**Utilice la tríada CID para proteger a las organizaciones**

Anteriormente, se le presentó la tríada de confidencialidad, integridad y disponibilidad (CID) y cómo ayuda a las organizaciones a considerar y mitigar los riesgos. En esta lectura, aprenderá cómo los analistas de ciberseguridad utilizan la tríada CID en el lugar de trabajo.

1. **La tríada CID para analistas**

La **tríada CID** es un Modelo que ayuda a informar sobre cómo las organizaciones consideran el riesgo cuando establecen sistemas y políticas de Seguridad. Se compone de tres elementos que los analistas de ciberseguridad y las organizaciones trabajan para mantener: confidencialidad, integridad y disponibilidad. Mantener un nivel de riesgo aceptable y garantizar que los sistemas y las políticas se diseñan teniendo en cuenta estos elementos ayuda a establecer una **postura de seguridad** satisfactoria, que se refiere a la capacidad de una organización para gestionar su defensa de los recursos y datos críticos y reaccionar ante los cambios.

* **Confidencialidad**

La **confidencialidad** es la idea de que sólo los usuarios autorizados pueden acceder a recursos o datos específicos. En una organización, la confidencialidad puede mejorarse mediante la implementación de principios de diseño, como el principio de privilegio mínimo. El principio de privilegio mínimo limita el acceso de los usuarios únicamente a la información que necesitan para completar las tareas relacionadas con el trabajo. Limitar el acceso es una forma de mantener la confidencialidad y la seguridad de los Datos privados.

* **Integridad**

La **integridad** es la idea de que los datos son verificablemente correctos, auténticos y fiables. Es esencial disponer de protocolos para verificar la autenticidad de los Datos. Una forma de verificar la integridad de los datos es a través de la criptografía, que se utiliza para transformar los datos de modo que las partes no autorizadas no puedan leerlos o manipularlos (NIST, 2022). Otro ejemplo de cómo una organización puede implementar la integridad es habilitando la encriptación, que es el proceso de convertir los datos de un formato legible a un formato codificado. La encriptación puede utilizarse para impedir el acceso y garantizar que los datos, como los mensajes de la plataforma de chat interna de una organización para que no puedan ser manipulados.

* **Disponibilidad**

La **Disponibilidad** es la idea de que los Datos son accesibles para aquellos que están autorizados a utilizarlos. Cuando un sistema se adhiere tanto a los principios de disponibilidad como a los de confidencialidad, los datos pueden utilizarse cuando sea necesario. En el lugar de trabajo, esto podría significar que la organización permite a los empleados remotos acceder a su red interna para realizar su trabajo. Cabe señalar que el acceso a los datos de la red interna sigue estando limitado, dependiendo del tipo de acceso que necesiten los empleados para realizar su trabajo. Si, por ejemplo, un empleado trabaja en el departamento de contabilización de la organización, podría necesitar acceso a las cuentas corporativas pero no a los datos relacionados con los proyectos de desarrollo en curso.

**Claves**

La tríada CID es esencial para establecer la postura de Seguridad de una organización. Saber qué es y cómo se aplica puede ayudarle a comprender mejor cómo trabajan los equipos de Seguridad para proteger a las organizaciones y a las personas a las que sirven.