MI 2021/2022 1.

Detect security and state and describe the basic requirements.

Security is a continuous process, the implementation of which ensures a certain state (of the system and/or data/information). The desired state is defined by certain requirements. When they are fulfilled, then we say that the system is safe, otherwise we say that an incident has occurred, i.e. that security has been violated.

The basic requirements are: Secrecy/Confidentiality (protection of secret information from attacks), Completeness/Integrity (protection against unauthorized changes), Availability (protection against denial of information availability to authorized users)

2. State the division of controls into groups and for each group, state several specific examples of controls.

Physical: cameras, security guards, armored doors,

Technical: cryptography, firewalls, attack detection systems, Administrative

controls: policies, regulations, various regulations by which we define what it means to be safe, how people must behave, how devices must be configured...

3. List the organizational factors that affect the security of the information system.

Organizational factors: Lack of budget, Short deadlines, Lack of management support, Lack of adequate risk assessment, Lack of security procedures

4. Why are systematic and operational records important and what should be done to make them safe and usable?

Because they enable the reconstruction of events and the detection of unexpected events. It is necessary to keep them in a separate place to prevent unauthorized changes. The CISO defines the way of managing system and operational records: it supervises, and in smaller organizations it is possible to analyze logs and request statements. Today's trend is for companies to monitor security in Security Operation Centers (SOC), which continuously monitor, improve the security situation and prevent, detect all security incidents.

5. What is the basic tool that the CISO uses for his work and why (what enables him)?

Risk management (process prescribed by internal acts). It allows to determine the risks to which the organization is exposed. This includes risk assessment, the possibility of risk prioritization, and based on this, the decision to approach the identified risks (whether to accept, master or transfer to a third party, but the organization's management has the final say in this decision).

6. The user *adminbp* created the *nastavabp* database **in the PostgreSQL system and created the following tables in the specified database: *student* and *exam* (with some attributes). The *adminbp*** user **revoked the user PUBLIC's permission to connect to the *nastavabp*** database **and all permissions for the public scheme in *nastavabp,* and then created the new user . Write the commands that *adminbp* will allow the user *novak*** to do **the following:** a) Connect to the *teaching* database and use the schema public and *teachingbp:* GRANT CONNECT ON DATABASE teachingbp TO novak; GRANT USAGE ON SCHEMA public TO novice; GRANT USAGE ON SCHEMA public TO novice; b) Review of all data in the *student* table except the address, with the fact that the *newbie* can assign this permission to others users:

GRANT SELECT(matBr, name, prez, pbr) ON student TO novice WITH GRANT OPTION; c) Review, entry, modification and deletion of all data in the *exam* table :

GRANT SELECT, INSERT, UPDATE, DELETE ON exam TO novice;

d) Modification of all data in the *student table,* but only for those n-tuples that refer to students from Zadar (postal code = 2300):

```
CREATE VIEW maintained AS
   SELECT * FROM student WHERE pbr = 2300 WITH CHECK OPTION;
GRANT UPDATE on grantee TO novice; e)
```

Using the already created *teacher role:* GRANT teacher TO novice; **7. The Bell-la Padula model (BLP)**

belongs to which access management?: a) discretionary access management, **b) mandated access management,** c) role-based access management

8. What does a typical file record contain for remembering the user's work (auditing)?

The SQL command being executed, the place from which the request was sent (terminal, IP address of the computer), the identifier of the user who initiated the operation, the date and time of the operation, n-tuples, the attributes to which the request refers, the old value of the n-tuple, the new n-tuple value **9. What do stored procedures enable in the enforcement of security policy, which cannot be solved only by table and virtual table permissions? Write a command that will** enable the ***novice*** user **to use the *calculate procedure.***

It enables the protection of data against unauthorized use at the function level.

```
GRANT EXECUTE ON calculate TO novice
```

10. Explain the strong-star-property principle of the mandated access policy in databases.
The user can write exclusively at his level, it is not possible to write to objects that can be read by entities with a lower level - information leakage is prevented.