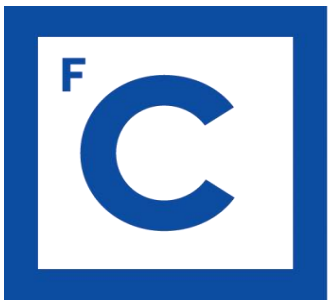

Ciências ULisboa

Faculdade de Ciências da Universidade de Lisboa

Faculdade de Ciências da Universidade de Lisboa

Departamento de Informática

Mestrado em Engenharia Informática e Segurança Informática

RELATÓRIO DE PROJETO

Análise e Gestão de Risco em Segurança Informática

PowerPlus Risk Management

Rodrigo Craveiro Rodrigues (Nº64370)

Diogo Serrano Sargaço (Nº58252)

Kevin Alexandre Lima dos Santos (Nº64874)

Professora: **Doutora Ana Respício**

1º Semestre Letivo 2024/2025

dezembro 2024

Resumo

A **PowerPlus**, é uma organização global especializada em infraestrutura energética, atua em 12 países diferentes e atende milhões de clientes, contando com um amplo quadro de colaboradores internos e externos. Comprometida com a inovação, sustentabilidade e segurança, a organização tem o objetivo de expandir as operações e investir em energias renováveis, com foco na proteção de dados e continuidade operacional.

A estrutura organizacional da organização é dividida entre os domínios da IT e OT, cada uma com necessidades de segurança específicas. A infraestrutura tecnológica da organização inclui milhares de servidores, bases de dados Oracle e *middleware* SAP, além de *data centers* com redundância geográfica para garantir a resiliência em desastres. Com aproximadamente 200 aplicações em uso, recorre a 20 dedicadas à gestão de dados pessoais de milhões de clientes, enfrentando desafios complexos de segurança.

A organização opera num ambiente regulamentado, onde está sujeita a exigências rigorosas, incluindo da GDPR na União Europeia e das normas NERC CIP nos Estados Unidos da América. Para cumprir esses requisitos, a organização adota normas internacionais, como os ISO/IEC 27001 e ISO/IEC 27005, para garantir que seus processos se encontram em conformidade com os padrões de segurança globais.

Índice

Capítulo 1: Preparação do SOC 7
1.1 Introdução 7
1.2 Objetivos do SOC 7
1.3 Estrutura Organizacional do SOC 8
1.4 Infraestrutura Tecnológica do SOC 8
1.5 Políticas e Procedimentos 9
Capítulo 2: Estabelecimento do Contexto 9
2.1 Enquadramento da organização 9
2.2 Missão e Valores 10
2.3 Objetivos 10
2.4 Visão Estratégica e Compromissos 10
2.5 Estrutura Organizacional 10
2.6 Infraestrutura e Recursos Tecnológicos 11
2.7 Fatores Internos e Externos 12
2.8 Stakeholders 12
2.9 Regulamentação e Conformidade 13
2.10 Critérios de Probabilidade 14
2.11 Critérios de Avaliação de Risco 14
2.12 Critérios de Impacto 15
2.13 Critérios de Aceitação de Risco 16
Capítulo 3: Apreciação de Risco 16
3.1 Identificação de Risco 16
3.1.1 Identificação do Risco 16
3.1.2 Identificação dos Ativos 17
3.1.3 Identificação das Ameaças 18
3.1.4 Identificação dos Controlos Existentes 19
3.1.5 Identificação das Vulnerabilidades 19
3.1.6 Identificação das Consequências 19
3.2 Análise de Risco 20

3.2.1 Análise de Risco 20
3.2.2 Metodologias de Análise de Risco 21
3.2.3 Avaliação de Consequências 21
3.2.4 Resultados Análise de Risco 22
3.3 Avaliação de Risco 23
Capítulo 4: Tratamento de Risco 24
4.1 Descrição 24
4.1 Deteção e Notificação 25
4.2 Contenção, Erradicação e Recuperação 25
Capítulo 5: Lições Aprendidas 27
5.1 Cenários de Incidentes 27
5.1.1 Cenário 1 27
5.1.2 Cenário 2 27
5.1.3 Cenário 3 27
Capítulo 6: Conclusão 28
Referências 30

Lista de Tabelas

Tabela 1 - Critérios de Probabilidade 14
Tabela 2 - Critérios de Avaliação de Risco 15
Tabela 3 - Critérios de Impacto 15
Tabela 4 - Critérios de Aceitação de Risco 16
Tabela 5 – Identificação de Riscos 17
Tabela 6 - Identificação de Ativos 18
Tabela 7 - Identificação de Incidentes 20
Tabela 8 - Análise de Risco 22
Tabela 9 - Tratamento de Risco 24
Tabela 10 - Tratamento de Risco Detalhado 26

Lista de Figuras

Figura 1 - Estrutura Organizacional da PowerPlus 10
Figura 2 - Macro arquitetura tecnológica da PowerPlus 11

Lista de Acrónimos

CISO *Chief Information Security Officer*

CSIRT *Computer Security Incident Response Team*

ENISA *European Union Agency for Cybersecurity*

GDPR *General Data Protection Regulation*

IoT *Internet of Things*

IT *Information Technology*

NERC CIP *North American Electric Reliability Corporation Critical Infrastructure Protection*

OT *Operational Technology*

SIEM *Security information and event management*

SOC *Security Operations Center*

MDM *Mobile Device Management*

BYOD Bring Your Own Device

MFA Multi-Factor Authentication

DDoS Distributed Denial of Service

DRP Disaster Recovery Plan

Capítulo 1: Preparação do SOC

1.1 Introdução

A segurança da informação é um componente crítico para a PowerPlus, uma organização global líder no setor energético, com operações em 12 países e atendendo a mais de 20 milhões de clientes. A proteção das infraestruturas críticas e dos dados sensíveis é fundamental para garantir a continuidade e a eficiência das operações em larga escala.

Este capítulo descreve a preparação necessária para o estabelecimento e operação eficaz do ***Security Operations Center*** (**SOC**), alinhado com a norma ISO/IEC 27005, que fornece diretrizes para a gestão de riscos em segurança da informação.

A preparação adequada do SOC é essencial para a organização manter a integridade, confidencialidade e disponibilidade dos seus sistemas e dados. Seguindo as melhores práticas e normas internacionais, como a ISO/IEC 27005, o SOC posiciona-se como uma componente vital na estratégia de segurança da informação da organização, garantindo a resiliência operacional e a confiança dos clientes e parceiros.

1.2 Objetivos do SOC

O principal objetivo do SOC é monitorizar, detetar e responder a incidentes de segurança da informação de forma proativa e eficiente. Os objetivos específicos incluem:

- **Proteção de Ativos Críticos:** Salvaguardar os sistemas **IT (*Information Technology*)** e **OT** (***Operational Technology***) contra ameaças cibernéticas.
- **Conformidade Regulamentar:** Assegurar o cumprimento de regulamentações como **GDPR** (***General Data Protection Regulation***), **NERC CIP** (***North American Electric Reliability Corporation Critical Infrastructure Protection***) e as diretrizes da **ENISA** (**European Union Agency for Cybersecurity**).
- **Resposta a Incidentes:** Estabelecer processos para deteção precoce e resposta eficaz a incidentes de segurança.
- **Gestão de Vulnerabilidades:** Identificar e mitigar vulnerabilidades nos sistemas e aplicações.
- **Sensibilização em Segurança:** Promover a cultura de segurança entre colaboradores e parceiros.
- **Gestão de Riscos Integrada:** Os riscos identificados pelo SOC são incorporados na avaliação geral de riscos da organização.
- **Melhoria Contínua:** Feedback do SOC contribui para a atualização das políticas e controlos de segurança.

