POLÍTICA DE RELACIONAMENTO COM FORNECEDORES

INORPEL
cybersecurity

INORPEL cybersecurity	POLÍTICA INORPEL CYBERSECURITY				Data de Criação: 08/06/2024
	Número: 0016	Localizador: POL-SI	Revisão: 1.0	Folhas: 11	Data para Revisão: 02/08/2025
Título: Política de Relacionamento com Fornecedores				Área Emitente: GRC/Processos	
Elaborador: João Pimentel			Aprovador: Comitê Gestor de Segurança da Informação		
Data da Publicação: 02/08/2024			Auditor: Setor de Auditoria		
Classificação da Informação: PÚBLICA					

SUMÁRIO

1. INTRODUÇÃO

1.1. Objetivo

O objetivo desta política é estabelecer diretrizes e procedimentos para a gestão de segurança da informação no relacionamento com fornecedores, garantindo a proteção adequada das informações da organização.

Além disso, busca essa política assegurar que todos os fornecedores cumpram com os requisitos de Segurança da Informação estabelecidos pela organização, bem como garantir que o relacionamento com os fornecedores esteja em conformidade com todas as leis, regulamentos e normativos, internos e externos, aplicáveis.

1.2. Escopo

Esta política se aplica a todos os fornecedores que tenham acesso à ativos, informações da organização ou que forneçam serviços que possam impactar a segurança da informação.

2. RESPONSABILIDADES

2.1. Gestão de Fornecedores

2.1.1. Setor de Suprimentos

Responsável por coordenar o processo de seleção e contratação de fornecedores, assegurando que todos os contratos incluam clausulas de Segurança da Informação apropriadas. Além disso, cabe ao setor de suprimentos:

a) Coordenar a seleção de fornecedores, solicitando, sempre que necessário, a realização de *due diligence* junto aos setores de GRC ou Jurídico;
b) Colaborar com os departamentos técnicos para avaliar a conformidade dos fornecedores.
c) Manter registro de todos os contratos e avaliações de fornecedores.

2.1.2. Blue Team

Responsável por avaliar os aspectos técnicos de segurança da informação dos fornecedores e fornecer suporte técnico no processo de seleção e monitoramento e definir os requisitos de segurança da informação aplicáveis aos fornecedores e garantir que esses requisitos sejam comunicados e cumpridos. Além disso, cabe ao setor técnico:

a) Avaliar a infraestrutura de TI dos fornecedores para garantir que atendam aos requisitos de segurança da organização.
b) Fornecer suporte técnico durante as auditorias e avaliações de fornecedores.
c) Realizar, por meio de seu White Team, auditorias sempre que solicitado pelos demais departamentos e/ou setores.
d) Monitorar a conformidade dos fornecedores com os requisitos técnicos e organizacionais de segurança.
e) Documentar e relatar quaisquer riscos de segurança identificados.
f) Desenvolver e manter os requisitos de segurança da informação para fornecedores.
g) Comunicar os requisitos de segurança da informação aos fornecedores.
h) Realizar auditorias e avaliações de segurança da informação dos fornecedores.

i) Investigar e responder a incidentes de segurança da informação relacionados aos fornecedores.
j) Manter registros de auditorias, avaliações e incidentes de segurança.

2.2. Fornecedores

Responsáveis por aderir aos requisitos de segurança da informação definidos pela organização e implementar medidas apropriadas para proteger as informações da organização. Além disso cumpre aos fornecedores:

a) Cumprir todas as cláusulas de segurança da informação incluídas nos contratos.
b) Implementar e manter controles de segurança adequados para proteger as informações da organização.
c) Notificar a organização imediatamente em caso de incidentes de segurança que possam afetar as informações da organização.
d) Participar de auditorias e avaliações de segurança conduzidas pela organização.
e) Fornecer evidências de conformidade com os requisitos de segurança da informação quando solicitado.

2.3. Diretoria

Responsável por aprovar a política de relacionamento com fornecedores e garantir que ela seja implementada e seguida em toda a organização. Além disso cumpre à diretoria:

a) Aprovar a política de relacionamento com fornecedores.
b) Alocar recursos necessários para a implementação e manutenção da política.
c) Revisar relatórios de auditorias e avaliações de fornecedores.
d) Apoiar ações corretivas e de melhoria contínua relacionadas à gestão de fornecedores.

