Deloitte.

¿Paranoia de la ciberseguridad, o realidad?

Nuevo paradigma incomprendido

Andrés Casas

San José, 28 de Junio 2013

Agenda

The game has changed

The game has changed

Video companies like yours

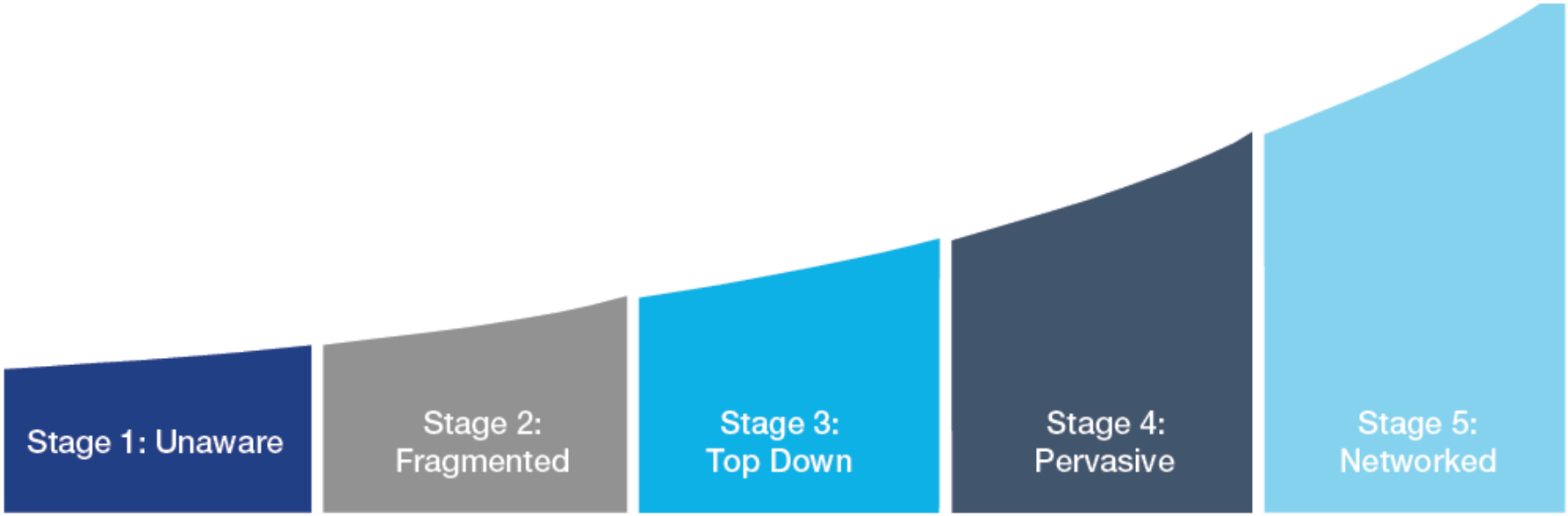
The game has changed – World Economic Forum

Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience

IT organizations have continued to construct security infrastructures around a disintegrating perimeter of increasingly ineffective controls.

Rethinking Personal Data: Strengthening Trust

The game has changed – World Economic Forum



The organization sees cyber risk as largely irrelevant, and cyber risk does not form part of the organization's risk management process. The organization is not aware of its level of interconnectedness.

The organization recognizes hyperconnectivity as a potential source of risk, and has limited insight in its cyber risk management practices. The organization has a siloed approach to cyber risk, with fragmented and incidental reporting.

The Chief Executive Officer has set the tone for cyber risk management, has initiated a top-down threat-risk-response program but does not view cyber risk management as a competitive advantage.

The organization's leadership takes full ownership of cyber risk management, has developed policies and frameworks, and has defined responsibilities and reporting mechanisms. It understands the organization's vulnerabilities, controls, and interdependencies with third parties.

Organizations are highly connected to their peers and partners, sharing information and jointly mitigating cyber risk as part of their day-to-day operations. Its people show exceptional cyberawareness and the organization is an industry leader in managing cyber risk management.

Fuente: Partnering for Cyber Resilience

The game has changed – Tendencias de tecnología

1. Tecnologías masivas
están llegando a la clase media

La tecnología seguirá aumentando la democratización y empoderamiento de empleados y clientes

3. Economías emergentes
están incrementando las fuentes de innovación

Mercados emergentes incluyendo Brasil, Rusia, India, y China son crecientemente una fuentes innovación gracias a su capital y vasta fuente de talento

2. Sostenibilidad
es un factor clave de las transformaciones

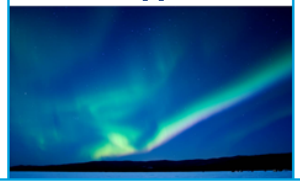
La sostenibilidad se está alejando de las iniciativas centralizadas en costos hacia la innovación y transformación corporativa

Tendencias de TI
están profundamente ajustadas por transformaciones socioeconómicas globales del 2013

4. Ahorro de costos
en economías avanzadas conlleva a la reinvención

La crisis financiera y los cambios demográficos en las economías avanzadas conllevan al gobierno a enfocarse en el ahorro de costos y reinvención en las industrias tales como la educación y la salud

Tendencias estratégicas de TI



Tendencias tecnológicas

Tendencias de tercerización

The game has changed – Tendencias de tecnología

Las tendencias estratégicas de TI dirigen el rol del CIO entre TI y el negocio hacia una estrategia de TI integrada con el negocio.