1.3 Estrutura Organizacional do SOC

O SOC está integrado na estrutura hierárquica da organização, sob a liderança do ***Chief Information Security Officer*** **(CISO)**.

- **Equipa de Monitorização contínua:** Responsável pela vigilância contínua dos sistemas e redes.
- ***Computer Security Incident Response Team*** **(CSIRT):** Equipa especializada na gestão e resposta a incidentes.
- **Analistas de Segurança:** Focam-se na análise de ameaças e tendências emergentes.
- **Especialistas em análise Forense Digital e Testes de Penetração:** Realizam investigações e avaliações de segurança aprofundadas.

Para assegurar a eficácia de um SOC, é fundamental garantir a presença de uma equipa composta por **profissionais qualificados**. Estes devem possuir competências abrangentes nas diversas áreas da segurança, incluindo análise de riscos, resposta a incidentes e gestão de crises relacionadas com ataques ou falhas de segurança. A capacitação técnica e a experiência prática são indispensáveis para que os membros do SOC possam detetar, analisar e mitigar ameaças de forma eficiente.

Além disso, é imprescindível implementar programas de **formação contínua**. A constante evolução tecnológica e o surgimento de novas ameaças exigem que os profissionais do SOC estejam sempre atualizados quanto às ferramentas, técnicas e tendências do setor. A formação regular permite que a equipa desenvolva um entendimento mais profundo dos desafios emergentes, garantindo uma resposta ágil e eficaz a incidentes cada vez mais sofisticados.

1.4 Infraestrutura Tecnológica do SOC

A infraestrutura tecnológica do SOC é composta por:

- **Plataforma SIEM (*Security Information and Event Management*):** Agrega e analisa dados de segurança de mais de 100 componentes de rede, bases de dados e aplicações.
- **Ferramentas de Monitorização e Deteção de Intrusões:** Para identificação de atividades suspeitas em tempo real.
- **Sistemas de Gestão de Vulnerabilidades:** Facilitam a identificação e correção de falhas de segurança.
- **Ambientes de Teste e Desenvolvimento Seguros:** Para realização de testes de penetração e análises forenses sem risco para os sistemas de produção.

1.5 Políticas e Procedimentos

O SOC opera com base em políticas e procedimentos bem definidos, incluindo:

- **Política de Segurança da Informação:** Alinhada com as normas ISO/IEC 27001 e ISO/IEC 27005.
- **Procedimentos de Resposta a Incidentes:** Definem as etapas para deteção, análise, contenção, erradicação, recuperação e aprendizagem pós-incidente.
- **Gestão de Logs e Eventos:** Estabelece a recolha, armazenamento e análise de logs de segurança.
- **Comunicação e Escalonamento:** Orientações sobre comunicação interna e externa durante incidentes.

A preparação do SOC segue as orientações bem definidas da norma ISO/IEC 27005:

- **Contextualização Organizacional:** Compreensão do ambiente interno e externo, identificando fatores que influenciam a gestão de riscos.
- **Identificação de Ativos:** Catalogação dos ativos de informação críticos e avaliação do seu valor.
- **Avaliação de Riscos:** Identificação de ameaças, análise de vulnerabilidades e avaliação dos impactos potenciais.
- **Tratamento de Riscos:** Seleção e implementação de medidas de segurança apropriadas para mitigar riscos.
- **Comunicação e Consulta:** Envolvimento das partes interessadas na gestão de riscos.
- **Monitorização e Revisão:** Avaliação contínua da eficácia das medidas implementadas e ajuste conforme necessário.

Capítulo 2: Estabelecimento do Contexto

2.1 Enquadramento da organização

A **PowerPlus** é uma organização global especializada na infraestrutura crítica de energias, com operações estabelecidas geograficamente distribuídas em **12 países** em diversos continentes. Atende aproximadamente **20 milhões de clientes de eletricidade** e **1,3 milhões de clientes de gás**, posicionando-se como um dos principais atores no setor energético internacional. Internamente, a organização é constituída por **10.000 colaboradores** e com apoio externo de **5.000 profissionais**, sendo estes dedicados à manutenção de aplicações e projetos, aonde a organização assegura a continuidade e a eficiência das suas operações em larga escala.

2.2 Missão e Valores

A missão da PowerPlus é garantir a entrega contínua de energia de forma sustentável com alto grau de inovação e qualidade, através de um relacionamento muito próximo com o cliente energia. É importante reforçar os valores da organização, na qual se centram na **sustentabilidade**, **segurança** e na **responsabilidade social**, com um forte foco na proteção da sua infraestrutura crítica contra ameaças físicas e no ciberespaço.

2.3 Objetivos

A organização tem como objetivos crescer em novas geografias e nas energias renováveis, proceder à integração de novas competências para transformar digitalmente a organização (transformação digital do negócio), manter o risco controlado, criar canais de proximidade com o cliente para poder antecipar necessidades e servir com mais qualidade.

2.4 Visão Estratégica e Compromissos

A visão estratégica engloba o compromisso com a expansão em novas áreas geográficas, com ênfase nas energias renováveis, alinhando-se às tendências globais de sustentabilidade. Além disso, a organização apresenta objetivos de **transformação digital contínua**, visto que pretende aumentar a **eficiência operacional** e melhorar o **atendimento aos clientes**. A organização integra tecnologias modernas para monitorizar e gerir a distribuição de energia de forma eficiente e sustentável embora a sua estrutura.

2.5 Estrutura Organizacional

A estrutura organizacional da PowerPlus reflete a complexidade e a criticidade das suas operações, especialmente à **IT** e **OT**. A organização é estruturada de forma hierárquica, tal como se pode observar na *Figura 1*, com departamentos específicos responsáveis por **IT**, segurança cibernética e operações de energia e gestão de riscos. A liderança na gestão de segurança da informação é atribuída ao **CISO**, que gere o **SOC**, dedicado à deteção e resposta a incidentes.

