6 - Segurança da Informação

- 6.1 - Lei Geral de Proteção de Dados
  - 6.1.1 - Pelo menos 25% dos sistemas informam o motivo da coleta e solicita o consentimento do titular dos dados.
  - 6.1.2 - 50% dos sistemas informam o motivo da coleta e solicita o consentimento do titular dos dados.
  - 6.1.3 - 75% dos sistemas informam o motivo da coleta e solicita o consentimento do titular dos dados.
  - 6.1.4 - 100% dos sistemas informam o motivo da coleta e solicita o consentimento do titular dos dados.
  - 6.1.5 - Faz uso de clausulas contratuais de sigilo nas relações operacionais e nas prestações de serviços que envolvem dados pessoais.
  - 6.1.6 - Pelo menos 25% dos contratos vigentes possuem as cláusulas de confidencialidade.
  - 6.1.7 - Pelo menos 50% dos contratos vigentes possuem as cláusulas de confidencialidade.
  - 6.1.8 - Pelo menos 75% dos contratos vigentes possuem as cláusulas de confidencialidade.
  - 6.1.9 - Pelo menos 100% dos contratos vigentes possuem as cláusulas de confidencialidade.
  - 6.1.10 - Em atendimento ao plano de adequação à LGPD, conforme decreto municipal vigente, foi elaborado o ROTDP (Registros das Operações de Tratamento de Dados Pessoais).
  - 6.1.11 - Tem contribuído com revisão e atualização periódica do ROTDP.

- 6.1.12 - O órgão setorial concluiu a etapa de autoavaliação para o diagnóstico amplo da LGPD.
- 6.1.13 - Em atendimento ao plano de adequação à LGPD, conforme decreto municipal vigente, foi elaborado o RIPD.
- 6.1.14 - Tem contribuído com revisão e atualização periódica do RIPD.
- 6.1.15 - RIPD foi direcionado para repositório CGM.
- 6.1.16 - A equipe de TIC possui membros capacitados em cursos relacionados a Lei Geral de Proteção de Dados (LGPD)
- 6.1.17 - Membro da equipe de TIC participa formalmente do grupo de trabalho da LGPD
- 6.1.18 - Membro da equipe de TIC é o encarregado da LGPD no órgão setorial

- 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.

6.1 - Lei Geral de Proteção de Dados

6.1.1 - Pelo menos 25% dos sistemas informam o motivo da coleta e solicita o consentimento do titular dos dados.

Detalhes do Critério

O que: Os sistemas de informação do órgão setorial que lidam com dados pessoais comunicam aos usuários sobre a finalidade da coleta de seus dados dando a oportunidade de consentir com o tratamento.

Por que: Para atender aos requisitos da Lei Geral de Proteção de Dados (LGPD) e garantir a transparência e o respeito aos direitos dos titulares dos dados.

Onde: Nas interfaces dos sistemas de informação.

Quando: Durante a interação dos usuários com esses sistemas, no momento da coleta de dados.

Quem: Os responsáveis pela gestão e desenvolvimento dos sistemas de informação do órgão setorial.

Como: Implementando funcionalidades nos sistemas que exibem as informações sobre a coleta e solicitam o consentimento.

Quanto: Pelo menos 25% dos sistemas em conformidade aos requisitos da LGPD.

6.1.2 - 50% dos sistemas informam o motivo da coleta e solicita o consentimento do titular dos dados.

Detalhes do Critério

O que: Os sistemas de informação do órgão setorial que lidam com dados pessoais comunicam aos usuários sobre a finalidade da coleta de seus dados dando a oportunidade de consentir com o tratamento.

Por que: Maior abrangência no atendimento aos requisitos da Lei Geral de Proteção de Dados (LGPD) e garantir a transparência e o respeito aos direitos dos titulares dos dados.

Onde: Nas interfaces dos sistemas de informação.

Quando: Durante a interação dos usuários com esses sistemas, no momento da coleta de dados.

Quem: Os responsáveis pela gestão e desenvolvimento dos sistemas de informação do órgão setorial.

