

ANEXO I

Relatórios para os Serviços especializados em segurança da informação

Os Serviços de Segurança da Informação visam garantir a confidencialidade, integridade e disponibilidade das informações da PPSA (Pré-Sal Petróleo S.A.), bem como assegurar a conformidade com as melhores práticas e legislações vigentes em segurança cibernética. Esses serviços envolvem a geração de relatórios especializados que abordam as vulnerabilidades, ameaças, incidentes e demais aspectos relacionados à segurança da informação no ambiente da PPSA.

A solicitação dos serviços de segurança será feita pela PPSA, conforme a necessidade, por meio da abertura de um chamado na ferramenta de Gerenciamento de Serviços de TI (ITSM), onde será especificado o tipo de relatório requerido e as informações relevantes para sua elaboração.

Após a abertura do chamado pela PPSA no **ITSM**, a CONTRATADA terá um prazo de até **5 (cinco) dias úteis** para:

- Confirmar o recebimento da solicitação e o início do processo de elaboração do relatório; ou
- Solicitar informações adicionais à PPSA, caso seja necessário um esclarecimento ou complementação de dados para a elaboração do relatório.

Após a confirmação do atendimento inicial ou o fornecimento das informações complementares, conforme aplicável, a CONTRATADA terá um prazo máximo de **60 (sessenta) dias corridos** para concluir e entregar o relatório solicitado.

O relatório deverá ser entregue por meio da ferramenta **ITSM**, acompanhado de todos os detalhes e evidências que fundamentem as análises e recomendações realizadas no âmbito da segurança da informação.

Após o recebimento do relatório, a **PPSA** terá um prazo de até **10 (dez) dias corridos** para revisar o documento e formalizar a aceitação do serviço, caso o mesmo esteja de acordo com os critérios estabelecidos.

Caso a **PPSA** identifique inconsistências ou a necessidade de ajustes no relatório, ela comunicará à CONTRATADA, por meio da ferramenta **ITSM**, descrevendo as correções necessárias. A CONTRATADA terá um prazo de **5 (cinco) dias corridos** para realizar as correções solicitadas e reenviar o relatório ajustado.

Se após a entrega das correções, o relatório ainda não atender aos requisitos estabelecidos, a **PPSA** poderá registrar formalmente a não conformidade do serviço e proceder com as ações previstas nos contratos, inclusive a aplicação de penalidades, se for o caso.

Ao final do processo de entrega e aceite dos relatórios, a PPSA aplicará os **Instrumentos de Medição de Resultado (IMR)** descritos no Termo de Referência, conforme critérios de qualidade, prazo e conformidade definidos. O desempenho da CONTRATADA será avaliado com base nesses indicadores, e os resultados poderão impactar diretamente o pagamento do relatório.

Abaixo apresenta-se a **estrutura mínima** que deverá estar presente em todos os relatórios elaborados pela CONTRATADA no âmbito dos **Serviços de Segurança da Informação**:

Estrutura Geral de Todos os Relatórios

1. Capa

- Título do Relatório
- Data de Emissão
- Autor(es)
- Confidencialidade

2. Sumário Executivo

- Visão geral dos principais pontos e recomendações
- Resumo das conclusões

3. Índice

- Listagem das seções e subseções com números de página

4. Introdução

- **Objetivo do Relatório:** Definir claramente o propósito e os objetivos específicos.
- **Escopo:** Delimitar o que será abordado e o que está fora do escopo.

- **Metodologia:** Descrever os métodos utilizados para coletar e analisar os dados.

5. Contextualização e Necessidades

- **Contexto Organizacional:** Breve descrição da PPSA e sua infraestrutura de TI relevante para o relatório.
- **Necessidades Identificadas:** Explicar as necessidades que motivaram a solicitação do relatório.

6. Análise Técnica

- **Descrição Detalhada:** Análise aprofundada do tema específico do relatório.
- **Identificação de Problemas/Vulnerabilidades:** Detalhar as questões encontradas.
- **Avaliação de Impacto:** Analisar as consequências potenciais das vulnerabilidades ou problemas identificados.

7. Recomendações Técnicas

- **Soluções Propostas:** Apresentar ações concretas para mitigar riscos ou resolver problemas.
- **Justificativas:** Explicar por que as recomendações são adequadas.
- **Plano de Implementação:** Sugestão de como as recomendações podem ser implementadas.

