Gestión de riesgos en ISO 27001
Experiencia práctica en la implantación y gestión en Nextel S.A.

Nextel S.A.

Índice

- Introducción
- Metodologías
- Gestión de riesgos
- Análisis de riesgos
- Tratamiento de riesgos
- Herramientas
- BS 7799-3 (ISO 27005)
- Experiencia practica Nextel, S.A.
- Conclusiones

Nextel S.A.

INTRO: ISO 27001 Implementación

Necesidades → Solución → Alcance

Identificación de procesos clave y de soporte

Identificación y valuación de activos (en su contexto de uso o empleo)

Amenazas ✍ Vulnerabilidades ✍ Probabilidades ✍ Impactos ✍ Restauración? ✍ Riesgos

Grado de seguridad / Niveles aceptables de riesgo

Selección de objetivos de control y controles

Análisis previo (Opcional)

Definición de método de implementación de cada control (si el existente no es satisfactorio)

Definir el Estado de aplicabilidad (SOA) (o Resumen de controles)

Implementación de controles de seguridad personales, procedimentales, físicos, y técnicos

Auditoria y revisión → Oportunidades de mejora

Nextel S.A.

INTRO: Gestión de riesgos en ISO 27001

“La organización demostrara que ha definido e identificado un método de análisis de riesgo adecuado, y que ha llevado a cabo un análisis de riesgo cubriendo todos los activos de información, tal y como indica la cláusula 4.2.1 de ISO 27001”

Nextel S.A.

INTRO: Gestión de riesgos y negocio (I)

· Es necesario establecer y comprender la organización y sus posibilidades, así como sus objetivos y la estrategia para lograr esos objetivos.

· Hay que establecer la relación entre la organización y su entorno, identificando sus fortalezas, debilidades, oportunidades y amenazas (DAFO)

Nextel S.A.

INTRO: Gestión de riesgos y negocio (II)

· Identificar los clientes externos e internos y considerar sus objetivos.

· La organización debería determinar los elementos esenciales que soportan o impiden su capacidad para gestionar los riesgos de seguridad de la información que afronta.

· Hay que determinar el Alcance y los parámetros de las actividades de la organización, en relación con el proceso de gestión de riesgos.

Nextel S.A.

INTRO: Gestión de riesgos y negocio (III)

· El proceso de análisis de riesgos debería de buscar el equilibrio entre los costos de los controles y su efectividad reduciendo el riesgo (Relación calidad/precio)

· Hay que establecer y prever los recursos y registros necesarios para la operatividad del proceso de gestión de riesgos.

Nextel S.A.

METODOLOGÍAS: Elementos

- ISO 13335-1:2004
- ISO 73
- AS 4360 (Australia)
- NIST SP 800-30 (USA)
- MAGERIT 2.0 (España)
- EBIOS (Francia)
- OCTAVE (Cert)

BS 7799-3:2006

Nextel S.A.

METODOLOGÍAS: Consideraciones

¿Identifica amenazas y vulnerabilidades?

¿Intenta evaluar la probabilidad de que las amenazas ocurran?

¿Podría alguien usando los mismos datos llegar a las mismas conclusiones?

¿El proceso es repetible y coherente?

¿Permite el análisis del impacto de los cambios?

Nextel S.A.

GESTIÓN DE RIESGOS

ANÁLISIS DE RIESGOS
+
TRATAMIENTO DE RIESGOS
=
GESTIÓN DE RIESGOS

Nextel S.A.

ANÁLISIS DE RIESGOS: Expectativas

· El proceso debería identificar cualquier riesgo significativo en todos los activos de información, y dentro de su contexto de uso.

· El proceso debería proporcionar un informe comprensible por la Dirección de la organización.

