Ciberseguridad = Tecnología + Cumplimiento

Salamanca, 6 de septiembre

José Ignacio Castillo. Consultor GRC

Hablemos sobre Normativa de Seguridad

- **Cómo afrontar el “Cumplimiento”.**
- **Caso de Uso: Apareció el Cisne Negro**

ÍNDICE

Normativa de Seguridad: Contexto

BOE: Código de Ciber-Derecho

Nuevos y Viejos Problemas

Privacidad, E-Commerce, Administración Digital

Ciberdelincuencia, Crypto, IA, Legaltech

Agilidad y Flexibilidad

Nuevo ENS, RGPD, LPIC, NIS 2

Incorporación de Tecnología

SOC, SIEM, EDR..

Alineamiento con estándares internacionales

ISO 27001, 22301

RIESGOS

¿Cómo me enfrento al Cumplimiento?

Director

YES	BUT
“La información es el petróleo del siglo XXI”	Todo es carísimo. Si cumplo estoy muerto
“El 99% de los incidentes es responsabilidad del usuario”	Mínimo esfuerzo en aplicar tecnología, formación y concienciación

Usuario

YES	BUT
“Tenemos mucho cuidado cuando vemos un virus”	Sistemas de Tickets desiertos
“Si, si cumplimos con lo que nos dijo el de la consultora”	………….

¿Qué tiene la ley contra mi?

- ¿Qué se protege?
  - La normativa protege derechos fundamentales, protege activos esenciales para la sociedad, previene efectos negativos en el uso de la tecnología y nos ayuda a implementar sistemas de gestión que nos ayuden a afrontar amenazas externas, pero también **internas.** Y esto, por no hablar de disponibilidad, confidencialidad, etc..
- ¿Por qué?

Los atacantes del Ayuntamiento de Castellón reivindican la filtración de 119 gigas en datos robad el 'ransomware' hace su agosto en las administraciones españolas

Ciberataque a una veintena de ayuntamientos

Los ciberataques se están volviendo cada vez más comunes y no contar con la seguridad adecuada puede paralizar todo el sistema de una empresa. Los empleados del Ayuntamiento de Arenys de Mar, quienes a principios de enero fueron atacados por hackers, sufrieron un bloqueo de todo el sistema informático. Los hackers, además, exigieron un rescate en bitcoins para restablecer el sistema.

Caso de Uso: Ransomware

Organismo Público/Empresa

- Carácter Nacional, varias sedes
- Cientos, sino miles de usuarios
- Información estratégica

Caso de Uso: Diagrama del caso

1- Usuario indica en redes sociales que no puede trabajar porque no puede acceder a la información.

2- No contentos con eso, escriben a la prensa sobre la importancia de su trabajo y de no poder trabajar.

¿Qué está fallando? No tenemos Análisis de Riesgos; No disponemos de medidas de VIGILANCIA, No disponemos de procedimientos ni herramientas para gestionar incidentes

1- Director saca una "Nota de Prensa".

2- **La Autoridad de Control** activa mecanismo para contener el ataque y desconectar los sistemas.

NO HABLAMOS EL MISMO IDIOMA QUE LA AUTORIDAD DE CONTROL

Caso de Uso: Diagrama del caso

"No, no teníamos aprobada Política de Seguridad"
ENS,RGPD,NIS,LPIC,ISO

"¿Yo responsable de lo que hagan los usuarios?"
SI. Fórmalos. Crea una CULTURA de Seguridad
RGPD, LOPDGDD, ENS, NIS, ISO…

"¿Responsable de Seguridad?. Si cumplimos, no trabajamos"
PERFILES DE CUMPLIMIENTO DEL ENS.

No es COSTE es INVERSIÓN.

