

CIBERSEGURIDAD

Principios de seguridad de la Información



CIBERSEGURIDAD

Principios de seguridad de la Información

En el ámbito de la seguridad de la información, existen una serie de principios fundamentales que guían las buenas prácticas en este campo. Uno de estos principios es el de la integridad de la información.

La integridad se refiere a la calidad de la información, asegurando que esta sea exacta, completa y no haya sido alterada de manera no autorizada. Es crucial que la información se mantenga íntegra a lo largo de su ciclo de vida, desde su creación, almacenamiento, transmisión y utilización. La integridad garantiza que la información sea confiable y precisa, evitando la corrupción de datos y la manipulación malintencionada.



A veces, nos encontramos con situaciones en las que un archivo infectado con un virus informático puede causar daños en la integridad de los datos. Al abrir dicho archivo, podemos experimentar problemas, como la imposibilidad de acceder a la información completa o visualizarla de manera incorrecta. Estos virus pueden modificar, borrar o corromper ciertos tipos de archivos, lo que afecta directamente la integridad de la información.

Es por eso que el principio de la integridad es esencial en la seguridad de la información. Se busca garantizar que la información se mantenga exacta, coherente y libre de alteraciones no autorizadas. Para ello, se implementan medidas de seguridad, como **controles de acceso, cifrado de datos y sistemas de detección de cambios no autorizados**, con el fin de preservar la integridad de la información y mantener su confiabilidad.

Otro principio importante es el de la disponibilidad. En este caso, nos referimos a que la información esté accesible en el momento adecuado, sin importar la hora o el dispositivo utilizado, ya sea una computadora, un celular o incluso un reloj inteligente. La disponibilidad implica que la red esté funcionando correctamente y que la información o archivo que se desea revisar esté disponible en el momento oportuno. Todo debe estar configurado adecuadamente para que las personas con los permisos adecuados puedan acceder y encontrar la información que necesitan.

Además, es necesario considerar que no solo es importante que la información esté correcta y que las personas tengan los permisos adecuados en los archivos y carpetas, sino que también es crucial que esté disponible cuando se requiera. Sin embargo, todo esto tiene un punto intermedio, que es el principio del no repudio o irrenunciabilidad. Este principio brinda garantías al receptor de una comunicación en cuanto a la autenticidad del mensaje. Es decir, cuando se recibe un archivo, un correo electrónico o cualquier otro tipo de mensaje, **se puede asegurar de alguna manera que realmente proviene de la persona indicada.**



El principio de disponibilidad asegura que la información esté accesible en el momento adecuado, mientras que el principio del no repudio garantiza la autenticidad de los mensajes recibidos. Ambos principios son fundamentales en la seguridad de la información y buscan garantizar que la información esté disponible cuando se necesite y que se pueda confiar en su origen.

Lo anterior es común que nos suceda con frecuencia en el ámbito bancario, ¿verdad? A veces recibimos mensajes o correos electrónicos que aparentemente provienen de un determinado banco, solicitándonos que cambiemos nuestra contraseña o que hagamos

clic en un enlace. Sin embargo, muchos de estos correos maliciosos son falsos y son enviados por atacantes con intenciones dañinas. No podemos estar seguros de si el emisor del mensaje es realmente quien dice ser, lo que nos lleva al principio del no repudio.

Es importante destacar los tres principios fundamentales de la seguridad de la información en este contexto. **El principio de integridad** busca asegurar que la información sea correcta y esté libre de alteraciones no autorizadas. Por otro lado, **el principio de disponibilidad** se refiere a que la información esté accesible cuando se requiera. Y finalmente, **el principio del no repudio** garantiza que el emisor de un mensaje no pueda negar su autoría, lo que resulta crucial en la verificación de la autenticidad de los correos y mensajes recibidos.

En resumen, es común encontrarnos con situaciones en las que recibimos correos electrónicos fraudulentos que aparentan provenir de entidades bancarias. Estos casos resaltan la importancia de los principios de seguridad de la información, como la integridad, la disponibilidad y el no repudio, para asegurar que la información sea precisa, esté disponible cuando se necesite y se pueda verificar su autenticidad.

