# Plan Implantación ISO/ IEC 27001:2005

# ¿Estamos seguros?

- ¿Estamos seguros?
- ¿Esta segura la información de LAMUTA?
- Si alguien ha podido responder a esto o bien se equivoca o …

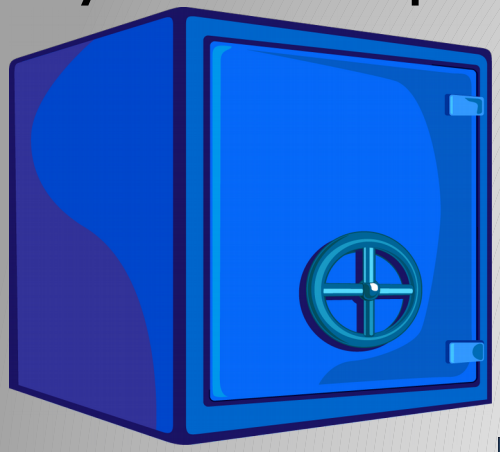
# ¿Estamos seguros?

- ¿Qué debemos asegurar?
- ¿Qué es crítico para LAMUTUA?
- ¿Cuánto "vale" eso que queremos asegurar?
- ¿Cuánto "cuesta" asegurarlo?
- ¿En que medida quedará protegido?
- ¿Quién debe asegurarlo y como?
- ¿Quién es el responsable?

# ¿Estamos seguros?

- ¿Qué amenazas tenemos?
- ¿Cómo nos pueden afectar esas amenazas?
- ¿Quién o qué nos puede proteger de esas amenazas?
- ¿Debo protegerme de todas las amenazas?
- … yo que pensaba que con el antivirus que me instalo mi cuñado era suficiente…

- …y ahora que hacemos….?



# ¿Estamos seguros?

- Elegir un camino
  - Una norma estándar
  - Medible
  - Certificable
  - Resultados fiables

# A trabajar!

# El camino.

- ISO/IEC 27001:2005
  - Magerit
- Esquema Nacional de Seguridad

***Tenemos que entender la seguridad como una actividad integral, en la que no caben actuaciones puntuales o tratamientos coyunturales, debido a que la debilidad de un sistema la determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas.***

# El eslabon mas debil

# ISO 27001 - Implantación

- Inventario de activos
  - ¿Cómo vamos a proteger algo si no sabemos que es lo que tenemos que proteger?
- Alcance
  - Los sistemas de información que dan soporte a la administración y acceso de los datos de las BBDD consideradas críticas en la organización.

- Política Seguridad
  - Implicación Dirección General.
  - Formación al personal.
  - Disciplina, sanciones.
  - Presupuesto.
  - Agenda de dirección

# ISO 27001 - Implantación

- Gestión de roles y responsabilidades de seguridad
  - Nombramientos
  - Apoyo
  - Responsabilidades
  - … las cosas no se hacen solas…

# ISO 27001 - Implantación

# ISO 27001 - Implantación

- Análisis de Riesgos
  - Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos.
  - La metodología empleada para el análisis de riesgos será Magerit en su versión 3. MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica.

- Valoración de activos
  - Valor propio
    - coste de **reposición**: adquisición e instalación
    - coste de **mano de obra** (especializada) invertida en recuperar (el valor) del activo
    - **lucro cesante**: pérdida de ingresos
    - **capacidad de operar**: confianza de los usuarios y proveedores que se traduce en una pérdida de actividad o en peores condiciones económicas
    - **sanciones por incumplimiento** de la ley u obligaciones contractuales
    - **daño a otros activos**, propios o ajenos
    - **daño a personas**
    - **daños medioambientales**
  - Valor acumulado

# ISO 27001 - Implantación

- **Dimensiones**
- De un activo puede interesar calibrar diferentes dimensiones:
  - **Confidencialidad**: ¿qué daño causaría que lo conociera quien no debe? Esta valoración es típica de datos.
  - **Integridad**: ¿qué perjuicio causaría que estuviera dañado o corrupto? Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcialmente falsos o, incluso, faltar datos.
  - **Disponibilidad**: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo? Esta valoración es típica de los servicios
  - **Autenticidad**: ¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
  - **Trazabilidad** del uso del servicio: ¿qué daño causaría no saber a quién se le presta tal servicio? O sea, ¿quién hace qué y cuándo?

# ISO 27001 - Implantación

- Amenazas
  - De origen natural.
  - Del entorno (de origen industrial)
  - Defectos de las aplicaciones
  - Causadas por las personas de forma accidental
  - Causadas por las personas de forma deliberada

# ISO 27001 - Implantación

# ISO 27001 - Implantación

- Salvaguardas
  - Reduciendo la probabilidad de las amenazas.
  - Limitando el daño causado.

- **Reales:** con los datos de *Reducción de probabilidad* y *Limitando el daño causado* reales actuales obtenidos del estudio actual de LAMUTUA.

- **Potenciales:** con los datos de *Reducción de probabilidad* y *Limitando el daño causado* potenciales obtenidos del estudio de las salvaguardas en otras instalaciones TIC y datos del mercado.

# ISO 27001 - Implantación

- **Gestión de Riesgos**
  - A raíz de los resultados obtenidos en el análisis de riesgos LAMUTA se plantea la necesidad de hacer un plan de mitigación de riesgos.
  - Este plan de mitigación de riegos que se basa en los resultados obtenidos en el análisis debe basarse en cifras reales y que estén aseguradas en el tiempo, en concreto nos tenemos que asegurar que las salvaguardas que LAMUTUA tiene desplegadas cumplan su función y a ser posible mejoren en eficiencia.
  - Pese a las salvaguardas desplegadas, el resultado de análisis de riesgos nos muestra que hay valores de análisis de riesgos que deben ser mitigados de inmediato con la aplicación de nuevas salvaguardas de imprescindible aplicación y cuya efectividad potencial ya se ha calculado y aprobado.
  - Ambos proyectos deben cumplir el ciclo de Deming para poder integrarlos dentro del SGSI.
  - Con la finalidad de cumplir estos requerimientos LAMUTUA ha desarrollado dos proyectos:

- 1.- Normalización, optimización y aseguramiento de salvaguardas actuales.
- 2.- Implantación de salvaguardas imprescindibles.

# Gestión de Riesgos

La ejecución de ambos planes de mejora tendrá una duración estimada de 1 año, su coste económico está valorado en un total de 55000€ y el impacto en la seguridad supone una disminución del riesgo de hasta un 400% para algunos activos y entorno al 50% para el resto.

| | | | | | |
|---|---|---|---|---|---|
| O.S. + S.G. - Servidores A.D./DNS | 1,8 | 31,5 | | 1,2 | 6 |
| O.S. + S.G. – Servidor Backup | 5,3 | 94,5 | | 3,7 | 18 |
| O.S. + S.G. – Clúster B.B.D.D. | 4,5 | 72 | | 3,2 | 13,7 |
| O.S. + S.G. – Clúster Aplicaciones | 1,3 | 27 | | 0,9 | 5,1 |
| O.S. + S.G. – Firewall Switches | 8,3 | 148,5 | | 5,8 | 28,2 |

| | | | | | |
|---|---|---|---|---|---|
| Switch Central | 0,6 | 229,5 | | 0,6 | 43,6 |
| Firewall | 0,6 | 162 | | 0,6 | 30,8 |
| Router | | 7,5 | | 0 | 1,4 |
| Switches LAN / Macrolan | | 25,5 | | 0 | 4,8 |

FIN!