Universidad del Rosario | Escuela de Ingeniería, Ciencia y Tecnología | MACC Matemáticas Aplicadas y Ciencias de la Computación | HINNT Hub de INNovación y Transferencia

Conceptos de ciberseguridad

Daniel Díaz-López

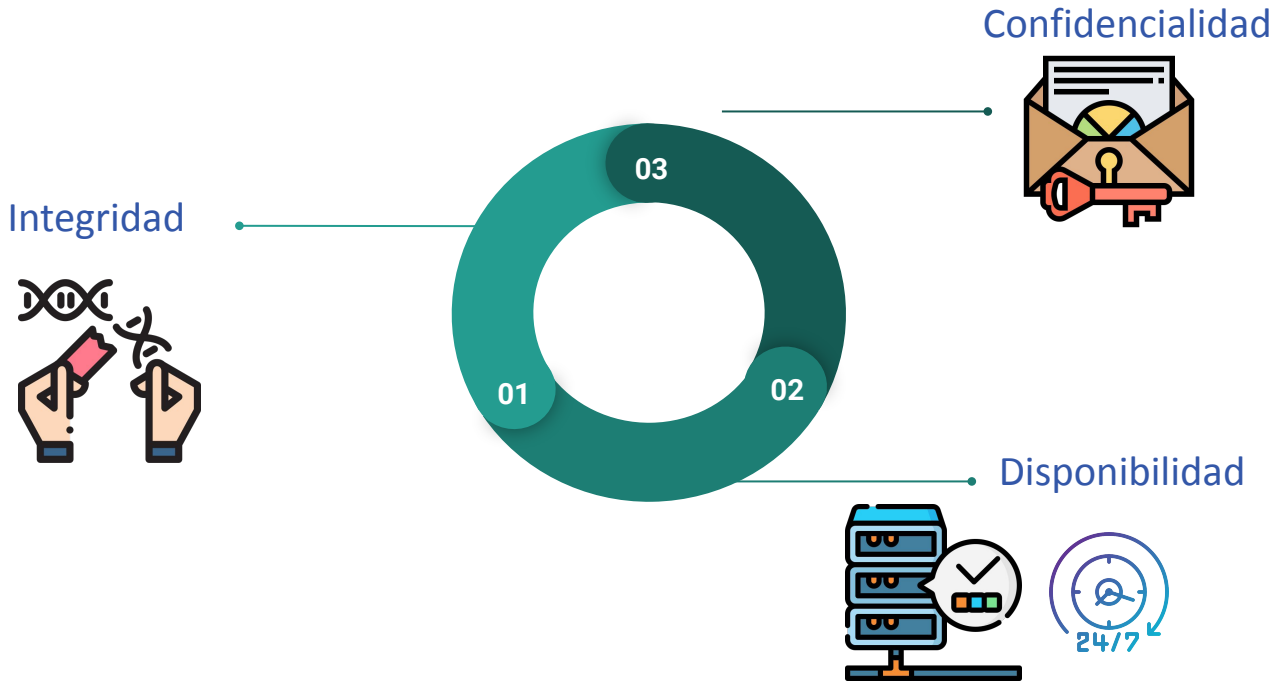
Líder de Ciberseguridad - MACC
Profesor principal de carrera

danielo.diaz@urosario.edu.co

@MACC_URosario | @MACC.URosario | macc_ur

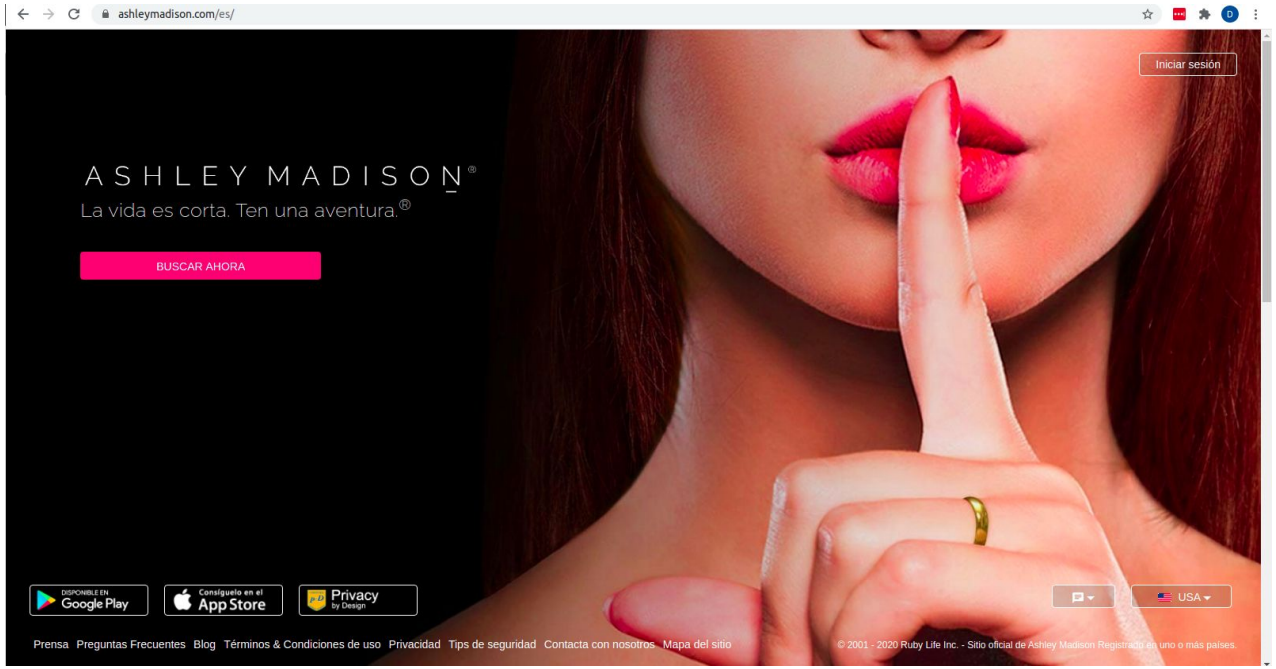
3 atributos claves

- Integridad: Protección de datos o sistemas de **modificación (reemplazo, adición)** no autorizada
- Disponibilidad: Protección de datos o sistemas frente a **disrupciones** en el acceso
- Confidencialidad: Protección de datos o sistemas de **acceso (lectura, visualización)** no autorizado



Confidencialidad

- Investigar sobre el caso de fuga de datos del portal Ashley Madison del 2015:
  - https://en.wikipedia.org/wiki/Ashley_Madison_data_breach
  - https://digitalguardian.com/blog/timeline-ashley-madison-hack
  - https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/
  - Otros disponibles en la web
- Q: ¿Qué tipos de datos que fueron expuestos?
- Q: ¿Como se logró la exfiltración de datos?
- Q: ¿Qué mecanismo(s) pudo haberse implementado para evitar la fuga de datos?



