El día a día en la Gestión de la Seguridad

Pau Julià Garcia

Responsable de Seguridad de la Información y Arquitectura IT

Servihabitat

CISA, CISM, OPST

Servihabitat

Información

- **Es el activo más importante**
- **No importa el sector.**

La Seguridad de la Información protege a ésta de una amplia gama de amenazas, tanto de orden fortuito como destrucción, incendio o inundaciones, como de orden deliberado, tal como fraude, espionaje, sabotaje, vandalismo, etc.

Estamos Seguros?

- NO
- Nunca al 100%

¿De dónde vienen las amenazas?

Ataques Externos

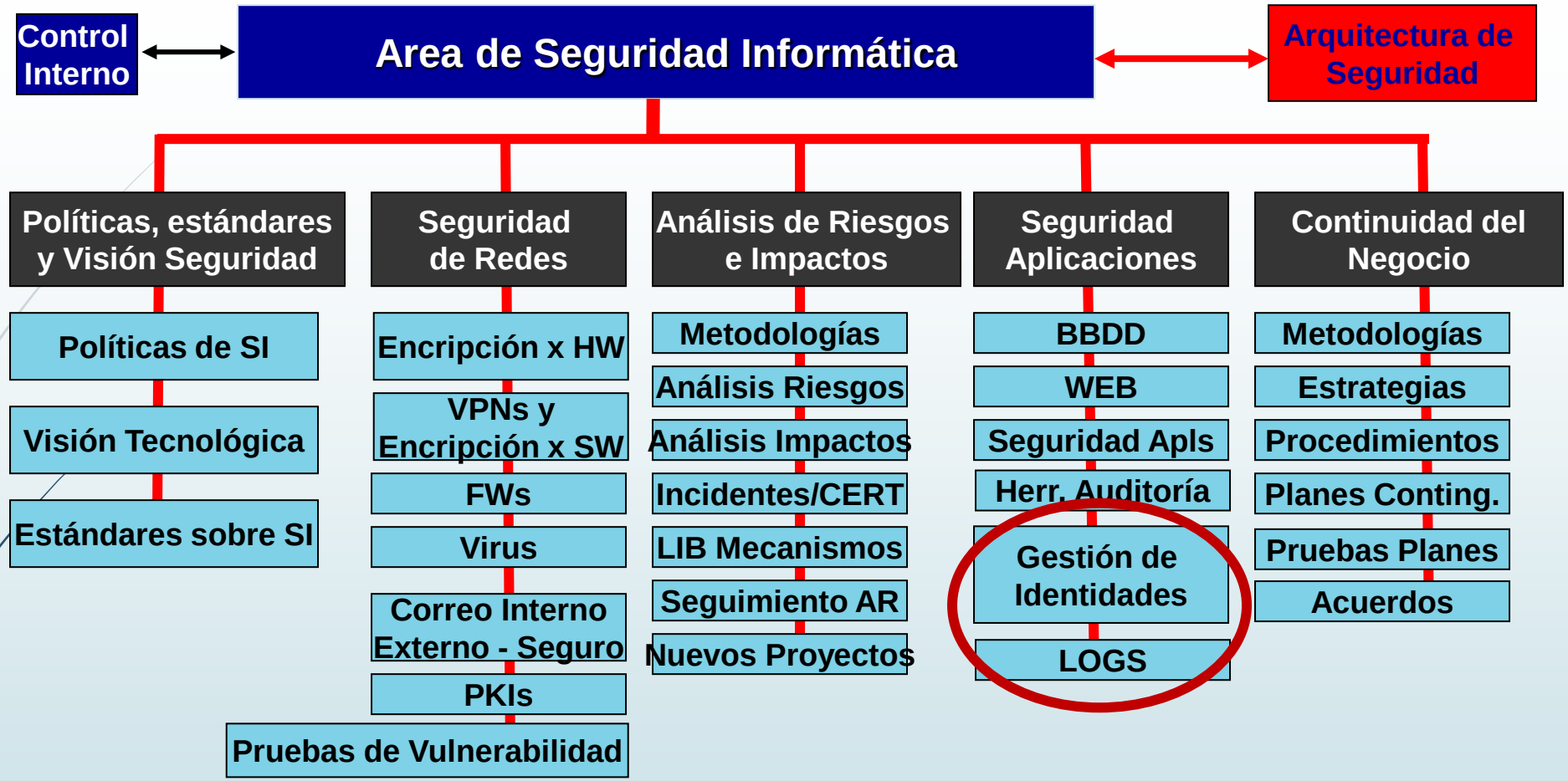
Ataques Internos

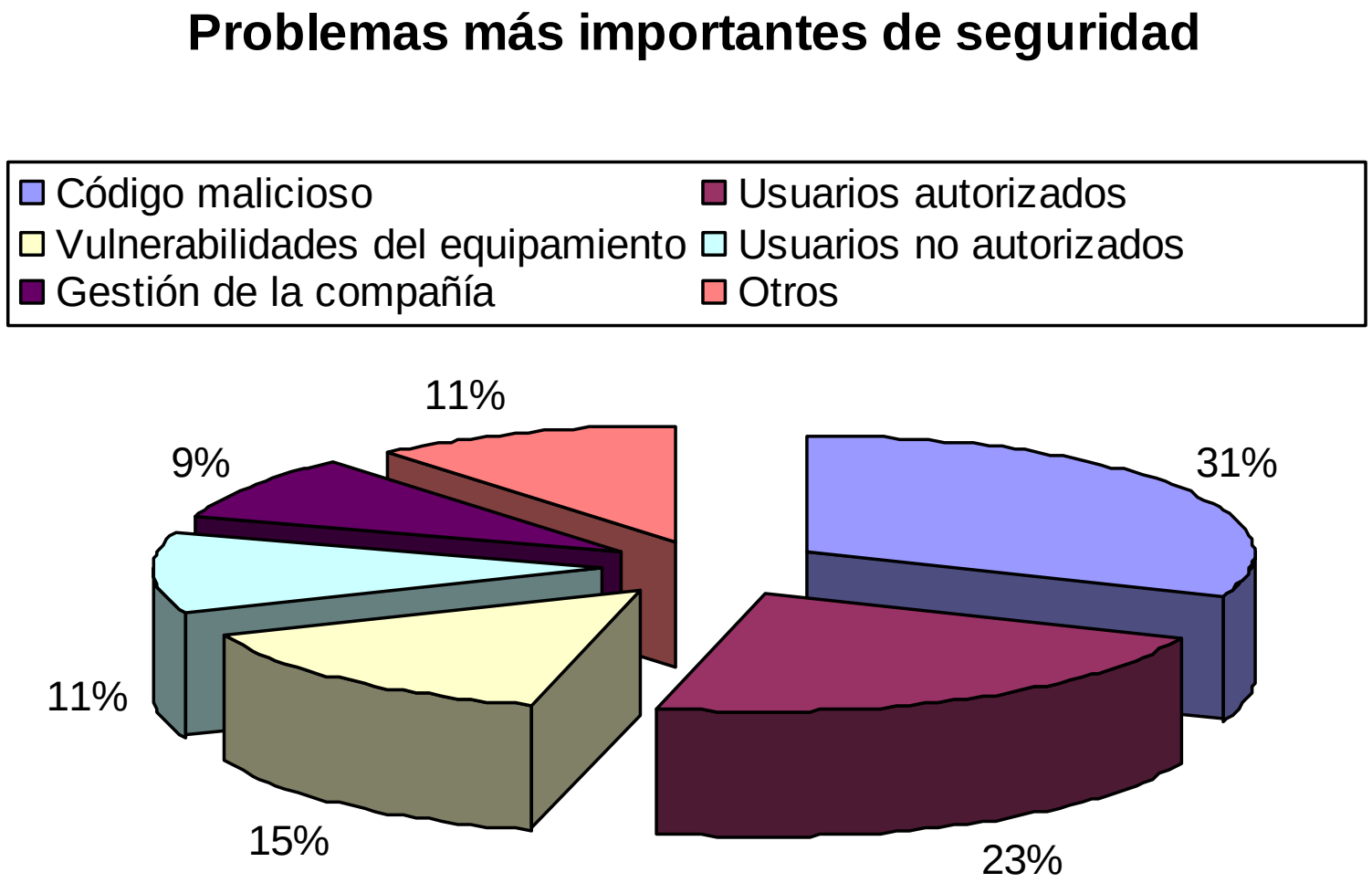
Interrupción de suministros

Errores

Accidentes

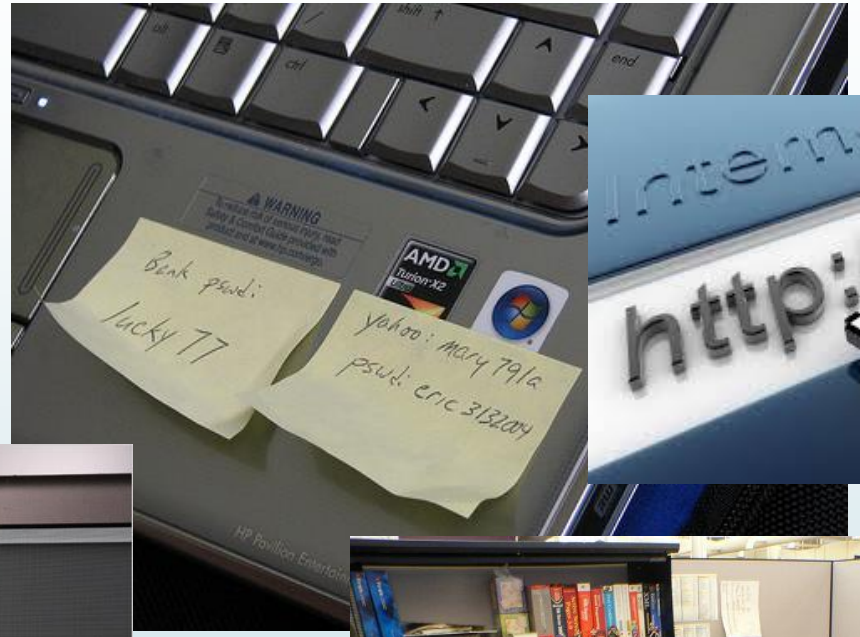
Las medidas reactivas no son suficientes, es necesario ser proactivo

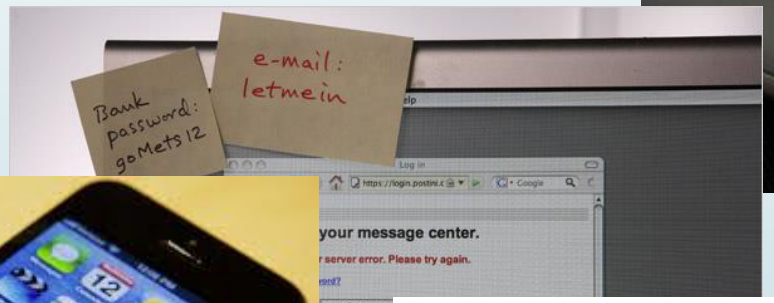

Control Interno
Area de Seguridad Informática
Arquitectura de Seguridad
Políticas, estándares y Visión Seguridad
Seguridad de Redes
Análisis de Riesgos e Impactos
Seguridad Aplicaciones
Continuidad del Negocio
Políticas de SI
Visión Tecnológica
Estándares sobre SI
Encripción x HW
VPNs y Encripción x SW
FWs
Virus
Correo Interno Externo - Seguro
PKIs
Pruebas de Vulnerabilidad
Metodologías
Análisis Riesgos
Análisis Impactos
Incidentes/CERT
LIB Mecanismos
Seguimiento AR
Nuevos Proyectos
BBDD
WEB
Seguridad Apls
Herr. Auditoría
Gestión de Identidades
LOGS
Metodologías
Estrategias
Procedimientos
Planes Conting.
Pruebas Planes
Acuerdos

