Cultura de seguridad

La manera en que **se percibe** la seguridad es determinante de la efectividad de la gestión de la misma.

¿Cómo se percibe?

- ¿es necesaria?
- ¿es una molestia?
- ¿es un inconveniente?
- ¿es un requisito del negocio?
- ¿agrega valor?

- La cultura de seguridad no es independiente de la **cultura organizacional**.
- Hay varias y no suele ser la dominante, salvo en una organización de seguridad: p.e. cultura de clientes, de RRHH, de calidad, de servicio, etc.

- Una definición de cultura organizacional es “la manera de hacer las cosas aquí”.
- La CO puede ser vista como la personalidad de la organización y es la amalgama social que une a los miembros de una organización.
- El comportamiento organizacional se refiere a que hace la gente en la organización y como su comportamiento afecta el desempeño de la misma.

Cultura de seguridad

- Es un **conjunto de** valores, comportamientos, creencias, supuestos, capacidades, actitudes y maneras de hacer las cosas que promueven la seguridad.
- La **cultura corporativa** provee el contexto dentro del cual los hechos y acciones son vistos y entendidos.

MINDSET

Una cultura de seguridad de la información se define como las **percepciones y actitudes** que son aceptadas y fomentadas a fin de incorporar las características de seguridad de la información como la forma en que se hacen las cosas en una organización.

Martins & Eloff

- Crear una cultura no significa poner la seguridad por encima del negocio, sino entender que la seguridad es un medio para que al negocio le vaya bien.
- Una cultura adecuada es la base para entender cuáles son los riesgos, qué activos están protegidos, que la seguridad está a favor de los intereses de la organización y de sus integrantes, y que las inversiones están justificadas.

- La necesidad de ver la seguridad desde un punto de vista holístico (sistémico).
- Desarrollar una cultura intencional.
- El balance entre la necesidad, el costo, la incomodidad, la velocidad, ….
- Sin esto, un sistema de seguridad tiende hacia la degradación

Por lo tanto…

una cultura de SI está basada en la interacción de los empleados con los activos informáticos y el comportamiento de seguridad que éstos exhiben.

El contexto influye en la cultura

- Época
- Impacto en el cliente
- Consecuencias en el negocio
- Regulaciones
- País (EEUU, Israel,…)
- Industria
- Riesgo
- Grado de delincuencia

Premisas

- ✓ La tecnología de la información se ha convertido en una parte integral de la vida moderna. Hoy en día, el uso de la información impregna todos los aspectos de los negocios y la vida privada.
- ✓ La mayoría de las organizaciones necesitan sistemas de información para sobrevivir y prosperar y por lo tanto tienen que tomar en serio la protección de sus activos de información.

Premisas

- ✓ Muchos de los procesos necesarios para proteger estos activos de información son, en gran medida, dependiente del comportamiento humano.
- ✓ Los empleados, ya sea intencionalmente o por negligencia, a menudo debido a la falta de conocimiento, son la mayor amenaza para la seguridad de la información.

Premisas

- ✓ Hoy día es ampliamente aceptado que el establecimiento de una cultura de la organización de seguridad de la información es la clave para la gestión de la seguridad de la información.

- ✓ Para alcanzar eficacia en el mundo actual, complejo e interconectado el tema de la seguridad debe ser una preocupación del nivel más alto de la organización y **no considerarlo como una especialidad técnica** de responsabilidad del área de TI.

Premisas

- ✓ La tecnología no es la única respuesta, los procesos y la gente importan
- ✓ La seguridad de la información no es solamente un problema técnico sino un **desafío de negocios y de gobierno** que involucra una adecuada gestión de los riesgos (actuales y emergentes).
- ✓ La seguridad es una responsabilidad de todos.

Premisas

- ✓ Es más fácil comprar una solución que cambiar una cultura.
- ✓ No hay tecnología, por segura que sea, que pueda cumplir su cometido si la gente no está bien informada, es descuidada o indiferente.
- ✓ Un programa de SI comprensivo implementa la seguridad de los activos informáticos a través de una serie de capas de medidas de protección, y controles tecnológicos y no tecnológicos.

La manera en que los empleados perciben e interactúan (se comportan) con los controles implementados para proteger los activos de información es una de las principales consideraciones para la protección de tales activos y el uso efectivo de la seguridad de la información.

Seguridad = **C**onfidencialidad+**I**ntegridad +**D**isponibilidad

- Hay amenazas ….
- También hay vulnerabilidades
- ¿Cuál es el impacto?
- Hay formas de combatir las amenazas
- Algunas son muy fáciles de implementar, otras no tanto
- Algunas son muy tecnológicas, otras son administrativas, otras tienen que ver con el comportamiento de la gente.
- No olvidarse del riesgo

- La seguridad depende, en gran medida, del comportamiento humano.

- El factor humano es el primer nivel de defensa en la SI y consiste en **dos dimensiones interralacionadas**.

  - **Primero**, el empleado debe tener el **conocimiento** suficiente de SI para poder efectivamente implementar y mantener los diversos controles de SI.

  - **Segundo**, deben tener la **actitud correcta** acerca de SI.

- Estas dos dimensiones están intimamente relacionadas y son mutuamente dependientes. Por ende hay que considerarlas en forma holística.

Migrando de una cultura funcional a una intencional I

Tecnología

De:	A:
• No esta muy claro el nivel de seguridad provisto por la tecnología	• La tecnología se utiliza basada en una evaluación del riesgo
• Ver a la tecnología de seguridad como algo molesto y difícil de usar	• Ver a la tecnología como un medio de hacer mejor los negocios

Migrando de una cultura funcional a una intencional II

Procesos

De:	A:
• Incorpora la seguridad frente a un incidente	• Planifica la seguridad desde el inicio
• El área de seguridad monopoliza el conocimiento sobre SI	• El área de seguridad comparte su conocimiento a través de toda la organización

Migrando de una cultura funcional a una intencional III

Gente

De:	A:
• El área de seguridad presiona para conseguir el cumplimiento	• El área de seguridad es un socio que crea concientización y compromiso
• La SI se canaliza exclusivamente a través del área de seguridad	• La SI es una responsabilidad de toda la organización

Migrando de una cultura funcional a una intencional IV

Organización

De:	A:
• Poca concientización de los problemas de seguridad	• Los miembros de la organización se mantienen actualizados sobre los riesgos.
• Seguridad basada exclusivamente en conocimiento técnico	• La SI incorporada en los procesos de negocios