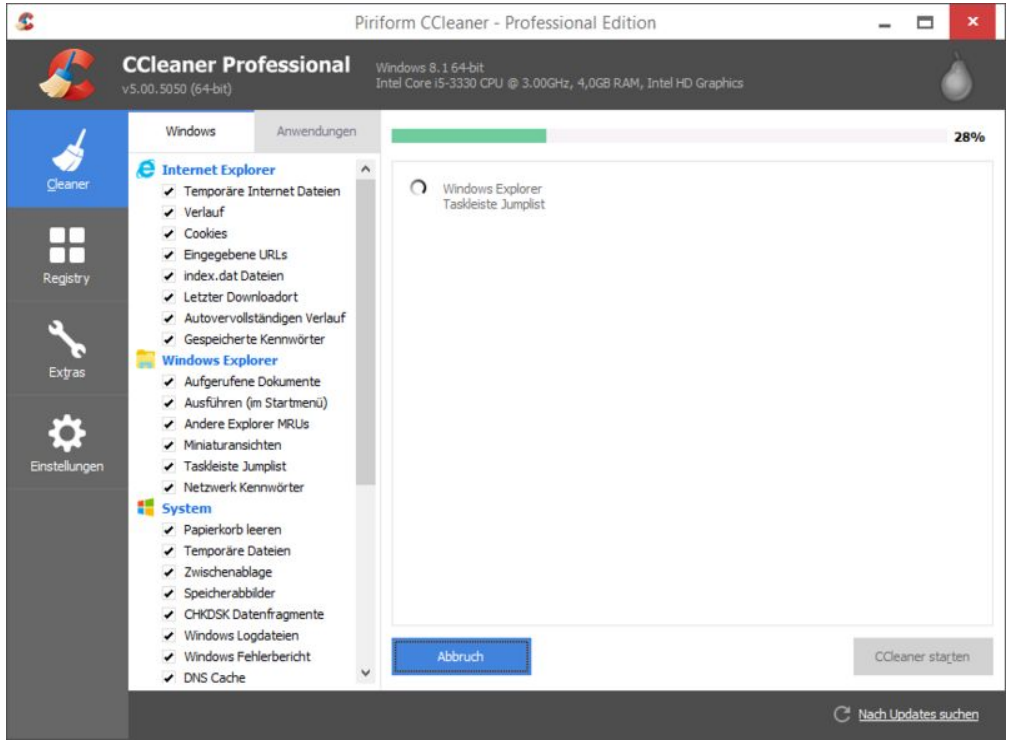
Confidencialidad

Pregunta de selección múltiple de validación de entendimiento del caso.

En el caso de Ashley Madison estudiado previamente puede verse la confidencialidad como (1 o más respuestas válidas):

a. Un atributo de los datos el cual fue afectado severamente debido a la no existencia de controles de seguridad adecuados.
b. Un atributo de los datos que hay que proteger sobre todo cuando se trata de información personal.
c. Un atributo de los datos que puede ser un diferencial en el momento de selección de una empresa proveedora de servicios por parte de un cliente.
d. Un atributo de los datos que se refiere a que estos no sean vistos por alguien no autorizado.

Integridad



- Leer el caso intrusión y modificación no autorizada de productos de AVAST:
  - https://www.forbes.com/sites/thomasbrewster/2019/10/21/avast-hacked-again-as-spies-steal-its-passwords/?sh=627d81206596
  - Otros disponibles en la web
- Q: ¿Cuál era el objetivo final del atacante?
- Q: ¿Cómo se logró la modificación de los datos o servicios?
- Q: ¿Qué mecanismo(s) pudo haberse implementado para evitar la intrusión y la modificación no autorizada?

Integridad

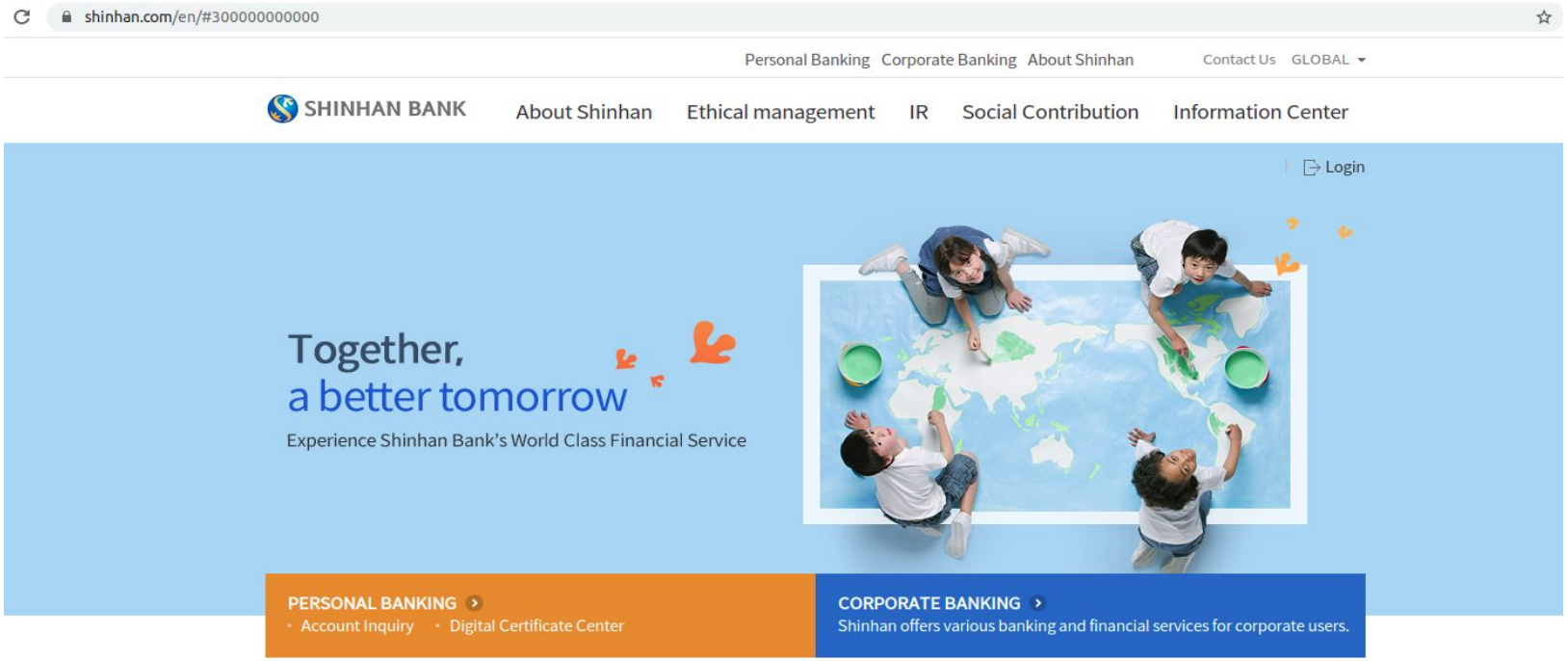
Pregunta de selección múltiple de validación de entendimiento del caso.