8. Conclusão

- Resumo das principais descobertas e recomendações.
- Considerações finais sobre a postura de segurança da PPSA.

9. Anexos

- Dados adicionais, gráficos, tabelas, etc.
- Referências Bibliográficas

Abaixo seguem os tópicos que deverão estar, no mínimo, presentes em cada tipo de relatório:

Estrutura Específica para Cada Tipo de Relatório

1. Relatório de Avaliação de Riscos de Segurança da Informação

Identificação de Riscos

- **Ameaças Internas:** Detalhar potenciais ameaças provenientes de dentro da organização.
- **Ameaças Externas:** Identificar ameaças externas que podem afetar a PPSA.
- **Vulnerabilidades:** Listar vulnerabilidades nos sistemas, processos e pessoas.

Análise de Riscos

- **Probabilidade de Ocorrência:** Avaliar a probabilidade de cada risco identificado.
- **Impacto Potencial:** Analisar o impacto que cada risco pode ter nos ativos da empresa.
- **Matriz de Riscos:** Apresentar uma matriz que relaciona a probabilidade e o impacto dos riscos.

Mitigação de Riscos

- **Estratégias de Mitigação:** Descrever as estratégias para reduzir ou eliminar riscos.
- **Planos de Ação:** Detalhar os passos necessários para implementar as estratégias de mitigação.

Conclusão

- Resumo dos Principais Riscos e Recomendações de Mitigação

Anexos

- Tabelas e Gráficos de Riscos

2. Relatório de Conformidade e Adequação Regulamentar

Contextualização e Necessidades

- Requisitos Legais e Regulamentares Aplicáveis (e.g., LGPD)
- Necessidade de Avaliação de Conformidade

Avaliação de Conformidade

- **Normas e Regulamentos Aplicáveis:** Listar as normas e regulamentos relevantes.
- **Análise de Lacunas (Gap Analysis):** Identificar onde a PPSA está em conformidade e onde não está.
- **Impacto das Não-Conformidades:** Avaliar as consequências das lacunas identificadas.

Recomendações para Adequação

- **Ações Corretivas:** Propor ações para fechar as lacunas de conformidade.
- **Plano de Implementação:** Detalhar como as ações corretivas devem ser implementadas.
- **Monitoramento e Revisão:** Sugerir mecanismos para monitorar a conformidade contínua.

Conclusão

- Resumo das Principais Lacunas e Recomendações de Adequação

Anexos

- Detalhamento das Normas Avaliadas
- Tabelas de Gap Analysis

3. Relatório de Revisão da Arquitetura de Segurança

Contextualização e Necessidades

- Descrição da Arquitetura de TI Atual da PPSA
- Necessidade de Revisão da Arquitetura de Segurança

Análise da Infraestrutura de TI

- **Redes:** Avaliação da segurança das redes.
- **Sistemas e Aplicativos:** Análise dos controles de segurança implementados.
- **Controles de Segurança:** Revisão de firewalls, criptografia, IDS/IPS, etc.

Identificação de Vulnerabilidades

- Detalhamento das Vulnerabilidades Encontradas na Arquitetura
- Avaliação do Impacto das Vulnerabilidades

Recomendações Técnicas

- **Melhorias na Arquitetura:** Propor alterações na infraestrutura para aumentar a segurança.
- **Implementação de Novos Controles:** Sugerir novos controles de segurança a serem implementados.
- **Plano de Ação:** Detalhar como as recomendações devem ser executadas.

Conclusão

- Resumo das Vulnerabilidades e Recomendações para a Arquitetura de Segurança

Anexos

- Diagramas da Arquitetura Atual e Proposta
- Listagem Detalhada de Vulnerabilidades

4. Relatório de Análise de Incidentes e Resposta a Emergências

Introdução

Contextualização e Necessidades

- Histórico de Incidentes de Segurança na PPSA
- Necessidade de Melhorar a Resposta a Incidentes

Análise de Incidentes

- **Descrição dos Incidentes:** Detalhar os incidentes ocorridos, incluindo datas, sistemas ou serviços afetados, tipo de ataque ou falha, e origem do incidente.
- **Tempo de resposta:** Medir o tempo decorrido entre a detecção do incidente e a conclusão da resposta, destacando pontos de melhoria no processo de resposta a incidentes.
- **Resposta Implementada:** Avaliar as ações tomadas durante a resposta, com ênfase na contenção, mitigação e recuperação do incidente.
- **Eficácia das Ações:** Analisar a eficácia das respostas.
- **Padrões Recorrentes:** Identificar padrões que indicam vulnerabilidades sistêmicas, com base em incidentes anteriores e nas áreas mais afetadas.
- **Recomendações para o futuro:** Sugerir ações preventivas, como reforço de controles, auditorias periódicas e implementação de novas tecnologias ou práticas de segurança.