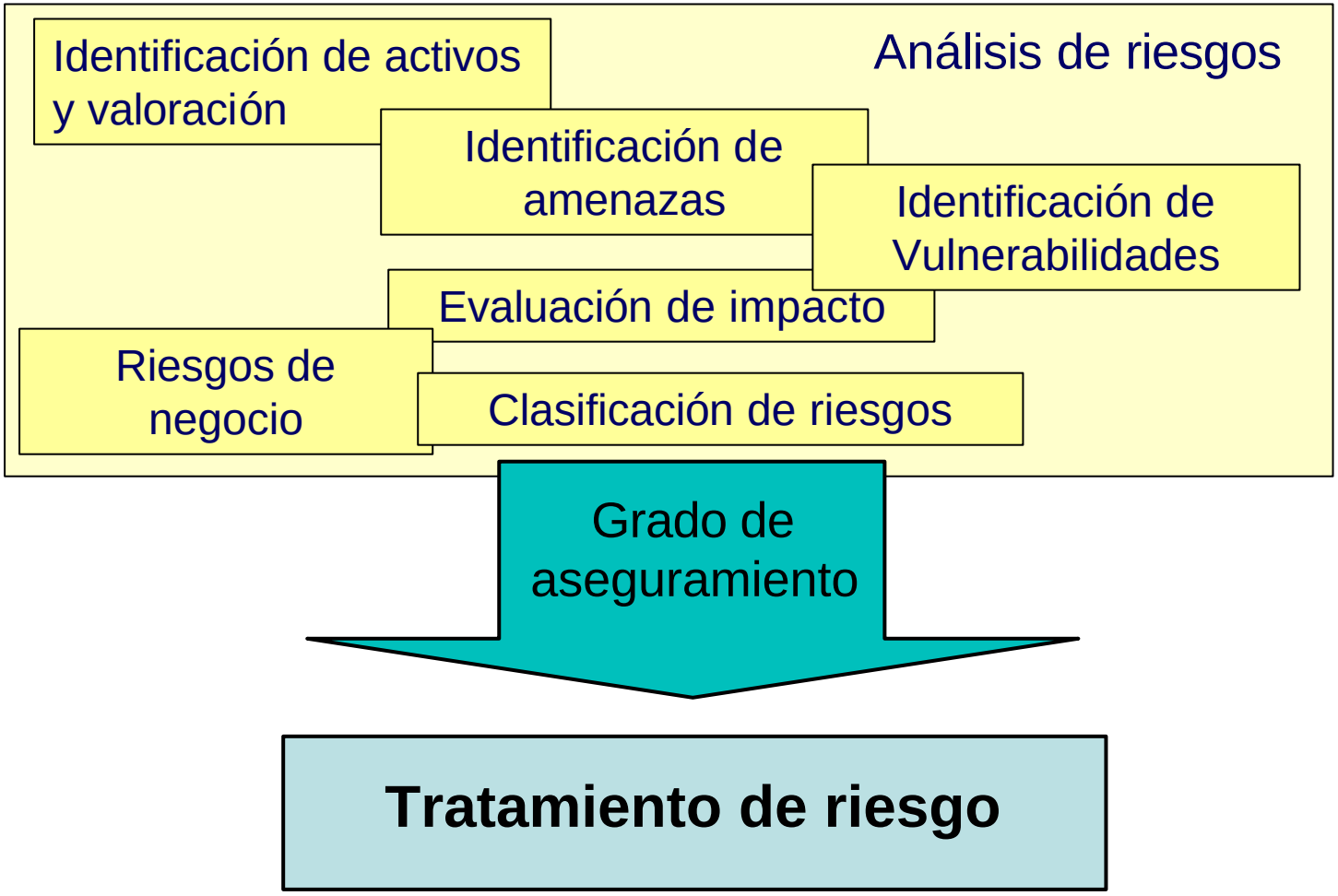
· El informe debería de establecer una cosificación de riesgos de acuerdo con el impacto potencial de estos en la organización y sus clientes internos o externo.

