6.2 - Política Interna

- 6.2.1 - Atende pelo menos 25% das recomendações da OT 013 ? Segurança da informação
- 6.2.2 - Atende pelo menos 50% das recomendações da OT 013 ? Segurança da informação
- 6.2.3 - Atende pelo menos 75% das recomendações da OT 013 ? Segurança da informação
- 6.2.4 - Atende 100% das recomendações da OT 013 ? Segurança da informação
- 6.2.5 - Atende pelo menos 25% das recomendações da OT 007 - Backup e armazenamento de dados
- 6.2.6 - Atende pelo menos 50% das recomendações da OT 007 - Backup e armazenamento de dados
- 6.2.7 - Atende pelo menos 75% das recomendações da OT 007 - Backup e armazenamento de dados
- 6.2.8 - Atende 100% das recomendações da OT 007 - Backup e armazenamento de dados
- 6.2.9 - Definiu procedimentos para incidentes de segurança da informação.
- 6.2.10 - Possui controle de registro de logs
- 6.2.11 - Possui matriz de risco em sistemas da informação.
- 6.2.12 - Frequência pelo menos anual de testes de vulnerabilidade e auditorias de segurança.

6.2.1 - Atende pelo menos 25% das recomendações da OT 013 ? Segurança da informação

Detalhes do Critério

O que: As recomendações estabelecidas na OT 013 ? Segurança da informação.

Por que: Para melhorar o nível de segurança da informação do órgão, seguindo as diretrizes da OT 013.

Onde: Na infraestrutura e nos processos do órgão setorial.

Quando: O atendimento a essas recomendações é uma condição contínua.

Quem: A área de Tecnologia da Informação (TIC) do órgão setorial e demais interessados são responsáveis por implementar essas recomendações.

Como: Implementando as recomendações e realizando as adequações necessárias.

Quanto: Pelo menos 25% das recomendações da OT 013.

6.2.2 - Atende pelo menos 50% das recomendações da OT 013 ? Segurança da informação

Detalhes do Critério

O que: As recomendações estabelecidas na OT 013 ? Segurança da informação.

Por que: Para aprimorar ainda mais a segurança da informação, buscando um nível mais elevado de conformidade com as melhores práticas.

Onde: Na infraestrutura e nos processos do órgão setorial.

Quando: O atendimento a essas recomendações é uma condição contínua.

Quem: A área de Tecnologia da Informação (TIC) do órgão setorial e demais interessados são responsáveis por implementar essas recomendações.

Como: Implementando um maior número de recomendações da OT 013.

Quanto: Pelo menos 50% das recomendações da OT 013.

6.2.3 - Atende pelo menos 75% das recomendações da OT 013 ? Segurança da informação

Detalhes do Critério

O que: As recomendações estabelecidas na OT 013 ? Segurança da informação.

Por que: Para alcançar um alto nível de segurança da informação, seguindo as melhores práticas estabelecidas na OT 013.

Onde: Na infraestrutura e nos processos do órgão setorial.

Quando: O atendimento a essas recomendações é uma condição contínua.

Quem: A área de Tecnologia da Informação (TIC) do órgão setorial e demais interessados sãp responsáveis por implementar essas recomendações.

Como: Implementando um número significativo de recomendações da OT 013.

Quanto: Pelo menos 75% das recomendações da OT 013.

6.2.4 - Atende 100% das recomendações da OT 013 ? Segurança da informação

Detalhes do Critério

O que: As recomendações estabelecidas na OT 013 ? Segurança da informação.

Por que: Para alcançar o máximo nível de segurança da informação, implementando todas as melhores práticas recomendadas na OT 013.

Onde: Na infraestrutura e nos processos do órgão setorial.

Quando: O atendimento a essas recomendações é uma condição contínua.

Quem: A área de Tecnologia da Informação (TIC) do órgão setorial e demais interessados são responsáveis por implementar essas recomendações.

Como: Implementando e mantendo todas as recomendações da OT 013.

Quanto: 100% das recomendações da OT 013.

6.2.5 - Atende pelo menos 25% das recomendações da OT 007 - Backup e armazenamento de dados

Detalhes do Critério

O que: O órgão setorial implementou pelo menos 25% das recomendações da OT 007, que trata de backup e armazenamento de dados.

Por que: Para garantir a proteção e a disponibilidade dos dados do órgão em caso de falhas ou incidentes, seguindo as diretrizes da OT 007.

Onde: Nos sistemas e na infraestrutura de armazenamento de dados do órgão setorial.

Quando: O atendimento a essas recomendações é uma condição contínua.

Quem: A área de Tecnologia da Informação (TIC) do órgão setorial e demais interessados são responsáveis por implementar essas recomendações.

Como: Implementando as recomendações e realizando as adequações necessárias nos processos de backup e armazenamento.

Quanto: Pelo menos 25% das recomendações da OT 007.

6.2.6 - Atende pelo menos 50% das recomendações da OT 007 - Backup e armazenamento de dados

Detalhes do Critério

O que: O órgão setorial atende a pelo menos metade das recomendações da OT 007 sobre backup e armazenamento de dados.

Por que: Para aprimorar a proteção e a disponibilidade dos dados, buscando um nível mais elevado de conformidade com as melhores práticas.

Onde: Nos sistemas e na infraestrutura de armazenamento de dados do órgão setorial.

Quando: O atendimento a essas recomendações é uma condição contínua.

Quem: A área de Tecnologia da Informação (TIC) do órgão setorial e demais interessados são responsáveis por implementar essas recomendações.

Como: Implementando um maior número de recomendações da OT 007.

