

**1. Report Event (All Users)**

Report the event by those who identified it, via Addvolt Jira.

**2. Incident/Action needed? (ISO)**

If it is an incident, register in Addvolt Jira platform to analyze incident and implication at the level of the ISMS

If there is a need for control measures, proceed to point (3), otherwise the incident report is closed.

**3. Immediate Control Measures (ISO)**

Implement and spread the needed control measures.

**4. Risk Situation Fault? (ISO)**

Check existence Failure risk situation – (threat contemplated in the risk endorsement matrix)

If yes, the risk matrix must be reviewed with the resulted information and proceed to point (5).

If there's no risk situation fault, proceed to Root Cause Analysis of the incident.

**5. Root Cause Analysis (ISMS Team)**

A root cause analysis must be performed by the ISMS Team in order to identify all the root causes and define future action and responsibilities for their implementation.

Perform actions follow up until their implementation.

**6. Effective Actions ?(ISO)**

Validate the ineffectiveness of the implemented actions to guarantee the incident resolution:

If they are effective the incident is closed.

If they are not effective the root cause of the incident must be analysed again until the effectiveness of the actions.

**Note:** Beside the information present on this procedure, more detailed information related to the Incident Management can be consulted into **Confluence Data base - Management Documents/Incident Recovery**

**Creation Date:**  
30/08/2024

**Revision Date:**  
30/08/2024

**Macro Process:** 02 - Integrated Management System  
**Process:** 02 4 - Information Security Management System  
**Procedure:** P 02 4 40 - Incident Management

**Creator:**  
C.Santos

**Approver:**  
M.Sousa