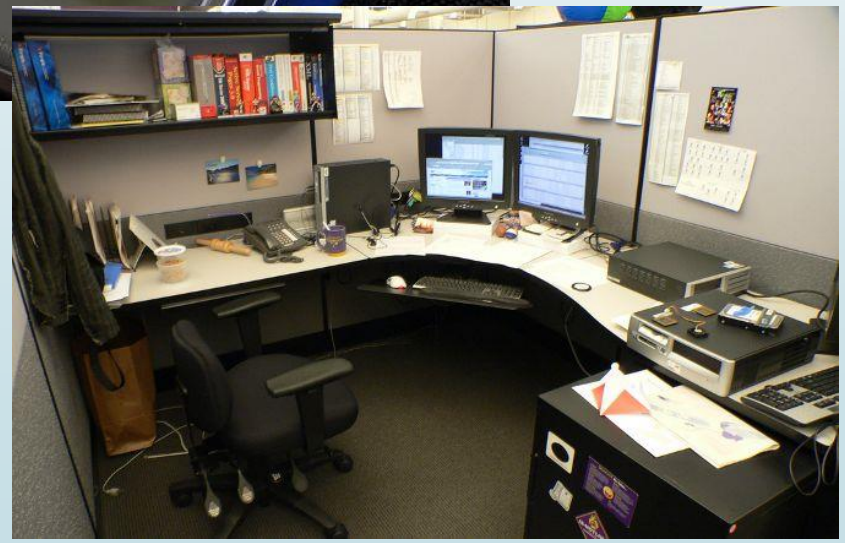

Problemas más importantes de seguridad
Código malicioso
Usuarios autorizados
Vulnerabilidades del equipamiento
Usuarios no autorizados
Gestión de la compañía
Otros
11%
9%
31%
11%
15%
23%

Principal amenaza

- Usuario







Pero.. ¿qué está ocurriendo?

- **Aunque tecnológicamente se consiguiera un sistema seguro, el problema sigue existiendo**

- Las técnicas criptográficas son computacionalmente seguras, pero los usuarios ...
  - No usan contraseñas de calidad
  - Se pasan usuarios entre ellos
  - No quieren u olvidan cifrar ficheros y correos
  - Los descifran y olvidan borrar el fichero en claro
  - Los imprimen y los dejan en ...

    la impresora, la mesa, la papelera, el metro
- Necesita del cuidado y supervisión continuo.
- **La seguridad basada en medidas tecnológicas es insuficiente, debe gestionarse**.

Gestión del Riesgo

La Gestión de Riesgos no es simple

... lleva tiempo
... cuesta dinero
... no vale una vez y para siempre

- Muchos activos
  - los sistemas son complejos
- Activos de muchos tipos
  - información, servicios, procesos de negocio
  - equipamiento: aplicaciones, equipos, comunicaciones, ...
  - locales: recintos, edificios, áreas, ..., en el campo
  - personas: usuarios, operadores, desarrolladores, ...
- Muchas amenazas
  - y muchas formas de hilvanar las amenazas
- Muchísimas salvaguardas
  - gestión, técnicas, seguridad física, recursos humanos

Metodología de Análisis y Gestión de Riesgos

La complejidad se ataca metódicamente

- una metodología es una aproximación sistemática
  - para cubrir la mayor parte de lo que puede ocurrir
  - para olvidar lo menos posible
  - para explicar a los gerentes qué se necesita de ellos
  - para explicar a los técnicos qué se espera de ellos
  - para explicar a los usuarios:
    - qué es un uso adecuado del sistema
    - qué es una respuesta urgente
    - cómo se gestionan los incidentes
- una metodología necesita modelos
  - elementos: activos, amenazas, salvaguardas
  - métricas: impacto y riesgo

Gestión de Riesgos.