· Debería identificar cualquier eliminación de riesgo inmediata donde sea posible para obtener una reducción de riesgo rápida y barata.

· Debería, si es posible identificar soluciones alternativas y sus ventajas y desventajas.

Nextel S.A.

ANÁLISIS DE RIESGOS: Esquema



Nextel S.A.

ANÁLISIS DE RIESGOS: Identificación de activos

Realizar un análisis por procesos nos servirá para separar las actividades o procesos en un grupo de elementos y poder establecer un Registro de activos.

Esto nos proporcionara un esquema lógico para identificación y análisis, y nos asegurara que no dejamos de analizar algún riesgo significativo.

Nextel S.A.

ANÁLISIS DE RIESGOS: Valor de activos

Una vez identificados los activos sujetos a análisis, el Comité de seguridad valuara los activos desde el punto de vista de la seguridad de la información, como activos de información, y no en base a su valor intrínseco.

Este será el **primer factor** de los tres que nos proporcionaran el Nivel de riesgo.

Nextel S.A.

ANÁLISIS DE RIESGOS: Identificación

Vulnerabilidades son debilidades asociadas a activos de información. En si mismas no causan daño.

Esas debilidades pueden ser explotadas por **Amenazas**, que pueden causar una rotura de seguridad que tenga como consecuencia daño o perdida de esos activos de información.

Nextel S.A.

ANÁLISIS DE RIESGOS: Impacto y probabilidad

El objetivo del análisis de riesgos es separar los riesgos menores de los mayores, y proveer de información para poder evaluar y controlar el riesgo.

El análisis de riesgos incluye consideraciones sobre el origen del riesgo, la determinación de la consecuencia (IMPACTO) y la probabilidad de que esas consecuencias sucedan (PROBABILIDAD).

Nextel S.A.

ANÁLISIS DE RIESGOS: Impacto (I)

Este elemento es subjetivo y será necesario considerar el resultado de una amenaza aprovechando una vulnerabilidad.

La organización debe de establecer el resultado de incidente sobre un proceso o activos, en términos de confidencialidad, integridad o disponibilidad.

Es conveniente tener en cuenta que el punto de vista de diferentes personas de la organización puede variar a la hora de establecer el impacto de la perdida de activos.

Las preguntas son:
¿Qué sucede si ese activo o proceso se pierde?
¿Cuánto tiempo podemos estar sin el?

Nextel S.A.

ANÁLISIS DE RIESGOS: Impacto (II)

La organización establecerá un método consistente para evaluar el impacto de una rotura en la seguridad en relación a sus objetivos y dentro del contexto de su negocio.

Cuando se mida el Impacto, es importante considerar la perdidas del activo en su totalidad, y su importancia en el alcance.

Este será el **segundo factor** de los tres que nos proporcionarán el Nivel de riesgo.

Nextel S.A.

ANÁLISIS DE RIESGOS: Probabilidad

Este elemento es a menudo subjetivo y necesitara ser evaluado en colaboración con el propietario de activos, y quizás, con asesoramiento experto.

Las principales cuestiones son:

· ¿Cual es la **probabilidad** de que suceda
· ¿Como de a menudo sucede
· ¿Cuando sucede?

Este será el **tercer factor** de los tres que nos proporcionaran el Nivel de riesgo.

Nextel S.A.

ANÁLISIS DE RIESGOS: Nivel de riesgo

VALOR (1- 5)

X

IMPACTO (1- 5)

X

PROBABILIDAD (1 – 5)

NIVEL DE RIESGO (1 – 125)

ANÁLISIS DE RIESGOS: Clasificación de riesgo

Nivel de factor de Riesgo	Valores
L	1 a 32
M	33 a 63
H	64 a 94
E	95 a 125

Nextel S.A.

Grado de aseguramiento

ISO 27001 Cláusula 4.2.1 C. establece que “Hay que desarrollar criterio para la aceptación del riesgo e identificar el nivel de riesgo aceptable.”