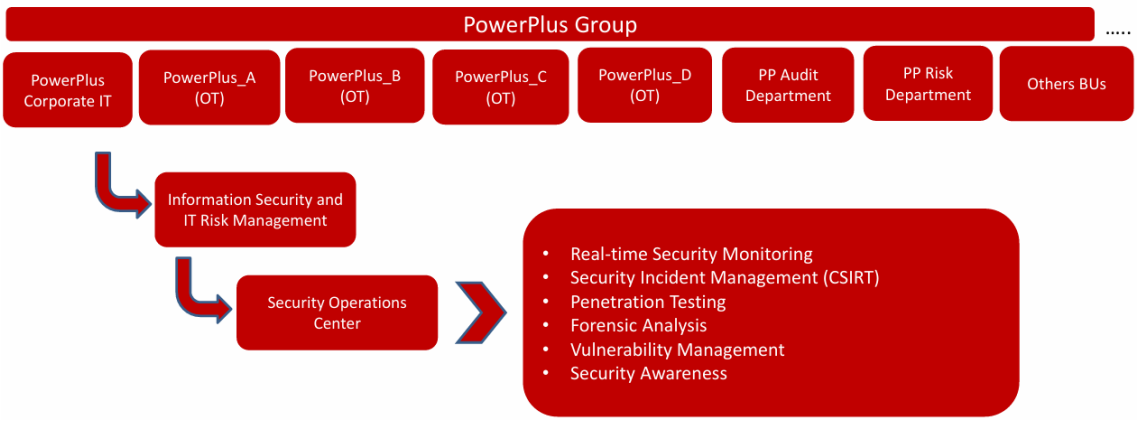

Figura 1 - Estrutura Organizacional da PowerPlus

O **SOC** opera interruptamente (24/7), que monitoriza em tempo real a segurança dos sistemas e redes. Adota uma abordagem baseada em monitorizar ameaças, gerir incidentes através de uma equipa especializada de **CSIRT**, realizar testes de penetração, análises forenses e manter práticas robustas de gestão de vulnerabilidades e conscientização em segurança. O **SOC** integra dados de aproximadamente **100 componentes de rede**, bases de dados e aplicações, onde recorre a uma plataforma de **SIEM** para detetar e responder proactivamente a ameaças emergentes.

A distinção entre IT e OT é fundamental devido às características e necessidades específicas de cada domínio. Enquanto a **IT** lida com **sistemas administrativos e de suporte aos negócios**, a **OT** é responsável pelos **sistemas de controle industrial que gerem a infraestrutura energética**. Esta separação exige abordagens especializadas na resposta a incidentes e na segurança reforçada para proteger os sistemas contra ameaças de ataques à segurança da informação que possam comprometer a continuidade operacional e a segurança dos dados dos clientes e colaboradores.

2.6 Infraestrutura e Recursos Tecnológicos

A PowerPlus opera num ambiente tecnológico altamente sofisticado e crítico, constituída por uma completa infraestrutura, tal como se pode observar na *Figura 2*.

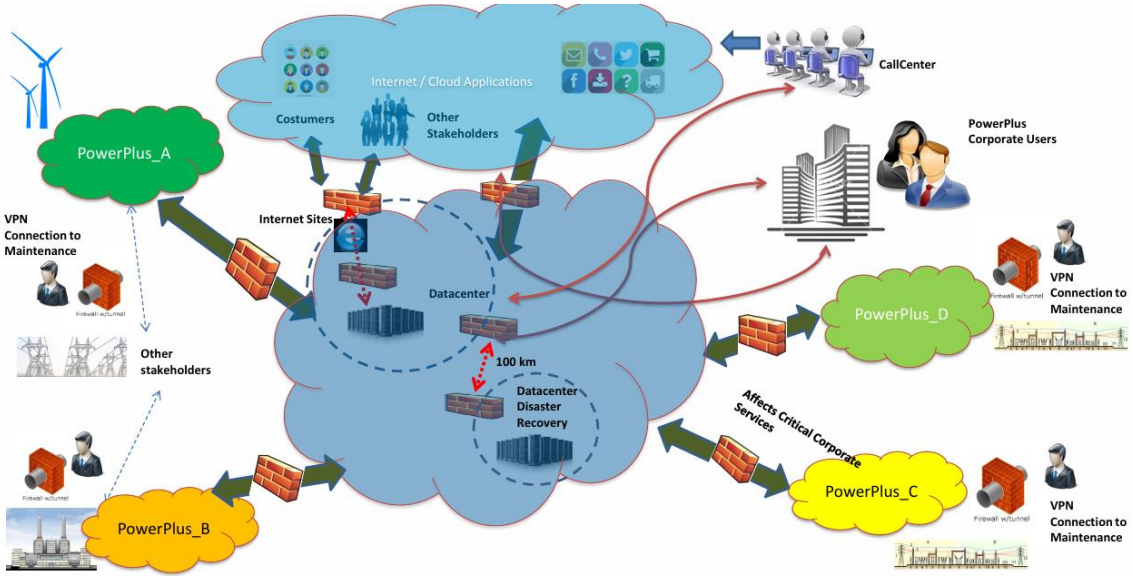

Figura 2 - Macro arquitetura tecnológica da PowerPlus

Com base na Figura 2, é possível identificar o seguinte ambiente tecnológico:

- A PowerPlus possui cerca de **1500** servidores **em produção**, **1100** servidores **em ambientes de pré-produção/testes**, e **900** servidores **de desenvolvimento**, sendo que todos estes tipos de servidores podem ser virtuais e físicos.
- Utiliza **10000** instâncias de bases de dados **produtivas**, 6000 instâncias de bases de dados de **pré-produção/testes**, e 500 instâncias de bases de dados de **desenvolvimento**,

A organização utiliza a tecnologia de **bases de dados Oracle**, enquanto o ***middleware*** é suportado por soluções da **Oracle** **e** **SAP**. Estes sistemas sustentam aplicações de missão crítica, incluindo sistemas com até **15 anos de operação**, o que prova a complexidade e a necessidade de compatibilidade tecnológica ao longo do tempo.

Para assegurar a continuidade dos negócios e a resiliência em situações de desastre, a organização mantém **2 *data centers*** geograficamente separados por **100 km**. Esta estratégia de redundância geográfica garante que, em caso de falhas ou incidentes num dos dois locais, as operações possam ser rapidamente transferidas para o outro *data center*, minimizando o impacto nos serviços prestados aos clientes.

No que diz respeito às aplicações, a organização utiliza aproximadamente **200 sistemas**, dos quais **20 sistemas** são diretamente dados pessoais de **6 milhões de clientes**. A manutenção dessas aplicações é realizada por seis fornecedores distintos, o que requer uma gestão eficaz

de fornecedores e de contratos para assegurar a qualidade e a segurança dos serviços. A gestão das identidades e dos acessos é centralizada através de um sistema especializado, garantindo a segurança ao longo do ciclo de vida dos clientes e o cumprimento das políticas de acesso estabelecidas.

Além disso, a organização adota a política da ***Bring Your Own Device*** (**BYOD**), onde permite que os colaboradores utilizem dispositivos pessoais para fins corporativos. Esta abordagem aumenta a flexibilidade e a produtividade, mas também amplia os desafios de segurança, exigindo medidas adicionais para proteger uma variedade de dispositivos e plataformas, incluindo *Android*, *iOS* e *Windows Phone*.

2.7 Fatores Internos e Externos

Fatores Internos

- **Recursos Humanos:** Uma força de trabalho altamente qualificada com expertise em manutenção de aplicações e segurança de sistemas IT e OT.
- **Infraestrutura Crítica:** Operações suportadas por dois *data centers* redundantes, tecnologia de ponta e uma arquitetura híbrida de servidores e bases de dados.
- **Cultura Organizacional:** Uma abordagem proativa na gestão de riscos e segurança cibernética, alinhada às melhores práticas internacionais.
- **Desafios Tecnológicos:** Necessidade de modernização contínua para lidar com sistemas de legado e adotar soluções inovadoras.

Fatores Externos

- **Regulamentação e Conformidade:** Operação em ambientes regulamentados pela GDPR na União Europeia, NERC CIP na América do Norte e diretrizes da ENISA.
- **Ameaças Cibernéticas:** Crescente sofisticação de ataques como ransomware, phishing e DDoS.
- **Mudanças no Mercado Energético:** Pressão para a transição energética e aumento do uso de fontes renováveis.

