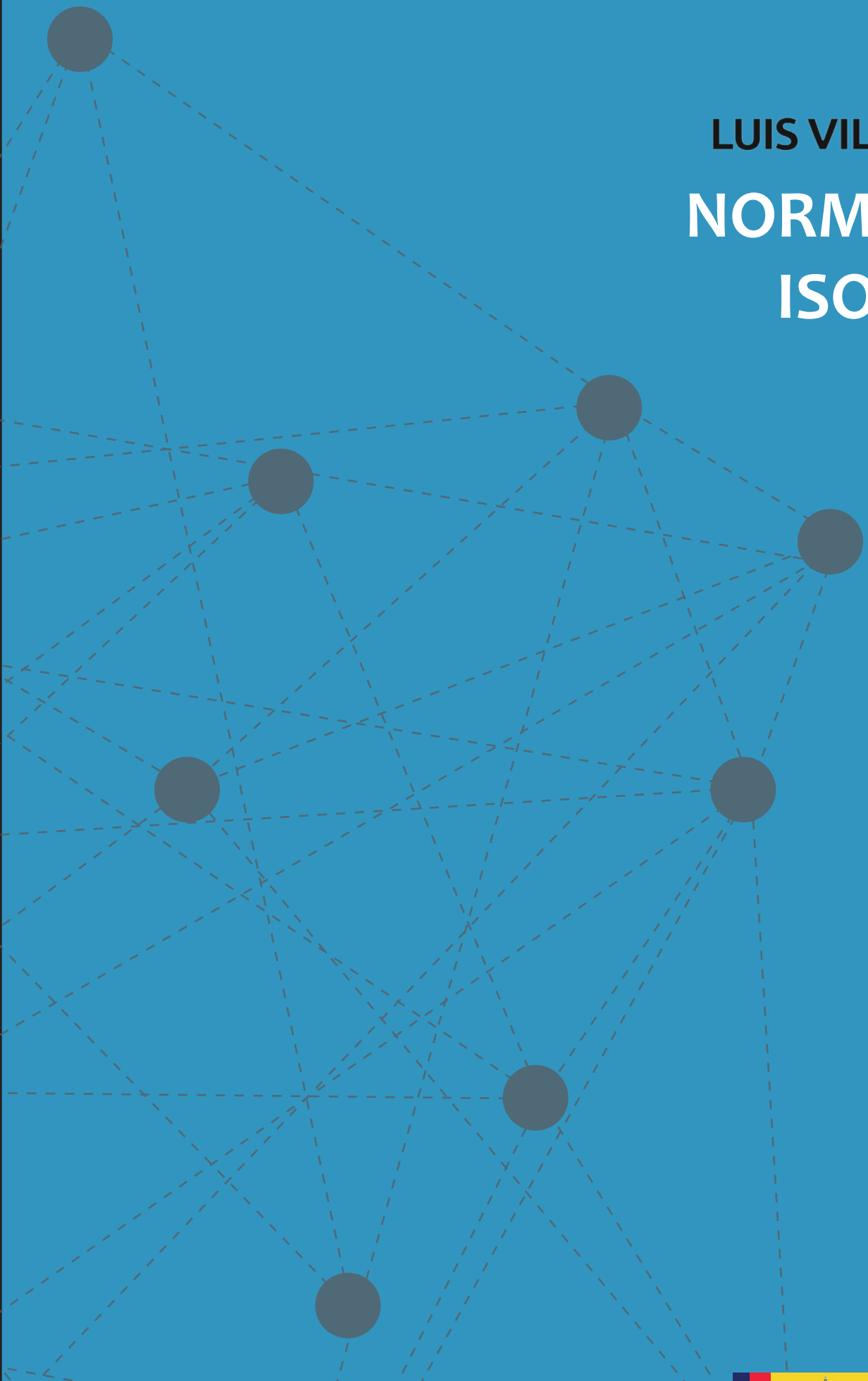
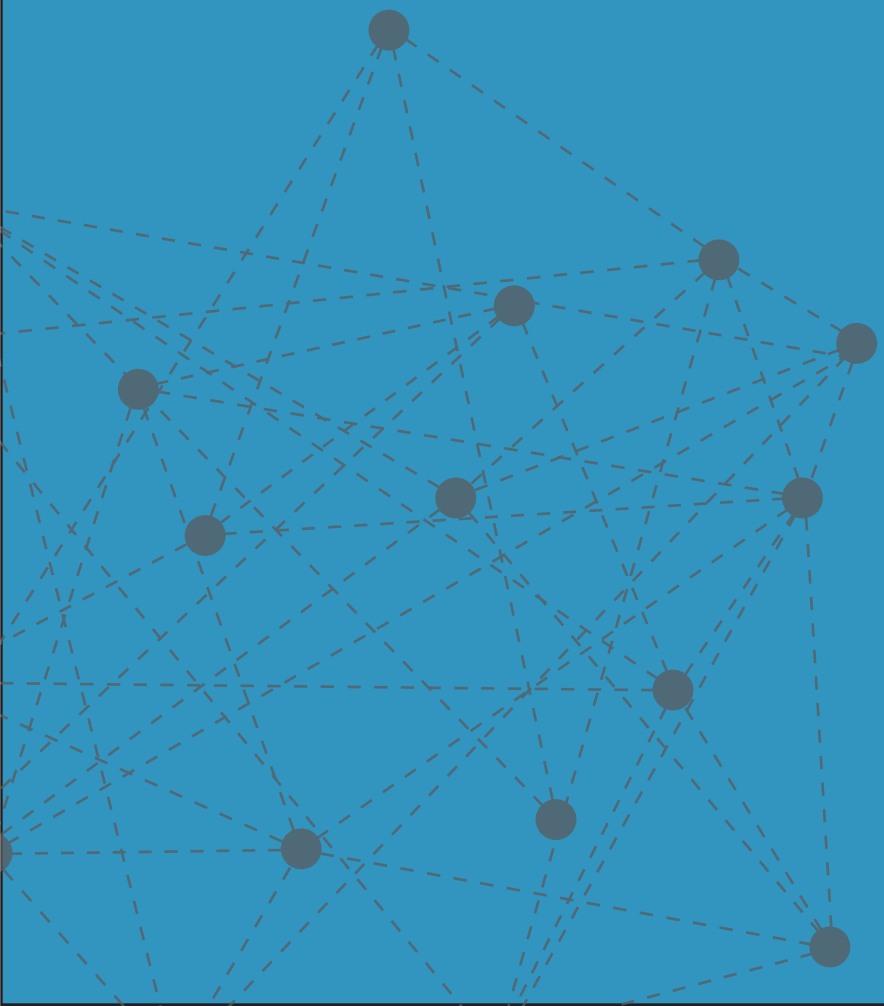
LUIS VILANOVA