Versiones previas de BS 7799-2 usaban el termino “Grado de aseguramiento” (que es requerido para los objetivos de control y los controles).

Aunque este termino ya no se usa en el estándar, en un concepto útil para cunado definimos como un objetivo de control y/o un control debe de ser implementado. (El estándar establece “Que” no “Como”).

Nextel S.A.

TRATAMIENTO DE RIESGOS: Base

RIESGOS:

Aceptar

Transferir

Gestionar

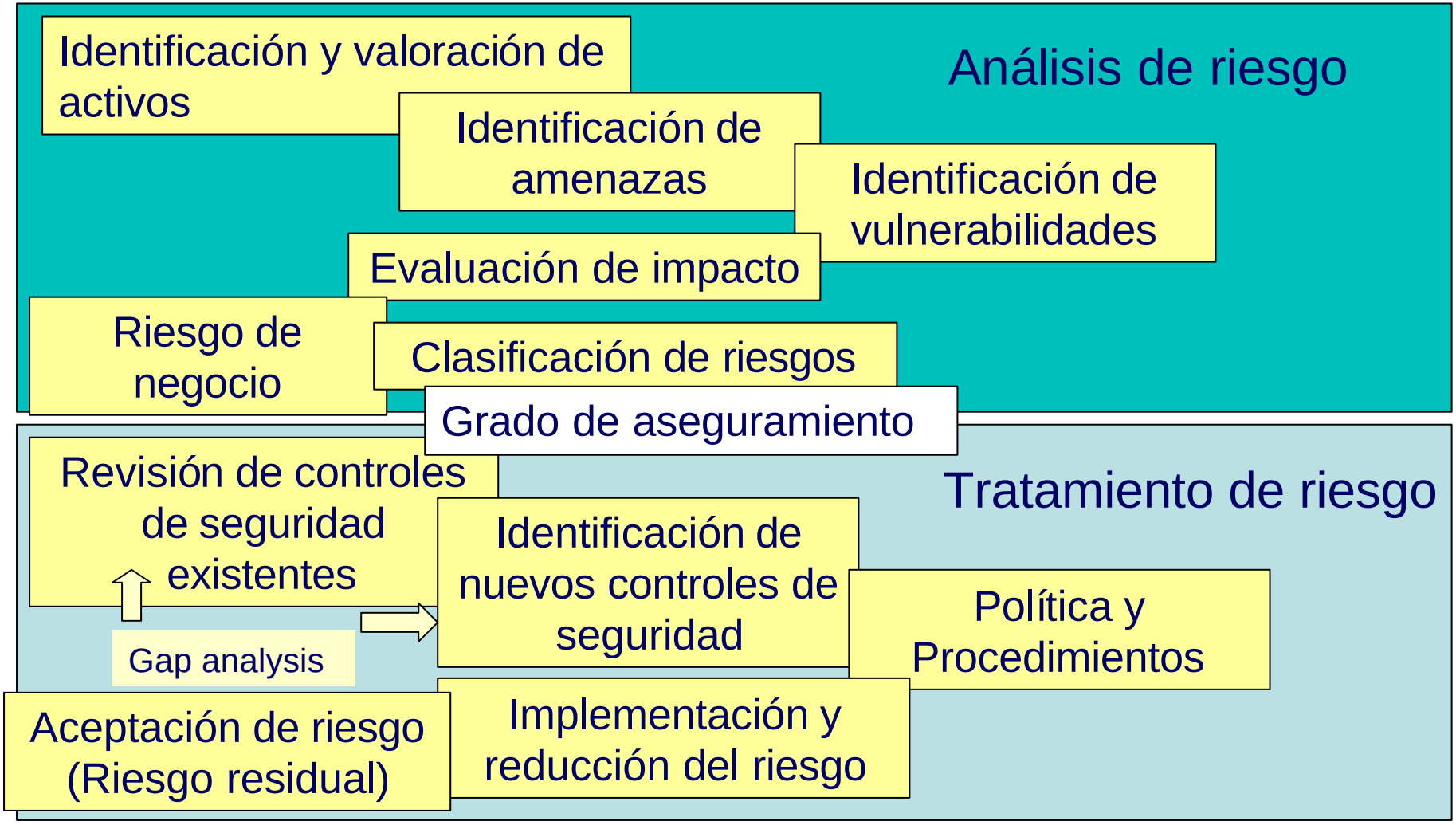
TRATAMIENTO DE RIESGOS: Criterio

El criterio según el cual los riesgos de seguridad de la información deben de ser evaluados debe de ser establecido.

Las decisiones en relación a la aceptación del riesgo y a los controles necesarios deben de estar basadas en alcanzar los objetivos de dirección, de organización y de estrategia.

Nextel S.A.

TRATAMIENTO DE RIESGOS: Esquema



TRATAMIENTO DE RIESGOS: Análisis previo

· ‘Acciones inmediatas’ pueden incluir algo tan simple como controlar el acceso físico cerrando una puerta.

· Eliminación de activos

· Controles ISO 27001

· Controles específicos

Nextel S.A.

TRATAMIENTO DE RIESGOS: Selección de controles

La importancia de investigar

ISO 27001 Cláusula 4.2.1g) establece que “ los objetivos de control y controles deberán ser seleccionados del Anexo A de este estándar”

Además establece que los objetivos de control y controles listados en el Anexo A no son exhaustivos y que se podrían elegir controles adicionales no relacionados en este anexo.

Nextel S.A.

TRATAMIENTO DE RIESGOS: Identificación de nuevos controles

La organización seleccionara objetivos de control y controles para gestionar los riesgos identificados en función del requerimiento 4 del estándar.

Eso incluirá:

- Controles de ISO 27001
- Controles legislativos y regulatorios,
- Requerimiento de clientes
- Requerimientos corporativos
- Cualquier otro elemento relevante

Nextel S.A.

