¿Realmente somos el eslabón más débil?

Rompiendo tópicos.

Antes de enero de 2014

- ☺ RD 3/2010 ENS: 24/48 meses para su implantación
- ☺ La Universidad de Sevilla contrata a una consultora en 2013
  - ☺ Valoración de servicios
  - ☺ Informe de estado del ENS
  - ☺ Análisis de riesgos
  - ☺ Plan de adecuación
- ☹ El proyecto lo lidera el Servicio de Informática y Comunicaciones (Área de Comunicaciones)

Año 2014

☺ Se aprueba el Plan de Adecuación al ENS

☺ Se aprueba la Política de Seguridad de la Información

☺ La Política incluye los roles y responsabilidades

☺ Se nombra la Comisión de Seguridad de la Información

☺ Se empieza a trabajar en las normativas de desarrollo de la Política de Seguridad

☹ El Responsable de Seguridad de la Información es el Director del Servicio de Informática y Comunicaciones

Octubre de 2015

- ☹ Más de un año y medio sin avances
- ☺ Se nombra a un Responsable Delegado de Seguridad de la Información con dedicación exclusiva al Plan de Adecuación
- ☺ Con el apoyo de la empresa consultora se actualizan:
  - ☺ Valoración de servicios
  - ☺ Informe de estado del ENS
  - ☺ Análisis de riesgos
  - ☺ Plan de adecuación
  - ☺ Se realiza una auditoría interna

Diciembre de 2016

- ☺ Se reúne por primera vez la Comisión de Seguridad
- ☺ Se aprueba la actualización de la Política de Seguridad
- ☺ Se aprueban las normativas de desarrollo y el Plan de Formación
- ☺ Se elaboran procedimientos de seguridad y guías de buenas prácticas
- ☺ Se empiezan a implantar medidas de seguridad:
  - ☺ Protección perimetral
  - ☺ Herramientas del CCN-Cert: sonda SAT y gestión de incidentes LUCIA
  - ☺ Campañas de formación y concienciación

A partir de enero de 2017

- ☺ Empezamos a dar formación y a hacer campañas de concienciación de forma masiva
- ☺ Empezamos a tener herramientas de seguridad
- ☺ Empezamos a tener visibilidad
- ☺ Empezamos a gestionar incidentes
- ☺ Empezamos a implantar las medidas técnicas del ENS en Servicios Corporativos
- ☺ Los roles responsables se empiezan a implicar
- ☺ Entra en vigor el RGPD y se nombra a un DPD

Empezamos a ver resultados...

☺ POSITIVOS	☹ NEGATIVOS
Se empieza a ver la seguridad como un proceso integral	No se dotan los recursos necesarios para implantarlo
Se establece un Sistema de Gestión de la Seguridad (SGSI)	Alcance limitado (SIC)
Se refuerzan las líneas de defensa	Inicialmente las políticas son muy laxas
Se registran eventos de forma masiva	No disponemos de recursos suficientes para revisarlos
Gestionamos incidentes	Crecen exponencialmente
En definitiva, se van implantando las medidas del Anexo II del ENS	A un ritmo muy lento por falta de manos

Campaña de concienciación

El Factor Humano

Las personas somos el eslabón más débil de la ciberseguridad.

No importa qué medidas apliquemos a las tecnologías si un fallo humano abre una puerta trasera al ciberdelincuente.

La concienciación y el sentido común, nuestras mejores armas.

Hay otros muchos problemas importantes

- ☹ Hay que limitar el uso de direccionamiento público
- ☹ Hay que maquetar equipos
- ☹ Hay que disponer de XDR en los puestos de trabajo
- ☹ Hay que ofrecer herramientas corporativas que cubran las necesidades de los usuarios
- ☹ Hay que controlar la infraestructura tecnológica que se compra
- ☹ Hay que formar a los técnicos informáticos para que las herramientas que desarrollan y/o administran sean seguras
- ☹ Hay que formar a los técnicos de Sistemas y Redes para que implanten las medidas de seguridad
- ☹ ...

¿De verdad somos el eslabón más débil?

El Factor Humano

Las personas somos el eslabón ~~más débil~~ de la ciberseguridad.

No importa qué medidas apliquemos a las tecnologías si un fallo humano abre una puerta trasera al ciberdelincuente.

La concienciación y el sentido común, nuestras mejores armas.

La cadena es larguísima

Sistema de gestión la seguridad de la información (SGSI)