➨¿Qué riesgos gestionar?

➨Para la gestión consideraremos las siguientes fuentes de necesidades de seguridad

- Legislación, estatutos, contratos
- Necesidades del negocio
- Análisis de riesgos

La seguridad se consigue combinando medidas tecnológicas y de gestión

Gestión de la Seguridad

Factores de éxito

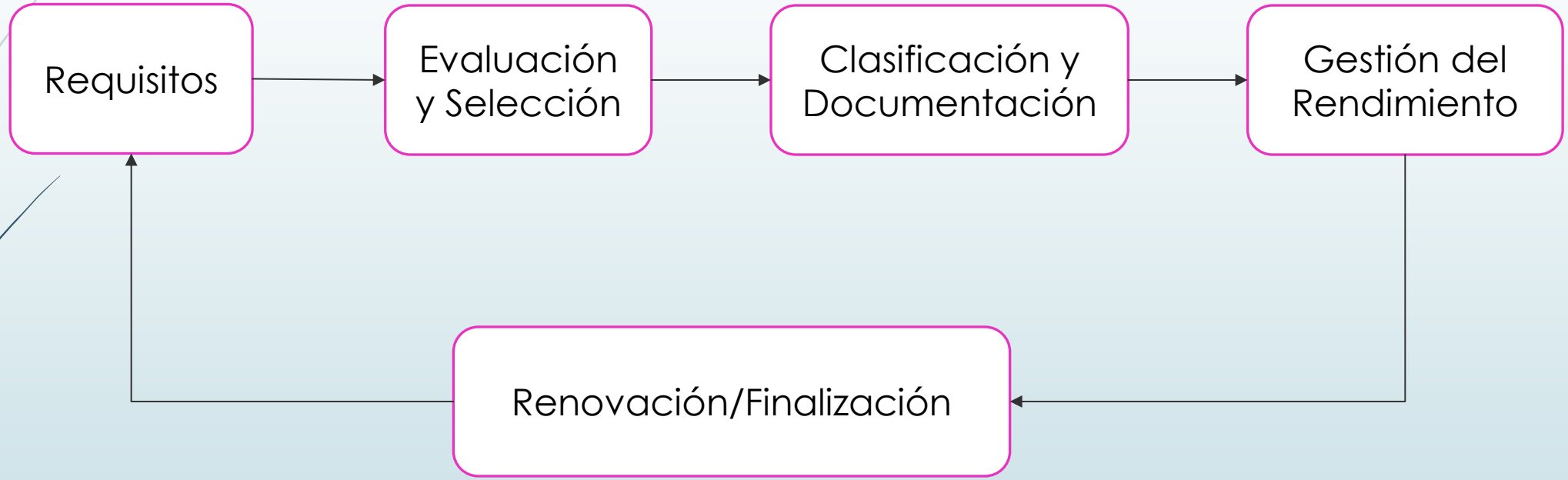
- Orientación al negocio
- Liderazgo de la dirección
- Participación del personal
- Seguridad basada en riesgo
- Enfoque basado en procesos, no en productos
- Enfoque de sistema de gestión
- Medición y mejora continua
- Toma de decisión basada en hechos
- Gestión planificada de incidentes

INDICADORES

Ideas Clave

- Campañas preventivas en toda la organización.
- Si ud. no prueba su SI, otros lo harán y posiblemente comprometerán sus activos y su imagen corporativa.
- Pruebas de Vulnerabilidad: Buena herramienta para validar el modelo de Seguridad
- Vital mantener Plan de Continuidad del Negocio robusto en la Organización.
- No existe la seguridad 100% pero si se pueden minimizar, evitar, transferir y/o aceptar riesgos.
- Es necesario seguir una metodología para estudio de la seguridad,
- Ataque la seguridad por frentes, sin perder su globalidad usando estándares
- Fundamental en toda Organización entender los conceptos e importancia de la Seguridad.