CIO como revolucionarios	Quedándose arriba	Buscando beneficios
El rol del CIO va más allá de “sentarse en la mesa” – estar a la vanguardia y ser un catalizador del impacto combinado de la información, colaboración y consumo de datos.	El CIO necesita transmitir una visión compartida, expresando como una estrategia integrada de TI y negocio permitirá mejorar el desempeño a través de toda la organización	Alcanzar beneficios de las inversiones en TI requiere de conversaciones activas, involucrando tanto al negocio como a TI. El negocio debe tratar a TI como a un socio que contribuye al valor
Gestionando seguridad & privacidad	**Servir profesionalmente**	**Involucrar respetuosamente**
El "oficial de seguridad" es ahora una función en su propio derecho, en vez de una que se integra dentro del departamento de TI	Los CIO deben ordenar su portafolio, profesionalizar TI, para asegurarse que “la mercancía es entregada" al negocio, y demostrar que se ha logrado	Tanto TI como el negocio se beneficiarán de involucrarse uno con el otro. Para involucrarse satisfactoriamente, los CIO deberían establecer una gestión de la demanda de TI estructurada, que permita empoderar al negocio

The game has changed – Tendencias de tecnología

Las tendencias tecnológicas siempre examinan el panorama evolutivo de la tecnología disponible para su uso en el negocio.

Visualización	Visualización geoespacial	"Big Data" va a trabajar	Análisis real
Análisis visual e interactivo de datos muy grandes, de alta densidad, estructurados y no estructurados para decisiones y acciones más efectivas	La visualización geoespacial agrupa la amplia información disponible a través de la visualización con tipos específicos de análisis que pueden ser realizados con datos relacionados a la ubicación	"Big data" es una evolución de antiguas disciplinas de información. Expande el rango de fuentes de datos, la cantidad de datos que puede ser procesados y la velocidad de las respuestas se pueden derivar	Aplicando análisis avanzados para aprovechar el valor de la información, de retrospectiva a introspectiva y prospectiva - cada vez más como un servicio gestionado

Computación social	Involucramiento del usuario	Movilidad aplicada	Nubes de capacidad
Colaboración, búsqueda de pericia y la sabiduría de la multitud tienen implicaciones empresariales inmediatas para la inteligencia de mercado, análisis y sistemas operacionales	Aplicando los principios de la web x.0 a los problemas del negocio basado en como el trabajo realmente se realiza, impulsado por el usuario de abajo y no el sistema de arriba	Las soluciones móviles han pasado de ser favoritos del consumidor y pasatiempo empresarial para convertirse en un habilitador clave de la innovación "de punta" del negocio	La evolución de nubes de capacidad; desde arquitecturas de aplicaciones y sistemas operativos en la nube hasta el soporte y entrega de servicios de negocio completos

The game has changed – Tendencias de tecnología

Las tendencias tecnológicas siempre examinan el panorama evolutivo de la tecnología disponible para su uso en el negocio.

El final de “la muerte del ERP”

La duradera importancia de verdaderos mecanismos de gestión de datos empresariales y procesos de automatización continuará siendo la base para información avanzada, involucramiento del usuario y estrategias en la nube

Identidades digitales

La gestión de las identidades digitales ha existido por décadas, desde sus inicios como inicios de sesión en mainframes, hasta credenciales empresariales y se espera una gran cantidad de nombres de usuario y contraseñas en 2013

Gamificación

La gamificación trata de tomar la esencia de los juegos - diversión, jugar y pasión - y aplicarlo al mundo real, a situaciones reales. Un resultado esperado de la gamificación es la participación activa

Aplicaciones “casi-empresariales”

Los CIO responden a la adopción del negocio de soluciones SaaS (Software como Servicio) y PaaS (plataforma como servicio) que son "solo lo sufrientemente buenas, justo lo suficiente resistentes, lo suficientemente grandes y justo a tiempo"

Ciber inteligencia

Un marco que combina la ciber-seguridad, ciber-forense, ciber-logística, y ciber análisis para proteger, inspeccionar y predecir penetraciones, ex filtración y extorsión

The game has changed – Tendencias de tecnología

Las tendencias de tercerización indican el potencial de soluciones de aprovisionamiento para alcanzar el servicio y resultados esperados por el negocio.

Alcanzando los proveedores socios

La tercerización de TI para TI y el negocio es una búsqueda de talento. Acuerdos en los niveles de servicio (SLA) que se encuentren alineados resultarán en una proporción superior de satisfacción

Demanda de la mesa de servicio para la tercerización

El mercado de tercerización de la mesa de servicios continúa siendo afectado por la industrialización, entrega global, automatización y multi-aprovisionamiento. La demanda es fuerte y está en incremento

Convergencia de las telecomunicaciones y servicios de red

La categoría de inversión más relevante para las operaciones de TI son las telecomunicaciones convergentes y gestión de la red, incluyendo la red área local, red de área amplia, voz, VoIP y telefonía

Multi-aprovisionamiento es inevitable

Los acuerdos de tercerización usualmente fallan al entregar el costo, servicio y resultados de negocio esperados. Competencias críticas de multi-aprovisionamiento deben ser desarrolladas para establecer una oficina de aprovisionamiento eficiente

Tercerización de todo TI ya no tiene demanda

Tercerización de toda la infraestructura de TI incluyendo mainframes, redes, centros de datos, sistemas de gama media, estaciones de trabajo y portátiles ya no se encuentra en alta demanda

The game has changed – ¿Qué está haciendo el vecino?

14. ¿Cuáles fueron las tres principales iniciativas de seguridad de su organización en el 2011?