En el caso de CCleaner estudiado previamente cuál fue el objetivo más probable del atacante (1 o más respuestas válidas):

a. Implantar código malicioso dentro del código fuente del aplicativo CCleaner con el objetivo de que cada persona que descargue CCleaner también descargue el código malicioso y se infecte.
b. Eliminar el código fuente de CCleaner para causar un impacto operativo a Avast.
c. Ingresar de manera no autorizada a la red de Avast para copiar secretos comerciales.
d. Comprobar que una empresa de seguridad no está exenta de tener vulnerabilidades.

Disponibilidad

- Leer el caso intrusión y eliminación no autorizada de datos bancarios
  - https://www.seeker.com/massive-data-deleting-attack-hits-south-korea-1767326593.html
  - Otros disponibles en la web
- Q: ¿Cuál era el objetivo final del atacante?
- Q: ¿Cómo se logró la eliminación de los datos o servicios
- Q: ¿Qué mecanismo(s) pudo haberse implementado para evitar la eliminación no autorizada de datos?



Disponibilidad

Pregunta de selección múltiple de validación de entendimiento del caso.

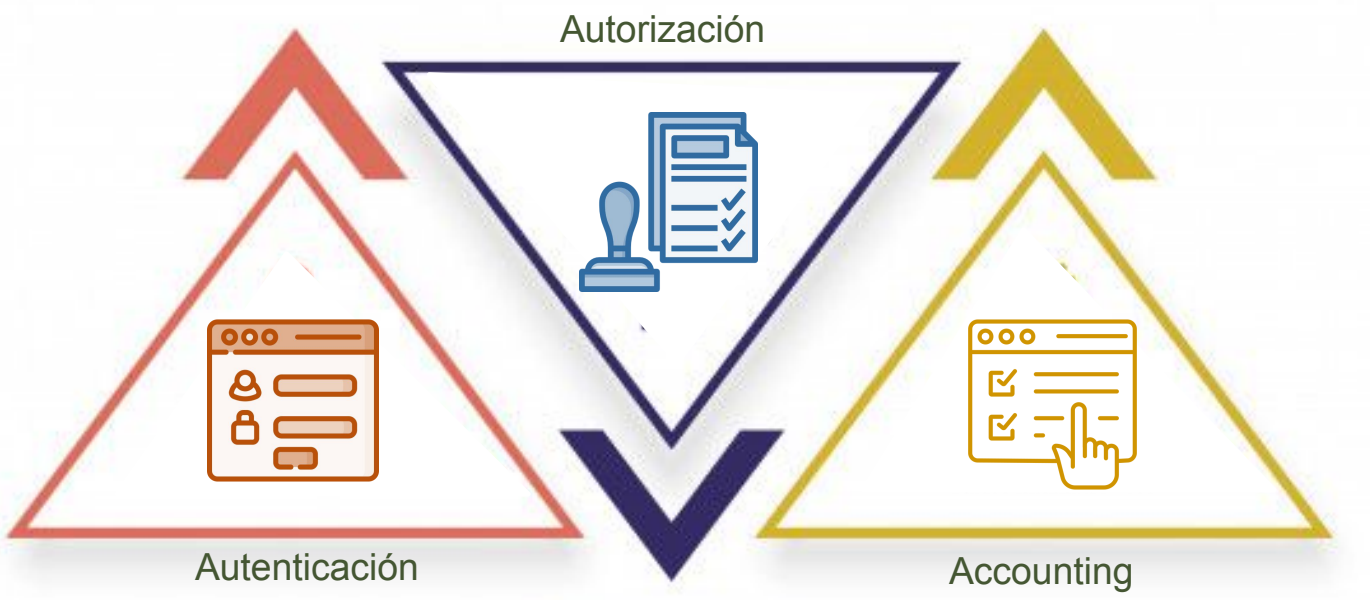
En el caso de Shinhan Bank estudiado previamente cuál fue el vector de entrada más probable utilizado por el atacante (1 o más respuestas válidas):

a. Explotación de una vulnerabilidad en el portal web de Shinhan Bank que permitió afectar el sistema operativo de las máquinas corporativas.
b. Equipos corporativos que hacían parte de una botnet y a través de los cuales fue posible la eliminación de archivos de sistema operativo.
c. Inserción de una USB infectada por parte de uno de los empleados, a través de la cual se realizó la implantación de un malware de corrupción del sistema operativo.

Obtener una copia del “2021 Verizon Data Breach Investigation Report” desde el siguiente link: https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf

Después de haber entendido los conceptos de Autenticación, Autorización y Accounting de slides 10-28 responder las siguientes preguntas:

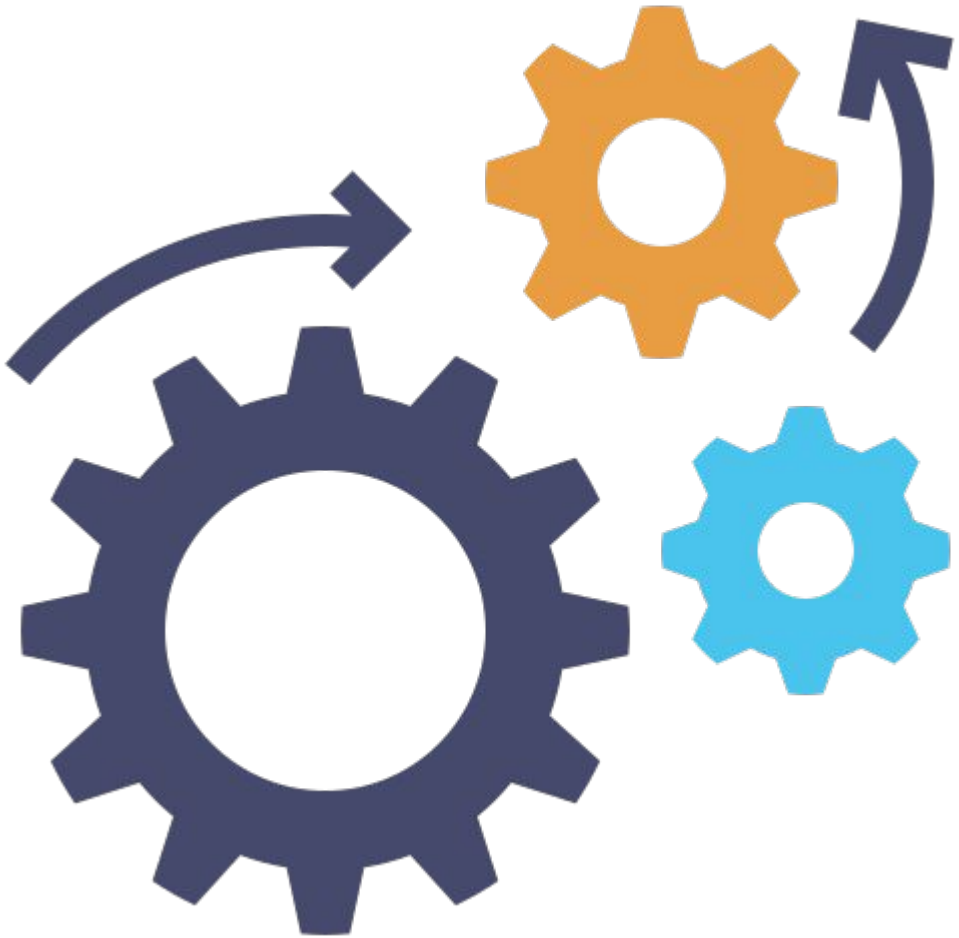
- Q: En la sección IV, identifica la ficha para el sector de la industria en el que trabajas. Identificar los patrones de incidentes más comunes, actores, motivaciones, tipos de datos comprometidos, top de controles de seguridad. Realiza un resumen para tu sector.
- Q: ¿Cómo puede ayudar la autenticación, autorización y accounting a incrementar la seguridad en el sector escogido previamente?
- Q: ¿Cuál de los 11 sectores no tiene control de acceso como parte de su “Top IG1 Protective Controls”?



3 atributos claves

- Autenticación: Validación de la identidad de un usuario o proceso
- Autorización: Validación de los permisos otorgados a un usuario o proceso
- Accounting: Registro de la actividad de un usuario o proceso.

Authorization
What can the user do and
does he have the authority?



Authentication
Who is the user and
does he have valid
credentials?

Auditing
What did the user do and
is it being recorded?

Authentication

e-authentication

Process of establishing confidence in user identities electronically in an information system

Authenticator Management

Processes and procedures for issuing and revoking **authenticators**. It applies to Hw and SW

Identity Management

It defines the process used to identify individuals before granting access to systems, facilities, and resources

- Passwords
- Tokens
- biometrics
- Public key infrastructure (PKI) certificates
- key cards
- Others

Authentication

The CISO should select the number of factors according to **data sensitivity** and **confidence required**:

- **Single-factor authentication** maps an authenticator (usually a password) to an account and facilitates authentication.
  - It is inexpensive but it may be weak depending on the length and the complexity of the password
  - A long password has more entropy, which reduce the predictability

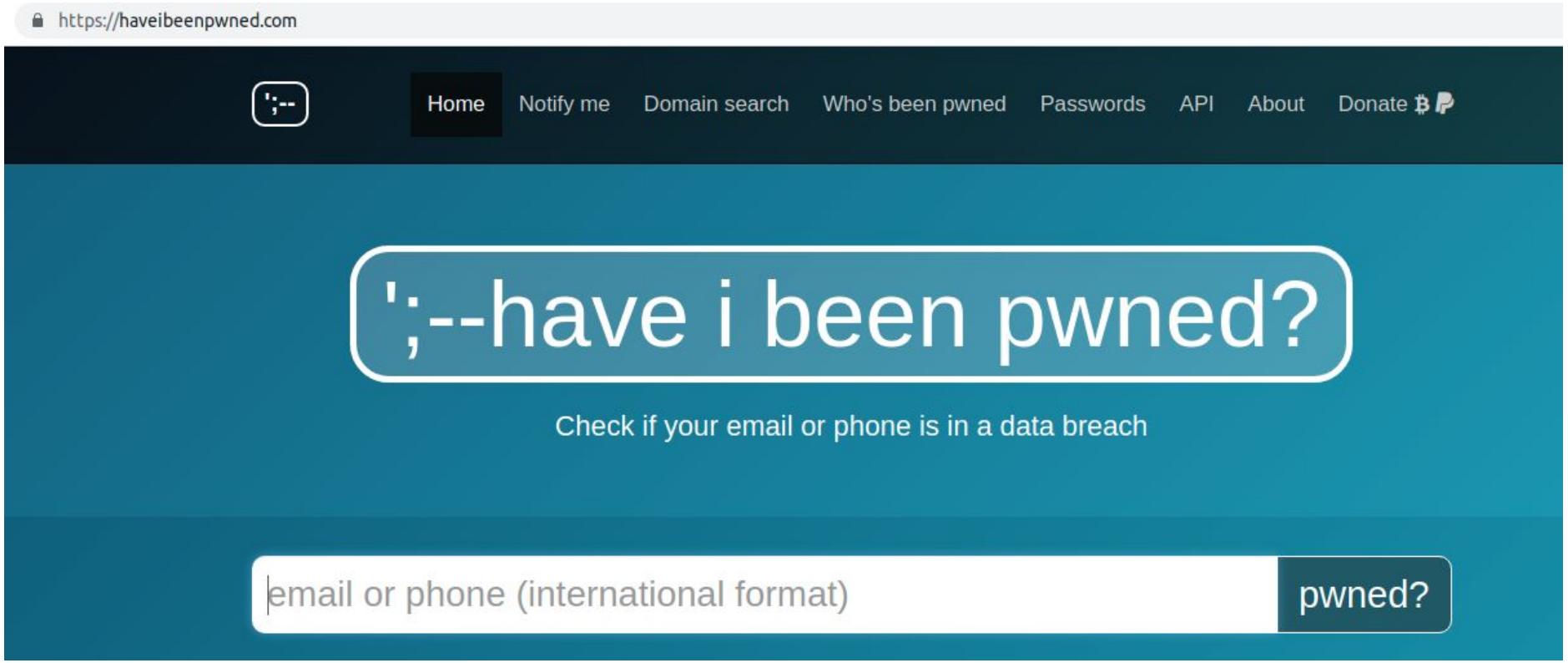
$$E = \log_2\left(R^L\right)$$

where E = password entropy, R = pool of unique characters,
and L = number of characters in your password.
Then R^L = the number of possible passwords and
$\log_2\left(R^L\right)$ = the number of bits of entropy.