TRATAMIENTO DE RIESGOS: Políticas y procedimientos

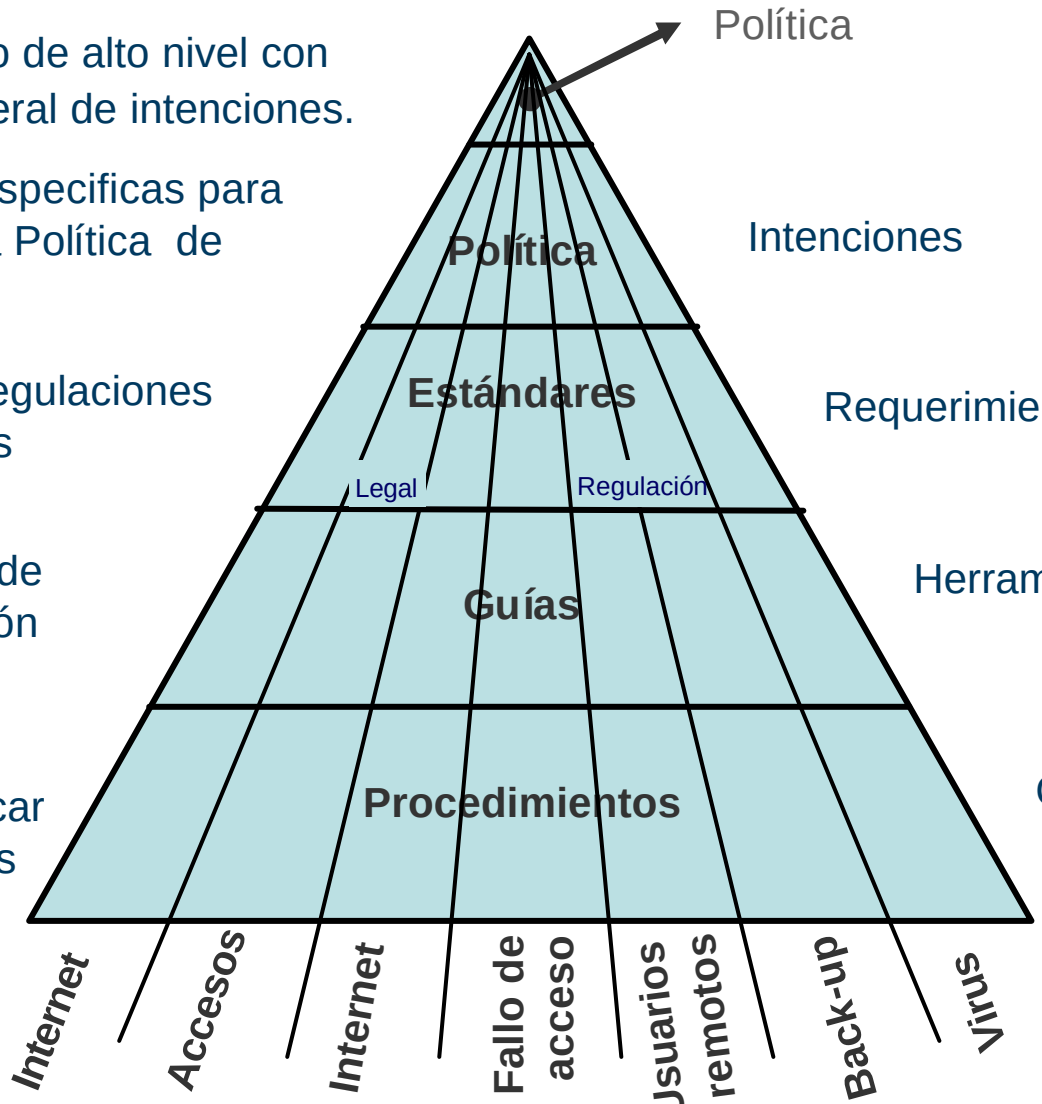
Documento de alto nivel con visión general de intenciones.

Políticas especificas para soportar la Política de alto nivel

Reglas y regulaciones obligatorias

Escenario de comprensión y trabajo

Como aplicar las políticas



Intenciones

Requerimientos

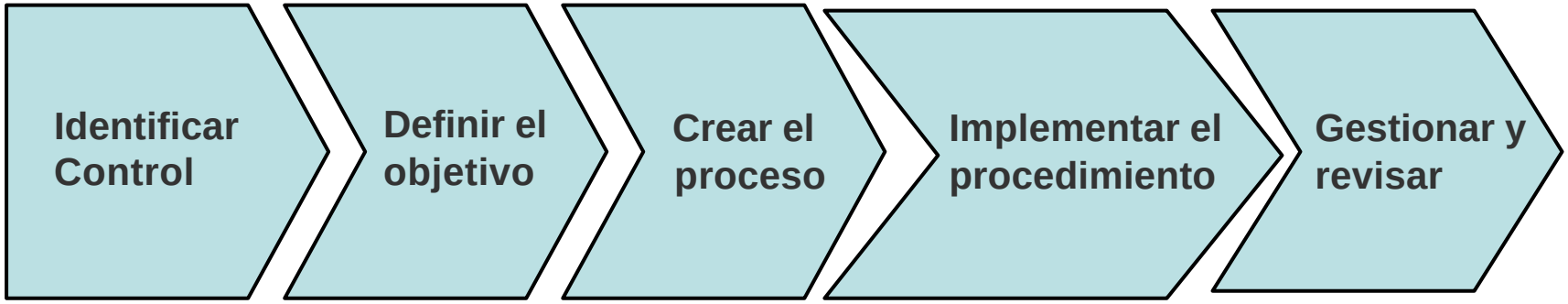
Herramientas para hacerlo

Como hacerlo

Nextel S.A.