Punto clave

Gobierno de seguridad de la información, administración de identidad y acceso, estrategia y roadmap de seguridad de la información, cumplimiento regulatorio y legislativo de seguridad de la información, protección de datos, medición y reporte de seguridad de la información y capacitación y sensibilización en seguridad de la información fueron las principales iniciativas para el 2011.

The game has changed – ¿De qué sufre el vecino?

12. ¿Cúales son los principales obstáculos que enfrenta su organización en su capacidad de formar un programa de seguridad de información efectivo?

Punto Clave

La mayoría de las organizaciones creen que la falta de recursos o presupuesto adecuado es el principal obstáculo para establecer un programa efectivo de seguridad de la información.

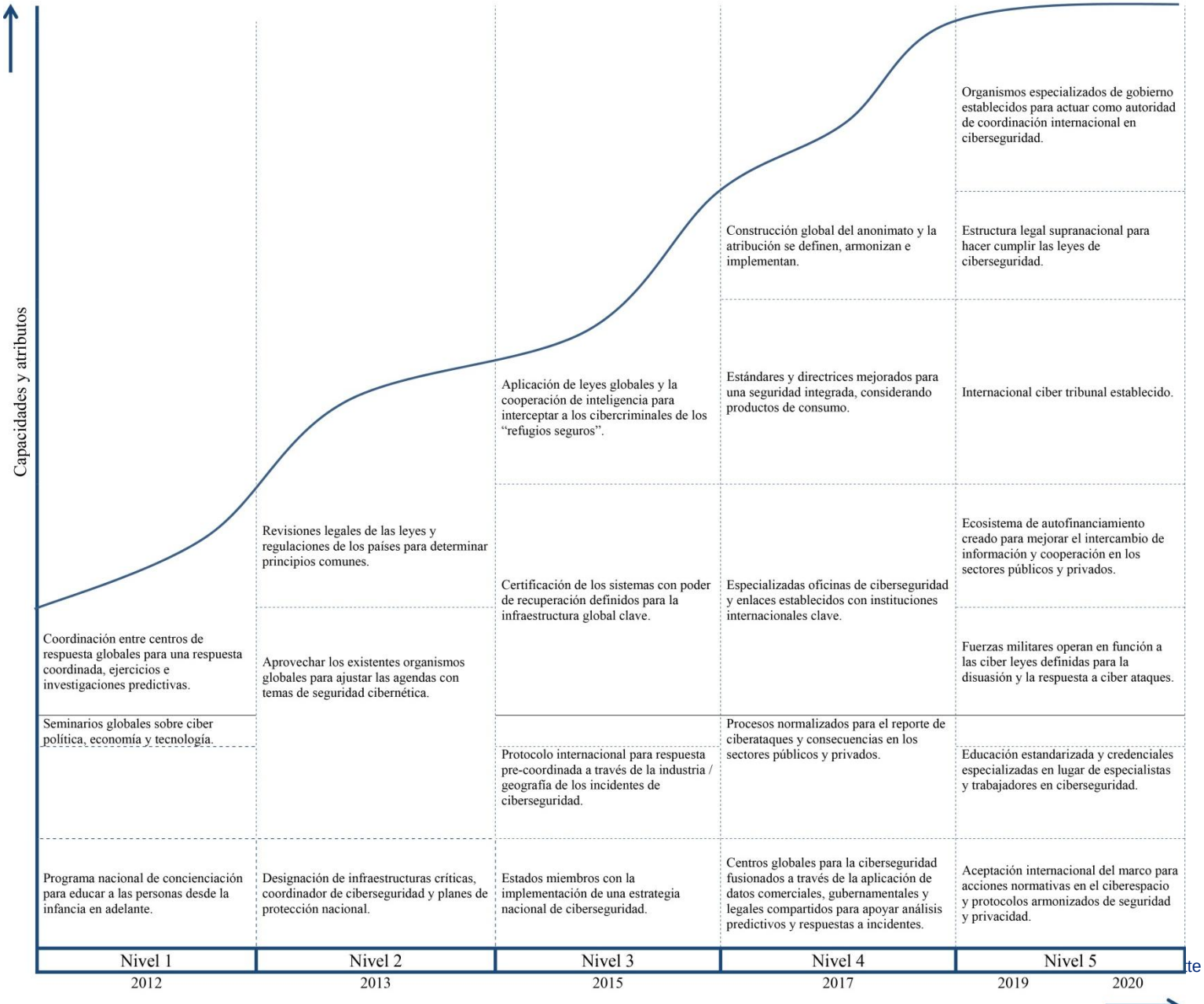
The game has changed – ¿De qué sufre el vecino?

21. ¿Qué capacidades están siendo utilizadas del Centro de Operaciones de Seguridad (SOC)?

Punto Clave

Para combatir las amenazas sofisticadas de hoy en día, monitoreando el tráfico y datos y activamente respondiendo a los incidentes y brechas son las capacidades top de los SOC utilizadas por las organizaciones. Sin embargo, una de cada 4 empresas aún no usan un SOC.

The game has changed – ¿Qué esperamos del mundo?



The game has changed – ¿Qué esperamos del mundo?

26. Utilizando una escala del 1-4, califique las siguientes amenazas a medida que visualiza su impacto dentro de los siguientes 12 meses (1=no es una amenaza, 2= amenaza baja, 3=amenaza promedio, 4=amenaza alta).

