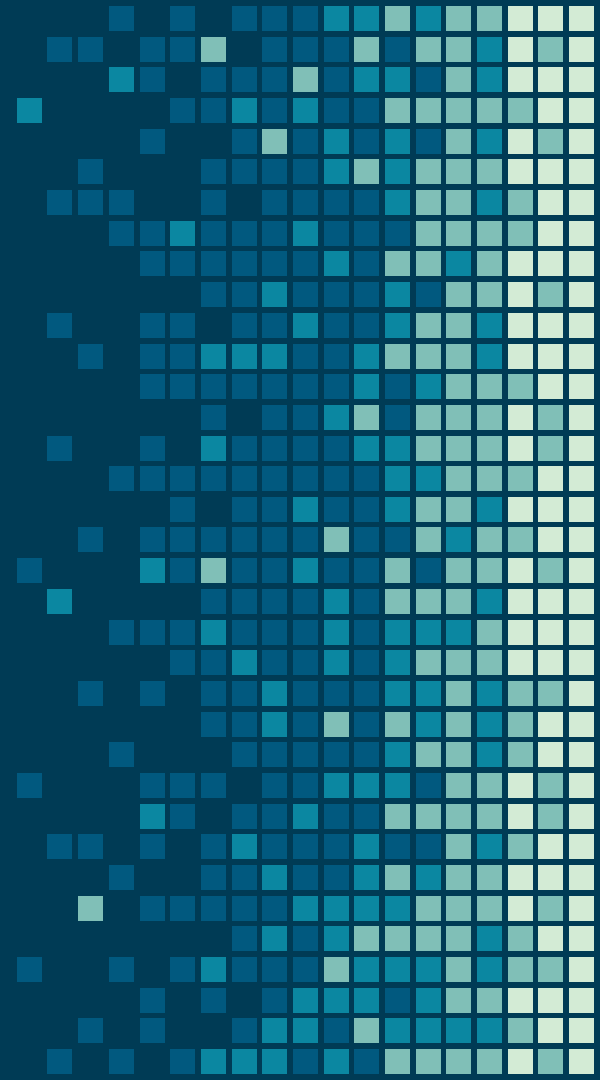

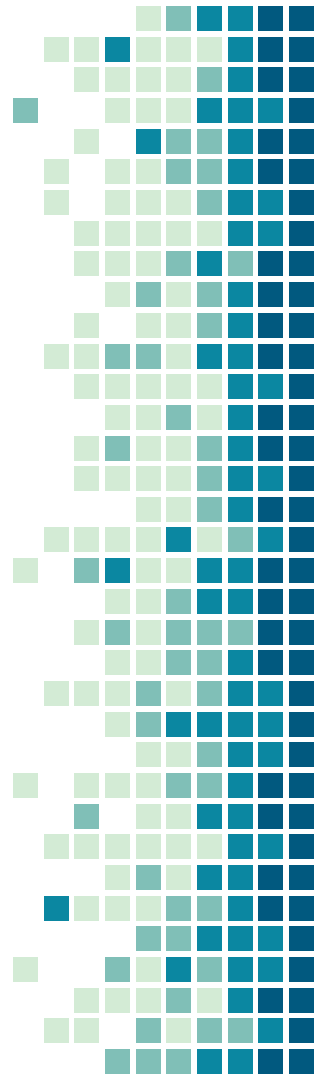


Seguridad

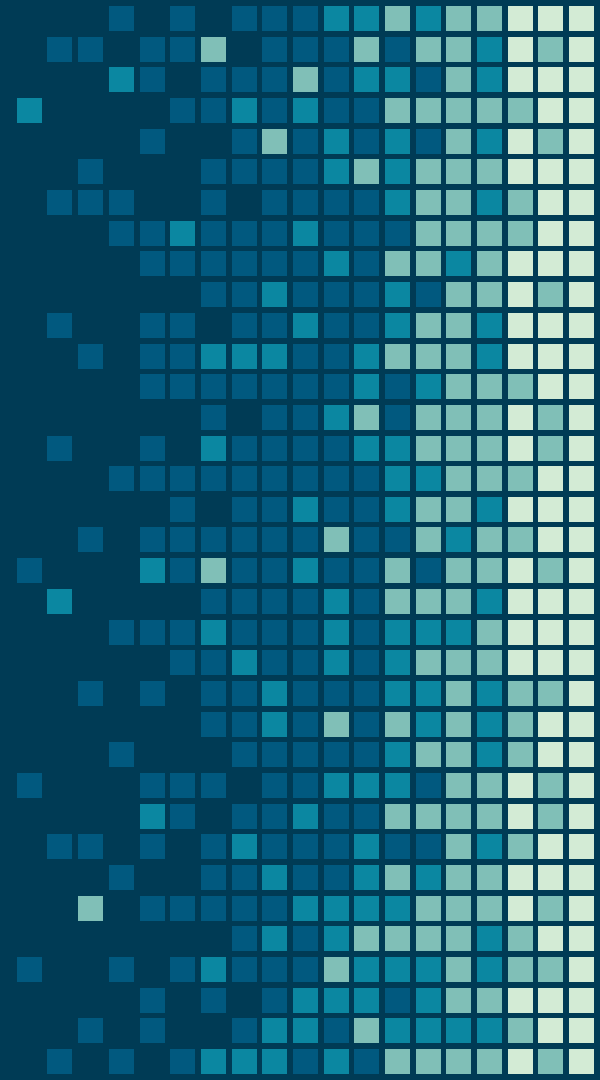


Agenda

- 
- **Introducción**
 - **Amenazas**
 - **Intrusos**
 - **Pérdida de datos**
 - **Criptografía**
 - **Autenticación**



Introducción





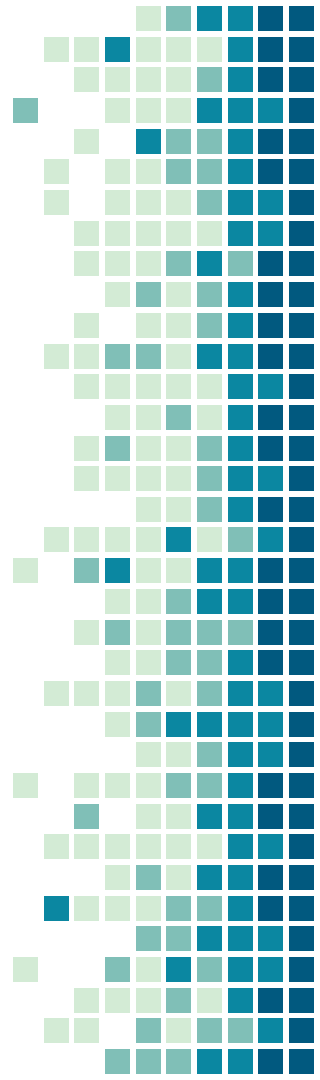
¿Qué papel juega la seguridad en sistemas computacionales?