Avaliação dos Processos de Resposta

- **Detecção de Incidentes:** Avaliar a eficácia dos processos de detecção.
- **Comunicação e Coordenação:** Analisar a comunicação interna durante os incidentes.
- **Recuperação e Restabelecimento:** Avaliar os processos de recuperação pós-incidente.

Recomendações para Melhorias

- **Aprimoramento dos Processos:** Sugerir melhorias nos processos de detecção e resposta.
- **Treinamento e Capacitação:** Recomendar treinamentos para a equipe.

- **Implementação de Ferramentas:** Sugerir ferramentas para melhorar a resposta a incidentes.
- **Plano de Ação:** Detalhar como as recomendações devem ser implementadas.

Conclusão

- Resumo das Análises e Recomendações para Melhoria na Resposta a Incidentes

Anexos

- Relatórios Detalhados de Incidentes
- Fluxogramas dos Processos de Resposta

5. Relatório de Análise de Maturidade em Segurança da Informação

Contextualização e Necessidades

- Importância da Maturidade em Segurança da Informação
- Necessidade de Avaliação da Maturidade na PPSA

Avaliação de Maturidade

- **Modelo Utilizado:** Descrever o modelo de maturidade adotado (e.g., COBIT, ISO 27001).
- **Níveis de Maturidade:** Definir os níveis de maturidade avaliados.
- **Avaliação Atual:** Analisar o nível atual de maturidade dos processos de segurança da PPSA.

Identificação de Gaps

- **Áreas de Baixa Maturidade:** Detalhar as áreas que estão abaixo do nível ideal.
- **Impacto dos Gaps:** Avaliar como os gaps afetam a segurança da informação.

Recomendações para Evolução da Maturidade

- **Ações Concretas:** Propor ações específicas para melhorar a maturidade.
- **Roadmap de Implementação:** Desenvolver um plano de evolução contínua.

- **Monitoramento e Avaliação Contínua:** Sugerir mecanismos para monitorar o progresso.

Conclusão

- Resumo das Avaliações de Maturidade e Recomendações para Melhoria

Anexos

- Detalhamento dos Critérios de Maturidade
- Tabelas de Avaliação de Maturidade

6. Relatório de Tendências em Segurança Cibernética e Tecnologias Emergentes

Contextualização e Necessidades

- Importância de Acompanhar Tendências em Segurança Cibernética
- Necessidade de Avaliação das Tecnologias Emergentes para a PPSA

Análise de Tendências Globais (As tecnologias descritas são exemplificativas)

- **Arquiteturas de Segurança Emergentes:** Zero Trust Architecture (ZTA), Extended Detection and Response (XDR), Secure Access Service Edge (SASE), etc.
- **Automação e Resposta a Incidentes:** Plataformas de automação como SOAR.
- **Novas Ameaças:** Ransomware-as-a-Service (RaaS), ataques à cadeia de suprimentos digitais, etc.

Impacto das Tendências na PPSA

- **Avaliação do Impacto Potencial:** Como as tendências identificadas podem afetar a segurança da PPSA.
- **Oportunidades de Adoção:** Benefícios da adoção das novas tecnologias.
- **Desafios e Riscos:** Potenciais desafios na implementação dessas tecnologias.

Recomendações para Adoção de Tecnologias Emergentes

- **Tecnologias Recomendadas:** Quais tecnologias adotar e por quê.
- **Plano de Implementação:** Como integrar as novas tecnologias na infraestrutura existente.
- **Mitigação de Riscos:** Estratégias para mitigar os riscos associados à adoção de novas tecnologias.

Conclusão

- Resumo das Tendências Analisadas e Recomendações para Fortalecimento da Postura de Segurança

Anexos

- Detalhes Técnicos das Tecnologias Emergentes
- Estudos de Caso e Referências