	No es amenaza	Amenaza baja	Amenaza promedio	Amenaza alta
Espionaje estatal o industrial	27%	43.8%	23.4%	5.9%
Ataques coordinados	14.9%	42%	28.2%	14.9%
Fraude financiero donde se involucran los sistemas de información	9.8%	23.9%	47.8%	18.4%
Abuso por parte de los empleados de los sistemas de TI y la información	8.6%	33.3%	47.1%	11%
Errores y omisiones de los empleados	4.7%	33.3%	48.2%	13.7%
Brechas seguridad de información, incluyendo datos sensibles de identificación personal	7.8%	29.8%	46.7%	15.7%
Ataques que se aprovechan de vulnerabilidades en redes móviles	20.8%	37.3%	31.8%	10.2%
Aprovechamiento de vulnerabilidades en las plataformas de comercio electrónicos utilizadas por la organización	14.2%	39.4%	37.4%	9.1%
Amenazas resultantes de la convergencia de las redes sociales y plataformas en línea dentro de la red corporativa	25.9%	39.6%	26.3%	8.2%
Amenazas derivadas de la adopción temprana de tecnologías emergentes que contienen posibles vulnerabilidades	25.5%	40.8%	24.3%	9.4%
Amenazas persistentes avanzadas	17.3%	44.3%	31.4%	7.1%
Riesgos sistémicos	12.3%	34.4%	44.7%	8.7%
Diferentes interpretaciones culturales de comportamiento de seguridad positiva	18.1%	45.7%	29.1%	7.1%
Brechas de seguridad que involucran a organizaciones de terceros	14.1%	31.6%	41.4%	12.9%
Hacktivismo o Ciberactivismo	17.7%	36.8%	30.3%	15.2%

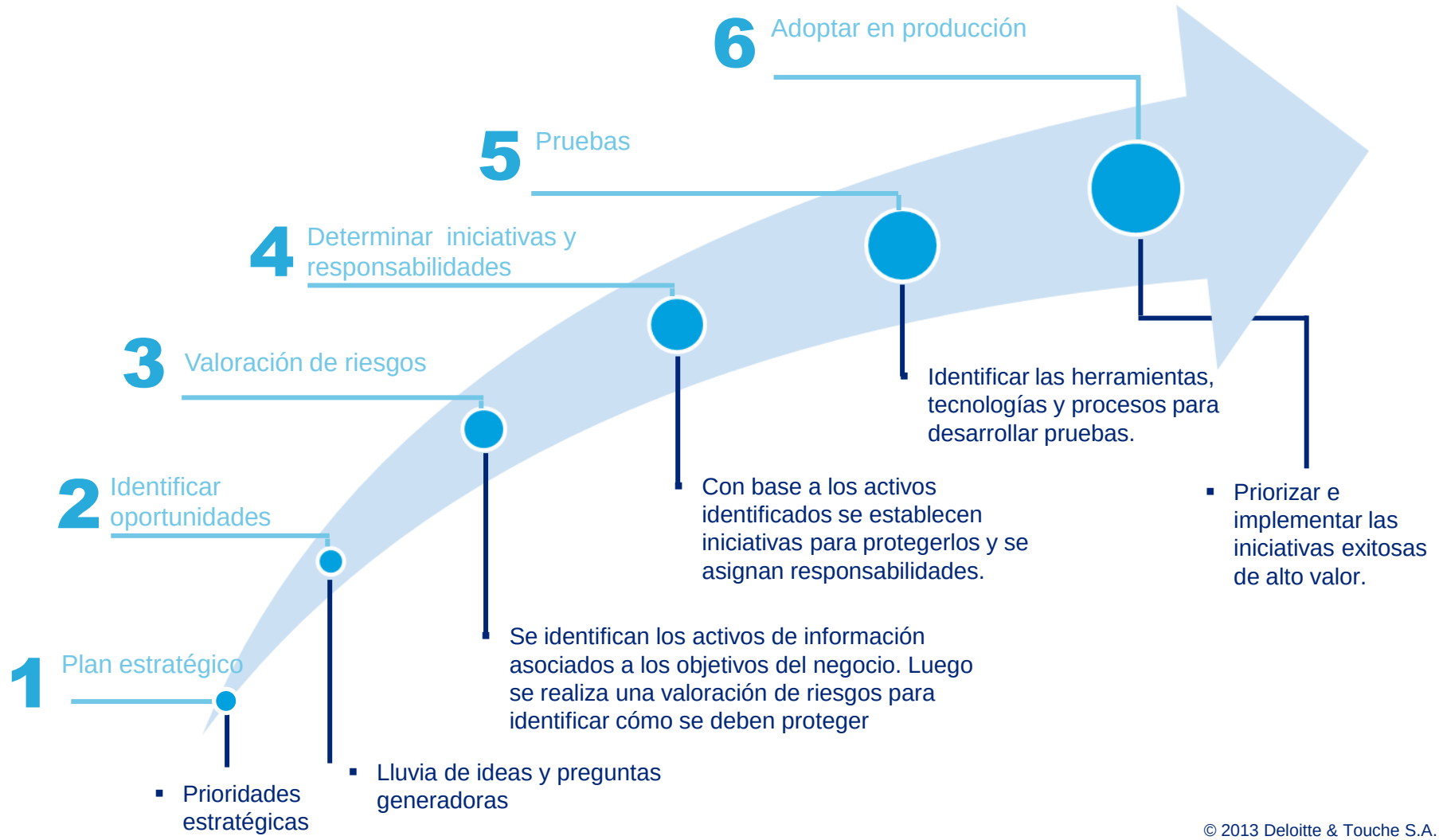
Punto clave

A medida que el uso de la tecnología y el internet se prolifera, el fraude financiero que implica a los sistemas de información, las brechas de seguridad de información, hacktivismo y los ataques coordinados son citados como las cuatro mayores amenazas.