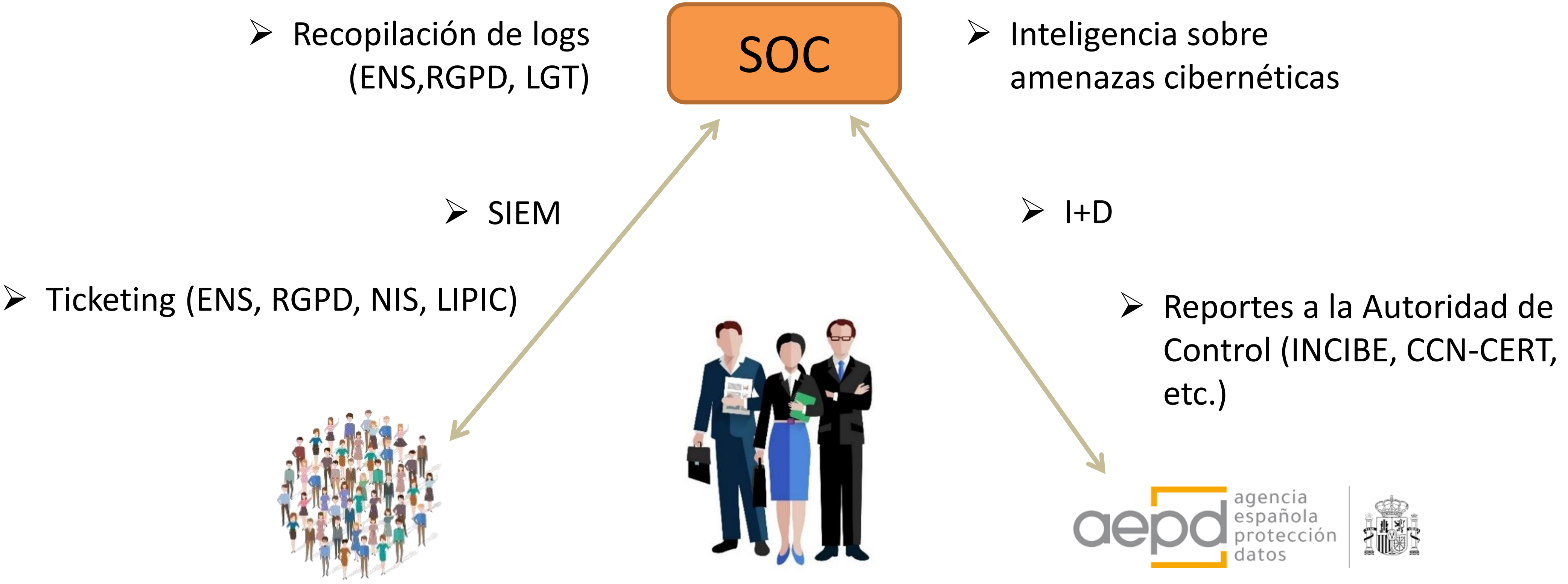
Caso de Uso: Tecnología al Servicio del Cumplimiento

Medidas Organizativas: Dota a tu organismo de un sistema con unas Políticas y Normas claras y responsables de Ejecutarlas

ANALIZA RIESGOS: JURÍDICOS, TECNOLÓGICOS, etc. (PILAR, INES, AMPARO)

IMPLEMENTA MEDIDAS DE SEGURIDAD: EDR, CMDB, AUDITORÍAS DE SEGURIDAD

Caso de Uso: Tecnología al Servicio del Cumplimiento



SOC

- Recopilación de logs (ENS,RGPD, LGT)
- Inteligencia sobre amenazas cibernéticas
- SIEM
- I+D
- Ticketing (ENS, RGPD, NIS, LIPIC)
- Reportes a la Autoridad de Control (INCIBE, CCN-CERT, etc.)

Caso de Uso: Cuando la amenaza es interna

El "Usuario"	Realidad
"Están usando el EDR para fiscalizar nuestro trabajo"	Siempre que exista información suficiente y una normativa en tal sentido, el organismo podrá emplear mecanismos para garantizar un correcto uso de los medios informáticos
"El SOC invade la privacidad de las personas y la mía como empleado"	La información personal que pudiera tratar un SOC o cualquier otra herramienta, tiene una finalidad legalmente establecida
"La organización vende nuestros datos personales"	Colega, ¿Y mi DPD?

Un Sistema de Cumplimiento Maduro, garantiza la correcta atribución de Responsabilidades

Gracias por su atención¡¡¡¡