¿Cuáles son las implicaciones del acceso a información crítica?

¿Están de acuerdo que el gobierno de Costa Rica implemente el expediente digital ?

¿Qué sucede sobre la información almacenada por el poder judicial?

¿Está de acuerdo que sus datos personales sea públicos?

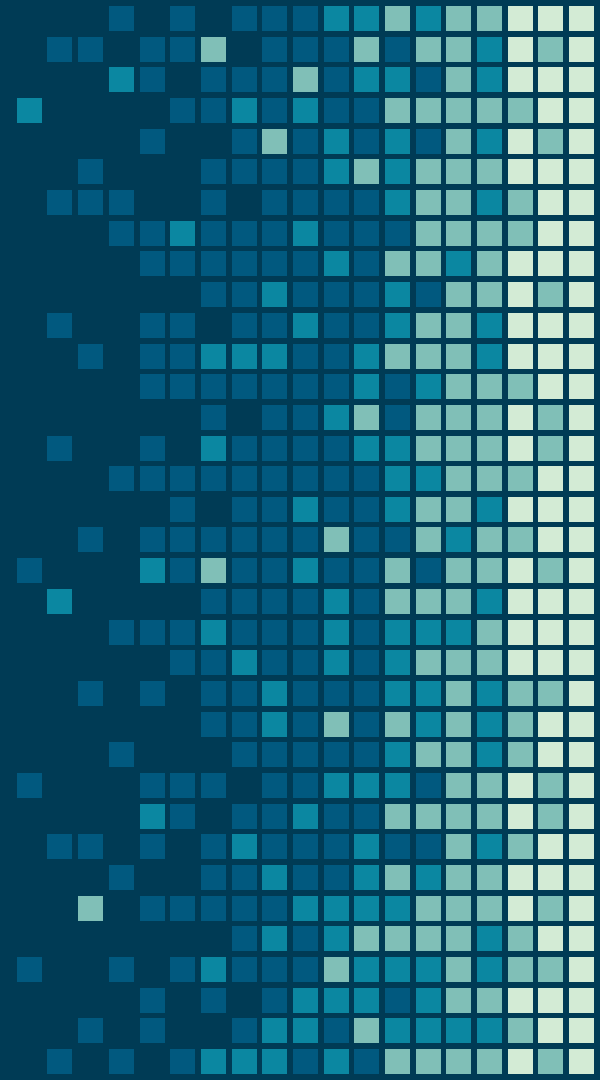


Recursos no apropiativos



- La seguridad es un problema general en el campo de la informática, por esto los sistemas operativos deben proporcionar mecanismos de protección que protejan los datos pertenecientes al sistema.

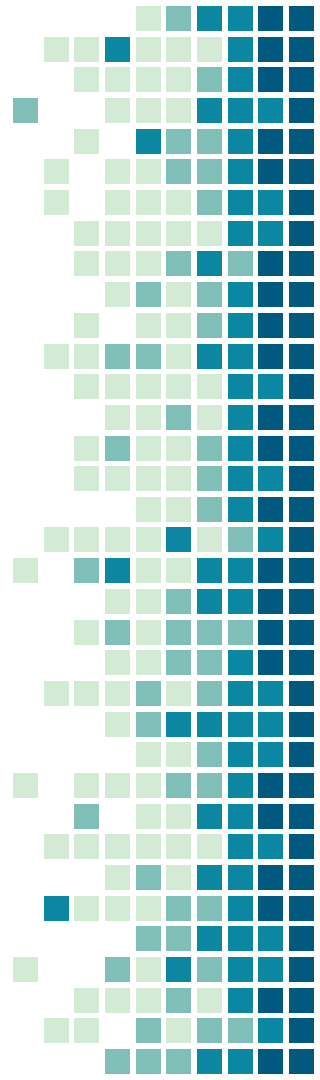
Amenazas



Amenazas



Se tienen cuatro objetivos primordiales con respecto a las amenazas que está expuesto un sistema computacional.



Confidencialidad de los datos

1

Consiste en que los datos secretos permanezcan en ese estado, hasta que el propietario decida lo contrario. El SO debe proporcionar los mecanismos para que las personas no autorizadas no tengan acceso a los datos.



Integridad de los datos

2

Se refiere a que los usuarios no autorizados no deben ser capaces de modificar datos sin el permiso del propietario. La modificación de datos implica eliminar, cambiar o ingresar información