NORMATIVA ISO 27001



1

LA SEGURIDAD INFORMÁTICA COMO INVERSIÓN



INTRODUCCIÓN

A menudo, cuando me he reunido con los departamentos presupuestarios y de finanzas de algunas empresas para explicarles el plan de Seguridad, su viabilidad y su coste, me he encontrado con la paradoja de que el único argumento al que verdaderamente se prestaba atención era al retorno de la inversión, o dicho de otro modo la pregunta era:

¿El riesgo merece la inversión?

Y es que la cultura de la reactividad frente a la preventiva está tan extendida, que si no se ha tenido recientemente un incidente de seguridad informática en una empresa, la lectura que se suele hacer es que *"si no se está teniendo accidentes es que todo se está haciendo bien, para qué entonces hacer más inversiones"*.

Se percibe entonces que la intención de inversión en Seguridad en la Información es **inversamente proporcional** a los resultados que se está obteniendo.

EL ROSI, RETORNO DE INVERSIÓN EN SEGURIDAD DE LA INFORMACIÓN

Tradicionalmente, para cualquier gestor una inversión debe tener unos ingresos superiores a la misma, de lo contrario no es viable.

¿Cómo cuantificar o medir entonces la rentabilidad de la seguridad?

El problema es que si bien podemos calcular el coste total de la inversión en Seguridad de la Información, los ingresos los deberíamos medir como el **ahorro de costes ante un incidente** en nuestros sistemas. Pero la opinión general en las empresas y de algunos profesionales de nuestro país es que es difícil de calcular y cuantificar.

Sin embargo, hay una manera de estimar los beneficios financieros (es decir, ahorro de costes) de seguridad de la información y de cuantificar la inseguridad.

En primer lugar, es necesario estimar **el coste del daño potencial** que se produciría ante un incidente, teniendo en cuenta los siguientes factores:

El alcance del incidente potencial, qué departamentos se verían afectados, unidades y procesos del negocio.

- El coste externo de la reposición de equipos, bienes y materiales que fueron dañados por el siniestro.
- El coste interno de los empleados dedicados a resolver el incidente.
- Sanciones legales y/o contractuales si no se cumple con la legislación vigente o con nuestros clientes.
- La pérdida de ingresos, tanto de los clientes actuales, como de los potenciales en el momento del siniestro.

