CIBERSEGURIDAD:

**Encriptación:**

La **encriptación** es el proceso de transformar datos en un código secreto para que solo las personas autorizadas puedan entenderlos. Se utiliza para proteger información confidencial, como mensajes, archivos o transacciones bancarias.

* **Simétrica**: usa la misma clave para encriptar y desencriptar (ejemplo: AES).
* **Asimétrica**: utiliza dos claves diferentes, una pública y una privada (ejemplo: RSA).

**Ejemplo:** Cuando haces una compra en línea, tu tarjeta de crédito se encripta antes de enviarse, de modo que si alguien intercepta la información, no podrá leerla sin la clave correcta.

**Auditorías en el control de versiones:**

Las auditorías en control de versiones son revisiones que se hacen en sistemas como Git para verificar quién hizo cambios, cuándo y con qué objetivo. Ayudan a detectar errores, mantener seguridad y garantizar que se cumplen las reglas del proyecto.

**Ejemplo:** Una empresa descubre un error en su software. Con la auditoría del control de versiones, revisan los registros y encuentran qué programador modificó esa parte del código y cuándo, lo que facilita corregirlo rápidamente.

**Firmas y certificados digitales:**

* **Firma digital:** garantiza que un mensaje o documento proviene de quien dice haberlo enviado y que no fue alterado.
* **Certificado digital:** es como un “DNI en internet” emitido por una autoridad confiable que asegura la identidad de una persona o empresa en línea.

**Ejemplo:** Cuando recibes un correo oficial firmado digitalmente, sabes que realmente lo mandó tu banco y no un estafador. Además, al entrar a un sitio web con “https://”, tu navegador usa un certificado digital para comprobar que la página es auténtica.

**Hashing:**

El **hashing** convierte datos de cualquier tamaño en una cadena corta y única de caracteres llamada “hash”. Este proceso no es reversible, y se usa principalmente para seguridad y verificación de integridad.

**Ejemplo:** Cuando guardas tu contraseña en una página, no se almacena la contraseña en sí, sino su hash. Así, aunque alguien acceda a la base de datos, no podrá ver tus contraseñas originales.

**Sistemas de control de accesos:**

Son mecanismos que regulan qué usuarios pueden entrar a un sistema o usar ciertos recursos, asignando permisos y roles específicos.

* **DAC (Discrecional):** el dueño de un archivo decide quién lo puede abrir.
* **RBAC (Por roles):** los permisos dependen del cargo del usuario.
* **ABAC (Por atributos):** se otorgan permisos según condiciones (horario, ubicación, dispositivo).

**Ejemplo:** En una empresa, solo el departamento de recursos humanos puede acceder a las nóminas, mientras que los demás empleados no tienen permiso.

**Mecanismos de autenticación robustos:**

Son métodos que aseguran que una persona realmente es quien dice ser, normalmente combinando varios factores de seguridad (MFA: autenticación multifactor).

* **Algo que sabes:** contraseña.
* **Algo que tienes:** un código en tu móvil o tarjeta de seguridad.
* **Algo que eres:** huella digital, rostro o iris.

**Ejemplo:** Para entrar a tu cuenta bancaria desde el móvil, además de la contraseña, te piden un código enviado por SMS y, en algunos casos, tu huella digital.

**No repudio**

El **no repudio** es un principio de seguridad informática que garantiza que una persona **no pueda negar** que realizó una acción digital, como enviar un mensaje, firmar un documento o hacer una transacción.  
Se logra con técnicas como las **firmas digitales** y los **certificados digitales**, que dejan evidencia verificable de la identidad del emisor y de la integridad del contenido.

**Ejemplo:** Si alguien firma digitalmente un contrato en línea, no podrá decir después que nunca lo firmó, porque la firma digital deja una prueba única y válida legalmente.