Quanto: Pelo menos 50% das recomendações da OT 007.

6.2.7 - Atende pelo menos 75% das recomendações da OT 007 - Backup e armazenamento de dados

Detalhes do Critério

O que: O órgão setorial atende a pelo menos 75% das recomendações da OT 007 relacionadas a backup e armazenamento de dados.

Por que: Para alcançar um alto nível de proteção e disponibilidade dos dados, seguindo as melhores práticas estabelecidas na OT 007.

Onde: Nos sistemas e na infraestrutura de armazenamento de dados do órgão setorial.

Quando: O atendimento a essas recomendações é uma condição contínua.

Quem: A área de Tecnologia da Informação (TIC) do órgão setorial e demais interessados são responsáveis por implementar essas recomendações.

Como: Implementando um número significativo de recomendações da OT 007.

Quanto: Pelo menos 75% das recomendações da OT 007.

6.2.8 - Atende 100% das recomendações da OT 007 - Backup e armazenamento de dados

Detalhes do Critério

O que: O órgão setorial atende a todas as recomendações da OT 007 sobre backup e armazenamento de dados.

Por que: Para garantir a máxima proteção e disponibilidade dos dados do órgão setorial, implementando todas as melhores práticas recomendadas na OT 007.

Onde: Nos sistemas e na infraestrutura de armazenamento de dados do órgão setorial.

Quando: O atendimento a essas recomendações é uma condição contínua.

Quem: A área de Tecnologia da Informação (TIC) do órgão setorial e demais interessados são responsáveis por implementar essas recomendações.

Como: Implementando e mantendo todas as recomendações da OT 007.

Quanto: 100% das recomendações da OT 007.

6.2.9 - Definiu procedimentos para incidentes de segurança da informação.

Detalhes do Critério

O que: O órgão estabeleceu um conjunto de procedimentos a serem seguidos em caso de ocorrências que comprometam a segurança da informação.

Por que: Para garantir uma resposta rápida, eficaz e coordenada a incidentes de segurança, minimizando danos e restaurando a normalidade o mais breve possível.

Onde: Os procedimentos são aplicados em toda a infraestrutura e nos sistemas de informação do órgão.

Quando: Sempre que um incidente de segurança da informação for detectado.

Quem: A área de TIC do órgão é geralmente responsável pela definição e execução desses procedimentos.

Como: Documentando os passos a serem seguidos para diferentes tipos de incidentes, definindo responsabilidades e fluxos de comunicação.

Quanto: A definição dos procedimentos.

6.2.10 - Possui controle de registro de logs

Detalhes do Critério

O que: O órgão setorial mantém um sistema de registro de eventos (logs) em seus sistemas de informação, permitindo o acompanhamento de atividades e a identificação de possíveis problemas ou incidentes de segurança (a necessidade de "escalonar em parciais" sugere diferentes níveis de detalhe ou abrangência dos logs).

Por que: Os logs são essenciais para monitorar a saúde dos sistemas, diagnosticar falhas, investigar incidentes de segurança e garantir a rastreabilidade das ações.

Onde: Nos servidores e sistemas de informação do órgão, onde os logs são armazenados.

Quando: O registro de logs é contínuo. A análise dos logs ocorre conforme a necessidade.

Quem: A área de TIC do órgão setorial é responsável pela implementação e manutenção do sistema de logs.

Como: Configurando os sistemas para registrar os eventos relevantes e implementando ferramentas para armazenamento e análise dos logs.

Quanto: Refere-se à implementação do controle de registro de logs.

6.2.11 - Possui matriz de risco em sistemas da informação.

Detalhes do Critério

O que: O órgão setorial desenvolveu e mantém uma matriz de risco que identifica e avalia as ameaças e vulnerabilidades aos seus sistemas de informação, bem como o impacto potencial desses riscos.

Por que: A matriz de risco é uma ferramenta fundamental para a gestão da segurança da informação, permitindo priorizar os esforços e os investimentos em medidas de proteção mais eficazes contra os riscos mais críticos.

Onde: A matriz de risco é um documento interno do órgão setorial.

Quando: A matriz de risco deve ser revisada e atualizada periodicamente.

Quem: A área de TIC do órgão setorial, possivelmente em colaboração com outras áreas, é responsável pela elaboração e manutenção da matriz de risco.

Como: Realizando análises de risco, identificando ativos, ameaças e vulnerabilidades, avaliando o impacto e a probabilidade dos riscos, e documentando tudo na matriz.

Quanto: A elaboração e manutenção da matriz de risco.

6.2.12 - Frequência pelo menos anual de testes de vulnerabilidade e auditorias de segurança.

Detalhes do Critério

O que: O órgão setorial realiza testes para identificar vulnerabilidades em seus sistemas e auditorias para avaliar a eficácia de suas medidas de segurança da informação, com uma frequência mínima de uma vez por ano.

Por que: Testes de vulnerabilidade e auditorias são importantes para identificar falhas de segurança que podem ser exploradas e para verificar se as políticas e os controles de segurança estão sendo implementados e estão funcionando corretamente. A frequência anual garante uma avaliação regular da postura de segurança do órgão.

Onde: Nos sistemas e na infraestrutura de TIC do órgão setorial.

Quando: Pelo menos uma vez a cada ano.

Quem: A área de TIC do órgão setorial, possivelmente com o apoio de empresas especializadas em segurança da informação.

Como: Utilizando ferramentas, metodologias ou frameworks específicos para realizar os testes e as auditorias, além de documentar os resultados e as recomendações.

Quanto: Pelo menos uma vez por ano.