Disponibilidad del sistema

3

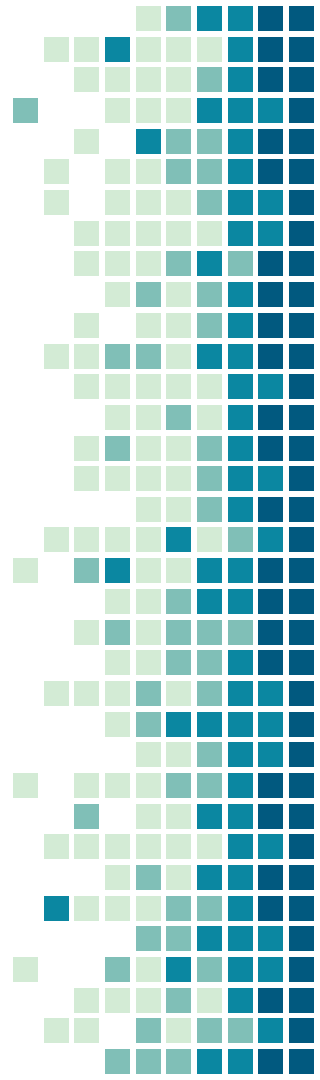
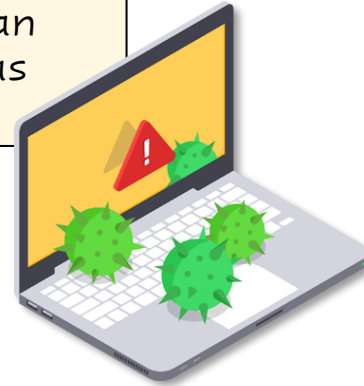
Consiste en que ningún usuario pueda dejar inútil el sistema.
Por ejemplo, un servidor que pueda procesar cierta cantidad de consultas y que en un momento dado lleguen más de dicha cantidad



Virus

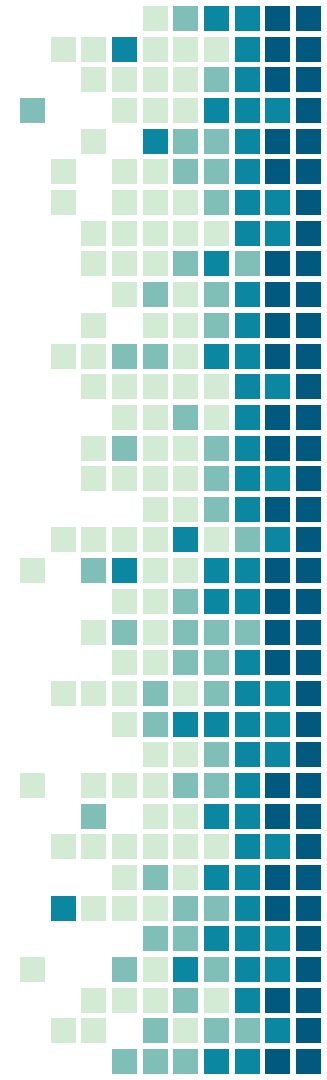
4

Usuarios externos toman el control de la computadora, o en su defecto, provocan daños mediante el uso de virus y así las convierten en zombies.

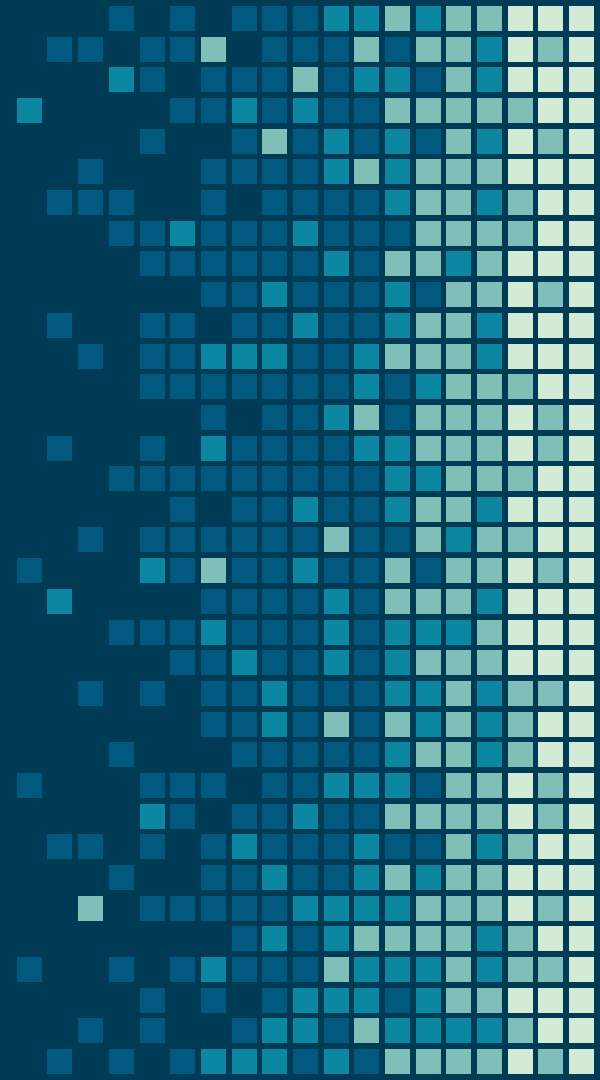


Resumen

Objetivos	Amenazas
Confidencialidad de los datos	Exposición de los datos
Integridad de los datos	Alteración de los datos
Disponibilidad del sistema	Negación del servicio
Exclusión de los usuarios externos	Los virus se apropian del sistema



Intrusos



Intrusos



Se refiere a las personas que husmean en lugares (Sistemas) donde no tienen que hacerlo.

Usuarios no técnicos

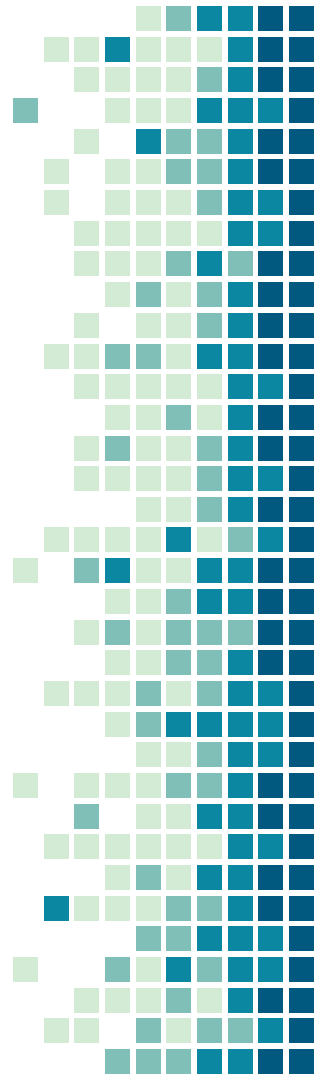
Se refiere a la naturaleza curiosa de los humanos, generalmente cuando se está conectado a un servidor algunos usuarios ven la información de otro si no existe las barreras de protección.