2.8 Stakeholders

A PowerPlus estabelece interações com um amplo conjunto de partes interessadas, refletindo o seu compromisso com a excelência operacional, a conformidade regulatória e a inovação sustentável. Entre as principais partes interessadas encontram-se os seus **clientes**, para os quais a organização prioriza a entrega de serviços de alta qualidade, garantindo ao mesmo tempo a proteção rigorosa dos dados pessoais.

Outro grupo essencial é constituído pelos **reguladores**, com quem mantém uma relação de conformidade estrita, cumprindo normas internacionais, como o GDPR e o NERC CIP, além de respeitar legislações nacionais específicas de cada região onde opera.

Os **fornecedores** desempenham igualmente um papel estratégico, especialmente os seis principais parceiros responsáveis pela manutenção de aplicações e pelo suporte técnico, cuja gestão eficaz de contratos assegura a qualidade e a segurança contínuas das operações.

Por fim, os **colaboradores** são incentivados a participar de uma cultura organizacional que promove a segurança e a responsabilidade, contribuindo para a proteção da infraestrutura crítica da organização. Além disso, a organização fomenta **parcerias** estratégicas voltadas para a inovação e sustentabilidade, reforçando o seu papel como líder no setor energético global.

2.9 Regulamentação e Conformidade

A PowerPlus opera nas regiões da **União Europeia** e na **Americana do Norte**, na qual são ambientes altamente regulamentados, assim está sujeita a exigências legais e normativas destinadas a assegurar a proteção das infraestruturas críticas e a segurança dos dados pessoais dos clientes. As principais regulamentações que impactam as operações da organização são:

- **GDPR** na União Europeia, que estabelece padrões para a proteção de dados pessoais e obrigações às organizações no tratamento e na segurança desses dados.
- **Normas NERC CIP** nos Estados Unidos da América, que definem requisitos para proteger os ativos de infraestrutura crítica do setor elétrico contra ameaças da segurança da informação.
- **ENISA**, que fornecem orientações sobre as melhores práticas relativo à segurança cibernética e proteção de infraestruturas críticas.
- **Legislações nacionais** específicas dos países em que a organização opera, incluindo leis de proteção de infraestruturas críticas e regulamentações setoriais.

A crescente ameaça de ataques de segurança da informação aumenta o nível de risco, exigindo uma elevada vigilância de forma constante e a adaptação contínua das políticas de segurança. Para cumprir essas regulamentações e assegurar os padrões de segurança da informação, a organização deve adotar práticas alinhadas às normas internacionais:

1. **ISO/IEC 27001**

Esta norma internacional constitui a base para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação (SGSI). Proporciona um quadro abrangente para a proteção de ativos digitais, alinhando práticas de segurança da informação às necessidades organizacionais e das partes interessadas. Com um enfoque na confidencialidade, integridade e disponibilidade da informação, a ISO/IEC 27001 ajuda a mitigar riscos e a demonstrar conformidade com requisitos legais e contratuais, contribuindo para a confiança dos clientes e parceiros.

2. **ISO/IEC 27005:2022**

Esta norma é especificamente dedicada à gestão de riscos de segurança da informação, fornecendo diretrizes detalhadas para a identificação, análise, avaliação e tratamento de riscos. Para a organização, isto traduz-se num suporte essencial na construção de uma estratégia de segurança que aborda vulnerabilidades específicas, aproveita oportunidades de melhoria e mantém os riscos dentro de limites aceitáveis. Esta abordagem permite uma gestão proactiva e fundamentada para proteger os ativos críticos da organização.

3. **ISO/IEC 27035-1**

Focada na gestão de incidentes de segurança da informação, esta norma oferece orientações práticas para a deteção, análise e resposta a incidentes. Com a adoção da ISO/IEC 27035-1, a

organização pode estruturar processos eficientes para lidar com eventos que possam comprometer a operação ou os dados da organização. Desde a preparação e identificação de incidentes até à recuperação e melhoria contínua, esta norma promove uma maior resiliência e capacidade de resposta às ameaças emergentes.

4. **ISO 31000:2018**

De âmbito mais geral, esta norma estabelece princípios e diretrizes para a gestão de riscos em todos os níveis organizacionais. A sua integração na estratégia da organização reforça a ligação entre a segurança cibernética e os objetivos organização riais, garantindo decisões informadas e alinhadas às prioridades estratégicas. Além disso, promove uma cultura organizacional centrada na gestão de riscos, abrangendo desde a análise estratégica até às operações diárias, contribuindo para a sustentabilidade e o crescimento da organização.

2.10 Critérios de Probabilidade

Os critérios de probabilidade fornecem uma classificação padronizada para avaliar a possibilidade de ocorrência de um evento de risco. Estes critérios variam entre "rara" e "quase certa", permitindo uma análise clara e objetiva da frequência esperada dos eventos.

Tabela 1 - Critérios de Probabilidade

Nivel	Descrição	Percentagem de Probabilidade	Exemplo de Ocorrência
1 - Raro	Evento muito improvável de ocorrer.	0% - 10%	Pode ocorrer uma vez a cada 20 anos.
2 - Improvável	Evento improvável, mas possível.	11% - 30%	Pode ocorrer uma vez a cada 10 anos.
3 - Possível	Evento com chances razoáveis de ocorrer.	31% - 60%	Pode ocorrer uma vez a cada 5 anos.
4 - Provável	Evento provável de ocorrer.	61% - 90%	Pode ocorrer uma vez por ano.
5 - Quase Certo	Evento quase garantido.	91% - 100%	Pode ocorrer várias vezes ao ano.

2.11 Critérios de Avaliação de Risco

Os critérios de avaliação cruzam os níveis de probabilidade e impacto para determinar a severidade do risco e a ação necessária. Estes são categorizados em três cores para facilitar a visualização. Esta categorização assegura que a organização tenha um entendimento claro das prioridades e mantenha um alinhamento estratégico na gestão de riscos.

Tabela 2 - Critérios de Avaliação de Risco

Probabilidade/ Verosimilhança	Impacto Insignificante	Impacto Pequeno	Impacto Moderado	Impacto Elevado	Impacto Catastrófico
Quase Certo >95%					
Provável >50%					
Possível >25%					
Improvável <=25%					
Rara <=1%					

Legenda:

- **Verde (Baixo):** Risco aceitável; monitorização contínua e revisão periódica.
- **Amarelo (Médio):** Requer atenção; planeamento de mitigação a médio prazo.
- **Laranja (Alto):** Não aceitável; implementar controlos corretivos imediatos.
- **Vermelho (Crítico):** Intolerável; ação urgente e priorização máxima.

2.12 Critérios de Impacto

Os critérios de impacto classificam a severidade das consequências de um risco, variando de impactos insignificantes a catastróficos. Esta classificação permite avaliar o potencial dano às operações, à reputação e aos ativos críticos da organização.

Tabela 3 - Critérios de Impacto

Nivel	Descrição	Exemplo de Impacto
1 - Insignificante	Sem interrupção ou perda de dados.	Interrupção mínima sem impacto operacional.
2 - Pequeno	Pequena interrupção com impacto limitado.	Exposição de dados não sensíveis ou interrupção leve.
3 - Moderado	Interrupção significativa ou impacto operacional.	Vazamento de dados moderadamente sensíveis ou interrupção prolongada.

