Política de Segurança da Informação – OmniSec

Essa é uma versão reduzida e pública da nossa **Política de Segurança da Informação**, cobrindo apenas os principais macro assuntos de forma sucinta. Caso tenha necessidade de acessar a versão completa, pedimos que entre em contato pelos canais oficiais deste site institucional que enviaremos o documento completo.

1. Objetivo

A **OmniSec** valoriza a segurança, a proteção de dados, informações e dos conhecimentos como princípios fundamentais de sua atuação. Esta política, em versão reduzida, tem como objetivo apresentar as diretrizes sobre o Sistema de Gestão de Segurança da Informação, Cibernética e Dados da OMNISEC, garantindo a confidencialidade, integridade, disponibilidade e autenticidade das informações e dos ativos da organização, promovendo orientações, requisitos legais, contratuais e de negócios que ajudem a minimizar os riscos, as violações de dados e permita um ambiente controlado, em constante melhoria e seguro aos negócios.

2. Abrangência

Aplica-se a todos os colaboradores, parceiros, fornecedores e afiliadas que façam uso das infraestruturas, serviços, dados e informações ofertados ou consumidos pela **OmniSec**.

3. Diretrizes gerais sobre a Segurança da Informação

Esta política, formaliza as diretrizes e as decisões da Administração, bem como as regras de negócios, os direitos, deveres e as responsabilidades no que diz respeito ao contexto de Segurança da Informação e seus domínios, servindo de material orientativo para a execução das demandas de Segurança, colaborando com a sinergia das normas, processos e procedimentos com os objetivos estratégicos da empresa e negócios.

Deve ser continuamente comunicada internamente, podendo ser divulgada para o público externo com autorização prévia da gestão em versão reduzida, ajudando assim com o processo de disseminação da cultura de Segurança da OMNISEC. Tais diretrizes, foram estruturadas de acordo com as seguintes seções e domínios:

3.1 Da Governança

Com estrutura e índice baseado no **NIST CyberSecurity Framework**, em sua última versão, a política cobre nesta seção de abertura todo o contexto estratégico, a abordagem de governança, do gerenciamento de risco de cibersegurança, dos envolvidos, comprometidos, seus respectivos papéis e responsabilidades, envolvendo o nível da alta supervisão a cadeia de relacionamento de fornecedores, internos e externos. Em sua versão completa, versa em ordem de aplicabilidade sobre:

3.1.1. Contexto Organizacional
3.1.2. Estratégia de Gerenciamento de Riscos
3.1.3. Papéis, Responsabilidades e as Autoridades de Cibersegurança
3.1.4. Política
3.1.5. Supervisão e Alta-Gestão
3.1.6. Gestão de Riscos Cibernéticos da Cadeia de Suprimentos

3.2 Da Identificação

Identificar para controlar. A segurança cibernética efetiva deve permitir o gerenciamento de ativos, garantindo visibilidade e controle sobre sistemas, dados, pessoas, fornecedores e outros ativos críticos e/ou relevantes.

Em linha a um modelo de avaliação de riscos que permita identificar ameaças e vulnerabilidades, priorizamos ações e investimentos que reduzam impactos à organização e permitam que **melhoria** contínua colabore com a evolução, sem deixar de lado a resiliência, as práticas, o aprendizado com incidentes que promovam a adaptação a novos cenários tecnológicos e regulatórios. Nesta seção, nossa política endereça:

3.2.1. Gerenciamento de ativos
3.2.2. Avaliação de riscos
3.2.3. Melhorias

3.3 Da Proteção

A proteção cibernética depende de práticas sólidas que sustentem a confiança e a resiliência organizacional. Gerenciamento de identidade, autenticação e controle de acesso garante que somente usuários autorizados tenham acesso adequado aos recursos no momento necessário.

Educação, treinamento e conscientização fortalecem a cultura de segurança, reduzindo riscos ligados ao fator humano, amparados pela segurança de dados e das plataformas. Por fim, a continuidade e a resiliência tecnológica permitem que, mesmo diante de incidentes, a capacidade de resposta e recuperação prevalecerá. A política endereça:

3.3.1. Gerenciamento de identidade, autenticação e controle de acesso
3.3.2. Conscientização e treinamento
3.3.3. Segurança de dados
3.3.4. Segurança da plataforma
3.3.5. Resiliência da infraestrutura tecnológica

3.4 Da Detecção

A maturidade em segurança exige capacidade de detectar e reagir rapidamente a incidentes, que exista monitoramento contínuo possibilitando visibilidade em tempo real sobre atividades, sistemas e comportamentos anômalos, permitindo resposta proativa e proporcional aos eventos.