Análisis y gestión de los riesgos

Gestión de personal y profesionalidad

Autorización y control de los accesos

Protección de las instalaciones e infraestructuras comunes

Adquisición/contratación de productos/servicios de seguridad

Mínimo privilegio e integridad y actualización del sistema

Protección de información almacenada y en tránsito

Prevención ante otros sistemas de información interconectados

Registro de actividad y detección de código dañino

Incidentes de seguridad

Continuidad de la actividad

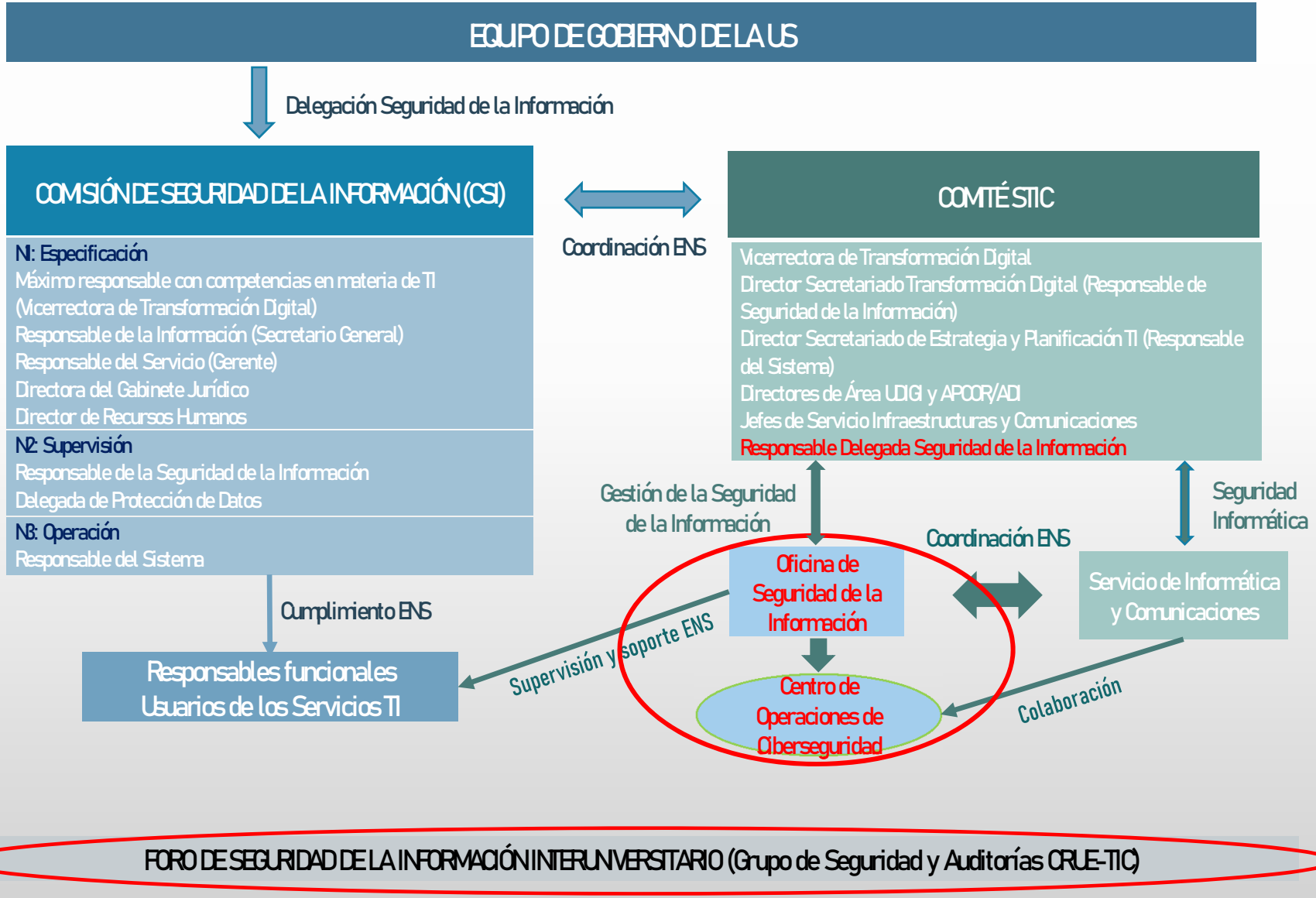
Mejora continua del proceso de seguridad.

¿Por dónde deberíamos empezar?

MARCO DE GOBERNANZA

- ☺ Adaptado a las posibilidades reales de decisión estratégica
- ☺ Con capacidad sobre el control de la gestión (SGSI) y la operación (TIC)
- ☺ Se articula a través de un Comité de Seguridad TIC.
- ☺ Se gestiona a través de una Oficina de Seguridad TIC.
- ☺ Se implementa mediante el Centro de Operaciones de Ciberseguridad – COCS (en colaboración con el Servicio de TI).
- ☺ Impulsa la colaboración del sector a través de un Foro de la Seguridad TIC.
- ☺ Adicionalmente, se puede constituir un Órgano de Auditoría técnica.

Marco de Gobernanza de la Universidad de Sevilla



Implantación real de LOPDyENS en la US

- ☺ Designamos roles: responsables delegados, responsables tecnológicos y gestores LOPDyENS.
- ☺ Trabajamos con los implicados usando excels de verificación de controles en los que vamos marcando las medidas aplicadas y el nivel de madurez del L0 a L5.
- ☺ Recopilamos evidencias de cumplimiento y las centralizamos en la plataforma de cumplimiento LOPDyENS (Redmine) a la que acceden los responsables delegados, tecnológicos y gestores.
- ☺ La aplicación LOPDyENS permitirá a un auditor interno o externo verificar las evidencias de cumplimiento, tanto de Protección de Datos como de Seguridad de la Información.

Muchas gracias

julia@us.es