Intrusos que husmean



- Los estudiantes, programadores, operadores y demás personal técnico a menudo consideran como un reto personal la acción de irrumpir en la seguridad de un sistema computacional.



Intrusos por dinero

Se refiere aquellos usuarios que realizan intentos de obtener dinero. Algunos trabajadores de los bancos han tratado de robar de diferentes maneras.

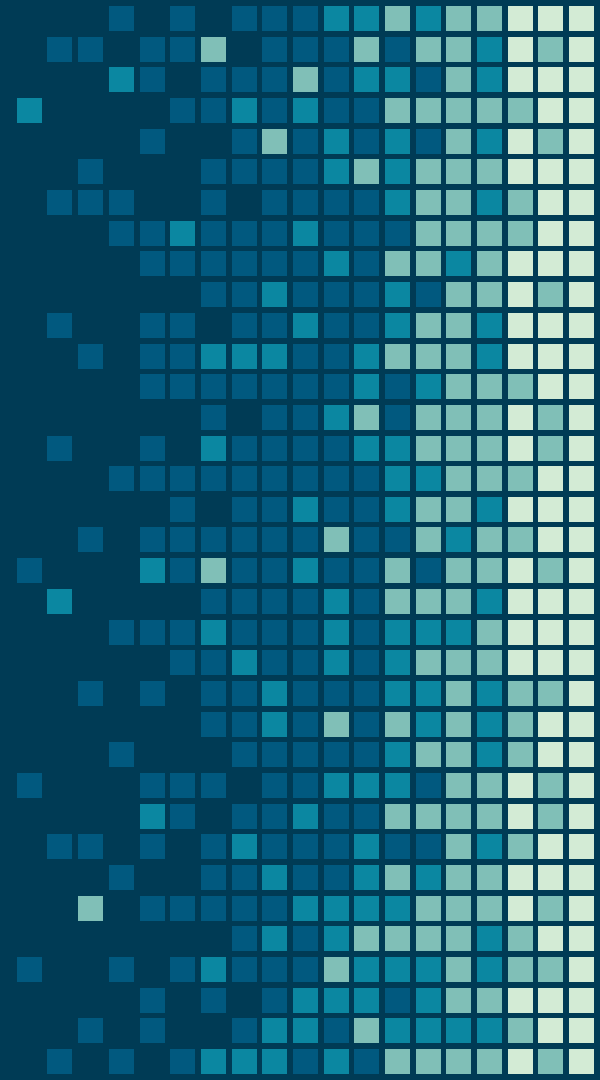


Espionaje comercial o militar

- Este tipo de espionaje se refiere a un intento serio y bien fundamentado para robar programas, secretos comerciales, ideas de patentes, tecnologías, diseños de proyectos entre otros .



Pérdida accidental de datos



Pérdida de datos

Desastre natural



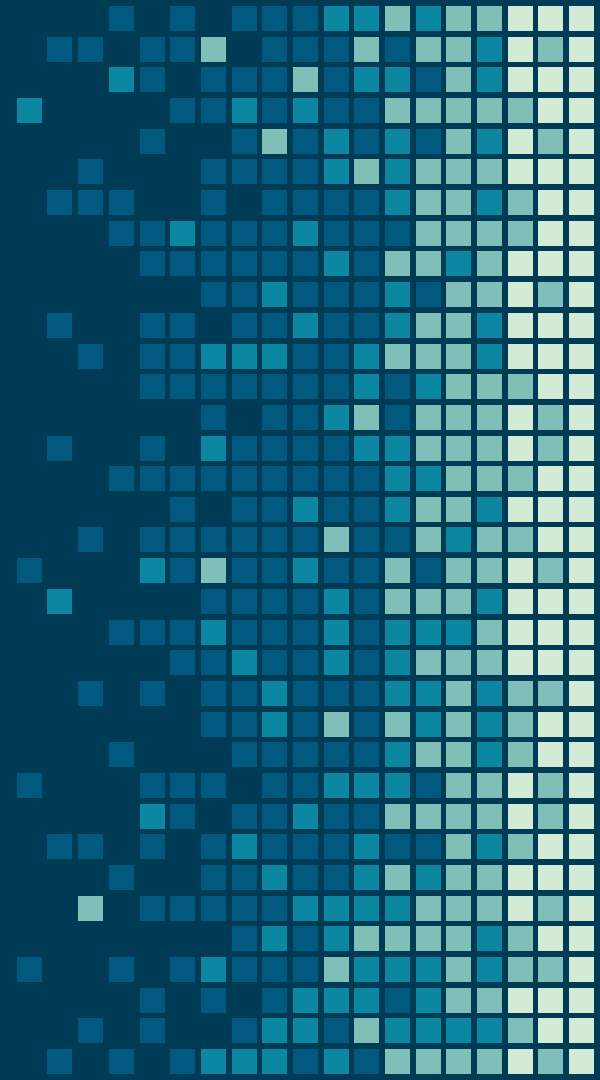
Error de hardware



Error humano



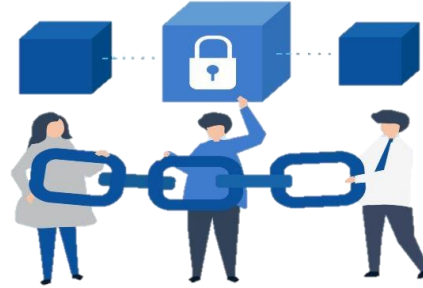
Criptografía



Criptografía



El propósito de la criptografía es tomar un mensaje o un archivo y convertirlo en texto cifrado de tal manera que sólo las personas autorizadas sepan cómo convertirlo nuevamente.



Los algoritmos de encriptación son públicos.