TRATAMIENTO DE RIESGOS:
Implementación de controles

Metodología:



Nextel S.A.

TRATAMIENTO DE RIESGOS: Plan de tratamiento de riesgos (I)

La organización identificara el MÉTODO para implementar los controles para alcanzar el grado de aseguramiento requerido por la dirección de la organización.

Un programa de gestión especifico en la forma de un Plan de Tratamiento de Riesgo será desarrollado y autorizado.

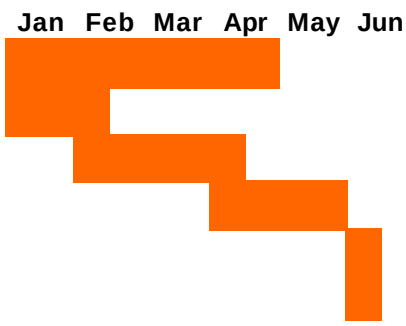
Nextel S.A.

TRATAMIENTO DE RIESGOS: Plan de tratamiento de riesgos (II)

A 10.7.3 Procedimiento de gestión de información

Seguridad física y control de documentación de clientes: En el Análisis de riesgos se ha detectado que contratos y documentación confidencial están almacenados en una zona no controlada, con el riesgo consiguiente de perdida, robo o difusión:

		Owner
Task 1	Print Security Sleevs	**Purchasing**
Task 2	Develop traininig course	HR
Task 3	Train Management/Staff	**HR**
Task 4	Distribute Security sleeves	**FM, Owners**
Task 5	Initiate process	QA
Task 6	Develop review process	Quality Man



Nextel S.A.

TRATAMIENTO DE RIESGOS: Riesgo residual

Ningún control nos puede ofrecer nunca seguridad absoluta, y por lo tanto, siempre quedara un riesgo residual.

La dirección de la organización, una vez definido el grado de aseguramiento requerido para los controles del SGSI, deberá aceptar el riesgo residual, y esto deberá ser tenido en cuenta si se produce un incidente de seguridad.

ISO 27001 Cláusula 4.2.1.h / I establece: “Obtener la aprobación de la dirección de la organización para el riesgo residual propuesto y para implementar y mantener el SGSI”.

Nextel S.A.

HERRAMIENTAS: Elementos

COMERCIALES:

· COBRA (Consultative, Objective and Bi-functional Risk Analysis)
· CRAMM (CCTA Risk Analysis and Management Method)
· RA2

GRATUITAS

· OCTAVE
· EBIOS
· PILAR

Nextel S.A.

HERRAMIENTAS: Características

La organización puede utilizar herramientas comerciales para realizar el análisis de riesgos o cualquier otro método apropiado que proporcione lo siguiente:

- establezca las vulnerabilidades, amenazas, y probabilidades de las amenazas para los activos definidos.

- que sea repetible y coherente

- proporcione a la organización una medida útil de riesgo.

Nextel S.A.

HERRAMIENTAS: Consideraciones

· Solo algunas pocas herramientas han sido desarrolladas específicamente para ISO 27001.

· Normalmente se concentran exclusivamente en activos IT.

· Esta herramientas asumen otros factores de influencia, por ejemplo el entorno y los recursos humanos.

· Pueden ser demasiado complejas para tener un uso repetible y coherente.

Nextel S.A.

BS 7799-3 (ISO 27005): Gestión de riesgos

BS 7799-3
ISMS: Part 3: Guidelines form information security risk management

ISO 27005

Nextel S.A.

EXPERIENCIA PRACTICA: Nextel S.A.

- Formación
- Implementación
- Certificación BS 7799-2
- Consultaría
- Formación
- Certificación UNE 71502
- Auditoría a terceros
- Migración a ISO 27001

Nextel S.A.

GRACIAS

alerma@nextel.es

Nextel S.A.