UNIVERSIDAD DE GUADALAJARA

CENTRO UNIVERSITARIO DE CIENCIAS

EXACTAS E INGENIERIAS

Computación tolerante a fallas

Principios y prevención de defectos

Hernández Ruvalcaba Dania Jazmín

Confidencialidad de la información

También conocida como **privacidad**, hace referencia a que la información sólo debe ser conocida por las personas que necesitan conocerla y que han sido autorizadas para ello. Este principio asegura que **la información no va a ser divulgada** de manera fortuita o intencionada.

Integridad de la información

Hace referencia a que la información que se encuentra almacenada en los dispositivos o la que se ha transmitido por cualquier canal de comunicación **no ha sido manipulada por terceros** de manera malintencionada. Esto garantiza que la información no será modificada por personas no autorizadas.

Disponibilidad de la información

Se refiere a que la información debe estar disponible siempre para las personas autorizadas para accederla y tratarla, y además **puede recuperarse** en caso de que ocurra un incidente de seguridad que cause su pérdida o corrupción. Es decir; permite que la información esté disponible cuando sea necesario.

Incrementar la seguridad

Algunas de las principales **buenas prácticas** que garantizan el cumplimiento de los tres principios fundamentales de la seguridad de la información son las que se comentan a continuación:

Política de mínimos privilegios

Las personas de una organización no deberían acceder a toda la información de esta, solo a aquella que sea de utilidad e importante para la ejecución de su trabajo. Aplicando efectivamente una **política de gestión de privilegios** de los usuarios, estamos minimizando los riesgos de fugas de información, manipulación no autorizada de la misma, etc. y minimizando la superficie de ataque de nuestra organización.

Política de control de acceso cerrado por defecto

Todos los accesos a la información y los sistemas que la tratan o almacenan deberían estar cerrados para todos los usuarios y se permitirá **solo para aquellos que estén autorizados** para acceder.

Segregación de funciones

Se debería definir e implementar una separación efectiva de las funciones y responsabilidades del personal de las organizaciones para evitar conflictos de intereses y minimizar los riesgos de seguridad de la información derivados de la **acumulación de privilegios y conocimiento** en las personas.

Defensa en profundidad

Ante la gran cantidad de riesgos para la seguridad de la información a la que están expuestas las organizaciones, derivadas de la utilización y dependencia de las TIC, cada vez la superficie de ataque de estas es mayor, por lo que sería necesario diseñar e implementar **varios niveles de seguridad** acorde a un análisis de riesgos riguroso de sus activos de TIC.

Formación en ciberseguridad

El eslabón más débil de la seguridad de la información de una compañía son las personas. La mayoría de los incidentes de seguridad que sufren las organizaciones están **originados por personal interno de estas de manera no intencionada** o fortuita y derivados de su desconocimiento de las mejores prácticas de ciberseguridad o de las políticas y procedimientos a tal efecto de la organización. Por eso, es fundamental definir e implementar planes formativos en seguridad informática para todo el personal de la compañía y acorde a sus funciones y responsabilidades.

Auditorías de seguridad informática

Es recomendable realizar controles de auditoría donde **se verifique la efectividad y el cumplimiento** de las políticas, procedimientos, medidas técnicas y organizativas de la seguridad de la información de la organización y que permitan detectar debilidades y/o vulnerabilidades que puedan ser explotadas por potenciales atacantes. En base a los resultados de las mismas, se deberían diseñar y poner en marcha planes de acción correctivos para solucionar los hallazgos detectados durante las mismas.

Como vemos, mantener unos principios de seguridad informática es básico para cualquier empresa u organismo por la importante cantidad de datos que pueden llegar a manejar. Cada entidad debe implementar sus controles y planes de seguridad (acordes a sus necesidades y características) para garantizar la integridad, confidencialidad y disponibilidad de la información. En UNIR México brindamos un plan de estudios innovador a través de la **Maestría en Seguridad Informática** con la que el profesionista puede especializarse en una de las áreas que más demanda el mercado tecnológico.