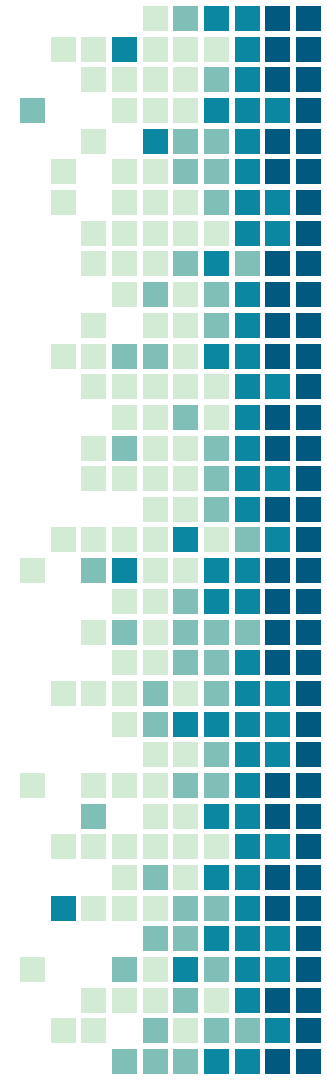
El secreto depende de los parámetros de los algoritmos.

Criptografía

—

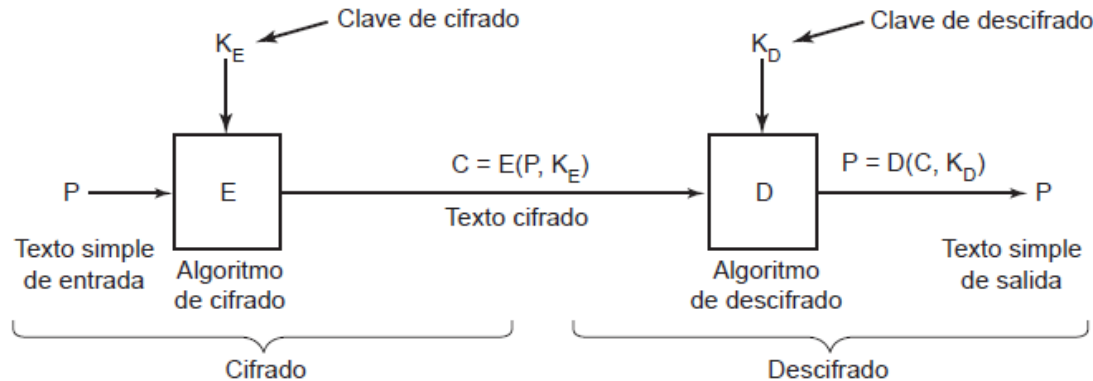
> Si P es un archivo de texto simple, K es la clave de cifrado, C es el texto cifrado y E es el algoritmo de cifrado, entonces se puede afirmar que $C=E(P,K)$.

- Lo anterior corresponde a la definición de cifrado, la cual indica que el texto cifrado se obtiene de mediante el uso del algoritmo de cifrado E , con el texto P y la clave K .
- Principio de Kerckhoffs.



Criptografía

Para obtener la información original se tiene que $P = D(C, K)$, donde D es el algoritmo de descifrado y K la clave de descifrado.



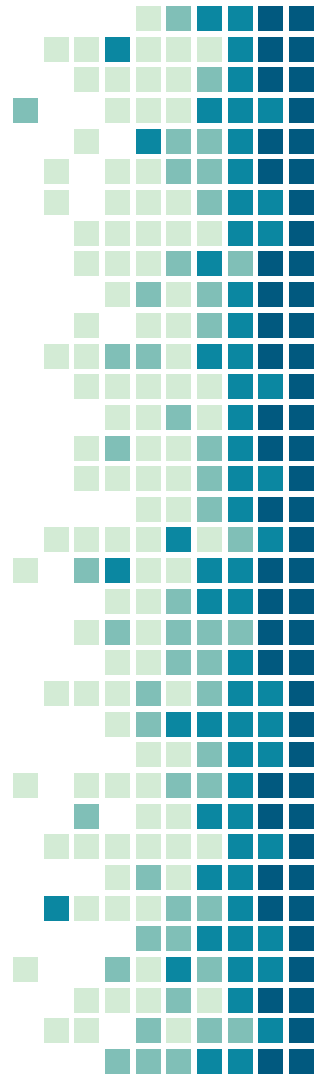
Criptografía de clave secreta

Dada la clave de cifrado se puede obtener la clave de descifrado.

Un ejemplo es la sustitución mono alfabética.

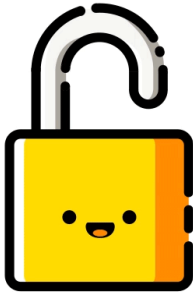
El monto de cálculos es razonable por lo que se puede considerar eficiente.

La desventaja es que el emisor y receptor deben tener la clave compartida.



Criptografía de clave pública

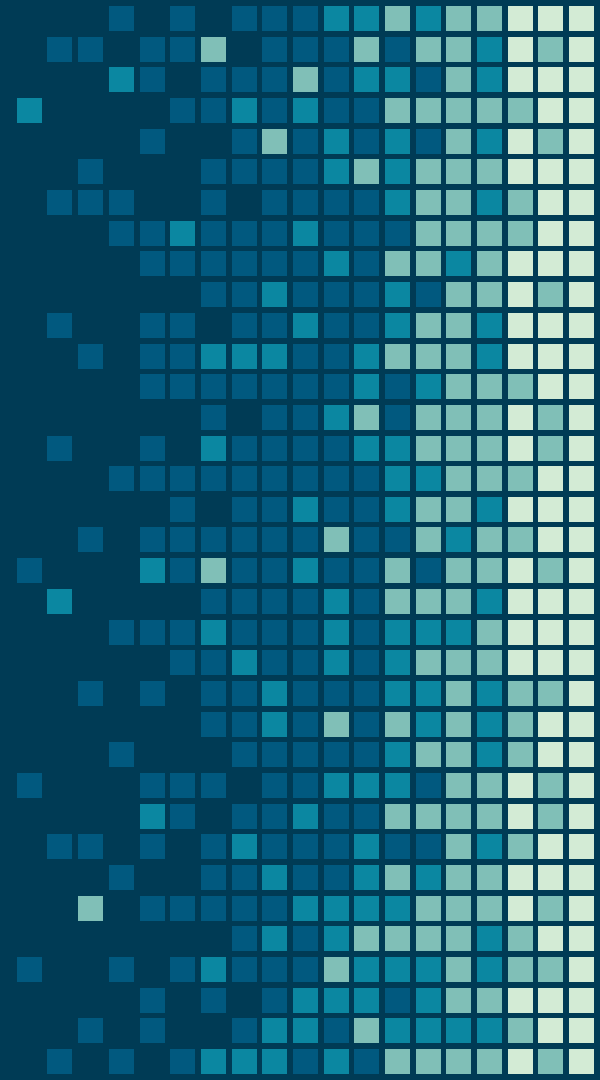
✎ Este sistema tiene la propiedad de que se utilizan distintas claves para el cifrado y el descifrado correspondiente.



