# Evidencia 15 – Crónica

**Apellidos**: Centeno Vega

**Nombre**: Javier

**Grupo**: Grupo 1

**Comité**: Comunicación

**Horas totales**: 1:00

## Evidencias:

1. El 4/11/2017, de 19:00 a 20:00, estuve 1:00 horas trabajando en la redacción de la crónica sobre la conferencia de María Carmen Romero sobre la seguridad en organizaciones.
2. Enlace a la tarea relacionada: https://github.com/InnosoftDaysPresidencia/Comunicacion/issues/51
3. Enlace al comiteo: https://github.com/InnosoftDaysPresidencia/Comunicacion/commit/bea4aeb171d4387f0e1d7b0787db51e03deaf240
4. Enlace a la noticia: https://institucional.us.es/innosoft/2017/11/06/gestion-de-la-seguridad-maria-carmen-romero/
5. Se adjunta la crónica en cuestión.

Crónica: María Carmen Romero. La seguridad, ¿Un incordio o una oportunidad para las organizaciones?

---

María Carmen Romero nos explica que la seguridad en sistemas de información tiene tres pilares: Confidencialidad, Disponibilidad e Integridad. En la actualidad, a estos pilares se añaden Privacidad y Confiabilidad. Estos pilares giran alrededor de la confianza que se puede tener en un sistema y su resiliencia, es decir, su capacidad para recuperarse de un suceso.

En una organización, es la organización la que debe asumir la responsabilidad de la seguridad, sin embargo, todos los componentes de

una organización se deben encargar de la seguridad, desde la directiva hasta los usuarios.

En este contexto, el riesgo se puede definir como la probabilidad de que una amenaza explote una vulnerabilidad de un activo generando un impacto o el efecto de la incertidumbre sobre los objetivos de la organización.

Se identifican varias maneras de administrar un riesgo. Es posible eludirlo, es decir, evitar realizar la acción que genere ese riesgo. También es posible transferirlo, o responsabilizar a otro de la acción que genera el riesgo, lo cual suele generar otros riesgos. Otra opción es reducirlo, es decir, tomar medidas para reducir la probabilidad. Sin embargo, la opción más simple es asumirlo; hay riesgos que solamente pueden asumirse.

La teoría define cómo se debería administrar un riesgo en una organización mediante un sistema eficiente de detección, evaluación y comunicación de los riesgos, aunque la práctica no suele corresponderse con el sistema perfectamente. Los usuarios suelen ignorar cuestiones de seguridad, la gestión del cambio es una molestia para ellos, puede incluso ser percibida como una pérdida de libertades.

Con todo ésto, la seguridad suele acabar como la última de las prioridades. Se piensa en las metas por encima de los riesgos y hay demasiado optimismo en su percepción. Como consecuencia, la mayoría de operaciones no tienen sus datos sensibles clasificados correctamente.

En contraste, también se aplica el principio de proporcionalidad. Las medidas de seguridad traen un coste, y es innecesario gastar enormes recursos en un sistema de seguridad desproporcionado para la cobertura de un riesgo bajo.

Ultimadamente, las personas son el eslabón más débil de la cadena. Los empleados causan vulnerabilidades y/o no las reportan. Ésto constituye el primer escollo de cualquier problema de seguridad.

Como entidad pública, la Universidad de Sevilla debe garantizar la seguridad y posee una normativa para ello, siguiendo el Esquema Nacional de Seguridad.