



La Continuidad de Datos de Negocio para Garantizar la continuidad laboral

Manel Medina
esCERT-UPC
medina@escert.upc.edu

Contenido

- El valor de los activos intangibles
- Tecnologías de gestión de los datos de ISMS
- Responsabilidad Social: Alineación legal
- El ciclo de vida de la seguridad y la calidad de vida de los trabajadores
- Valor añadido de la Concienciación
- De las Buenas a las Mejores prácticas
- Conclusiones

El valor de los activos intangibles

- Principio básico: Datos = Información
- Aproximación de negocio a la seguridad:
- Indicadores (NIST 800-30, Risk Mngmt):
Monitorización de los activos de negocio
 - Tangibles
 - Intangibles
 - Información

Preservación del valor de los activos

- Controles de seguridad, Objetivos:
 - Formación
 - Concienciación: Cuadro de mando
- Retorno de la inversión:
 - Optimización del tiempo de retorno

Tecnologías de Gestión de los datos de ISMS

- Vulnerabilidades
- Amenazas
- Centralización de Logs
- Análisis Forense
- Gestión de Vulnerabilidades
- Gestión de Identidades
- Segmentación de Redes
- Gestión de Incidentes
- Procedimientos Operativos: ISO, NIST

Responsabilidad Social: Alineación legal

- Ley de Firma-e
- Protección d datos en comunicaciones electrónicas, Retención de datos telecomunicaciones, LOPD
- Creación de ENISA, INTECO-CERT, CATA, CCI-CERT
- Decisión Marco ataques a sistemas de información, DM2005/222
- Decisión Marco para combatir terrorismo
- LSSI-ce
- Ley Acceso Electrónico a las AAPP, LISI, Council Resolution on EU approach to a culture of security

Ataques contra SI

- **DECISIÓN MARCO 2005/222/JAI DEL CONSEJO de 24 de febrero de 2005**
- espacio Europeo de libertad, seguridad y justicia
- Acceso ilegal o Intromisión en SI (DoS) o Datos: infracción penal si transgrede medidas de seguridad (2 a 5 años)
- Inducción, complicidad o tentativa (1 a 3 años)
- Personas Jurídicas son responsables si:
 - Las acciones benefician a la Persona Jurídica
 - falta de vigilancia o control por personas
 - Multas, no-ayudas, cese actividad comercial, vigilancia
- Transposición antes de 16 marzo 2007:
Arts.197 y 264 Cod. Penal (BOCG 15-1-2007, nº 119-1)

El ciclo de vida de la seguridad y la calidad de vida de los trabajadores

- Prevenir
- —————> Reprimir
- Detectar
- —————> Detener
- Restablecer
- —————> Transferir
- Restaurar
- —————> Mejorar y/o Corregir

Aproximación a la Seguridad orientada al negocio

- Todos los servicios que ofrecemos deben basarse en la seguridad para:
- Reducir coste fallos, ataques, desastres, etc.
- Proporcionar respuesta a la continuidad
- Dar garantías a clientes en términos de “CIA”
- Mantener e incrementar la robustez y resistencia de las infraestructuras críticas
- La confianza de nuestros clientes es crucial

De las Buenas a las Mejores prácticas

- Gasto
- Reaccionar
- Restablecer
- Compromiso
- Recomendar
- Externalización
- Auto-evaluación
- Implantación
- Respuesta a Incident.
- Inversión (Beneficios)
- Prevenir (Calidad Vida)
- Continuidad
- Formación
- Forzar
- Cooperación
- Auditoría independiente
- Consultoría
- Coordinación

Conclusiones

- Aplicar las mejores prácticas de gestión de seguridad (ISO 27000, NIST 800) para desarrollar, sostener y mejorar procesos
- Y garantizar su calidad de ejecución
- Gestión Riesgo Personalizada
- Alinear controles con riesgos del negocio:
 - Clasificación de la información: CIA
 - Valoración de los RRHH
 - Compromiso con la Sociedad y Legalidad