INSTRUÇÃO NORMATIVA Nº. 007/2025

"Dispõe sobre a politica de incidente de segurança da informação."

POLÍTICA DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO CÂMARA MUNICIPAL DE BURITIS

1. DEFINIÇÃO

Um Incidente de Segurança da Informação (SI) pode ser definido como qualquer indício de fraude, sabotagem, espionagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer ou ameaçar a segurança da informação. Exemplos comuns desses incidentes são:

- O desfiguramento do portal web de uma instituição;
- A evasão de informações confidenciais;
- A propagação de um vírus ou worm por meio da lista de contatos de e-mails;
- Envio de spam;
- Indisponibilidade de um servidor de banco de dados;
- Tentativas não autorizadas de acesso.

Todo incidente de segurança deve ser tratado seguindo uma metodologia previamente definida pela instituição. Essa metodologia é chamada de Processo de Gerenciamento de Incidentes de Segurança.

O Gerenciamento de Incidentes de Segurança da Informação está voltado para proteger a informação e seus critérios de confidencialidade, integridade e disponibilidade. É uma metodologia organizada para gerir consequências de uma violação de segurança da informação, no intuito de minimizar o impacto de um incidente e permitir o restabelecimento dos sistemas o mais rápido possível.

1.1. Os objetivos do Gerenciamento de Incidente de Segurança da Informação são:

- Identificar se o incidente está no escopo da segurança da informação;
- Identificar o incidente o quanto antes visando neutralizar e mitigar a ameaça;
- Garantir a detecção de eventos e tratamento adequado, incluindo a categorização destes como incidentes de segurança da informação ou não;
- Avaliar e responder da maneira mais adequada possível;
- Minimizar os efeitos adversos de incidentes de segurança a informação (tratando-os o mais brevemente possível);
- Reportar as vulnerabilidades de segurança da informação, além de tratá-las adequadamente;
- Ajudar a prevenir futuras ocorrências, através da manutenção de uma base de lições aprendidas (algo parecido com a base dados de erros conhecidos).

1.2. A Notificação de Incidentes de Segurança é uma atividade de grande importância que ajuda a identificar problemas e prevenir novas ocorrências, visto que:

- Melhora a capacidade de detecção de incidentes;
- Contribui para a segurança geral imagem institucional: ao notificar uma tentativa de ataque da qual foi vítima, ao invés de apenas mitigá-la, busca-se a solução do problema e demonstra-se comprometido com questões de segurança;
- Pode ajudar a conter danos e prejuízos: notificações podem ser instrumentos eficazes na mitigação de incidentes e na contenção dos prejuízos, como por exemplo, em casos de fraudes;
- Permite gerar estatísticas, correlacionar dados e identificar tendências que ajudarão a elaborar recomendações e materiais de apoio, a orientar campanhas pela adoção de boas práticas e a estabelecer ações em cooperação;
- Esta cartilha tem por objetivo orientar, de forma simples, como proceder ao Processo de Notificação de Incidentes de Segurança.

2. FATOS DETERMINANTES: ANÁLISE E POSSÍVEIS OCORRÊNCIAS

2.1. Gravidade 1: Descrição Baixa - Uma Pessoa

- O equipamento ou serviço apresenta falha, mas por necessidade do usuário não há possibilidade de intervenção imediata ou de paralisação;
- O serviço afetado está operando, mas no modo de contingência;
- A requisição pode ser atendida em algum horário posterior sem que haja prejuízo do desempenho das atividades do usuário;
- A solicitação é uma requisição de mudança programada;

2.2. Gravidade 2: Descrição Média - Grupo Pequeno

- A falha afeta o trabalho diário de um ou mais usuários. O equipamento ou serviço de uso coletivo encontra-se operando de modo normal, mas algumas funções secundárias apresentam falhas ou lentidão;
- Trata-se de requisição de serviço cujo não atendimento imediato não impede o trabalho principal do usuário;

2.3. Gravidade 3: Descrição Elevada - Apenas um Grupo

- A falha impossibilita o trabalho diário de um ou mais usuários (ex. problema em um equipamento ou sistema específico, falha no funcionamento do acesso à rede em uma sala ou setor, indisponibilidade da estação de trabalho do usuário, problema em serviço essencial para o usuário);

2.4. Gravidade 4: Descrição Alta - Vários Grupos

- Incidentes que impeçam ou inviabilizem os trabalhos de múltiplas áreas da organização;
- Indisponibilidade ou mau funcionamento de conjunto de serviços ou recursos essenciais;

- O equipamento ou serviço fornecido está operacional, mas apresenta algumas funções principais degradadas;
- Confidencialidade;

2.5. Gravidade 5: Descrição Altíssima - Toda a Organização

- Qualquer incidente relativo à indisponibilidade ou mau funcionamento generalizado de sistemas ou recursos críticos ou sensíveis;
- Incidentes que geram o vazamento de informações confidenciais, causando impacto negativo e danos na imagem institucional da organização;
- Qualquer incidente venha comprometer a integridade e confidencialidade de sistemas institucionais
- Qualquer incidente cujo não atendimento comprometa os serviços de TI prestados. Qualquer incidente ou requisição reportado por usuário estratégico.

3. PROCEDIMENTO

A informação do incidente é uma das etapas do Gerenciamento de Incidentes, que deverá ser registrado e comunicado ao Assessor de Segurança da Informação para acompanhamento e monitoramento do atendimento até sua resolução. O Relatório de Incidentes de Segurança da Informação é a ferramenta de registro e acompanhamento do incidente, onde deverá constar um código de prioridade de acordo com a análise.