  - Calculate the entropy of your password:
    - https://www.omnicalculator.com/other/password-entropy
  - *"For non-vital accounts, 25-30 bits of entropy are enough. For more important accounts, aim for 60-80 bits of entropy, up to 100 for crucial ones."*

Authentication

- Even if you force your users to have a good entropy there are human factors that limit the effectiveness of a long password because:
    - Users often **reuse corporate passwords** for authentication on social networking platforms and in other places that may have weaker controls.
        - Find out if some of your account have been hacked:



Authentication

- Even if you force your users to have a good entropy there are human factors that limit the effectiveness of a long password because:
    - Users often select passwords that are **easy to remember** and may be easy to determine using standard password-cracking techniques.

Dictionaries of words per language:

- https://github.com/CSL-LABS/CrackingWordLists
- https://github.com/danielmiessler/SecLists/tree/master/Passwords

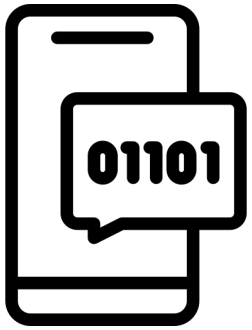
Authentication

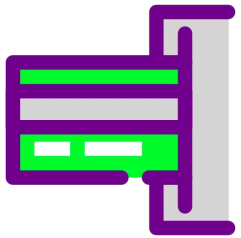
The CISO should select the number of factors according to **data sensitivity** and **confidence required**:

- **Multifactor authentication** increases the likelihood that the system can accurately confirm the identity of a user. This strategy combines: something you know + something you have + something you are.
- It increase costs, so a balance is required!

https://lastpass.com/

Password with good entropy, or PIN





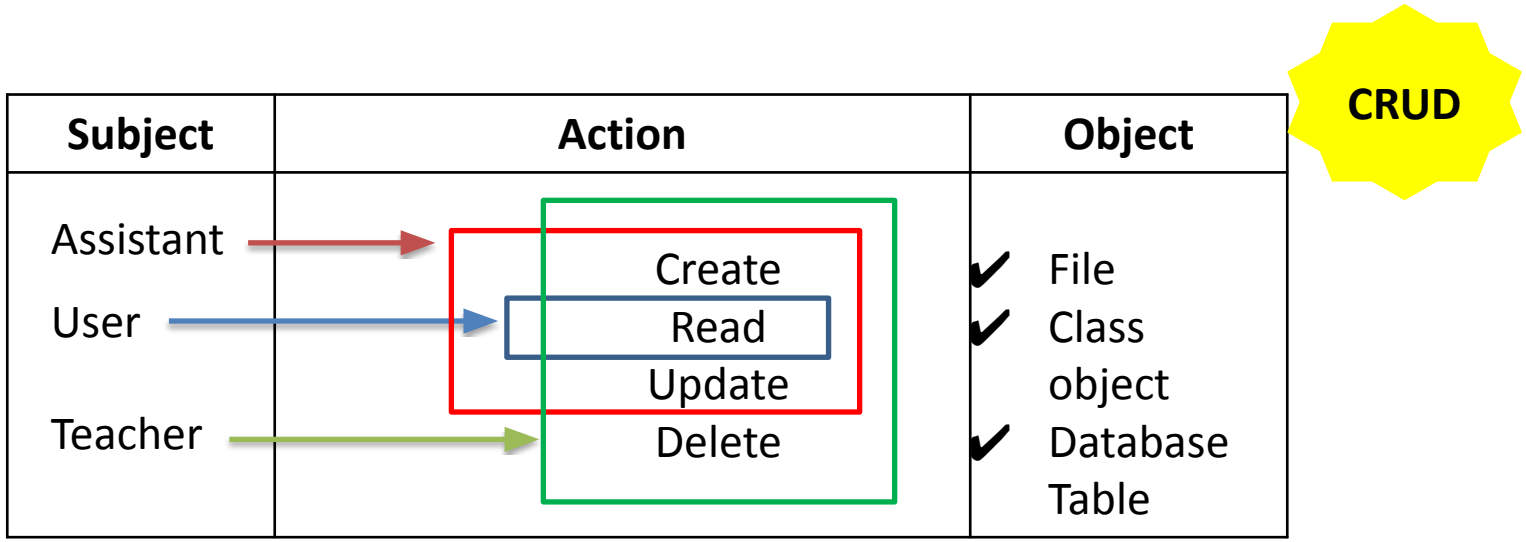
Hardware or software token

Biometric element

- For example, physical tokens that combine a one-time password with a personal identification number (PIN) increase confidence in the identity of the user.

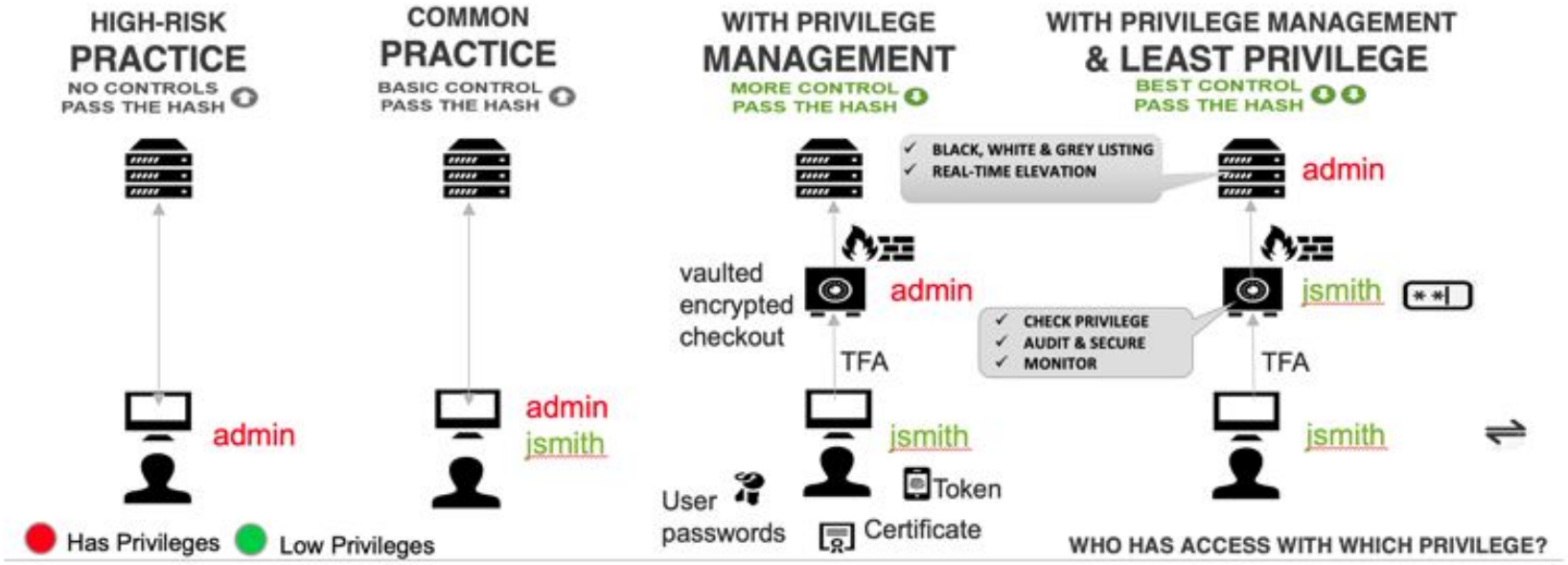
Autorización:

- Los permisos otorgados a un usuario o proceso deben ser otorgados por el propietario de los datos o del sistema de acuerdo a una política de acceso.



Autorización:

- **Least privilege principle** states that
  - Individuals or systems should only have the minimum access/permissions necessary to perform specific activities required for their job.
  - It ensures that what can be done with the information (read, change, delete, or execute) is limited to the least amount of access necessary to perform those actions.



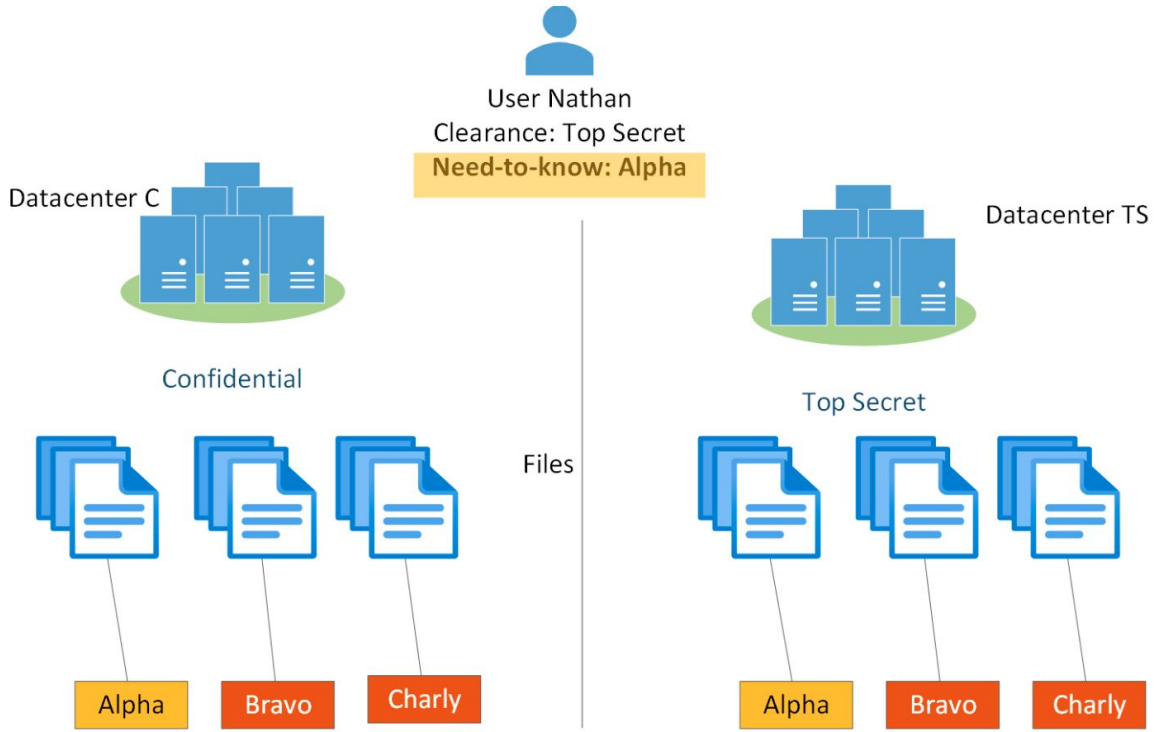
https://thycotic.com/glossary/least-privilege/

Once you have audited the environment you can start to remove or reduce privileges from users who no longer require them.

For those who actively require them, you can replace privileges with policies that allow the task to be elevated **on demand** without the user becoming over-privileged.

Autorización:

- **Need to know principle** states that
  - Access to systems should only be granted to individuals with a legitimate need to know the information contained within those systems.
  - The access is provided according to the minimum amount of information that is necessary to perform the task.
  - Highly classified information may also require elevated security clearances to access information

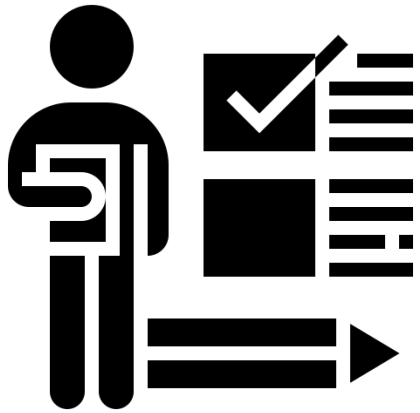


Just because Nathan has a Top Secret clearance, does not mean he can see Top Secret data.

He must have a Need-to-know. Otherwise, all such data would be redacted.

Accounting:

- La actividad de los usuarios o procesos generalmente se registra en logs.
- No todas las actividades tienen que ser registradas, solo aquellas que sean importantes en función de la criticidad de los datos sobre los cuáles están siendo aplicadas.
- Los logs deben tener un periodo de retención definido, de lo contrario sería muy costoso su almacenamiento.
- Los logs ayudan a garantizar el “no repudio” por parte de un usuario.



“It is not just logs, it is evidence”

Accounting:

- CISOs should NOT assume authenticated and authorized users will behave or use information in a proper manner.

- The following outlines the **minimum** level of user account auditing:
  - Failed data accesses when an authorized system or person user tries to access restricted information.
  - Privilege use performing create, read, update, or delete (CRUD Security Matrix) activities.