4 - Elevado	Interrupção grave ou impacto financeiro elevado.	Exposição de dados sensíveis ou interrupção de um dia.
5 - Catastrófico	Interrupção total ou impacto financeiro crítico.	Perda de sistemas críticos ou exposição de dados confidenciais.

2.13 Critérios de Aceitação de Risco

Os critérios de aceitação de risco definem os níveis de risco que a organização está disposta a tolerar, com base no impacto potencial e na probabilidade de ocorrência. Estes critérios ajudam a priorizar a implementação de medidas de mitigação e assegurar que os recursos sejam alocados de forma eficiente.

Tabela 4 - Critérios de Aceitação de Risco

Nivel de Risco	Ação
1 - Baixo	Aceitável. Monitorização contínua e revisão periódica.
2 - Médio	Requer atenção. Planeamento de mitigação em médio prazo.
3 - Alto	Não aceitável. Implementar controles corretivos imediatos.
4 - Crítico	Intolerável. Ação urgente e priorização máxima.

Capítulo 3: Apreciação de Risco

3.1 Identificação de Risco

A apreciação de risco constitui um elemento fundamental na gestão da segurança da informação, permitindo identificar, analisar e avaliar os riscos que podem afetar a organização. Nesta primeira fase, seguindo as diretrizes da norma ISO/IEC 27005, procede-se à identificação dos riscos, dos ativos, das ameaças, dos controlos existentes, das vulnerabilidades e das possíveis consequências associadas. Este processo sistemático é essencial para compreender o panorama de risco da PowerPlus e para orientar a implementação de medidas de mitigação adequadas.

3.1.1 Identificação do Risco

No contexto operacional da organização, foram identificados riscos relacionados com a **interrupção dos serviços energéticos**, decorrentes de ataques cibernéticos aos sistemas de OT, que podem causar falhas na distribuição de energia e gás. Existe também o risco de **comprometimento de dados pessoais** de aproximadamente seis milhões de clientes, violando

as disposições do GDPR.

Adicionalmente, a organização enfrenta ameaças de ataques sofisticados, como ***ransomware*** e ***phishing***, que podem resultar em **perdas financeiras** significativas e **danos reputacionais**. As ameaças internas, provenientes de ações maliciosas ou negligentes de colaboradores ou fornecedores com acesso privilegiado, constituem igualmente um risco relevante.

Tabela 5 – Identificação de Riscos

Risco	Probabilidade	Impacto	Nível
Comprometimento de dados pessoais de milhões de clientes	Improvável	Elevado	Médio
Ataque de ransomware aos sistemas IT	Alto	Catastrófico	Crítico
Falhas em sistemas OT que afetam a distribuição de energia	Possível	Elevado	Crítico
Ataques de phishing direcionados a colaboradores	Quase Certo	Alto	Crítico
Indisponibilidade de data centers devido a DDoS	Alta	Catastrófico	Crítico
Erro humano causando acesso não autorizado	Provável	Moderado	Médio
Exploração de vulnerabilidades em sistemas legados	Possível	Elevado	Critico
Comprometimento de fornecedores externos com acesso privilegiado	Provável	Elevado	Critico

3.1.2 Identificação dos Ativos

A organização opera com cerca de **1.500 servidores de produção**, **1.100 servidores em ambientes de pré-produção** e **900 servidores de desenvolvimento**, abrangendo tanto sistemas virtuais como físicos. As **bases de dados** constituem outro ativo crítico, com **10.000 instâncias produtivas**, **6.000 instâncias de pré-produção** e **500 instâncias de desenvolvimento**, utilizando tecnologia Oracle. Estes sistemas suportam cerca de **200**

aplicações, das quais 20 processam diretamente dados pessoais de clientes. Os **dois *data centers*** geograficamente separados, que garantem a redundância e a continuidade das operações, são igualmente ativos estratégicos.

Além disso, a informação sensível, incluindo **dados pessoais de clientes e colaboradores**, **propriedade intelectual** e **informações comerciais**, representa um ativo intangível de elevado valor para a organização.

Tabela 6 - Identificação de Ativos

Ativo	Tipo	Localização	Proprietário	Valor do Ativo
Servidor de Produção	Hardware	Data Center Primário	Equipa de Infraestrutura	Alto
Base de Dados Oracle	Dados	Data Center Secundário	Departamento de TI	Muito Alto
Middleware SAP	Software	Servidor Centralizado	Gerente de Operações	Alto
Aplicações Críticas	Software	Cloud Privada Corporativa	Departamento de TI	Muito Alto
Dados Pessoais de Clientes	Dados	Servidor de Banco de Dados	CISO	Muito Alto

3.1.3 Identificação das Ameaças

A organização enfrenta **ameaças de ciberataques externos,** incluindo **hackers**, **grupos criminosos organizados** e **atores estatais** que visam infraestruturas críticas.

As ameaças de ***malware*** e ***ransomware*** são particularmente preocupantes, dado o potencial para danificar ou comprometer sistemas críticos. Os ataques de ***phishing*** e **engenharia social** representam riscos significativos, visando obter credenciais ou informações sensíveis através do engano de colaboradores. Ataques de **DDoS** podem causar a indisponibilidade dos serviços essenciais.

As **ameaças internas**, resultantes de **comportamentos maliciosos** ou **negligentes de colaboradores ou fornecedores,** podem levar ao comprometimento de sistemas e informações. Além disso, **falhas tecnológicas**, como defeitos de hardware ou software, e **desastres naturais**, como sismos ou inundações, constituem ameaças que podem afetar a continuidade das

operações.

3.1.4 Identificação dos Controlos Existentes

A equipa de CSIRT é responsável pela gestão e resposta a incidentes de segurança. A organização utiliza uma plataforma de **SIEM** que integra dados de aproximadamente **100 componentes de rede**, **bases de dados e aplicações**, permitindo a deteção proativa de ameaças emergentes.

As políticas e procedimentos de segurança estão alinhados com as melhores práticas internacionais e regulamentações aplicáveis, como a ISO/IEC 27001. A gestão centralizada de identidades e acessos assegura o cumprimento das políticas de segurança e a proteção ao longo do ciclo de vida dos clientes. Programas de sensibilização em segurança promovem uma cultura organizacional orientada para a segurança da informação. A redundância geográfica dos *data centers* e a gestão eficaz dos fornecedores contribuem para a resiliência e a segurança das operações.

3.1.5 Identificação das Vulnerabilidades

Na PowerPlus, foram identificadas várias possíveis vulnerabilidades, como a existência de **sistemas com até 15 anos** de operação pode representar riscos devido à falta de compatibilidade com as atualizações de segurança mais recentes. A política de BYOD amplia os desafios de segurança, uma vez que os **dispositivos pessoais dos colaboradores** podem não estar adequadamente protegidos ou controlados.

A dependência de diversos fornecedores para a manutenção das aplicações pode introduzir inconsistências nas práticas de segurança e dificultar a gestão unificada de riscos. A possível existência de **atrasos na aplicação de atualizações** e ***patches* de segurança** pode expor os sistemas a vulnerabilidades conhecidas.

A **formação insuficiente** ou inadequada dos colaboradores em matéria de segurança da informação pode levar a comportamentos negligentes ou imprudentes. A **falta de segmentação** adequada entre as redes IT e OT pode facilitar o movimento lateral de atacantes dentro da infraestrutura. A gestão de vulnerabilidades pode ser insuficiente se não houver processos eficazes para identificar e corrigir proactivamente as fraquezas nos sistemas.

