## UC: Network Security

## TP1 Report – Simplified Risk Analysis /Análise de Risco simplificada

**Students (N / Name):** 78232 Cláudia Dias – 79625 David Alves

| Threats / Ameaças | Attacks / Ataques | Vulnerabilities / Vulnerabilidades |
|---|---|---|
| Espionagem industrial (Confidencialidade e Integridade) | Controlo remoto indesejado dos sensores; Visualização dos métodos de processo da empresa | Acesso direto à Control System LAN e Corporate LAN (sem uso de Firewall) por parte das empresas externas; o uso de RTU/PLC sem medidas de segurança adicionais |
| Falha no acesso aos emails e website da empresa (Disponibilidade) | Sobrecarregar servidores com mensagens indevidas do atacante | Fracas medidas de segurança nos Web Servers e Email Servers |
| Acesso indevido por trabalhadores não autorizados (Confidencialidade e Integridade) | Roubo de credenciais de acesso às workstations e aos HMI e consequente controlo dos processos da empresa (através dos HMI) assim como acesso a dados confidenciais presentes nas bases de dados (através das workstations) | Wokstations e HMI diretamente ligadas à Corporate LAN e Control System LAN |

**Critical resource / Recurso crítico: (justified / justificado)**

O recurso crítico que consideramos mais importante, são os trabalhadores da empresa (recurso humano), dado que neles se baseia grande parte do funcionamento desta indústria, sendo que caso através de algum deles ocorram fugas de informação, estas poderão causar graves danos na empresa, desde dados relativos ao funcionamento interno da empresa, como também acederem a dados guardados nas bases de dados.

**Security control / Controlo de segurança: (justified / justificado)**

Para controlo de segurança deve-se:

- Qualificar os funcionários para se protegerem de ataques (com, por exemplo formações em segurança informática);
- Contratar pessoal especializado em segurança informática, para resolver de forma mais imediata, os problemas de segurança;
- Fazer com todos os funcionários se comprometam com um acordo de confidencialidade, para que não haja fugas de informação, mesmo depois de estes já não trabalharem na empresa;
- Introduzir medidas de autenticação reforçadas, para que mesmo que uma workstation fique infetada, seja mais difícil de aceder à restante rede;
- Introdução de protocolos de uso e acesso à informação.