de seguridad poco realistas, por lo que habría que corregirlas a un nivel aceptable por el negocio.
  - Incompetencia o abandono de responsabilidades, por lo que habría que tomar acciones disciplinarias.
  - Falta de formación, por lo que habría que impartir formación de emergencia, modificar programa de formación.
  - Si el proceso lleva a fallos repetidos, hay que corregir el proceso.
  - Si las responsabilidades no están asignadas correctamente, corregirlo.
  - Si la tecnología no da los resultados esperados, cambiar o adaptar la tecnología.

Métricas

Las métricas ayudan a detectar y prevenir condiciones anormales

Diagnosis	Business Decision
Fault in Plan-Do-Check-Act cycle leading to repetitive failures in a process	Fix the process
Weakness resulting from lack of transparency, partitioning, supervision, rotation or separation of responsibilities (TPSRSR)	Fix the assignment of responsibilities
Technology failure to perform as expected.	Change / adapt technology.
Inadequate resources .	Increase resources or adjust security targets.
Security target too high.	Revise the security target if the effect on the business would be acceptable.
Incompetence, dereliction of duty.	Take disciplinary action.
Inadequate training.	Institute immediate and/or long-term training of personnel

1. Estándares de Seguridad
2. Enfoque del Negocio
3. Mejoramiento Contínuo
4. Orientación a Procesos
5. Niveles de Responsabilidad
6. Retorno de inversión
7. Metodología de Análisis de Riesgos
8. Visión General
9. Metricas
10. **Ventajas**
11. Resumen

AGENDA

- **¿Cómo puedo ponerme de acuerdo con mis interlocutores sobre qué es "seguridad", "vulnerabilidad", "amenaza", etc?**
- ISM3 utiliza definiciones repetibles e independientes del observador.
- **Otros métodos, no.**

Ventajas de ISM3

- **¿Qué hay que proteger?**

- ISM3 explica como derivar los objetivos del sistema de gestión de las necesidades de negocio, técnicas y de cumplimiento.

- **Otros métodos no.**

Ventajas de ISM3

- **¿Cuales son las responsabilidades de seguridad y quien debe cumplirlas?**

- ISM3 describe las líneas de reporte de los departamentos de seguridad, de sistemas y de la dirección para los accionistas.

- **Otros métodos no.**

Ventajas de ISM3

- **¿Qué se puede hacer para proteger lo que hay que proteger?**

- ISM3 describe todas las actividades de la dirección, del departamento de seguridad, y de sistemas. La distribución de responsabilidades se explica de una forma que todos pueden comprender.

- **Otros métodos detallan numerosas actividades, pero no quien debe desempeñarlas, ni son tan completos (p.e no mencionan calidad de la información, no diferencian archivado de backup, no diferencian gestión de eventos de gestión de incidentes de análisis forense, etc)**

Ventajas de ISM3

- **¿Cómo de seguro está lo que hay que proteger? ¿Que riesgo le afecta? ¿De que hay que protegerlo? ¿Cómo se valora el costo de un incidente?**

- ISM3 tiene un método de análisis de riesgos que modela la organización, con una clasificación de amenazas a nivel de gestión y una valoración de incidentes.

- **Hay muchos otros métodos de análisis de riesgos, pero no modelan la organización, sólo enumeran los sistemas o activos (sin aclarar lo que son).**

Ventajas de ISM3

- **¿Cómo, cuando y donde habría que protegerlo?**
- ISM3 contiene referencias a los métodos existentes para implementar cada proceso.
- **Otros métodos, no.**

Ventajas de ISM3

- **¿Funciona la protección?**
- ISM3 usa Metas de Seguridad para comprobar el éxito del sistema de gestión.
- **Otros métodos, no.**

Ventajas de ISM3

- **¿Cómo puedo corregir y mejorar la protección?**

- ISM3 define los resultados de los procesos en términos positivos y usa métricas y técnicas de gestión probadas, y aplicables día a día para la mejora continua, proceso por proceso.

- **Otros métodos definen los resultados en términos negativos "evitar que", y utilizan Auditoria como técnica de mejora, aplicada al SGSI en su conjunto en plazo largos.**

Ventajas de ISM3

- **¿Cuáles son los cambios que mejorarán más la seguridad en relación con su coste?**
- Los niveles de madurez de ISM3 priorizan los procesos más rentables, optimizando la inversión.
- **Otros métodos, no.**

Ventajas de ISM3

- ¿Cómo sabemos que nuestros asociados hacen lo razonable para mantener la seguridad? ¿Cómo saben ellos que hacemos lo mismo?

- **Los niveles de madurez de ISM3 son certificables. El alcance mínimo certificable son los sistemas que soportan el negocio. Los niveles de madurez permiten demostrar que se hace todo lo razonable, no necesariamente todo lo posible**.

- **Otros métodos certificables admiten alcances arbitrarios y no tienen niveles de madurez.**

Ventajas de ISM3

1. Estándares de Seguridad
2. Enfoque del Negocio
3. Mejoramiento Contínuo
4. Orientación a Procesos
5. Niveles de Responsabilidad
6. Retorno de inversión
7. Metodología de Análisis de Riesgos
8. Visión General
9. Metricas
10. Ventajas
11. **Resumen**

AGENDA

- Los niveles de madurez facilitan priorizar y optimizar la inversión en seguridad de la información.
- Certificaciones compatibles con ISO9001; Algunas compañías no pueden hacer grandes inversiones. Es bien conocido que el 20% de la inversión puede dar 80% de los resultados, pero no hay manera de mostrarlo. Los niveles 1 a 3 de ISM3 pueden ayudar.
- Escala entre pequelas y grandes compañías. El uso de la separación de procesos en cada ambiente previene utilizar procedimientos para ambientes restrictivos a lo largo de la organización.

Resumen

- Soporta explicitamente el uso de outsourcing en gestión de seguridad y procesos operativos. El resultado por cada proceso es definido y las responsabilidades para efectuar cada proceso son definidas tambien.
- Proporciona métricas de salida, que ayudan a gestionar los procesos y miden el éxito del SGSI.
- Proporciona guianza para el modelo de gobierno de seguridad.
- Utiliza un proceso de análisis de riesgos simple y fácil de entender para la gerencia.

Resumen

1. Enfoque en el Negocio
2. Orientación a Procesos
3. Metodología de Análisis de Riesgos
4. Gestionable (con métricas)
5. Compatible (ITIL, ISO27001, ISO9001)
6. Adaptable
7. Flexible
8. Estándar abierto, accesible!

Resumen

- ¿Como puedo implantar ISM3? ¿Cuanto me va a costar? ¿como puedo certificarme con ISM3?

- ISM3 es más una evolución que una revolución, ya que describe métodos comunes a todas las organizaciones.

- El detalle de los procesos de ISM3 hace posible el outsourcing gestionandolo con SLAs (ANSs).

- El Consorcio ISM3 proporciona la certificación ISM3, mientras se gestiona como estándar ISO.

FAQs!

GRACIAS!

Juan Carlos Reyes Muñoz
jcreyes@seltika.com