POLÍTICA DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

SUMÁRIO

1. OBJETIVO

Art.1º. A Política de Gestão de Incidentes de Segurança da Informação é o documento que estabelece princípios, conceitos, diretrizes e responsabilidades sobre a gestão de incidentes de segurança da informação do sistema OGMO-RJ e 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. ABRANGÊNCIA

Art.2º. A Política de Gestão de Incidentes de Segurança da Informação tem abrangência corporativa no OGMO-RJ, ou seja, afeta todas as suas áreas de negócio, filiais, escritórios e demais operações no que se refere a ocorrência de incidentes de segurança da informação.

3. CONCEITOS E DEFINIÇÕES

Art.3º. Informação: Qualquer conjunto de dados que resulte em algum significado compreensível. A informação pode possuir algum valor para o OGMO-RJ, seus clientes, parceiros e colaboradores, bem como pode ser de propriedade da empresa ou estar sob sua custódia;

Art.4º. Colaborador: Entende-se como colaborador qualquer pessoa que trabalhe para o OGMO-RJ, quer seja: funcionário com registro em carteira de trabalho, terceiro, estagiário, aprendiz ou trainee;

Art.5º. Gestor: Colaborador que exerce cargo de liderança, como: presidente, vice-presidente, diretor, gerente, coordenador, líder ou chefe de seção;

Art.6º. Recurso: Qualquer ativo, tangível ou intangível, pertencente a serviço ou sob responsabilidade do OGMO-RJ, que possua valor para a empresa. Podem ser considerados recursos: pessoas, ambientes físicos, tecnologias, serviços contratados, em nuvem, sistemas e processos.

4. DIRETRIZES

Art.7º. Esta Política não será extinta ou cancelada. Será revisada em períodos

não superior a um ano, quando será publicada uma nova versão, caso haja necessidade de ajustes.

Art.8º. Será, portanto, substituída por outra com mesmo objetivo e valor que a administração entender cabível ou necessário.

5. PAPÉIS E RESPONSABILIDADES

Art.9º. As responsabilidades do Gestor de TI e do DPO (Data Protection Officer) são:

I. Condução do processo de Gestão de Incidentes de Segurança da Informação;

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

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

IV. Comunicação aos Gestores responsáveis;

V. Realização de análises pós-incidentes (post mortem) 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.

Art.10. As responsabilidades dos Colaboradores são:

I. Devem informar imediatamente à área de Gestão de TI e ao DPO todas as violações às políticas de segurança da informação, incidentes, violações de acessos ou anomalias que possam indicar a possibilidade de incidentes, sobre os quais venham a tomar conhecimento.

Art.11. As responsabilidades da área de TI são:

I. Provimento dos acessos necessários para que a área de Gestão de TI e DPO que possa realizar a identificação e investigação de incidentes de segurança;

II. Responsável pelo provimento de trilhas de auditoria e evidencias para a

investigação de incidentes;

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

Art.12. As responsabilidades dos Gestores são:

I. Ao serem notificados sobre incidentes que envolvam recursos ou informações sob sua responsabilidade, devem colaborar com eventuais investigações e tratar os incidentes com a devida urgência e SLA's pré-definidos pela área de Gestão de TI e DPO.

Art.13. As responsabilidades da área Jurídica são:

I. Suporte às questões legais relacionados a incidentes de segurança da informação.

6. DOS CRITÉRIOS GERAIS SOBRE OS INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Art.14. São considerados Incidentes de Segurança da Informação quaisquer fragilidades ou eventos adversos de segurança, confirmados ou sob suspeita, que levem ou possam levar ao comprometimento de um ou mais dos princípios básicos de segurança da informação: confidencialidade, integridade, disponibilidade e conformidade, colocando o negócio e seus objetivos em risco;

Art.15. Todos os colaboradores devem estar em capacidade de identificar incidentes de segurança da informação quando for testemunhado.

Art.16. Todos os colaboradores devem notificar qualquer evento de segurança ou fragilidade observada que possam causar: prejuízos, interrupções, maus funcionamentos, imprecisão ou vazamento de informação nos sistemas da empresa.

Art.17. Vulnerabilidades ou fragilidades suspeitas não deverão ser objeto de teste ou prova pelos colaboradores, sob o risco de violar a política de segurança cibernética e da informação, bem como provocar danos aos serviços ou recursos tecnológicos.

Art.18. A lista a seguir exemplifica, mas não esgota os possíveis incidentes de segurança da informação tratados nesta política:

I. 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;

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

III. Vazamento de informações confidenciais (informações de clientes, informações estratégicas, outros);

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

V. Ato de violar uma política de segurança, explícita ou implícita;

VI. Uso ou acesso não autorizado a um sistema;

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

VIII. Compartilhamento de senhas.

Art.19. O conteúdo da notificação precisa ser claro, em formato simples e deve incluir as informações necessárias para a rápida e correta identificação do problema e da ação requerida.

Art.20. Os eventos de incidente de segurança da informação devem ser categorizados e classificados através de uma matriz de severidade com intuito de se ter uma melhor visibilidade, tratamento e prioridade quanto a sua gestão.

Art.21. Os eventos abaixo não são considerados eventos de segurança da informação:

I. Eventos acidentais (falhas de hardware ou sistêmicas) não intencionais;

II. Eventos não maliciosos (erro humano ou descuido que não infrinja as regras de segurança da informação).

Art. 22. Todo e qualquer incidente que se caracterize como uma CRISE (extrema severidade) deve seguir o Plano de Crise do OGMO-RJ.