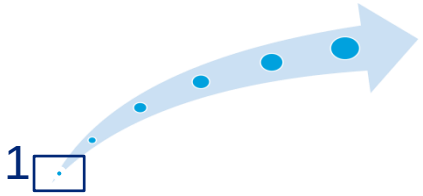
¿Cómo identificar el alcance?

Hoja de ruta recomendada para seguridad de información

Plan de trabajo de seguridad comienza con los tomadores de decisiones y sus preguntas crujientes y luego procede a las fuentes de datos y las tecnologías que se requieren para proteger los intereses.



Todo proyecto de seguridad de información inicia con una pequeña fase de planeamiento y definición del alcance



Identificar oportunidades

2

La identificación de oportunidades estratégicas comienza con realizar preguntas generadoras que nos permitan recopilar las principales necesidades de la organización.

Preguntas generadoras

Clientes y redes sociales
- Qué información de nuetros clientes es confidencial?
- Quién revisa y aprueba la información que se publica en redes sociales?
- Existen amenazas contra la empresa en redes sociales?

Empleados
- Qué investigamos de nuestros empleados antes de contratarlos?
- Qué tipo de acceso poseen a la información?
- Poseen segregación de funciones?
- Qué hacemos con los equipos y accesos de un empleado cuando cambia de puesto o sale de la organización?

Cumplimiento
- Existe regulación asociada a seguridad de información que debemos acatar?
- Existen políticas de la empresa relacionadas a seguridad de la información?
- Existen penalizaciones por un tratamiento inadecuado de la información?

Proveedores
- Conocemos cómo nuestros proveedores gestionan nuestra información?
- Qué dependencia tenemos de nuestros proveedores para poder operar?
- Qué acceso tienen los proveedores a nuestra información?

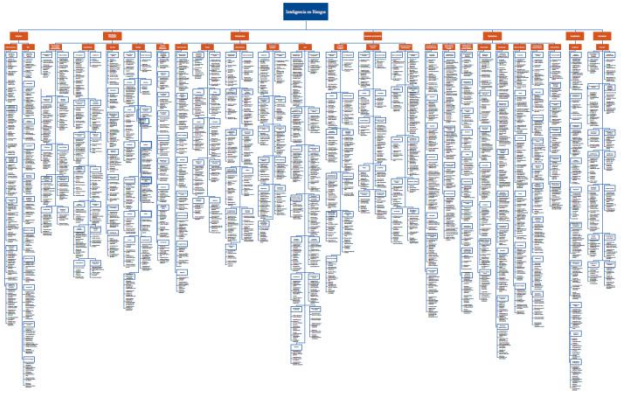
Activos
- Conocemos como identificar y tratar la información según su nivel de confidencialidad? (Pública, uso interno, confidencial, privada).
- Dónde almacenamos y cómo procesamos la información confidencial?
- Cuáles son los activos que dependemos para operar?

Incidentes
- Qué incidentes hemos tenido relacionados a seguridad de información?
- Qué tan rápido hemos actuado para mitigar los incidentes?
- Los empleados y proveedores están capacitados para atender incidentes?

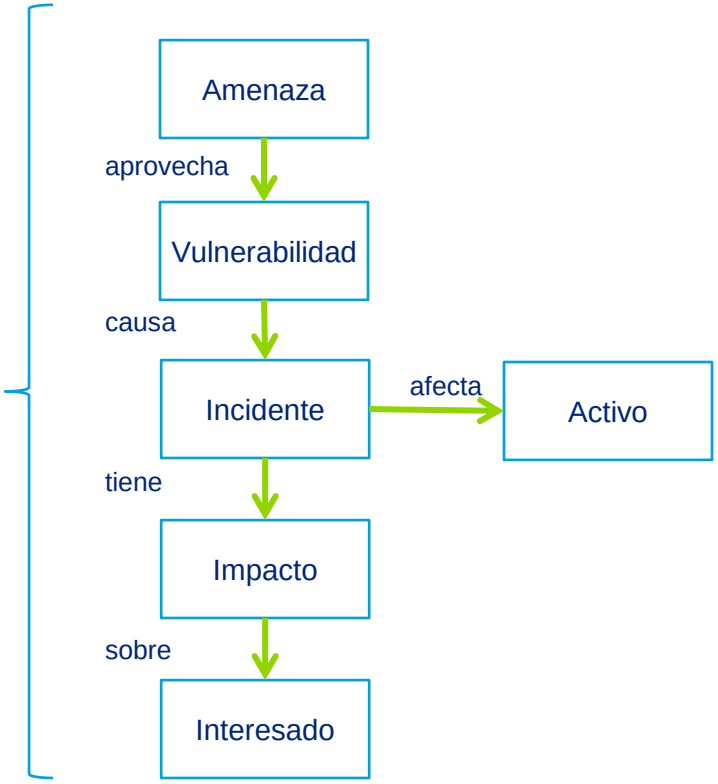
Valoración de riesgos

El riesgo es un posible evento que podría causar daño o pérdidas, o afectar la habilidad de alcanzar objetivos de la organización. A partir de las necesidades del negocio se identifican los principales activos que deben ser protegidos de las posibles amenazas.