4	Permission Groups - Security Roles	Application Administrator	Application Author	Application Deployment Manager	Asset Manager	Company Resource Access Manager <R2>	Compliance Settings Manager	Endpoint Protection Manager	Full Administrator	Infrastructure Administrator	Operating System Deployment Manager	Operations Administrator	Read-only Analyst	Remote Tools Operator	Security Administrator	Software Update Manager	Permission Groups - Permissions
5	Alert Subscription						X	X			X	X					Alert Subscription
6	Alerts	X	X	X		X	X	X	X	X	X	X	X			X	Alerts
7	Antimalware Policy							X	X			X	X				Antimalware Policy
8	Application	X	X	X					X		X	X	X				Application
9	Boot Image Package								X		X	X	X				Boot Image Package
10	Boundaries	X	X	X					X	X	X	X	X			X	Boundaries
11	Boundary Group	X	X	X					X	X	X	X	X			X	Boundary Group
12	Certificate Profile <R2>					X			X			X	X				Certificate Profile <R2>
13	Client Agent Setting	X		X	X				X	X		X	X			X	Client Agent Setting
14	Cloud Subscription								X	X		X	X				Cloud Subscription
15	Collection	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	Collection
16	Communications Provisioning Profile <R2>					X			X			X	X				Communications Provisioning Profile <R2>
17	Computer Association								X		X	X	X				Computer Association
18	Configuration Item						X		X			X	X				Configuration Item
19	Configuration Policy					X	X	X	X			X	X				Configuration Policy
20	Deployment Templates	X		X					X			X	X			X	Deployment Templates
21	Device Drivers								X		X	X	X				Device Drivers
22	Distribution Point	X	X	X					X	X	X	X	X			X	Distribution Point
23	Distribution Point Group	X	X	X					X	X	X	X	X			X	Distribution Point Group
24	Driver Package								X		X	X	X				Driver Package
25	Firewall Settings							X	X			X	X				Firewall Settings
26	Global Condition	X	X	X					X			X	X				Global Condition
27	Inventory Reports				X				X	X		X	X				Inventory Reports
28	Migration Job								X	X		X	X				Migration Job
29	Migration Site-to-Site Mappings								X	X		X	X				Migration Site-to-Site Mappings
30	Mobile Device Enrollment Profiles	X		X	X				X	X		X	X				Mobile Device Enrollment Profiles
31	Operating System Image								X		X	X	X				Operating System Image
32	Operating System Installation Package								X		X	X	X				Operating System Installation Package

Matrix of Role-Based Administration (RBA) Permissions for Microsoft System Center ConfigMgr

Accounting:

These behaviors should be recorded within an access audit system

When user account audits are performed, the following should be reviewed

User logged on in from more than one location simultaneously
Sign-ins while users are on vacation, sick leave, or otherwise absent from work
Inappropriate access attempts for job responsibilities
User access lapses of more than 30 days
Suspicious patterns of accesses
Suspicious time and day access
Other?

To ensure that you are auditing user activity that makes sense and not simply creating abnormally large log files, create an **Audit Policy**

Autenticación - Autorización - Accounting

Pregunta de selección múltiple.

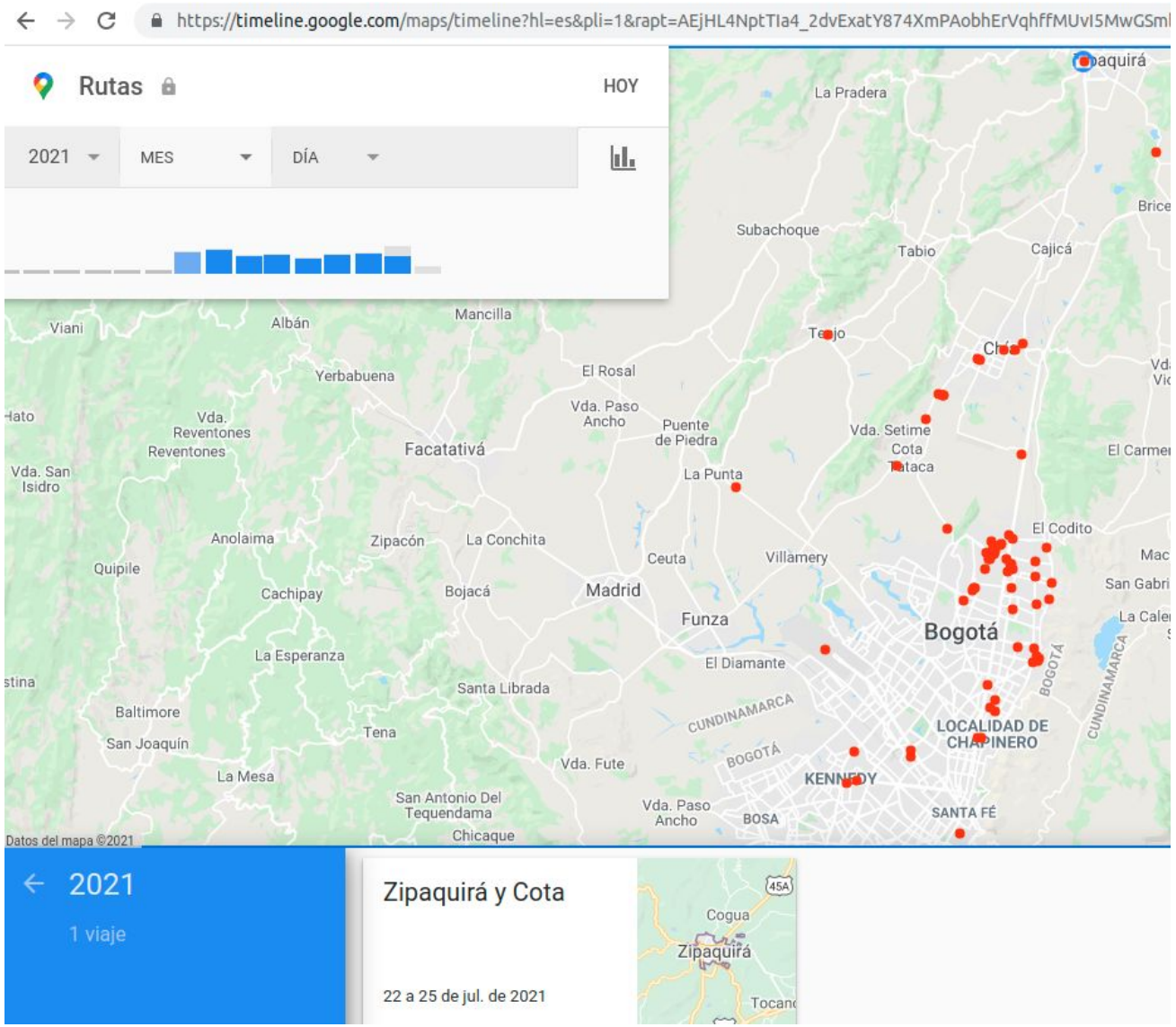
Una empresa tiene un sistema de telefonía corporativo que permite que cada empleado pueda llamar a números de teléfono local, internacional, celular y números especiales, en función de su cargo dentro de la empresa. Recientemente se ha evidenciado que desde la cuenta de uno de los empleados se han realizado múltiples llamadas internacionales a pesar de que dicho usuario no tenía permisos para realizar dichas llamadas. ¿Cuál de los siguientes módulos del sistema de telefonía probablemente fué la causa del fallo? (1 o más respuestas válidas):