3. SELEÇÃO E CRITÉRIO DE AVALIAÇÃO DE FORNECEDORES

3.1. Critérios de Seleção

Para garantir que os fornecedores selecionados atendam aos requisitos de segurança da informação da organização, os seguintes critérios de seleção devem ser aplicados:

a) Conformidade com Normas de Segurança: Os fornecedores devem demonstrar conformidade com normas de segurança da informação, como ISO 27001, ou outras normas relevantes.
b) Capacidade Técnica: Avaliar a capacidade técnica do fornecedor para proteger informações sensíveis e implementar controles de segurança.
c) Histórico de Segurança: Considerar o histórico de segurança do fornecedor, incluindo incidentes anteriores e medidas corretivas adotadas.
d) Reputação e Confiabilidade: Avaliar a reputação e confiabilidade do fornecedor no mercado.
e) Requisitos Legais e Regulatórios: O fornecedor deve estar em conformidade com todos os requisitos legais e regulatórios aplicáveis.
f) Políticas e Procedimentos Internos: O fornecedor deve possuir políticas e procedimentos internos de segurança da informação bem definidos.

3.2. Processo de Due Diligence

Antes da contratação, a organização deve realizar um processo de due diligence para avaliar a capacidade do fornecedor em cumprir com os requisitos de segurança da informação:

a) Questionário de Avaliação: Enviar um questionário detalhado de avaliação de segurança da informação ao fornecedor.
b) Auditoria de Segurança: Realizar auditorias de segurança, se necessário, para verificar a conformidade com os requisitos de segurança.
c) Visitas In Loco: Realizar visitas às instalações do fornecedor para avaliar as medidas de segurança implementadas.
d) Referências: Solicitar e revisar referências de outros clientes do fornecedor.

3.3. Contratações de Fornecedores

Após a seleção e a avaliação positiva, a contratação do fornecedor deve incluir cláusulas específicas sobre segurança da informação:

a) Acordos de Nível de Serviço (SLAs): Estabelecer SLAs que definam claramente os requisitos de segurança da informação e as responsabilidades do fornecedor.
b) Cláusulas Contratuais: Incluir cláusulas contratuais que abranjam aspectos como confidencialidade, integridade, disponibilidade, notificação de incidentes e conformidade com a política de segurança da informação da organização.

3.4. Monitoramento e Auditoria

A organização deve implementar um processo contínuo de monitoramento e avaliação dos fornecedores para garantir a conformidade contínua com os requisitos de segurança da informação:

a) Avaliações Periódicas: Conduzir avaliações periódicas da segurança da informação dos fornecedores, incluindo auditorias e revisões de conformidade.
b) Relatórios Regulares: Requerer que os fornecedores forneçam relatórios regulares sobre suas práticas de segurança da informação e quaisquer incidentes relevantes.
c) Reuniões de Revisão: Realizar reuniões periódicas com fornecedores para revisar o desempenho de segurança e discutir quaisquer questões ou melhorias necessárias.

3.5. Exceções

Sempre que necessário, e devidamente justificado e fundamentado, pode haver a dispensa de algum dos requisitos acima quando da contratação de fornecedor, devendo haver a sinalização dessas exceções para monitoramento e acompanhamento por parte do responsável pelo contrato.

4. CONTRATOS E ACORDOS

4.1. Cláusulas Contratuais de Segurança da Informação

Para garantir a proteção adequada das informações, todos os contratos com fornecedores devem incluir cláusulas específicas sobre segurança da informação. As cláusulas devem cobrir, no mínimo, os seguintes aspectos:

a) Confidencialidade: Os fornecedores devem assegurar que todas as informações confidenciais fornecidas pela organização sejam mantidas em sigilo e não sejam divulgadas a terceiros sem consentimento prévio por escrito.
b) Integridade: O fornecedor deve garantir a precisão e a completude das informações fornecidas e processadas.
c) Disponibilidade: O fornecedor deve assegurar que os serviços e informações estejam disponíveis conforme acordado, incluindo a implementação de planos de continuidade de negócios.
d) Conformidade Legal, Regulatória e Normativa: O fornecedor deve estar em conformidade com todas as leis e regulamentos aplicáveis relativos à proteção de dados e segurança da informação.
e) Notificação de Incidentes: O fornecedor deve notificar a organização imediatamente em caso de qualquer incidente de segurança que possa comprometer as informações.
f) Direitos de Auditoria: A organização deve ter o direito de auditar as práticas de segurança da informação do fornecedor, podendo solicitar à qualquer tempo e quantas vezes for necessário, pela comprovação da conformidade.