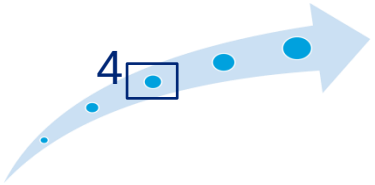
Mapa de Inteligencia de Riesgo de Deloitte



El Mapa de Inteligencia en Riesgos está planeado para servir como una guía útil en el trayecto hacia la Inteligencia en Riesgos ayudando al personal, de todas las funciones de una organización, a ampliar su perspectiva sobre el riesgo y a mejorar su capacidad para ejecutar sus responsabilidades relacionadas con el riesgo.



Determinar iniciativas y responsabilidades



Con base a las amenazas identificadas, se debe identificar las acciones que permitan mitigar su impacto sobre activo de información y el interesado. Estas acciones se pueden agrupar en iniciativas donde se considere su valor, prioridad, complejidad, impacto y plazo de implementación.

NOR003 Implementar una metodología para el desarrollo seguro de sistemas.

Objetivo

Implementar una metodología de desarrollo seguro para los sistemas

Valor	Prioridad	Complejidad	Impacto	Plazo
● Alto	● Alta	● Alta	● Alto	○ Corto Plazo
○ Medio	○ Media	○ Media	○ Medio	● Mediano Plazo
○ Bajo	○ Baja	○ Baja	○ Bajo	○ Largo Plazo

Actividades

Fase I: Definición de la metodología de Desarrollo

- Definir las políticas, procesos y procedimientos para el ciclo de vida de desarrollo seguro.
- Crear el procedimiento para la administración de versiones.
- Ajustar los procedimientos según la criticidad del cambio (emergencia, etc.)
- Definir claramente roles y responsabilidades por proceso.

….

Dependencias

- Esta iniciativa no posee dependencias.

Recursos

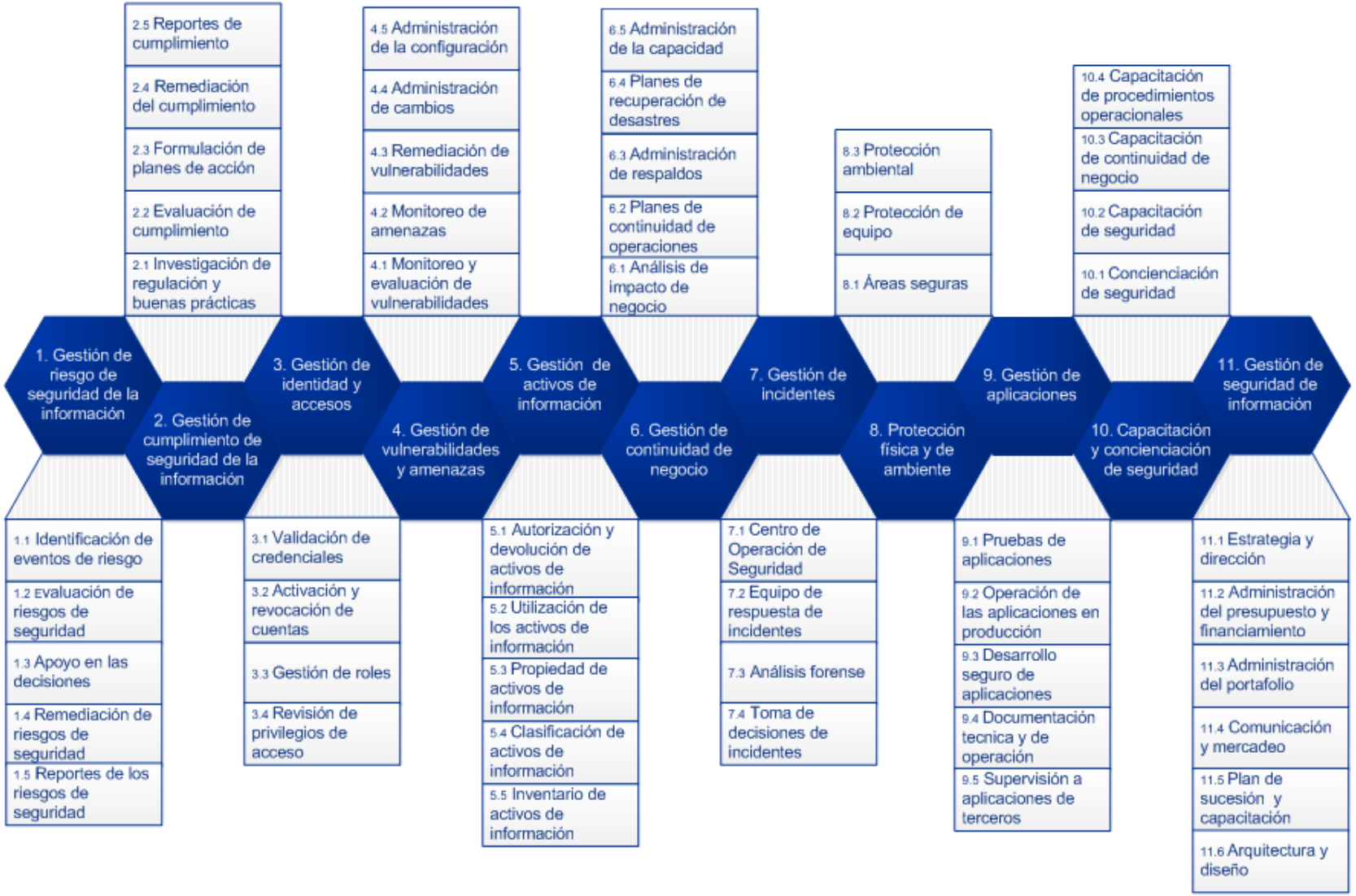
- Responsable: Desarollo de sistemas

Beneficios

- Prevención de incidentes desde el momento del diseño de nuevas funcionalidades.
- Prevención de incidentes de seguridad aplicativa desde el diseño de nuevas funcionalidades.
- Disminución de tiempos, costos y riesgos de desarrollo de nuevas funcionalidades.
- Concientizar a los programadores, de la importancia de sus desarrollos y el potencial impacto en el negocio.