Como: Implementando funcionalidades nos sistemas que exibem as informações sobre a coleta e solicitam o consentimento.

Quanto: 50% dos sistemas em conformidade aos requisitos da LGPD.

6.1.3 - 75% dos sistemas informam o motivo da coleta e solicita o consentimento do titular dos dados.

Detalhes do Critério

O que: Os sistemas de informação do órgão setorial que lidam com dados pessoais comunicam aos usuários sobre a finalidade da coleta de seus dados dando a oportunidade de consentir com o tratamento.

Por que: Nível ainda mais elevado aos requisitos da Lei Geral de Proteção de Dados (LGPD) e garantir a transparência e o respeito aos direitos dos titulares dos dados.

Onde: Nas interfaces dos sistemas de informação.

Quando: Durante a interação dos usuários com esses sistemas, no momento da coleta de dados.

Quem: Os responsáveis pela gestão e desenvolvimento dos sistemas de informação do órgão setorial.

Como: Implementando funcionalidades nos sistemas que exibem as informações sobre a coleta e solicitam o consentimento.

Quanto: 75% dos sistemas em conformidade aos requisitos da LGPD.

6.1.4 - 100% dos sistemas informam o motivo da coleta e solicita o consentimento do titular dos dados.

Detalhes do Critério

O que: Os sistemas de informação do órgão setorial que lidam com dados pessoais comunicam aos usuários sobre a finalidade da coleta de seus dados dando a oportunidade de consentir com o tratamento.

Por que: Total conformidade aos requisitos da Lei Geral de Proteção de Dados (LGPD) e garantir a transparência e o respeito aos direitos dos titulares dos dados.

Onde: Nas interfaces dos sistemas de informação.

Quando: Durante a interação dos usuários com esses sistemas, no momento da coleta de dados.

Quem: Os responsáveis pela gestão e desenvolvimento dos sistemas de informação do órgão setorial.

Como: Implementando funcionalidades nos sistemas que exibem as informações sobre a coleta e solicitam o consentimento.

Quanto: 100% dos sistemas em conformidade aos requisitos da LGPD.

6.1.5 - Faz uso de clausulas contratuais de sigilo nas relações operacionais e nas prestações de serviços que envolvem dados pessoais.

Detalhes do Critério

O que: O órgão setorial utiliza acordos de confidencialidade em suas operações e contratos de serviço onde há tratamento de dados pessoais.

Por que: Para garantir a proteção e a confidencialidade dos dados pessoais compartilhados com terceiros ou manuseados por funcionários, em cumprimento à LGPD e às boas práticas de segurança da informação.

Onde: Nos documentos contratuais e nos acordos internos.

Quando: Na formalização de contratos e no estabelecimento de relações operacionais que envolvem dados pessoais.

Quem: A área jurídica ou de contratos do órgão é responsável por incluir essas cláusulas, e os funcionários e prestadores de serviço que lidam com dados pessoais.

Como: Incluindo cláusulas específicas de confidencialidade nos contratos e formalizando acordos internos de sigilo.

Quanto: Refere-se à prática geral do órgão.

6.1.6 - Pelo menos 25% dos contratos vigentes possuem as cláusulas de confidencialidade.

Detalhes do Critério

O que: Uma parcela de pelo menos 25% dos contratos atualmente em vigor no órgão setorial contém cláusulas que tratam da confidencialidade de dados pessoais.

Por que: Pode ser uma fase inicial de adequação à LGPD ou uma aplicação seletiva das cláusulas a contratos mais sensíveis.

Onde: Nos documentos contratuais vigentes.

Quando: Na edição das minutas ou aditivos contratuais.

Quem: Área jurídica ou de contratos do órgão setorial.

Como: Incluindo as cláusulas em uma parte dos contratos.

Quanto: Até 25% dos contratos possuem cláusula de confidencialidade.

6.1.7 - Pelo menos 50% dos contratos vigentes possuem as cláusulas de confidencialidade.

