Análise e Gestão de Risco em Segurança Informática 2024/25

Project

This project consists of **the risk assessment** and an initial **incident response plan** for PowerPlus, the study scenario presented in class. The result to be delivered is a report addressed to the Information Security and IT Risk Management. The document must have a maximum of 30 pages (excluding cover and table of contents). All attachments supporting the results presented, e.g., spreadsheet(s) must be submitted. The project should be carried out in groups of three to four elements.

The report should contain the following chapters (or others with similar content): *Introduction*, *Establishing the Context*, *Risk Assessment*, *Incident Scenarios*, *SOC Preparation*, *Conclusions*, and *References*. Additional chapters and annexes, e.g. *Treatment Proposal*, may be included. The chapter "*Risk Assessment*" shall present the results of the various stages of risk assessment according to ISO/IEC 27005:2022 (ISO/IEC, 2022). The eight most important types of risk should be identified. If deemed appropriate, concrete controls may be proposed for each identified risk. In the chapter "*Incident Scenarios*", three attack scenarios should be conceptualised. The " *SOC Preparation*" chapter should describe the aspects to be monitored by PowerPlus's SOC and describe in detail three incident response cases.

As we do not have access to all data on PowerPlus, the assessment of risks and conception of incident scenarios should consider the information provided and the options revealed to be appropriate, which should be justified.

References should be used to support the methodology and options. In particular, the concepts and processes in ISO/IEC 27005:2022 (ISO/IEC, 2022), ISO/IEC 27001:2022 (ISO/IEC, 2022), and ISO 31000:2018 (ISO/IEC, 2018) should be adopted. It is possible to integrate other *guidelines*/methodologies, such as the one described by Ross et al. (2012). References should follow the APA style (APA, 2016). The cover of the paper must contain the name and student number of all authors.

Deliverables

1. First deliverable – chapter "*Establishing the Context*" – pdf file to submit in Moodle – the sooner you deliver, the sooner you have feedback to continue. This deliverable should be reviewed and integrated into the Second deliverable.
2. Second and final deliverable – the full report – zip file to submit in Moodle.

References

APA Style (2016). Quick Answers — References. Accessed 2.11.2023 http://www.apastyle.org/learn/quick-guide-on-references.aspx .

ISO (2018). NP ISO 31000:2018 – Gestão do risco – Linhas de orientação (Norma Portuguesa tradução do IPQ). International Organization for Standardization.

ISO/IEC (2022a). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems. International Organization for Standardization and International Electrotechnical Commission.

ISO/IEC (2022b). ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks. International Organization for Standardization and International Electrotechnical Commission.

Ross, R. S. et al. (2012). Guide for Conducting Risk Assessments (NIST SP-800-30rev1). *The National Institute of Standards and Technology (NIST), Gaithersburg*. Accessed 2.11.2023 http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.