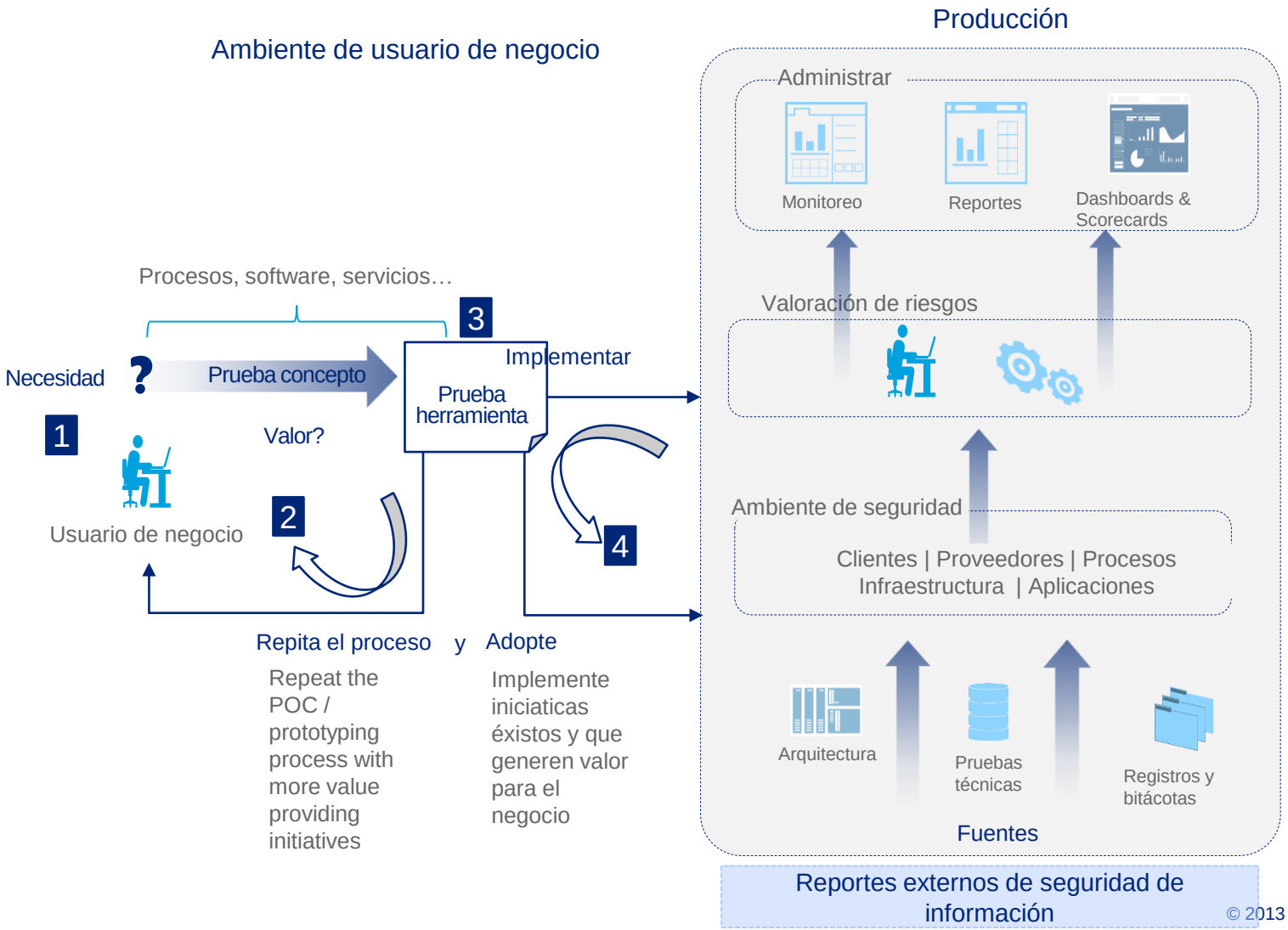
Determinar iniciativas y responsabilidades

La mayoría de las veces ya existen áreas de la organización que desempeñan un papel en la seguridad de información, por lo cual se debe identificar y dar trazabilidad.



Pruebas y adoptar en producción

Se puede ahorrar tiempo y dinero mediante la adopción de un enfoque basado en el usuario donde experimente o cree prototipos basada en negocios que apunta a proporcionar valor iniciativas.



Incorporando la seguridad en las finanzas de la empresa

Considerando el ROSI

El ROSI (Return on Security Investment) es un indicador que permite medir la relación entre el beneficio y el costo de una inversión de Seguridad.

Mediante este indicador la organización esta en capacidad de comparar las “Inversiones en Seguridad” que son capaces de disminuir los “Riesgos” de la entidad.

Hoy día, se manejan tres tipos de enfoques para la determinación del ROSI:

1. Enfoque Cualitativo
2. Enfoque Estadístico
3. Enfoque Probabilístico

Enfoque Cualitativo

Se **debe basar** en:

- ✓ Autoconocimiento de la entidad
- ✓ Estimación del Impacto
- ✓ Estimación de la Probabilidad

Este método es **útil** para:

- ❑ Desarrollo de Análisis de Brechas en la entidad
- ❑ Priorización de tareas de TI

Ventajas

1. Fácil aplicación
2. Rápido desarrollo

Desventajas

1. Falsa sensación de seguridad
2. Difícil de entender y aceptar para personas ajenas al contexto

Considerando el ROSI

El ROSI (Return on Security Investment) es un indicador que permite medir la relación entre el beneficio y el costo de una inversión de Seguridad.