Art.23. Todos os eventos de incidente de segurança da informação devem ser registrados nos controles e/ou ferramentas para a devida triagem e tratamento.

Art.24. A Gestão de Incidentes de Segurança da Informação deve contemplar processos que atendam aos seguintes objetivos:

I. Detecção: identificação de incidentes por meio de monitoração, relatórios, denúncias, informações obtidas de áreas parceiras ou qualquer outra análise de eventos adversos;

II. Registro e análise: registro dos incidentes, análise, classificação quanto ao tipo, severidade e priorização;

III. Comunicação: comunicação do incidente às partes envolvidas e caso necessário entidades externas;

IV. Resposta: contenção do incidente, análises forenses, custódia de evidências, tratamento do incidente e da causa raiz;

V. Finalização: encerramento formal e análise *pós mortem* para identificação de possíveis melhorias em processos, controles e na própria Gestão de Incidentes.

Art.25. É de extrema importância que o horário de servidores e equipamentos de redes estejam sincronizados com uma fonte confiável de tempo (ex: via protocolo NTP) para que não haja disparidades na correlação de eventos, logs e outros dados.

Art.26. Violações ou tentativas de violação da Diretriz de Segurança da Informação, de normas ou de controles de segurança da informação, intencionais ou não, são considerados incidentes de segurança.

Art.27. Incidentes de segurança podem ser identificados por processos de

monitoração da área de infraestrutura por Colaboradores que observem fragilidades, anomalias e violações que coloquem a segurança da empresa em risco.

Art.28. Todos os incidentes de segurança da informação devem ser documentados, classificados, priorizados de acordo com a criticidade do OGMO-RJ e comunicados aos gestores responsáveis no momento apropriado.

Art.29. Deve ser definido um plano de comunicação de incidentes de segurança da informação que esteja de acordo com a classificação e o nível de criticidade do incidente. Em casos mais simples e de baixa criticidade apenas o gestor responsável pelo recurso ou informação deve ser comunicado. Em casos mais graves a Diretoria Executiva, a área Jurídica ou outros departamentos pertinentes devem ser comunicados.

Art.30. A investigação de incidentes de Segurança da Informação deve ser realizada exclusivamente pelas áreas de Gestão de TI e DPO, de forma a garantir a privacidade e o sigilo das informações obtidas.

Art.31. Sendo necessárias informações ou levantamentos, para os quais devam ser analisadas trilhas de auditoria (logs), acessos à Internet, fluxo de mensagens ou conteúdo de caixas de correio, ou outras informações que coloquem em risco a privacidade de colaboradores e o sigilo das informações do OGMO-RJ, deve ser aberto um incidente junto a área de Gestão de TI e DPO para que estes realizem as investigações.

§1º As informações obtidas e arquivadas pelo processo de Gestão de Incidentes de Segurança da informação devem ser protegidas de forma a garantir a privacidade de colaboradores e o sigilo das informações do grupo, não podendo ser fornecidas a outros departamentos ou auditorias.

§2º A identificação de incidentes de segurança pode ocasionar o corte imediato dos acessos de colaboradores envolvidos ou a desconexão de sistemas, até que sejam concluídas as investigações necessárias.

§3º O acesso às evidências e relatório de incidentes de segurança da informação é permitido apenas a área de Gestão de TI, DPO e aos Gestores diretamente envolvidos nos incidentes.

§4º A documentação de incidentes, resultados de investigações, evidências e suas soluções devem ser atualizadas logo após a conclusão do tratamento do incidente.

§5º O contato para a notificação de incidentes de segurança da informação deve ser feito diretamente a área de Gestão de TI e ao DPO através de canais previamente definidos.

7. DAS PENALIDADES

Art.32. O Colaborador que presenciar o descumprimento de alguma das regras acima tem o dever de denunciar tal infração. Ademais, o descumprimento das regras e diretrizes impostas neste documento poderá ser considerado falta grave, passível de aplicação de sanções disciplinares.

8. DA REVISÃO E ATUALIZAÇÃO DA POLÍTICA DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Art.33. A política de gestão de Incidentes de Segurança da Informação deverá ser revista e atualizada, ao menos anualmente, com vistas a se manter em sintonia com as regras de negócios, com as melhores práticas do mercado, leis, regulamentos e demais aspectos.

9. REFERÊNCIAS

Art.33. Para um entendimento mais abrangente sobre a política de gestão de Incidentes de Segurança da Informação, deve-se consultar os documentos abaixo referenciados:

I. Política de Segurança Cibernética e da Informação;
II. NSI 007 Norma de Administração de Ambientes Tecnológicos;
III. NSI 008 Norma de Gestão de Riscos em Segurança da Informação;
IV. ISO 22301;
V. ISO 27.000/2013;
VI. Cobit 5 – DS4;
VII. NIST 800-30;
VIII. NIST 800-39.

10. DAS DÚVIDAS

Art.34. Em caso de dúvida solicitar esclarecimento a área de Gestão de TI e DPO.

11. CONTROLES DE REGISTROS

Identificação	Armazenamento	Segurança/ Proteção	Recuperação/ Rastreabilidade	Tempo de Retenção	Descarte

12. DISPOSIÇÕES FINAIS

Art.35. Esta Política de Gestão de Incidentes de Segurança da Informação foi aprovada em 22/09/2021 pelos principais gestores do OGMO-RJ.

VERSÃO	DATA	RESPONSÁVEL	FUNÇÃO
1.00	22/09/2021	Frederico S Santos	Gestor de TI