El siguiente paso consiste en **estimar la probabilidad del suceso**. Para ello hay que tener en cuenta las amenazas y vulnerabilidades de nuestro actual sistema, así como las medidas de seguridad existentes en el momento de la evaluación. La mejor manera es evaluar la frecuencia temporal con la que un incidente de este tipo podría tener lugar.

Cuando se multiplica la esperanza de pérdida y la probabilidad del suceso, obtenemos la Esperanza Perdida Anualizada (**ALE**).

Por último, es necesario estimar cuánto va a costar las medidas de seguridad a implantar teniendo en cuenta los siguientes factores:

- Valor de adquisición. Coste del hardware, del software, servicios de implementación, etc…
- Valor residual de las medidas de seguridad.
- Los costes externos de mantenimiento.
- Los costes internos de mantenimiento, principalmente empleados destinados al efecto.

Cuando tengamos todos estos gastos en conjunto, sabremos si el **Retorno de Inversión en Seguridad** es positivo o no (la disminución en el riesgo tiene que ser mayor que el coste total de las medidas de seguridad) es decir, que el cálculo de las posibles pérdidas anualizadas tiene que ser mayor que el coste anual de las medidas de seguridad adoptadas.

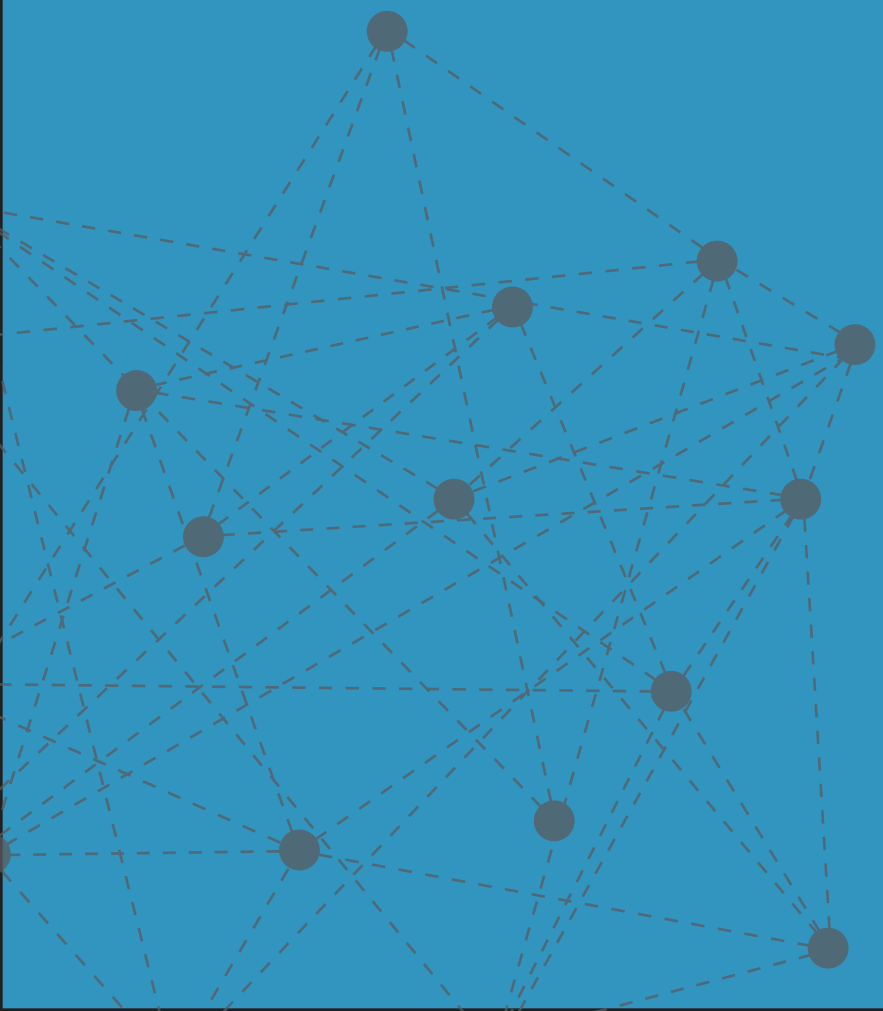
Por ejemplo, si el coste estimado para nuestra empresa de un ataque de un software malicioso es de 30.000 euros y la probabilidad de que esto suceda es una vez cada 5 años, el **ALE** resultante es de 6.000. Por lo tanto, cualquier inversión que impida el ataque de ese tipo de software por debajo de esa cifra en concepto de Seguridad en la Información sería rentable.