Pessoal capacitado deve prover condições para a análise de eventos adversos, assegurando investigação estruturada de ocorrências, identificando causas, impactos e medidas corretivas para evitar reincidências, enumerar riscos e fortalecer a resiliência organizacional. Para esta cobertura, elencamos:

3.4.1. Monitoramento contínuo
3.4.2. Análise de eventos adversos

3.5 Da Resposta

A resposta para lidar com incidentes é essencial para preservar a continuidade dos negócios e a confiança de nossas partes interessadas, mesmo em momentos de anormalidades. O gerenciamento de incidentes organiza processos, executores e as responsabilidades pela resposta estruturada, com o fornecimento da análise de incidentes compreendendo as causas e os impactos, direcionando ações corretivas eficazes e melhores a cada novo aprendizado.

A comunicação e os relatórios de resposta devem estar sinérgicos entre os times, garantindo transparência interna e externa alinhada as partes, times e áreas interessadas, sem esquecer da mitigação com foco na contenção e redução de danos, restaurando a operação dentro de prazos e condições preestabelecidos, fortalecendo todo o processo de continuidade e resiliência organizacional. Abordamos e perseguimos:

3.5.1. Gerenciamento de incidentes
3.5.2. Análise de incidentes
3.5.3. Comunicação e relatórios de resposta a incidentes
3.5.4. Mitigação de incidentes

3.6 Da Recuperação

A recuperação eficiente após incidentes é determinante para restaurar a confiança e a continuidade das operações, a partir da execução de planos e subplanos de recuperação de incidentes e/ou desastres, assegurando que sistemas e serviços sejam restabelecidos de forma estruturada e conforme critérios definidos.

Os métodos e momentos da comunicação de recuperação de incidentes mantém partes interessadas informadas sobre o progresso e resultados, garantindo transparência e alinhamento durante e após o processo de retomada, demais ações de contenção e readequação. A redação completa endereça:

3.6.1. Execução do plano de recuperação de incidentes
3.6.2. Comunicação de recuperação de incidentes

3.7 Dos Contextos Complementares

A proteção operacional exige controles que assegurem tanto o ambiente físico quanto o digital, sejam instalações físicas, facilities, predial ou o manuseio, transporte, armazenamento e descarte de mídias, ações que colaboram com a preservação da integridade da informação em todo o seu ciclo de vida. Recomendações de mesa limpa reforçam a disciplina no uso de documentos e dispositivos físicos e lógicos, associados a ações de backup/restore assegurando disponibilidade e recuperação de dados quando necessário.

O uso dos recursos computacionais, redes, internet e e-mails em linha a esta política, promove boas práticas de utilização, a proteção contra códigos maliciosos, uso de IA de forma controlada, desenvolvimento seguro de códigos fortalecendo nossa a resiliência tecnológica e proteção. Gerenciamento de patches e vulnerabilidades, nesta ordem, reduz riscos por meio de atualizações contínuas, finalizando com a conexão com nossas recomendações de privacidade que asseguram conformidade legal e proteção de dados pessoais, reforçando a confiança dos titulares, da sociedade e de nossos clientes. Nesta seção, nossa redação oferta:

3.7.1. Instalações físicas, facilities e predial
3.7.2. Manuseio, transporte, armazenamento e descarte de mídias
3.7.3. Mesa Limpa
3.7.4. Backup e Restore das Informações
3.7.5. Uso dos Recursos Computacionais, Redes, Internet e E-mails
3.7.6. Códigos Maliciosos
3.7.7. Desenvolvimento Seguro de Código
3.7.8. Gerenciamento de Patches e Vulnerabilidades
3.7.9. Privacidade

4. Responsabilidades e direitos

Todos os colaboradores e terceiros que tenham acesso a dados e informações estão obrigados a cumprir esta política e os demais normativos internos, mantendo sigilo e promovendo o uso responsável das informações em linhas aos seus direitos e deveres.

5. Sanções

O descumprimento das regras desta política pode resultar em sanções disciplinares, bem como em responsabilização administrativa, civil e criminal, conforme a gravidade da violação.

6. Referências

Esta política, em constante revisão, tem como referência:

- **NIST CyberSecurity Framework 2.0**
- **NIST Privacy Framework 1.1**
- **Lei Geral de Proteção de Dados Pessoais - LGPD**
- **CIS Critical Security Controls – v8.1**
- **ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27014, ISO/IEC-27701, ISO-27035 e ISO/IEC 31000**

7. Atualizações e Revisões

Esta política será revisada periodicamente, sempre que houver alterações legais, regulatórias ou operacionais relevantes. O histórico de versões é mantido em nossos documentos e padrões para garantir a rastreabilidade e transparência em sua versão original e completa. Modificações com aplicabilidade imediata podem ocorrer sem prévio aviso e/ou pelo menos uma (1) vez ao ano conforme nossas políticas internas.

8. Contatos

Dúvidas, sugestões, recomendações e solicitações podem ser feitas diretamente por nossos canais oficiais, parcialmente mascarados para evitar coleta de emails por bots, cadastramentos indevidos e ferramentas de rastreamento web (web crawling).

- **dpo** [arroba] omnisecorp [ponto] com
- **security** [arroba] omnisecorp [ponto] com
- **csirt** [arroba] omnisecorp [ponto] com
- **denuncia** [arroba] omnisecorp [ponto] com