a. Módulo de autenticación
b. Módulo de autorización
c. Módulo de Accounting

User as element of monitoring:

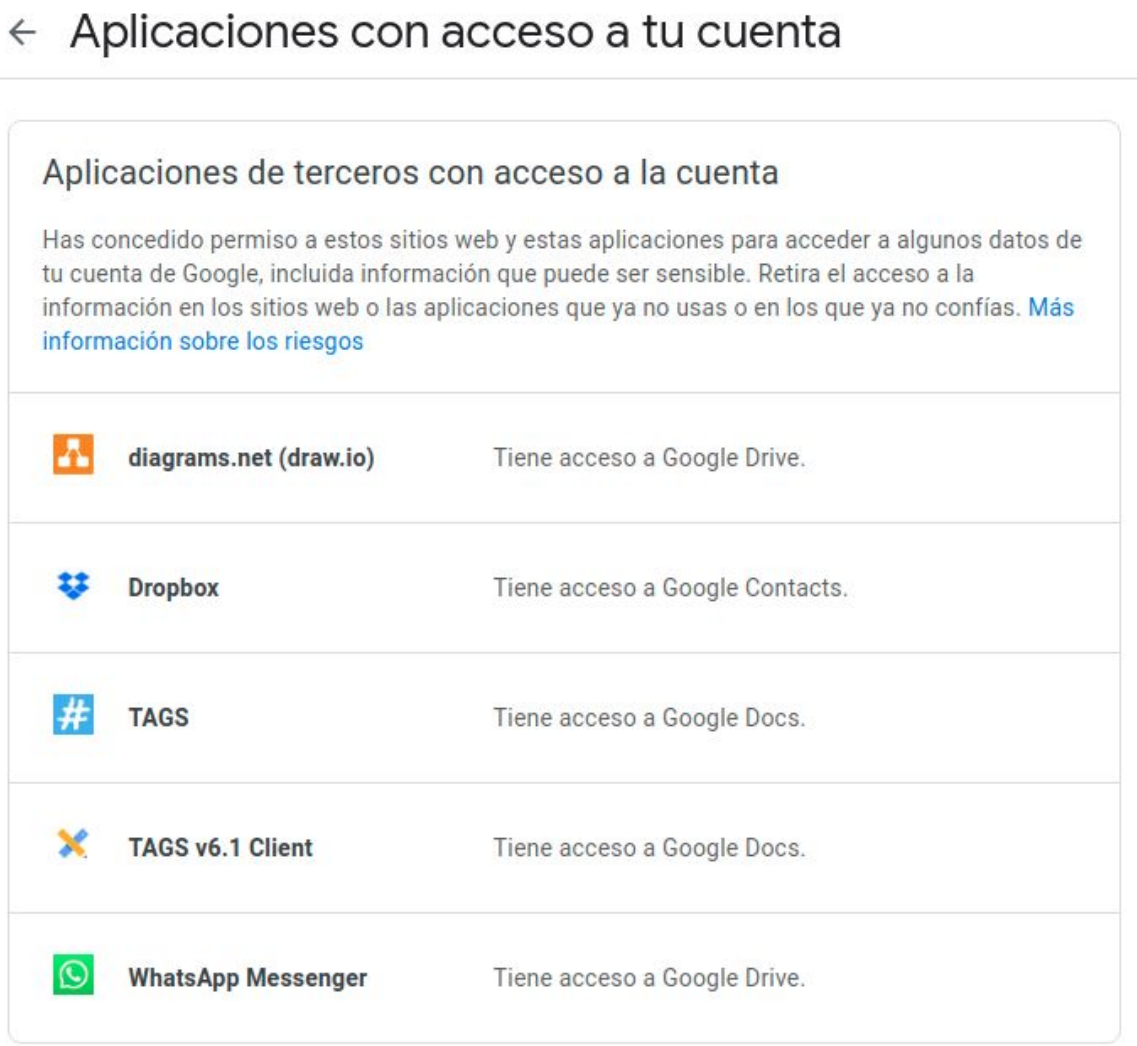
- Users can be instrumental in reporting or preventing potential system abuse if they have the right tools to report them.

- Access control systems should provide users with a notification of the following:
    - **Last sign in:** Notifying the end user of the last sign in
    - **Locations**



User as element of monitoring:

- **Unsuccessful sign ins:** Limiting the number of unsuccessful sign in attempts by a user during a specific period. A common mobile device control is to erase information if a certain number of sign ins have been attempted.
- **Concurrent sessions:** Additional sessions using the same credentials might be an indication of malicious behavior or a compromised account.
- **Applications with access to the user account**



Behavior management

- **Separation of duties:** Divides the responsibilities associated with an action or process to decrease the opportunity for misbehavior or policy violations through collusion. As more individuals become involved in a process, it becomes less likely that all parties will agree to the malicious or inappropriate action.
    - For example, personnel who implement controls should not audit the controls for effectiveness.

- **Banners** that notify the user they are accessing a confidential system and, if they access this system, that they may be subject to monitoring and audits within the system.
    - Notices often include the right to pursue criminal prosecution or impart civil penalties if the individual should not access the system or inappropriately use it. Users are requested to accept these conditions before gaining access.

Universidad del Rosario | Escuela de Ingeniería, Ciencia y Tecnología | MACC Matemáticas Aplicadas y Ciencias de la Computación | HINNT Hub de INNovación y Transferencia

GRACIAS

Daniel Díaz-López

Líder de Ciberseguridad - MACC
Profesor principal de carrera

danielo.diaz@urosario.edu.co

@MACC_URosario @MACC.URosario macc_ur