3.1. A Comunicação do Incidente

Os incidentes que deverão ser registrados e comunicados ao Assessor de Segurança da Informação que estão definidos nos critérios da análise, devem cumprir as informações classificadas abaixo:

3.1.1. Impacto Altíssimo (Gravidade 5) e Impacto Alto (Gravidade 4)

Passo a passo para realizar nesses casos:

I. Acionar imediatamente (pessoalmente ou por meio de contato telefônico) relatando os fatos determinantes
II. Preencher o Relatório de Incidentes de Segurança da Informação – RISI
III. Descrever o incidente: identificar resumidamente o que ocorreu
IV. Período em que ocorreu o incidente
V. Severidade do incidente: o grau de prioridade,
VI. Tipo de impacto
VII. Origem do alerta (serviço, sistema ou componente)
VIII. Data da notificação do Assessor de Segurança da Informação
IX. Detalhamento do incidente: descrever o que ocorreu, extensão e impactos do incidente, bem como detalhar as causas prováveis do incidente, áreas envolvidas na investigação do incidente, etc
X. Tratamento do Incidente: descrever as ações executadas para a contenção e/ou contorno do problema/incidente, equipes/pessoas envolvidas
XI. Análise e Encerramento do Incidente: Descrever, se necessárias, outras ações

e recursos para finalizar o tratamento do incidente e/ou para evitar que o incidente volte a ocorrer. Se possível, informar prazos e responsáveis para a execução.

3.1.2. Impacto Elevado (Gravidade 3) e Impacto Alto (Gravidade 2)

Notificar por e-mail o Assessor de Segurança da Informação relatando os fatos determinantes e resolução do incidente.

3.1.3. Impacto Baixo (Gravidade 1)

Notificar por e-mail o Assessor de Segurança da Informação relatando os fatos determinantes e resolução do incidente.

IMPORTANTE:

Toda informação relevante durante o ciclo de vida do incidente deve ser registrada. Quando incidente de segurança da informação decorrer de suspeita de descumprimento da Política de Segurança da Informação, será observado o sigilo durante todo o processo, ficando as evidências, informações e demais registros restritos aos envolvidos na investigação.

3.2. O assessor de segurança da informação

O Assessor de Segurança da Informação é o responsável pelo processo de Gerenciamento dos Incidentes de Segurança da Informação. Entre suas atribuições estão:

- Garantir que o Relatório de Incidentes de Segurança da Informação;
- Assegurar a adequada avaliação de impacto do incidente;
- Promover ciclos de análise de riscos de segurança da informação atuais e iminentes, propondo ações para sua mitigação, considerando critérios como: potencial impacto e riscos;
- Promover a melhoria contínua dos indicadores de Segurança da Informação;
- Manifestar-se de ofício ou mediante solicitação, nos assuntos concernentes a Segurança da Informação;
- Propor e revisar as normas relativas à Segurança da Informação.

3.3. Comunicação das Partes Envolvidas

De acordo com a Lei Geral de Proteção de Dados (LGPD), no caso de um incidente de segurança da informação que envolva dados pessoais, o responsável pelo tratamento desses dados (controlador) deve notificar os titulares dos dados afetados.

O procedimento para avisar os titulares dos dados afetados após a ocorrência de um incidente de segurança deverá seguir os seguintes passos:

1) Identificação do Incidente

- Assim que o incidente for identificado e confirmado como uma violação de dados pessoais, o responsável pelo tratamento dos dados deverá iniciar a notificação aos titulares afetados.

2) Avaliação do Impacto

- Antes de fazer a notificação, é importante conduzir uma avaliação do impacto da violação de dados pessoais. Isso ajudará a determinar a extensão do incidente, as categorias de dados afetados e o possível risco para os titulares.

3) Preparação da Notificação

- A notificação aos titulares deve ser clara, concisa e fornecer informações relevantes sobre o incidente e seus impactos.

- A notificação deve incluir informações como a natureza dos dados pessoais afetados, a data provável da violação, as medidas adotadas ou que serão adotadas para mitigar os riscos e os meios de contato para mais informações.

4) Tempo para Notificação

- A LGPD não estabelece um prazo específico para a notificação dos titulares afetados, mas é necessário que a notificação seja feita de forma rápida e eficiente, assim que a violação de dados for confirmada e o impacto for avaliado.

5) Forma de Notificação

- A notificação aos titulares dos dados poderá ser realizada por meios diretos de comunicação, como e-mail, correio físico, mensagem por aplicativo ou por meio de publicações em sites ou jornais, caso a notificação afete muitos titulares.

6) Comunicação Transparente

- A notificação aos titulares deve ser transparente e não deve esconder informações relevantes sobre o incidente.

- Os titulares têm o direito de saber o que aconteceu com seus dados pessoais e quais medidas estão sendo tomadas para protegê-los.

7) Registro da Notificação

- Será necessário registrar todas as notificações enviadas aos titulares dos dados afetados, bem como as ações tomadas para mitigar os riscos decorrentes do incidente.

É importante destacar que a LGPD também prevê que, em casos de incidentes de

segurança de dados que possam acarretar riscos ou danos aos titulares dos dados, a Autoridade Nacional de Proteção de Dados (ANPD) também deverá ser notificada. A ANPD poderá orientar sobre as medidas necessárias para tratar o incidente e cumprir com as obrigações legais decorrentes da LGPD.

Buritis/RO, 23 de Maio de 2025.

Alexandre Castoldi Boareto
Controlador Interno

Publicado no Mural
Câmara Municipal de Buritis

De: 26/05/25 A: 29/06/25