✎ Si la clave de cifrado se elige bien, la clave de descifrado es difícil de averiguar.

✎ Todos eligen un par claves (pública y privada), y se publica la clave pública (de cifrado) y sólo los que tengan la privada podrán descifrar el mensaje encriptado.

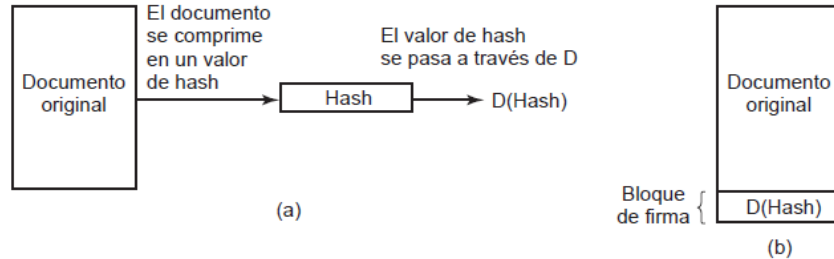
Firma digital



Firma digital

Se pasa el documento por una función de hashing criptográfico por ejemplo MD5 o SHA-1.

El propietario del documento aplica la llave privada al hash y lo adjunta al documento.



¿Cómo se puede implementar la firma digital con los conceptos de criptografía?

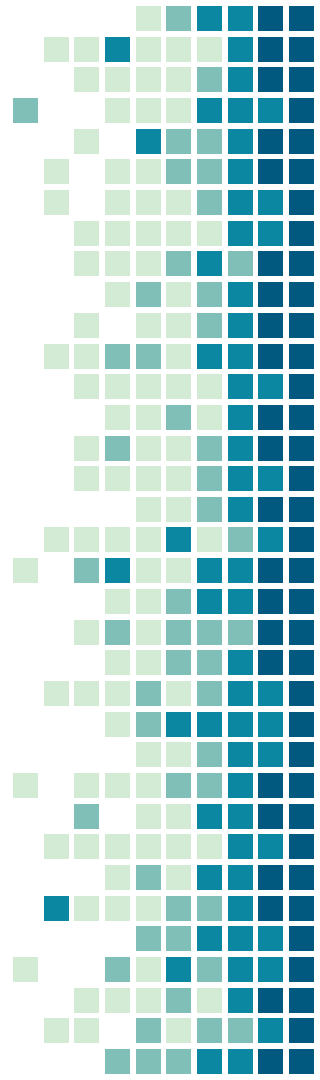


Firma digital

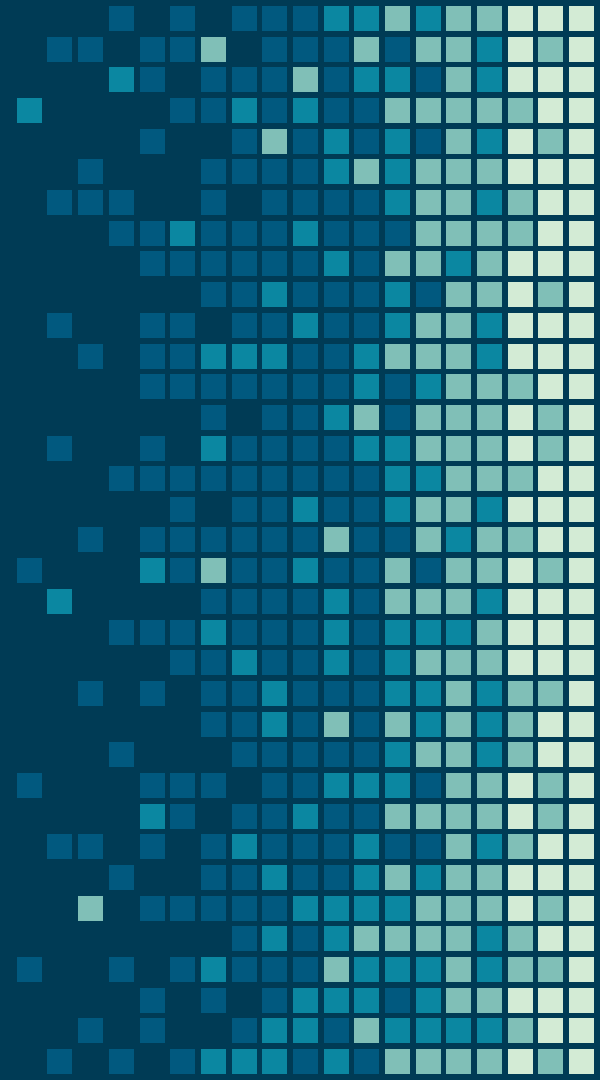
El receptor calcula el hash y utiliza la llave pública para verificar la firma.
Si el hash no coincide significa que algo cambió, el documento, la firma o ambas.
El algoritmo RSA es conmutativo por lo que se utiliza para este tipo de verificación.