Mediante este indicador la organización esta en capacidad de comparar las “Inversiones en Seguridad” que son capaces de disminuir los “Riesgos” de la entidad.

Hoy día, se manejan tres tipos de enfoques para la determinación del ROSI:

1. Enfoque Cualitativo
2. Enfoque Estadístico
3. Enfoque Probabilístico

Enfoque Estadístico

Se **debe basar** en:

- ✓ Historia de la Entidad y mercado
- ✓ Historia de la ubicación física
- ✓ Estadísticas de terceros

Este método es **útil** para:

- ❑ Concienciación
- ❑ Justificación de: Pruebas de Penetración, Análisis de Riesgos, etc.
- ❑ Autoevaluación de TI

Ventajas

1. La información está disponible
2. Fácil de actualizar

Desventajas

1. Poca confianza en la información
2. Difícil de entender y aceptar para personas ajenas al contexto

Considerando el ROSI

El ROSI (Return on Security Investment) es un indicador que permite medir la relación entre el beneficio y el costo de una inversión de Seguridad.

Mediante este indicador la organización esta en capacidad de comparar las “Inversiones en Seguridad” que son capaces de disminuir los “Riesgos” de la entidad.

Hoy día, se manejan tres tipos de enfoques para la determinación del ROSI:

1. Enfoque Cualitativo
2. Enfoque Estadístico
3. Enfoque Probabilístico

Enfoque Probabilístico

Se **debe basar** en:

- ✓ Información de la Empresa
- ✓ Información del Negocio
- ✓ Análisis probabilísticos

Este método es **útil** para:

- ❑ Justificación de inversiones
- ❑ Análisis de Riesgos.

Ventajas

1. Multidisciplinario
2. Fácil de actualizar
3. Conservador
4. Considera interacción entre eventos y amenazas

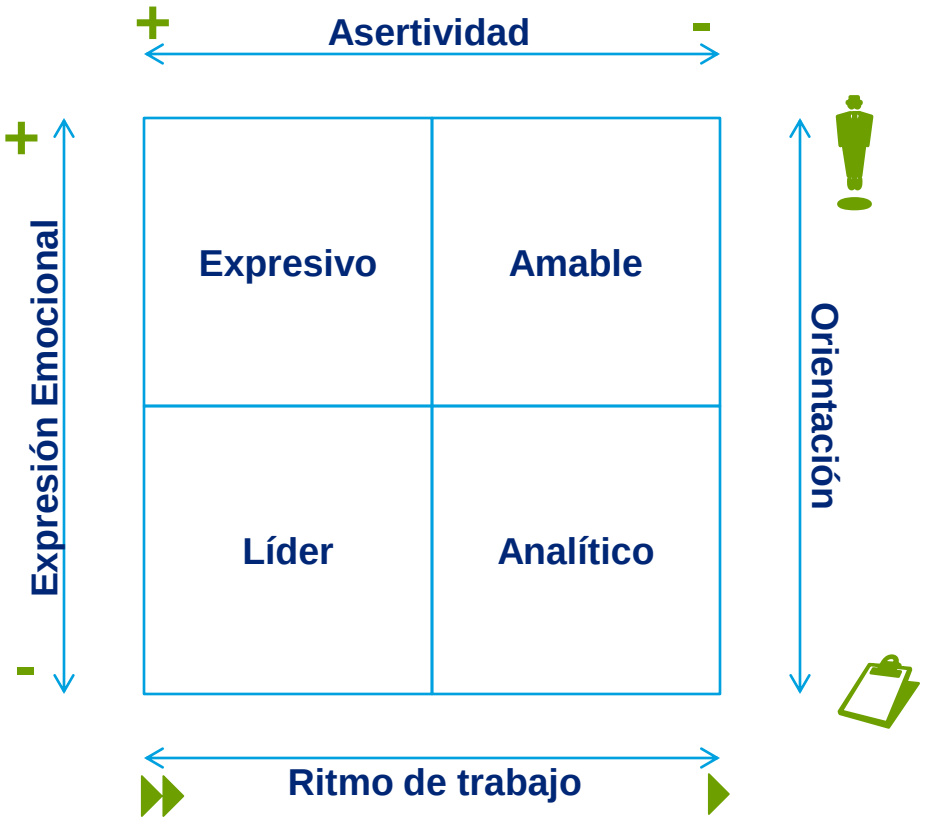
Desventajas

1. Complejo
2. Tiempo para desarrollarlo aprox. 8 a 16 semanas

Trabajando con el CEO y ejecutivos de la empresa

Estilos de Trabajo de los CEO y ejecutivos de la empresa

Ciertamente la frase “cada cabeza es un mundo” es algo que se debe considerar al tratar de trabajar con los CEO y ejecutivos de la empresa especialmente si necesitamos su apoyo para la inversión en recursos de seguridad.



Contacto

Para información adicional, por favor contactar a-

Andrés Casas

Deloitte Cybersecurity
Director
+506 2246-5209
ancasas@deloitte.com

Alonso Ramírez

Deloitte Cybersecurity
Manager
+506 2246-5103
aloramirez@deloitte.com

Depende!!!