3.1.6 Identificação das Consequências

Para a PowerPlus, a **interrupção dos serviços energéticos** pode afetar milhões de clientes, resultando em prejuízos económicos e sociais consideráveis, bem como em danos à confiança do público na organização. A perda financeira pode ser agravada pelos custos associados à **recuperação das operações**, às **multas regulatórias** decorrentes da não conformidade com leis como o GDPR, e à perda de receitas.

Os **danos reputacionais** podem comprometer a posição da organização no mercado,

dificultando a retenção e atração de clientes e parceiros. A **exposição de dados pessoais** pode levar a ações legais e a indemnizações significativas, além de comprometer a privacidade e segurança dos indivíduos afetados. O **comprometimento de propriedade intelectual** ou de **informações estratégicas** pode afetar a vantagem competitiva da organização e favorecer concorrentes.

Adicionalmente, como a organização opera **infraestruturas críticas**, **incidentes de segurança** podem ter implicações a nível nacional, afetando a segurança energética e a estabilidade económica dos países onde opera.

Tabela 7 - Identificação de Incidentes

Tipo de Incidente	Descrição	Severidade
Vazamento de dados pessoais	Exposição de dados de milhões de clientes	Alta
Ataque de Ransomware	Encriptação de dados críticos e exigência de resgate	Muito alta
Interrupção de serviços de OT	Paralisação de infraestruturas energéticas	Alta
Phishing direcionado	Roubo de credenciais ou informações sensíveis	Alta
Ataque DDoS	Indisponibilidade de serviços devido a sobrecarga	Muito alta
Erro humano com impacto em segurança	Negligência causando falhas de segurança	Média
Acesso não autorizado a sistemas críticos	Uso indevido de permissões privilegiadas	Alta
Falhas de fornecedores externos	Dependência de práticas inconsistentes de segurança por terceiros	Alta

3.2 Análise de Risco

3.2.1 Análise de Risco

Os riscos identificados foram examinados em função dos critérios de probabilidade e impacto estabelecidos no Capítulo 2. Foram consideradas as ameaças específicas, as vulnerabilidades existentes e a eficácia dos controlos atuais. A combinação destes fatores permitiu quantificar o risco e estabelecer prioridades para o seu tratamento.

3.2.2 Metodologias de Análise de Risco

Foram seguidos os seguintes passos metodológicos:

- **Avaliação da Probabilidade**: Para cada risco, foi avaliada a probabilidade de ocorrência com base em dados históricos, tendências atuais e conhecimento especializado. Isto envolveu a análise de incidentes passados, a frequência de tentativas de ataque registadas pelo SOC e a presença de vulnerabilidades conhecidas.
- **Avaliação do Impacto**: O impacto potencial de cada risco foi determinado considerando as possíveis consequências para a organização, incluindo efeitos operacionais, financeiros, legais e reputacionais. Foram considerados cenários de pior caso e impactos cumulativos.
- **Determinação do Nível de Risco**: Combinando a probabilidade e o impacto, o nível de risco foi determinado utilizando a matriz de risco estabelecida nos critérios de avaliação. Esta matriz permite classificar os riscos em níveis que variam de "Baixo" a "Crítico".
- **Documentação e Registo**: Todos os riscos avaliados foram registados num registo de riscos formal, documentando as avaliações de probabilidade e impacto, bem como os controlos existentes e as recomendações para o tratamento.

A utilização desta metodologia assegura a consistência e a transparência no processo de análise, permitindo à organização priorizar os riscos que requerem atenção imediata e planear adequadamente os recursos para o tratamento de riscos.

3.2.3 Avaliação de Consequências

Os principais tipos de consequências avaliadas foram:

- **Impacto Operacional**: Interrupções nos sistemas de IT e OT podem afetar a distribuição de energia e gás, prejudicando milhões de clientes. A indisponibilidade dos serviços pode resultar em consequências sociais e económicas graves, incluindo a interrupção de serviços essenciais e a perda de confiança do público.
- **Impacto Financeiro**: Incidentes de segurança podem levar a custos substanciais relacionados com a recuperação de sistemas, multas regulatórias, indemnizações a clientes afetados e perda de receitas. Violações ao GDPR, por exemplo, podem resultar em multas significativas que afetam a saúde financeira da organização.
- **Impacto Legal e de Conformidade**: O não cumprimento das regulamentações aplicáveis pode levar a sanções legais e ações judiciais. A organização está sujeita a diversas normas e regulamentos, incluindo o GDPR e as normas NERC CIP, que exigem níveis elevados de proteção e resposta a incidentes.
- **Impacto Reputacional**: A exposição de dados pessoais ou interrupções nos serviços podem afetar negativamente a reputação da organização, reduzindo a confiança dos clientes, parceiros e reguladores. A reputação é um ativo intangível crucial que influencia a posição competitiva da organização no mercado.
- **Impacto na Segurança Nacional**: Como operadora de infraestruturas críticas, incidentes graves podem ter implicações para a segurança e estabilidade dos países onde a organização opera, aumentando a responsabilidade da organização na gestão eficaz dos riscos.

Esta avaliação detalhada das consequências permite compreender a gravidade potencial dos riscos e reforça a importância de implementar medidas de mitigação adequadas e eficazes.

3.2.4 Resultados Análise de Risco

Entre os **riscos considerados prioritários**, destacam-se os ataques de ***ransomware*** que representam uma **probabilidade classificada como "Provável"** e um **impacto avaliado "Catastrófico"**. Este cenário pode resultar na completa indisponibilidade dos sistemas críticos, além da perda irreparável de dados sensíveis, comprometendo a continuidade das operações. Também o comprometimento dos **sistemas de OT** foi identificado como uma ameaça significativa, onde se atribui uma **probabilidade classificada** como **"Possível"** e um **impacto igualmente "Catastrófico"**. Tal situação pode gerar interrupções graves na distribuição de energia e gás, com efeitos potencialmente desastrosos para a organização e os seus *stakeholders*. E por fim, é considerado também a **exposição de dados pessoais** que se destacou como um risco relevante, com uma **probabilidade classificada** como **"Possível"** e **impacto "Elevado".** Este risco abrange potenciais violações de dados de milhões de clientes, acarretando repercussões legais, financeiras e de reputação que podem ser severas.

Além dos riscos prioritários, foram identificados outros **riscos elevados**, como as **vulnerabilidades em sistemas obsoletos**, decorrentes de tecnologias desatualizadas, aumentam a probabilidade de exploração de falhas conhecidas, comprometendo a segurança da infraestrutura. A adoção da **política de BYOD**, sem a implementação de medidas de segurança adequadas, amplifica os riscos de acesso não autorizado e de perda de dados críticos. Por fim, também foi considerado as **ameaças internas**, destacando-se a possibilidade de **ações negligentes** ou então **maliciosas** por parte de **colaboradores ou fornecedores** com acesso privilegiado, representando um risco significativo para os ativos da organização.

Os riscos **classificados como "Médio" e "Baixo"** também foram tomados em consideração. Embora, estes riscos não sejam prioritários para tomar ações de forma imediata, é estritamente necessário ter em atenção e planear as suas mitigações a médio prazo.