CONCLUSIÓN

Aunque es difícil y laborioso confeccionar un informe económico al objeto de valorar el impacto real que tendría en nuestro negocio un desastre en la información, la realidad es que la mejora continua que nos garantiza la implantación de una norma como la **ISO27001**, y la elaboración frecuente de procesos para el cálculo del **ROSI**, permitirá que nuestro sistema de Seguridad se mantenga vivo en el tiempo y pueda así responder con las garantías oportunas y suficientes ante las nuevas amenazas en materia de seguridad que puedan ir surgiendo.

2

SEGURIDAD INFORMÁTICA. ISO 27001



SEGURIDAD INFORMÁTICA. ISO 27001

La seguridad informática sigue siendo una de las asignaturas pendientes de muchas empresas. Cada día la seguridad informática es violada por hackers y usuarios que acceden a información privilegiada, así como realizan operaciones no permitidas. El valor de su información y la seguridad de que es utilizada por quién usted considera y permite, es fundamental, en muchos casos, para la competitividad de su negocio.

En materia de seguridad informática, actualmente exite un referente a nivel mundial denomninado Auditoria de seguridad informática ISO 27001. En España, gracias a iniciativas como los planes AVANZA, se ha introducido como un estándar mas a cumplir por las empresas. La normativa ISO 27000 establece 4 clausulas y 133 puntos de control que preparan a una empresa u organización para poder certificarse en ISO 27001.

Aunque uno de los objetivos es que las empresas se auditen y se certifiquen, digamos consiguiendo una 'medalla' que reconoce mundialmente sus buenas prácticas, no solo ganan en cuestiones de seguridad sino también en imagen al exterior

Las empresas que deben de seguir el camino de asegurar su SGSI (sistema de gestión de la seguridad de la información) son organizaciones que valoran y dan peso especifico a las TI dentro de su estrategia, independientemente de su tamaño, abarcando sl's de 8-9 trabajadores hasta multinacionales, pasando por organizaciones públicas.

La ISO 27001 va dirigido a organizaciones que:

1. Ven las ventajas de aplicar las buenas prácticas de un estándar de seguridad de la información.
2. Pertenecen a un grupo y se marca como directriz certificarse en seguridad TI.
3. Las TI son base para su estrategia. Por ejemplo, empresas que dan mucho valor a su TI o que incluso reducen personal en Pro de crear servicios a través de Internet.

Las ventajas de una empresa en el cumplimiento de esta norma son muchas, entre ellas:

· Demostrar la conformidad y la eficacia de las elecciones organizativas y de las actividades operativas puestas en práctica para garantizar la:

- Confidencialidad
- Integridad
- Disponibilidad de la información incluida en el perímetro cubierto por el SGSI (Sistema de gestión de la seguridad de la información).

· Asegurar la continuidad del business:

- Minimización de los daños en caso de incidentes (siendo estos, de hecho, inevitables).
- Maximización de las inversiones efectuadas para la implementación y la gestión de la seguridad.
- Mejora continua de la eficacia organizativa y operativa.
- Construir o supervisar la seguridad perimetral.
- Concienciar al personal mediante documentos de seguridad.

En la consultoría de implantación de ISO 27001, mi objetivo, es ofrecer a las empresas el camino para implantar la norma, adecuándose al alcance que la empresa quiera certificar.

Preguntémonos las siguientes cuestiones:

- ¿Sabemos que nuestra organización está procediendo bien para asegurar nuestros sistemas ante intrusos, robos de información, ataques…?
- ¿Estamos aplicando buenas prácticas para proteger nuestras implantaciones LOPD?
- ¿Están nuestros empleados utilizando los SI de forma segura y dentro de la funcionalidad para que hayan sido entregados?
- ¿Los datos privados del negocio a los cuales nadie más que el CEO deberían tener acceso están suficientemente protegidos?
- ¿Estamos cumpliendo el marco legal a nivel de licencias, leyes de propiedad intelectual,…?

La ISO 27001 mide el riesgo de estas y otras muchas cuestiones, para poder aplicar medidas y procedimientos que aseguren un sistema SGSI óptimo y que de respuesta al alineamiento de las Ti con la estrategia empresarial.

Si tiene cualquier necesidad respecto de implantación, medición o auditoria en materia de seguridad informática, **no dude en contactar conmigo.**

Luis Vilanova
Interim Manager Experto en Tecnologías de la Información
luis@luisvilanova.es
606954593