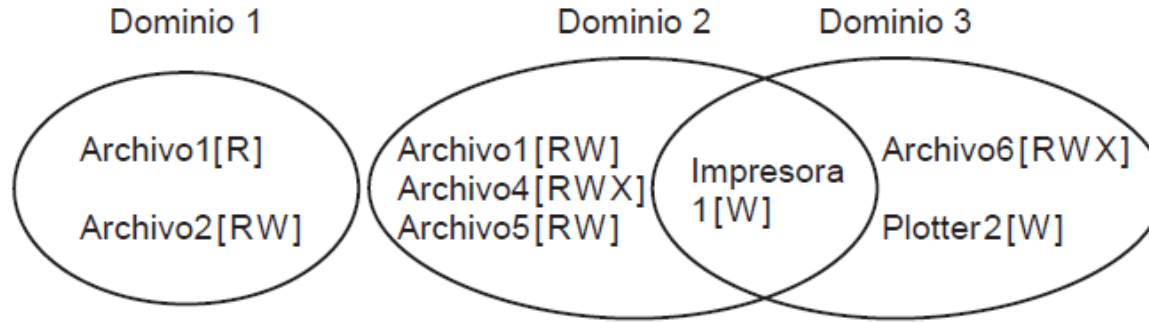
Cuando el documento llega al receptor ¿Qué sucede?



Mecanismos de protección



Dominios de protección



Un dominio es un conjunto de pares (objeto, permisos). Cada par especifica un objeto y cierto conjunto de operaciones que se pueden realizar en él.

- Se muestran tres dominios diferentes con algunos recursos en más de uno

Dominios de protección

- Una manera de implementar los dominios es por medio de una matriz.

		Objeto							
		Archivo1	Archivo2	Archivo3	Archivo4	Archivo5	Archivo6	Impresora1	Plotter2
Dominio	1	Lectura	Lectura Escritura						
	2			Lectura	Lectura Escritura Ejecución	Lectura Escritura		Escritura	
	3						Lectura Escritura Ejecución	Escritura	Escritura

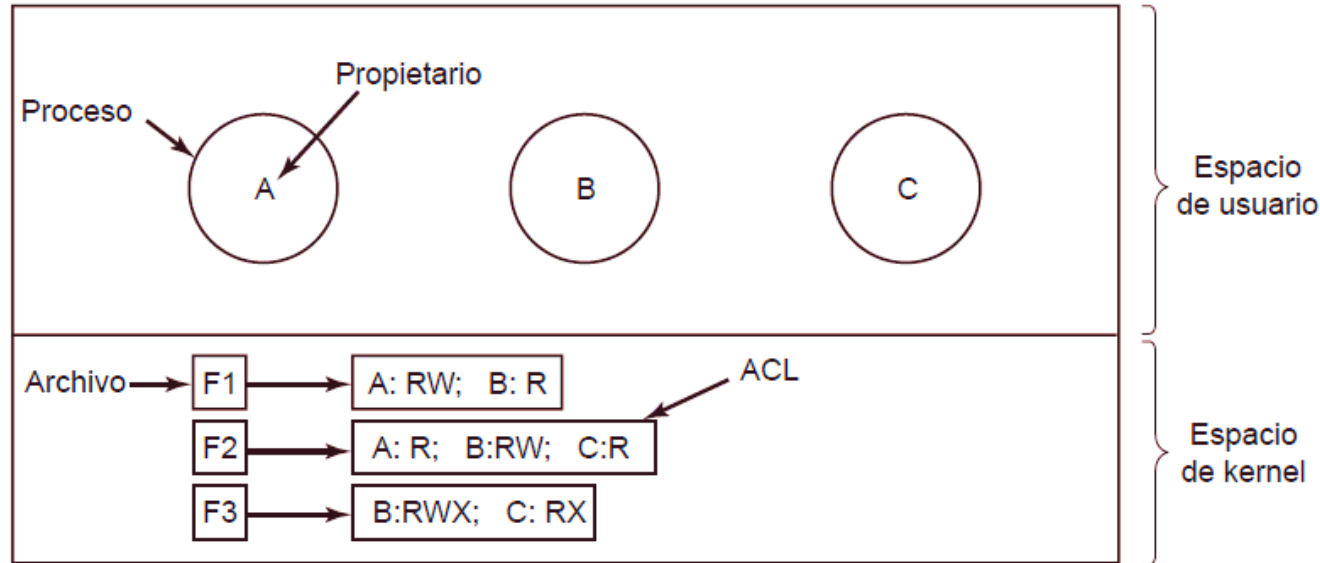


Listas de control de acceso

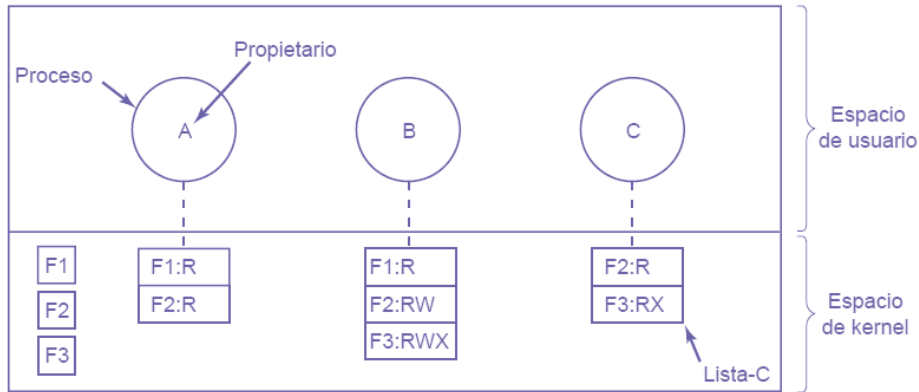
Tener una matriz con todo el mapeo es ineficiente por el hecho de que puede haber valor nulos. Una de las soluciones es almacenar los datos por fila o columna con sólo los valores no nulos. La idea fundamental es tener una lista ordenada que contenga todos los dominios que pueden acceder al objeto y la forma que lo hacen.