Tabela 8 - Análise de Risco

Risco	Probabilidade	Impacto	Nivel de Risco
Ataques de Ransomware	Alta	Catastrófico	Crítico
Exploração de Vulnerabilidades	Média	Elevado	Alto

Indisponibilidade de *Data Centers*	Média	Elevado	Alto
Phising	Alta	Médio	Médio
Erros Humanos	Média	Médio	Médio

3.3 Avaliação de Risco

A avaliação de risco realizada na PowerPlus seguiu as diretrizes estabelecidas pelas normas ISO/IEC 27005. O processo focou-se na categorização detalhada dos riscos identificados, com a atribuição de níveis de severidade baseados na combinação de probabilidade de ocorrência e impacto potencial. Para isso, foram utilizados critérios padronizados que classificaram a probabilidade de cada risco em uma escala que varia de "Raro" a "Quase Certo" e o impacto em níveis de "Insignificante" a "Catastrófico". O cruzamento desses critérios foi operacionalizado por meio de uma matriz de risco, permitindo determinar a prioridade de cada cenário em níveis que variaram entre Baixo, Médio, Alto e Crítico.

Os riscos classificados como **críticos e altos** foram destacados como **prioritários para tratamento**, dado o seu potencial de causar danos significativos às operações e à reputação da empresa. Isto assegurou que os recursos sejam direcionados de forma eficiente, focando-se nas áreas mais vulneráveis e de maior impacto para a continuidade das operações e a segurança dos ativos da organização. Além disso, a análise incluiu uma avaliação da adequação dos **critérios de aceitação de risco** definidos na fase de estabelecimento do contexto e assim os riscos que não atendiam aos critérios foram marcados para tratamento imediato, com a definição de estratégias específicas para mitigação ou controlo.

A saída deste processo incluiu um conjunto estruturado de informações para gestão de riscos, consolidado num registo formal que contém uma **lista de riscos priorizados**, acompanhada dos **cenários associados**, a necessidade de **tratamento identificada** para cada risco e **sugestões concretas de gestão**. Isto não apenas forneceu uma visão clara das vulnerabilidades, mas também apoiou a tomada de decisão informada, orientando a implementação de medidas eficazes de mitigação e garantindo a resiliência contínua da organização frente a ameaças diversas.

Capítulo 4: Tratamento de Risco

4.1 Descrição

O tratamento de risco é um processo essencial para garantir a segurança da informação, sendo fundamental para mitigar, transferir, aceitar ou evitar os riscos identificados. A segurança da informação enfrenta desafios crescentes devido à evolução de ameaças cibernéticas e à complexidade dos ambientes tecnológicos. Para a PowerPlus, uma abordagem estruturada permite priorizar e tratar riscos de forma eficiente, minimizando potenciais impactos adversos e assegurando a continuidade das operações. Este processo encontra-se alinhado com os princípios e recomendações da norma ISO/IEC 27005, que fornece uma estrutura reconhecida internacionalmente para a gestão de riscos no contexto de sistemas de informação.

Este processo inclui cinco etapas principais:

- **Modificação (Defesa):** Implementação de barreiras tecnológicas adicionais, como *firewalls*, segmentação de rede e listas de bloqueio dinâmicas, que dificultam o acesso de agentes maliciosos.
- **Modificação (Mitigação):** Redução do impacto dos riscos através de medidas como a criação de backups frequentes e a implementação de planos de contingência robustos.
- **Partilha (Transferência):** Contratação de seguros cibernéticos para cobrir eventuais danos derivados de riscos residuais.
- **Retenção (Aceitação):** Monitorização proativa dos riscos considerados aceitáveis.
- **Evitação (Terminação):** Eliminação de sistemas ou processos que apresentem um risco inaceitável.

Tabela 9 - Tratamento de Risco

Risco	Estratégia	Ação
Ransomware	Reduzir	Implementação de backups regulares e testes
Acesso Não Autorizado	Evitar	Aplicação de autenticação multifator (MFA)
Phising	Reduzir	Conscientização de treinamento
Exploração de Vulnerabilidades	Mitigar	Atualizações regulares e gestão de *patches*

Falha de Sistemas OT	Transferir	Contratação de seguro para equipamentos

4.1 Deteção e Notificação

A deteção e a notificação constituem os primeiros passos na resposta aos riscos, sendo fundamentais para assegurar uma resposta rápida e eficaz a potenciais incidentes.

O SOC da PowerPlus, que opera 24 horas por dia, sete dias por semana, desempenha um papel crucial nesta fase. A monitorização de riscos deve ser continuamente optimizada através da adopção de ferramentas tecnológicas avançadas, nomeadamente soluções baseadas em inteligência artificial. Estas ferramentas permitem a análise e identificação de anomalias ou padrões de comportamento suspeitos em tempo real, aumentando a capacidade de resposta proactiva.

Para uma visibilidade abrangente, é essencial integrar os sistemas de IT e OT (Tecnologias Operacionais). Esta integração é particularmente importante, dado que os sistemas de OT são frequentemente geridos por fornecedores externos, podendo introduzir riscos adicionais se não forem devidamente monitorizados.

Relativamente à notificação, é imprescindível a implementação de fluxos de comunicação eficazes e rápidos. Estes fluxos devem garantir a escalada imediata de incidentes graves para os decisores estratégicos e as autoridades reguladoras competentes. Este processo não apenas assegura a conformidade legal e regulatória, mas também fortalece a confiança dos stakeholders na capacidade da organização de identificar, gerir e mitigar ameaças de forma eficiente.

4.2 Contenção, Erradicação e Recuperação

A contenção, a erradicação e a recuperação são passos essenciais para limitar os danos causados por incidentes e restaurar as operações normais de forma segura.

A **contenção** envolve a implementação de segmentação de rede eficaz entre os sistemas IT e OT, evitando a propagação de ataques. Além disso, o uso de listas de bloqueio dinâmicas permite isolar rapidamente sistemas comprometidos, reduzindo assim a superfície de ataque.

Na fase de **erradicação**, o foco é a eliminação completa das ameaças identificadas. Isto inclui o desenvolvimento de *playbooks* específicos para o tratamento de incidentes em sistemas de OT e a definição de protocolos claros para colaboração com fornecedores externos, garantindo uma remediação eficaz e centralizada. A utilização de soluções robustas para a gestão de *patches* também é imprescindível.

Por fim, a **recuperação** requer um planeamento rigoroso e testes regulares. Os backups, que devem ser mantidos isolados e regularmente validados, garantem a integridade dos dados durante o processo de restauração. É essencial assegurar que os sistemas restaurados estejam livres de infeções residuais antes de retomar as operações. Simulações periódicas de cenários de desastre ajudam a identificar lacunas nos planos de recuperação e fortalecem a resiliência da organização.

Com estas ações, a PowerPlus está mais bem preparada para lidar com ameaças, minimizando os impactos financeiros e operacionais, enquanto reforça a confiança dos seus *stakeholders*.

