Process of notifying, managing and responding to security incidents

Security incident is understood to be any breach of the regulations developed in the Security Document, as well as any anomaly affecting the security of the personal data of Kube Group.

Some examples of incidents are: computer system failures allowing the access to personal data to unauthorized persons; unauthorized attempt of the exit of a document or support; loss of data or destruction of IT supports; change of physical location of databases; knowledge of passwords by unauthorized persons; modification of data by unauthorized persons, etc.

The procedure for notifying security incidents is as follow:

- Any user becoming aware of an incident that affects or could affect the confidentiality and integrity of the protected personal data of Kube, should notify the security manager immediately by email to help@kube.group.
- This notification must describe in detail the type, date and time of the incident, the person signing the notification and the identification of any person related to the incident, if any, and the effects of the incident.
- Once the incident is reported, he will receive an acknowledgment of receipt from the security manager.

Registry of incidents, in charge of the security manager, will be computerized and will include the type of incident, date and time of the incident or the time of its detection, the person making the notification, the person communicating the incidence, the effects that may have occurred and the corrective measures applied.

If it is necessary to perform a data recovery procedure, the incident log will record this procedure, which must include the person executing the process, the restored data and, where appropriate, what data has been necessary to manually record in the process of recovery.

INCIDENT NOTIFICATION FORM

INCIDENT Nº (to be filled by the security manager) Notification Date:
Incident Date: Incident Time:
Incident Type:
Incident Description:
Incident Effects:
Persons related to the incident (if any):
Corrective measures:
Recovery Data (if needed) Process: Restored Data: Data manually recorded: Person making the recovery:
Signature of the person responsible for the file
Person making the notification: