POLÍTICA DE RESPOSTA DE INCIDENTE

1. INTRODUÇÃO

Esta norma visa orientar o funcionamento do processo de gestão de incidentes de segurança cibernética e da informação, de forma que estes sejam tratados adequadamente reduzindo ao máximo os impactos para o negócio.

2. OBJETIVO

Estabelecer princípios, conceitos, diretrizes e responsabilidades sobre a gestão de incidentes de segurança da informação.

3. ESCOPO

A gestão de incidentes de segurança da informação tem o escopo limitado as situações relacionadas ao ambiente, ativos, projetos, desenvolvimento, operacional e tecnológico que tem relação ao processo de negócio da IT TECH SOLUTIONS.

4. Contexto

Essa gestão de resposta a incidente tem como contexto a preparação para a criação de um plano de resposta a incidente.

5. DIRETRIZES

5.1. A direção da IT TECH SOLUTIONS entende que a resposta ao incidente correta é essencial para sua existência e a manutenção da funcionalidade normal das suas atividades.

5.2. A direção da IT TECH SOLUTIONS entende que uma resposta ao incidente incorreta, não treinada ou mal preparada poderá acarretar problemas de disponibilidade, confidencialidade, integridade, financeiro, operacional, de imagem e até jurídico.

5.3. A gestão de incidentes de segurança da informação tem como principal objetivo assegurar que incidentes de segurança da informação sejam identificados, registrador e avaliados em tempo hábil, com a tomada de medidas e contenção e/ou solução adequada.

5.4. Estão abrangidos por esta norma os eventos, confirmados ou suspeitos, relacionados a segurança de sistemas ou redes de computadores, que comprometam o ambiente da IT TECH SOLUTIONS, seus ativos, informações e negócio, bem como aqueles que contrariem os termos da Politica de Segurança da Informação, e dos quais decorrem interrupção, parcial ou total, de serviços essencial ao desempenho das atividades, vulnerabilidades de segurança, divulgação, alteração ou destruição de informações e/ou prática de ato definido como crime ou infração administrativa.

5.5. A IT TECH SOLUTIONS disponibiliza dispositivos de monitoramento, ferramentas de segurança, detecção de intrusão, a fim de subsidiar e auxiliar as atividades da Gestão de Incidentes e Gestão de Segurança da informação.

5.6. A notificação de incidente poderá ser feita por qualquer pessoa, sem necessidade de prévia autorização, através do e-mail paulo@lgpdsolution.com.br ou telefone, no qual irá tomar as primeiras medidas de análise, comunicação e mitigação do incidente.

5.7. O colaborador tem obrigação de notificar, o mais breve possível, os incidentes de segurança da informação e vulnerabilidades das quais ele tenha conhecimento ou suspeita. Entenda incidentes, fragilidade ou vulnerabilidade como algo que pode causar prejuízos, interrupções, mau funcionamento, imprecisão ou vazamento de informação.

5.8. O colaborador é proibido de fazer qualquer teste em fragilidade ou vulnerabilidade que ele venha ter conhecimento ou suspeita.

5.9. Os incidentes de segurança da informação pode ser, mas não se limita a:

5.9.1. Qualquer evento adverso confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores, bem como estruturas físicas e lógicas associadas, que comprometa a confidencialidade, a integridade e a disponibilidade do ambiente da organização.

5.9.2. Indisponibilidade do ambiente tecnológico em virtude de ataque maliciosos interno e externo.

5.9.3. Vazamento de informações confidenciais (informações de cliente, financeira, estratégica e outros)

5.9.4. Tentativas interna ou externa de ganhar acesso não autorizado a sistemas, a dados ou até mesmo comprometer o ambiente de TI

5.9.5. Ato de violar uma política de segurança explicita ou implícita

5.9.6. Uso ou acesso não autorizado a um sistema

5.9.7. Modificações em um sistema, sem o conhecimento, instruções ou consentimento prévio do dono do sistema.

5.9.8. Compartilhamento de senha

5.9.9. Não bloqueio do dispositivo ao não estar usando ou ao sair da frente do equipamento.

5.9.10. Qualquer falha generalizada que impeça o funcionamento normal das operações deverá ser acionados os protocolos adotados na Política de Continuidade de negócio e na Política de Gestão de crise.

5.10. O tratamento da informação deve ser realizado de forma a viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação, com retorno das operações à normalidade no menor prazo possível, bem como evitar futuras ocorrências, com a proposição de ações de solução, quando existentes.

5.11. A Comissão de Segurança e Equipe de Tratamento e Resposta a Incidente de Segurança da Informação devem trabalhar em conjunto com as demais áreas, investigar o incidente e artefatos maliciosos, propondo e implementando as ações de contenção, comunicando as áreas afetadas e coletando os dados necessários.

5.12. Todos os incidentes de segurança da informação devem ser documentados, classificados e priorizados de acordo com a sua criticidade.

5.13. Quando o incidente de segurança da informação decorrer de suspeita de descumprimento da Política de Segurança da Informação ou qualquer norma adotada pela IT TECH SOLUTIONS, será coletado evidências e será submetido ao conselho de segurança da informação para que delibere as medidas que será adotada de punição e de conscientização.

5.14. Quando houver indícios de ilícitos criminais durante o gerenciamento dos incidentes de segurança, o conselho de segurança da informação e o administrativo, deverão avaliar as providências cabíveis.

5.15. A avaliação do processo de gestão de incidentes de segurança da informação ocorrerá através do histórico de incidentes, com verificação das oportunidades de melhoria.

5.16. Toda e qualquer comunicação externa pública deverá ser feita única e exclusivamente pela área de relações públicas

5.17. A substituição ou alteração dessa norma se dará mediante ao entendimento do conselho de segurança.

6. PROCESSO

6.1. O processo de Gestão de Incidentes é composto pelas seguintes etapas:

6.1.1. Identificação: Compreende a identificação por meio de monitoramento, notificação, relatórios, registro ou qualquer outra que aponte eventos adversos. No qual será feito o devido encaminhamento da identificação e investigação.

6.1.2. Comunicação: Compreende por comunicar o incidente as áreas envolvidas, conselho de segurança, diretoria, entidades externas e imprensa quando for considerado necessário.

6.1.3. Coordenação: Compreende a análise do incidente, com verificação da necessidade de outras ações, providências ou comunicações, e após seu cumprimento, o encerramento do incidente.

6.1.4. Mitigação: Compreende por entender o problema e agir prontamente para contorná-lo, minimizado ou eliminá-lo a modo que a funcionalidade do ambiente fique estável

6.1.5. Investigação: compreende a investigação e tratamento do incidente, coleta de dados, comunicação às áreas afetadas, proposição e aplicação de ações de contenção, quando necessárias.

6.1.6. Aprendizado: Compreende a avaliação do histórico de incidentes, com consolidação das informações e indicadores e verificação das oportunidades de melhoria e lições aprendidas

6.2. Os incidentes, notificados ou detectados, devem ser objeto de registro, com a finalidade de assegurar a manutenção do histórico e auxiliar na geração de indicadores.

6.3. Os procedimentos e fluxo de atuação a ser adotados será mais bem detalhado no plano de resposta a incidente.

6.4. O Plano de resposta a Incidente será elaborado pela equipe de segurança da informação, resposta a incidente e gestão de risco.

7. PAPÉIS E RESPONSABILIDADES

7.1. Área de Gestão de Risco

7.1.1. Condução do processo de gestão de incidentes de segurança da informação;

7.1.2. Investigação de incidentes, levantamento, cadeia de custódia e segurança das evidências;

7.1.3. Acompanhamentos dos planos de tratamento junto aos responsáveis pelos incidentes e criação de indicadores e relatórios;

7.1.4. Comunicação aos gestores responsáveis;

7.1.5. Realização de análises pós-incidentes para identificação e tratamento de causas raiz e aprimoramento de processos da empresa e do próprio processo de gestão de incidentes de segurança da informação.

7.2. Equipe de Resposta a Incidente

7.2.1. A equipe de resposta a incidente é composta Ad-Hoc com membros da gestão de risco, segurança da informação, infraestrutura, desenvolvimento e demais áreas se julgado necessário.

7.2.2. Auxilia na investigação de incidente e em toda a responsabilidade atribuída a área de gestão de risco.

7.3. Colaboradores

7.3.1. Devem informar imediatamente á área de resposta a incidente todas as violações as políticas de segurança da informação e suas normas complementares, incidentes, violações de acesos, anomalias que possam indicar a possibilidade de incidentes, sobre os quais venham a tomar conhecimento.

7.4. Infraestrutura e Desenvolvimento:

7.4.1. Provimento dos acessos necessários para que a área de gestão de risco e resposta a incidente possa realizar a identificação e investigação de incidentes de segurança;

7.4.2. Responsável pelo provimento de trilhas de auditoria e evidências para a investigação de incidentes

7.4.3. Suporte as investigações através do fornecimento de informações e esclarecimentos sobre o ambiente tecnológico e os processos da área.

7.4.4. Gestores:

7.4.5. Ao serem notificados sobre incidente que envolvam recursos ou informações sob sua responsabilidade, devem colaborar com eventuais investigações e tratar os incidentes com a devida urgência.

7.5. Jurídico

7.5.1. Suporte às questões legais relacionadas a incidentes de segurança da informação.

7.6. Relações Públicas

7.6.1. Entender a ocorrido e as medidas adotadas e junto com os responsáveis escrever uma nota de imprensa

7.6.2. Emitir nota publica caso necessário sobre o ocorrido e as providências tomadas

8. SANÇÕES E PUNIÇÕES

O descumprimento dessa norma pode acarretar sanções e punições aos envolvidos.

9. REVISÕES

Esta norma deverá ser revisada anualmente ou extraordinariamente quando acontecer algum incidente que requeira aperfeiçoamento das medidas adotadas.