Tabela 10 - Tratamento de Risco Detalhado

Risco	Impacto Potencial	Probabilidade	Responsável	Opção de Tratamento	Prazo
Comprometimento de dados pessoais	Multas regulatórias (RGPD), perda de confiança dos clientes e prejuízo reputacional	Provável	CISO e equipa de IT	-Implementar encriptação de ponta a ponta. - Fortalecer controlo de acessos.	6 Meses
Ataque a sistemas OT (Operacional)	Paragem de operações críticas (energia e gás), falha na distribuição energética	Possível	Responsável de OT	Segmentação de rede OT-IT. - Atualização de software OT.	9 meses
Indisponibilidade de sistemas críticos	Perda de serviços aos clientes, impacto financeiro elevado e perda de dados	Provável	CIO e equipa de IT	- Plano de *Disaster Recovery*. -Monitorização 24/7 (SOC).	12 meses
Acessos não autorizados (BYOD)	Riscos de fuga de dados e exploração de dispositivos móveis	Possível	Equipa de segurança de IT	- Políticas robustas de BYOD. - Aplicação de MDM (*Mobile Device Management*).	6 meses
Ransomware nos sistemas IT	Encriptação de dados críticos, exigência de resgates financeiros e interrupção de serviços	Provável	SOC e equipa de Segurança	- Backup regular e testes de restauração. - Educação em segurança cibernética.	3 meses

Capítulo 5: Lições Aprendidas

5.1 Cenários de Incidentes

As análises de lições aprendidas servem como um pilar essencial na gestão de riscos, pois permitem à PowerPlus fortalecer a sua resiliência face a incidentes futuros. Este processo baseia-se em cenários reais e hipotéticos, que refletem os desafios enfrentados pela organização. Considerando a natureza das operações da organização, foram selecionados três cenários distintos para ilustrar as lições aprendidas que estão abaixo mencionados.

5.1.1 Cenário 1

A PowerPlus gere dados pessoais de mais de 6 milhões de clientes através de 20 aplicações críticas, o que representa um risco significativo de comprometimento de dados sensíveis. Este cenário inclui possíveis explorações de vulnerabilidades em aplicações empresariais ou acessos não autorizados resultantes de falhas nos controles de acesso implementados. Caso um incidente desse tipo ocorra, a organização estará sujeita a graves consequências, incluindo multas significativas pela violação do RGPD, perda de confiança por parte dos clientes, danos a reputação e custos operacionais associados à mitigação do incidente.

Para mitigar este risco, recomenda-se a implementação de autenticação multi-fator (MFA) em todas as aplicações críticas, garantindo níveis adicionais de proteção contra acessos indevidos. Além disso, é essencial realizar auditorias regulares para identificar e corrigir vulnerabilidades nos sistemas que processam dados sensíveis. O uso de ferramentas de monitorização contínua, como plataformas SIEM, permitirá a deteção em tempo real de tentativas de acesso não autorizado, reduzindo o tempo de resposta e minimizando os impactos.

5.1.2 Cenário 2

O ataque direcionado a sistemas de tecnologia operacional é um dos cenários mais críticos para a organização, dado o impacto direto na operação das infraestruturas físicas, como parques eólicos, centrais nucleares e redes de distribuição de energia. Este tipo de incidente pode envolver *malware* especializado, ataques de *ransomware* ou acessos maliciosos devido à falta de integração dos sistemas OT com os processos de monitorização central. Como resposta, é essencial fortalecer a segmentação entre OT e IT, garantir atualizações regulares dos sistemas OT e exigir o cumprimento rigoroso de normas de segurança pelos fornecedores externos que mantêm estas infraestruturas. Além disso, a realização de testes regulares de penetração específicos para OT é fundamental para antecipar potenciais vulnerabilidades.

5.1.3 Cenário 3

A indisponibilidade de sistemas críticos da PowerPlus, que suportam os serviços de 20 milhões de clientes de eletricidade e 1,3 milhões de clientes de gás, pode resultar de falhas em *data*

centers, ataques de negação de serviço (DDoS) ou problemas nas infraestruturas *cloud* utilizadas pela organização. Um incidente deste tipo pode causar uma interrupção massiva nos serviços, impactando negativamente a confiança pública e gerando perdas financeiras significativas. Além disso, a incapacidade de cumprir os Acordos de Nível de Serviço (SLAs) pode resultar em ações legais e custos operacionais elevados.

Para mitigar este cenário, é recomendado reforçar os mecanismos de redundância entre *data centers,* assegurando que o *failover* automático seja ativado em casos de falha em um dos locais. A adoção de SLAs mais rigorosos com fornecedores de infraestrutura *cloud* também é essencial para garantir a disponibilidade contínua dos serviços. Por fim, a realização regular de testes de recuperação de desastres (DRP) é indispensável para simular cenários de falha total, permitindo avaliar a eficácia das medidas de contingência e a resiliência dos sistemas.

Capítulo 6: Conclusão

Com este relatório foi possível fazer a análise e gestão de risco em segurança informática de uma organização, a PowerPlus, onde se destacou a importância de uma abordagem estruturada e abrangente na proteção dos ativos críticos. A implementação das normas internacionais, como as ISO/IEC 27001, ISO/IEC 27005 e ISO 31000, foi essencial para estabelecer um quadro robusto que assegure a gestão proativa dos riscos e a resiliência da organização face às ameaças emergentes.

A análise detalhada apresentada nos capítulos anteriores demonstrou a complexidade do panorama de risco enfrentado pela organização, considerando tanto fatores internos como externos. A organização opera numa infraestrutura tecnológica sofisticada, sustentada por sistemas críticos, aplicações essenciais e uma rede de *data centers* que garantem a continuidade operacional. Este contexto, aliado à crescente sofisticação das ameaças cibernéticas, reforça a necessidade de uma gestão de riscos eficaz, integrada e adaptável.

Os resultados da apreciação de risco destacaram os principais desafios que a organização enfrenta, incluindo vulnerabilidades tecnológicas, ameaças externas e internas, bem como os impactos potenciais em termos financeiros, reputacionais e operacionais. Além disso, o enquadramento regulamentar, com destaque para o GDPR e as normas da NERC CIP, apresenta requisitos rigorosos que demandam um compromisso contínuo com a conformidade e a melhoria das políticas de segurança.

Neste contexto, a criação e operacionalização da equipa de SOC destaca-se como elementos cruciais na estratégia de segurança da organização, pois não apenas monitorizam e respondem a incidentes de forma proativa, mas também fornecem feedback importante para o aperfeiçoamento contínuo das medidas de segurança, alinhando às melhores práticas internacionais. A formação contínua de todas as equipas internas e a utilização de ferramentas

tecnológicas avançadas, garante que a organização se encontre preparada para enfrentar ameaças cada vez mais sofisticadas.

Neste relatório também se destacou a relevância da gestão de riscos como um processo dinâmico e colaborativo. A identificação de ativos, ameaças, vulnerabilidades e consequências permitiu mapear diversos cenários de riscos de forma abrangente. Além disso, a aplicação dos critérios de probabilidade, impacto e aceitação de risco foi essencial para priorizar as ações de mitigação e assegurar a utilização eficiente dos recursos.

Concluindo, ao aplicar de uma forma eficaz a gestão riscos de uma organização não é apenas uma questão de conformidade regulamentar, mas é essencialmente uma estratégia fundamental para garantir a sustentabilidade e o crescimento da organização. A PowerPlus, ao adotar uma abordagem integrada e orientada das normas internacionais, encontra-se bem posicionada para proteger os seus ativos críticos, assegurar a confiança de todos os seus *stakeholders* e promover a sua missão de inovação e a sustentabilidade no setor energético. Com este relatório podemos confirmar o compromisso da organização com a melhoria contínua, contribuindo para a resiliência e competitividade num ambiente global cada vez mais desafiante.

Referências

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

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

[3]. 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.

[4]. 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.

[5]. 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