Detalhes do Critério

O que: Pelo menos metade dos contratos ativos do órgão setorial contêm as cláusulas de confidencialidade para dados pessoais.

Por que: Indica um avanço na inclusão dessas cláusulas em comparação com o item anterior.

Onde: Nos documentos contratuais vigentes.

Quando: Na edição das minutas ou aditivos contratuais.

Quem: Área jurídica ou de contratos do órgão setorial.

Como: Inclusão das cláusulas em mais da metade dos contratos.

Quanto: Até 50% dos contratos possuem cláusula de confidencialidade.

6.1.8 - Pelo menos 75% dos contratos vigentes possuem as cláusulas de confidencialidade.

Detalhes do Critério

O que: Pelo menos 75% dos contratos atualmente em vigor no órgão incluem as cláusulas de confidencialidade para dados pessoais.

Por que: Demonstra um esforço significativo para garantir a proteção de dados em grande parte das relações contratuais.

Onde: Nos documentos contratuais vigentes.

Quando: Na edição das minutas ou aditivos contratuais.

Quem: Área jurídica ou de contratos.

Como: Inclusão das cláusulas em um número maior de contratos.

Quanto: Até 75% dos contratos possuem cláusula de confidencialidade.

6.1.9 - Pelo menos 100% dos contratos vigentes possuem as cláusulas de confidencialidade.

Detalhes do Critério

O que: A totalidade dos contratos atualmente em vigor no órgão contém cláusulas específicas sobre a confidencialidade de dados pessoais

Por que: Garante a proteção de dados em todas as relações contratuais do órgão que envolvam tratamento de dados pessoais, representando a melhor prática em conformidade com a LGPD.

Onde: Nos documentos contratuais vigentes.

Quando: Na edição das minutas ou aditivos contratuais.

Quem: Área jurídica ou de contratos.

Como: Inclusão das cláusulas em todos os contratos.

Quanto: 100% dos contratos possuem cláusula de confidencialidade.

6.1.10 - Em atendimento ao plano de adequação à LGPD, conforme decreto municipal vigente, foi elaborado o ROTDP (Registros das Operações de Tratamento de Dados Pessoais).

Detalhes do Critério

O que: Em cumprimento ao plano de adequação à Lei Geral de Proteção de Dados (LGPD), e conforme o decreto municipal nº 59767/20, o órgão elaborou o Registros das Operações de Tratamento de Dados Pessoais (ROTDP).

Por que: O ROTDP é um documento exigido pela LGPD em certas situações, com o objetivo de identificar e avaliar os possíveis riscos à privacidade e à proteção de dados decorrentes de atividades de tratamento.

Onde: O ROTDP é um documento interno do órgão setorial.

Quando: Em algum momento após a publicação do decreto e como parte do plano de adequação à LGPD.

Quem: A equipe responsável pela adequação à LGPD no órgão setorial, envolvendo a área de TIC e a Controladoria Geral do Município.

Como: Realizando a análise dos processos de tratamento de dados e documentando as conclusões no formato do ROTDP.

Quanto: Na elaboração do ROTDP.

6.1.11 - Tem contribuído com revisão e atualização periódica do ROTDP.

Detalhes do Critério

O que: O órgão setorial mantém um processo contínuo de revisão e atualização do Registros das Operações de Tratamento de Dados Pessoais (ROTDP).

Por que: Para garantir que o ROTDP reflita as práticas atuais de tratamento de dados do órgão setorial, identifique e avalie adequadamente os riscos em constante mudança. A LGPD exige a revisão periódica do relatório.

Onde: O ROTDP é um documento interno que passa por revisões.

Quando: Regularmente, em intervalos definidos ou sempre que houver mudanças significativas nos processos de tratamento de dados.

Quem: A equipe responsável pela adequação à LGPD no órgão setorial, envolvendo a área de TIC e a Controladoria Geral do Município.

Como: Realizando análises periódicas e documentando as alterações no ROTDP.

Quanto: As revisões e atualizações periódicas.