Listas de control de acceso

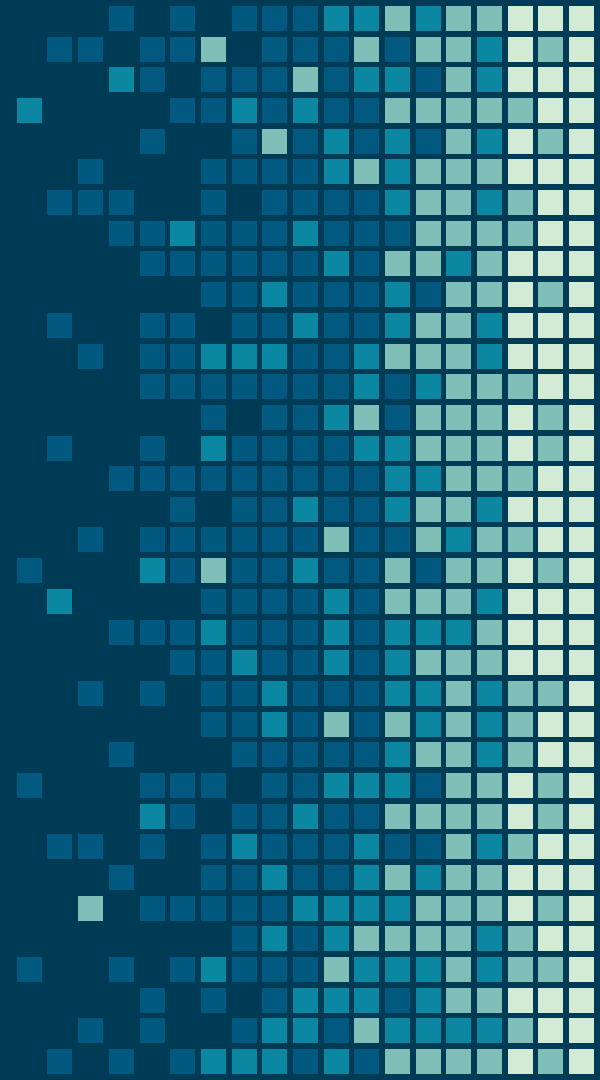


Capacidades



A cada proceso se le asocia una lista de objetos que puede utilizar, junto con una indicación de las operaciones permitidas en cada uno de ellos. A esta lista se le llama lista de capacidades o **lista-C**.

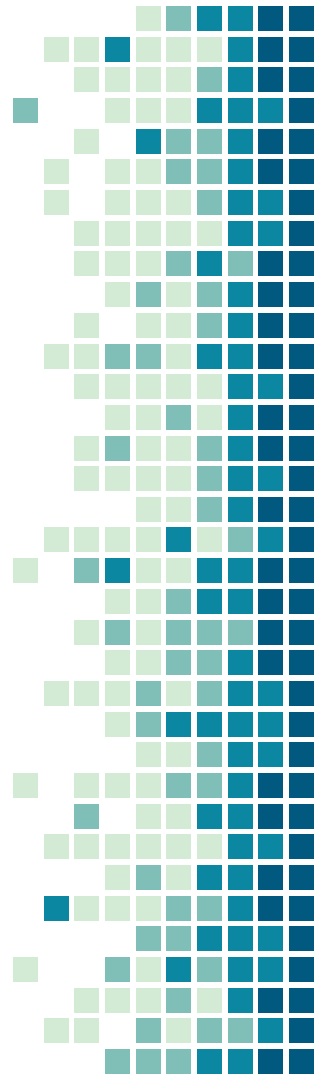
Autenticación



Autenticación

Todo sistema computacional debe requerir que todos los usuarios se autenticuen al momento de iniciar sesión. El sistema operativo no puede estar seguro de quién es el usuario, tampoco a los recursos que puede acceder.

¿Qué se hace para que el SO identifique al usuario ?



Autenticación por el uso de contraseñas



- Es la manera más simple de autenticación.
- Consiste en un nombre y contraseña.
- Se mantiene una lista de pares (usuario-contraseña).
- Si ambos coinciden el sistema proporciona el acceso.

Autenticación por el uso de objeto físico



- Consiste en verificar a los usuarios mediante un objeto físico que posean en lugar de lo que sepan.
- Generalmente son tarjetas que brindan acceso al sistema.

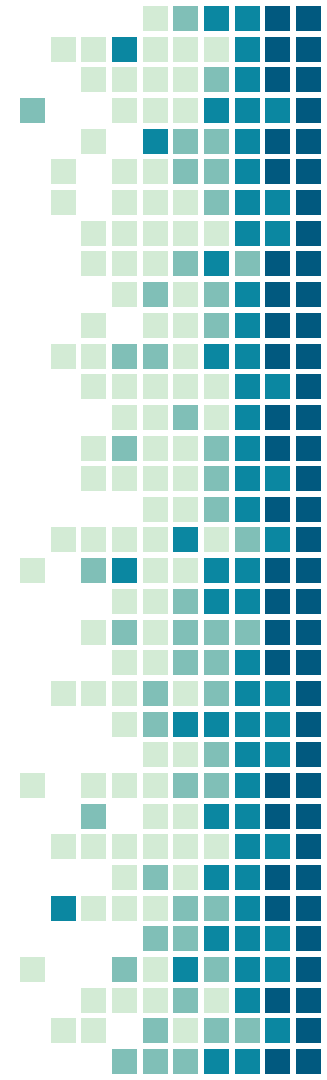
Autenticación por biométrica

- Consiste en autenticar por medio de características físicas del usuario.
- Por ejemplo huellas digitales, reconocimiento de voz o del iris del ojo.
- Los datos del usuario deben estar en el sistema para comprobar el acceso las demás veces en el mismo sistema.



Referencias

-▶ Tanenbaum, A. S. (2015). *Sistemas operativos modernos*. Pearson Educación.
-▶ Stallings, W. (1997). *Sistemas operativos*. Martin Iturbide.
-▶ CPerlman, R. (2005, December). *File system design with assured delete*. In *Third IEEE International Security in Storage Workshop (SISW'05)* (pp. 6-pp). IEEE.



¿Preguntas?

Realizado por: Jason Leitón Jiménez.

Tecnológico de Costa Rica

Ingeniería en Computadores

2024

TEC