Selección Proveedores



Contratación

- Analizar las estrategias generales de la organización y los servicios que se prestan para definir las necesidades de contratación.
- Han de tenerse en cuenta,
  - los informes económicos proporcionados por la Gestión Financiera,
  - los niveles de calidad acordados con los clientes desde la Gestión de Niveles de Servicio,
  - y la previsión de la capacidad necesaria para desplegar el servicio que haya definido la Gestión de la Demanda.
- Estudiar a fondo las condiciones del servicio a prestar y el papel que desempeñarán los proveedores en el proceso.
- Una vez recogidos y analizados estos inputs, la Gestión de Proveedores debe preparar:
  - Requisitos que se van a exigir a los proveedores.
  - Caso de Negocio inicial sobre el que trabajar durante las negociaciones con los proveedores.

Evaluación y Selección de proveedores

- **A la hora de elegir un nuevo suministrador han de tenerse en cuenta:**
  - Su adecuación a los requisitos previamente definidos.
  - Referencias de otros competidores.
  - Disponibilidad y capacidad.
  - Aspectos financieros.
- **Negociar los términos del servicio**. El resultado debe quedar reflejado en el Contrato de Provisión del Servicio, un documento legal que atestigua la relación entre la organización TI y el suministrador.
- Es importante que queden reflejadas las metas y responsabilidades del proveedor de cara al cumplimiento de los SLAs.

Clasificación y Documentación de proveedores

- Una vez que se han acordado y negociado los servicios de un determinado proveedor, es preciso crear una Base de Datos de Proveedores y Contratos donde se recogerá toda la información relacionada:
  - Contratos de provisión del servicio.
  - El nivel de actuación del proveedor:
    - Estratégico (directivos),
    - táctico (mandos intermedios),
    - operativo (nivel ejecutor).
  - Relaciones con otros elementos del ciclo de vida.

Gestión del Rendimiento de los proveedores

- A grandes rasgos, se trata de verificar si efectivamente se están cumpliendo los niveles de calidad y disponibilidad acordados en los contratos:
  - ¿El suministrador se integra adecuadamente a los procesos de la organización TI?
  - ¿Cuál es el procedimiento para informar al proveedor en caso de recibir una incidencia?
  - Si un elemento de configuración relacionado con el proveedor cambia, ¿cuál es el procedimiento a seguir?

INDICADORES

Renovación o terminación de contratos

- Esta actividad consiste en llevar a cabo renovaciones de contratos, asesorar a la dirección acerca de si éstos son relevantes y terminar la relación contractual en caso de que ya no se necesiten más los servicios del proveedor.
- **Los aspectos a considerar para tomar la decisión de renovar a un proveedor incluyen**:
  - El buen funcionamiento del contrato y su relevancia de cara al futuro.
  - Cambios que es preciso acometer: servicios, productos, contratos, acuerdos, objetivos.
  - Perspectivas futuras de la relación con el proveedor: crecimiento, estancamiento, cambio, terminación, transferencia, etc.
  - Rendimiento comercial del contrato (criterios de cobro, estructura de precios, etc.)
  - Buenas prácticas para la gestión de contratos.

Atención!

- Subcontratación…
- El conocimiento no se subcontrata.
- Falta de recursos o infrautilización de los mismos
- Problemas de comunicación y sincronización entre todos los agentes implicados
- Falta de preparación o pobre comunicación sobre los objetivos buscados
- Finalización de contrato o cambio de proveedor.

Conclusiones finales

- **Cada persona es responsable de la información a la que tiene acceso y/o maneja como consecuencia de su actividad.**

- **La eficacia de la seguridad es un esfuerzo de equipo que implica la participación y apoyo de TODOS los empleados y colaboradores.**

Muchas Gracias