6.1.12 - O órgão setorial concluiu a etapa de autoavaliação para o diagnóstico amplo da LGPD.

Detalhes do Critério

O que: Aplicar uma autoavaliação estruturada sobre a maturidade do órgão em relação à LGPD, com base em controles definidos pela CGM - Controladoria Geral do Município.

Por que: Identificar o nível de conformidade do órgão setorial, orientar ações corretivas e subsidiar a atuação da CGM - Controladoria Geral do Município.

Onde: Realizada internamente em cada órgão setorial, com consolidação e envio à CGM por sistema ou formulário oficial.

Quando: Anualmente ou conforme cronograma definido pela CGM; preferencialmente no início de cada exercício de planejamento.

Quem: Realizada por equipe responsável pela LGPD no órgão setorial, com apoio do encarregado local e da área de TIC, quando aplicável.

Como: Preenchimento do diagnóstico

Quanto: Sem custo financeiro direto; requer alocação de tempo da equipe. Capacitações podem ser exigidas em caso de baixa maturidade.

6.1.13 - Em atendimento ao plano de adequação à LGPD, conforme decreto municipal vigente, foi elaborado o RIPD.

Detalhes do Critério

O que: Em cumprimento ao plano de adequação à Lei Geral de Proteção de Dados (LGPD), e conforme o decreto municipal nº 59767/20, o órgão elaborou o Relatório de Impacto à Proteção de Dados Pessoais (RIPDP).

Por que: O RIPDP é um documento exigido pela LGPD, com o objetivo de identificar e avaliar os possíveis riscos à privacidade e à proteção de dados decorrentes de atividades de tratamento dos dados.

Onde: O RIPDP é um documento interno do órgão.

Quando: Em algum momento após a publicação do decreto e como parte do plano de adequação à LGPD.

Quem: A equipe responsável pela adequação à LGPD no órgão setorial, envolvendo a área de TIC, jurídica e outras relevantes.

Como: Realizando a análise dos processos de tratamento de dados e documentando as conclusões no formato do RIPDP.

Quanto: A elaboração do RIPDP.

6.1.14 - Tem contribuído com revisão e atualização periódica do RIPD.

Detalhes do Critério

O que: O órgão setorial mantém um processo contínuo de revisão e atualização do Relatório de Impacto à Proteção de Dados Pessoais (RIPDP).

Por que: Para garantir que o RIPDP reflita as práticas atuais de tratamento de dados do órgão setorial, identifique e avalie adequadamente os riscos em constante mudança. A LGPD exige a revisão periódica do relatório.

Onde: O RIPDP é um documento interno que passa por revisões.

Quando: Regularmente, em intervalos definidos ou sempre que houver mudanças significativas nos processos de tratamento de dados.

Quem: A equipe responsável pela adequação à LGPD no órgão setorial, envolvendo a área de TIC e a Controladoria Geral do Município.

Como: Realizando análises periódicas e documentando as alterações no RIPDP.

Quanto: As revisões e atualizações periódicas.

6.1.15 - RIPD foi direcionado para repositório CGM.

Detalhes do Critério

O que: O Relatório de Impacto à Proteção de Dados Pessoais (RIPDP) do órgão foi encaminhado para um repositório da Controladoria Geral do Município (CGM).

Por que: Para cumprir requisitos de transparência ou fiscalização da CGM em relação à adequação dos órgãos à LGPD.

Onde: No repositório da CGM.

Quando: Após a elaboração ou atualização do RIPDP.

Quem: A equipe responsável pela adequação à LGPD no órgão setorial, envolvendo a área de TIC e a Controladoria Geral do Município.

Como: Seguindo os procedimentos definidos pela CGM para o envio e armazenamento do RIPDP.

Quanto: O envio do RIPDP para o repositório.

6.1.16 - A equipe de TIC possui membros capacitados em cursos relacionados a Lei Geral de Proteção de Dados (LGPD)

Detalhes do Critério

O que: Capacitar membros da equipe de TIC em temas relacionados à Lei Geral de Proteção de Dados (LGPD).

Por que: Garantir a conformidade legal com a LGPD, reduzir riscos no tratamento de dados pessoais e aumentar a maturidade em proteção de dados no órgão.

Onde: Preferencialmente em ambiente institucional (escola de governo, cursos EAD oficiais) ou por meio de plataformas reconhecidas (ENAP, SENAC, etc.).

Quando: Sempre que necessário, quando houver mudanças relevantes na legislação ou diretrizes internas.

Quem: Servidores da área de TIC indicados pela chefia imediata ou coordenação de tecnologia; prioridade para os que atuam diretamente com tratamento de dados.

Como: Por meio de cursos presenciais ou a distância, com carga horária mínima recomendada para conhecimento de fundamentos da LGPD, princípios, bases legais, direitos dos titulares, segurança da informação e governança de dados.

Quanto: Preferencialmente com uso de recursos gratuitos (ENAP, Controladoria Geral, outros órgãos públicos); caso necessário, orçamento previsto no plano de capacitação da secretaria.

6.1.17 - Membro da equipe de TIC participa formalmente do grupo de trabalho da LGPD

Detalhes do Critério

O que: Designar formalmente pelo menos um membro da equipe de TIC para participar do grupo de trabalho responsável pela implementação e acompanhamento da LGPD no órgão setorial.

Por que: Garantir integração entre a área de tecnologia e as ações de proteção de dados, promovendo suporte técnico e segurança nas decisões do grupo de trabalho, conforme boas práticas de governança de dados.

Onde: No âmbito do órgão setorial e, se necessário, em articulação com o órgão central de proteção de dados da Prefeitura (CGM/CPD).

Quando: Sempre que necessário, quando houver alterações na equipe de TIC. A participação deve ser contínua durante o funcionamento do grupo de trabalho.

Quem: Membro da equipe de TIC, preferencialmente com conhecimento técnico em sistemas, segurança da informação e gestão de dados. Nomeado por ato administrativo (ex.: portaria interna).

Como: Por meio de documento formal (portaria ou ofício) que designe o representante da TIC no GT da LGPD, com participação em reuniões, apoio técnico e elaboração de planos de ação e relatórios.

Quanto: Custo indireto, relativo ao tempo do servidor. Sem necessidade de orçamento adicional, salvo em casos de capacitação específica ou ampliação da equipe.

6.1.18 - Membro da equipe de TIC é o encarregado da LGPD no órgão setorial

Detalhes do Critério

O que: Designar formalmente um membro da equipe de TIC como Encarregado pelo tratamento de dados pessoais (Data Protection Officer ? DPO) do órgão, conforme previsto na LGPD.

Por que: Cumprir o art. 41 da LGPD e o Decreto Municipal nº 59.767/2020, garantindo a existência de um canal de comunicação com os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD), além de orientar a organização sobre práticas de tratamento de dados.

Onde: No âmbito de cada órgão setorial, com comunicação oficial à Controladoria Geral do Município (CGM) e registro no sistema municipal (como o portal LGPD da CGM).

Quando: A designação deve ocorrer formalmente assim que o órgão iniciar a estruturação da sua governança de proteção de dados. Recomenda-se reavaliar periodicamente, especialmente em caso de mudanças de pessoal ou estrutura.

Quem: Membro da equipe de TIC com perfil técnico e institucional, preferencialmente com conhecimento em proteção de dados, segurança da informação e governança. Deve ser nomeado por ato oficial (portaria ou equivalente).

Como: Atribuição formal via portaria do dirigente máximo do órgão, publicada internamente e, se necessário, enviada à CGM. O encarregado deve atuar como ponto de contato, participar de comitês, responder a solicitações e promover a conscientização interna sobre a LGPD.

Quanto: Custo indireto relacionado à alocação de tempo e responsabilidades do servidor. Pode envolver capacitações específicas, que podem ser realizadas com recursos próprios, gratuitos (como ENAP) ou via orçamento de capacitação.

6.2 - Política Interna

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.