4.2. Acordos de Níveis de Serviço (SLA's)

Os SLAs devem definir claramente os requisitos de segurança da informação e as expectativas de desempenho. Os SLAs devem incluir:

a) Objetivos de Segurança: Especificar os objetivos de segurança que o fornecedor deve alcançar.
b) Indicadores de Desempenho: Definir indicadores claros e mensuráveis para monitorar o desempenho do fornecedor.
c) Responsabilidades de Relato: Especificar os requisitos de relato regular de desempenho e conformidade pelo fornecedor.

4.3. Gestão de Mudanças Contratuais

Os contratos devem incluir um processo claro para a gestão de mudanças, garantindo que quaisquer alterações nos requisitos de segurança da informação sejam formalmente documentadas e aprovadas.

4.4. Encerramento do Contrato

Os contratos devem prever a proteção das informações e dados, pessoais e da organização em caso de encerramento do contrato com o fornecedor. Deve haver especificação de procedimento para devolução e/ou destruição segura dos dados, pessoais ou não, das informações da organização.

5. COMUNICAÇÃO E TREINAMENTO

Cumprirá à organização providenciar treinamento e comunicação de todos os requisitos de Segurança da Informação, antes e durante a contratação do serviço. Além disso, em caso de contratos encerrados, e sempre que necessário, deverá a organização manter canal de comunicação com o fornecedor para o caso de comunicações relativas à eventuais dados e informações que o fornecedor precise manter em caso de cumprimento de requisitos legais e regulamentares.

6. DIVULGAÇÃO

Esta Política deve ser divulgada através de todos os meios, fóruns e âmbitos disponíveis, priorizando os meios de comunicação internos como espaço de disseminação a todos os funcionários e colaboradores da INORPEL.

7. CONSIDERAÇÕES FINAIS

Qualquer situação não contemplada neste procedimento, deve ser validada com o gestor direto, coordenador de área, gerência técnica ou diretoria técnica, respectivamente.

8. RESOLUÇÕES E OBJETIVOS CONFLITANTES

Esta diretriz destina-se a cumprir as leis e regulamentos no local de estabelecimento e nos países em que a INORPEL opera. No caso de qualquer conflito entre esta Política e as leis e regulamentos aplicáveis, estes últimos prevalecerão.

9. VIGÊNCIA

Esta política entra em vigor a partir da data de sua publicação.

10. DOCUMENTOS DE REFERÊNCIA

- POL-SI-0001 - Política de Segurança da Informação;
- Código de Ética e Conduta da INORPEL

11. HISTÓRICO DE VERSÕES E ASSINATURA

VERSÃO	APROVADOR	DATA	ASSINATURA
v 1.0	Comitê Gestor de Segurança da Informação	01/08/2024	Via D4

ANEXO A – CRITÉRIOS DE SELEÇÃO DE FORNECEDORES

Este anexo detalha os critérios que devem ser considerados ao selecionar fornecedores para garantir que eles atendam aos requisitos de segurança da informação da organização.

1. Conformidade com Normas de Segurança

a) ISO 27001: O fornecedor deve possuir certificação ISO 27001 ou equivalente, demonstrando conformidade com um Sistema de Gestão de Segurança da Informação (SGSI).

- Evidência: Apresentar certificado de conformidade válido.

b) Outras Certificações: Certificações adicionais, como SOC 2, PCI-DSS, etc., são desejáveis dependendo da natureza dos serviços fornecidos.

- Evidência: Apresentar certificados adicionais relevantes.

2. Capacidade Técnica

a) Infraestrutura de Segurança: Avaliar a robustez da infraestrutura de segurança do fornecedor, incluindo firewalls, sistemas de detecção de intrusão, criptografia, etc.

- Evidência: Relatórios técnicos e auditorias de segurança.

b) Gestão de Acessos: Políticas e práticas de gestão de acessos devem ser bem definidas e implementadas.

- Evidência: Documentação de políticas de gestão de acessos e relatórios de auditoria.

3. Histórico de Segurança

a) Histórico de Incidentes: Revisar o histórico de incidentes de segurança do fornecedor e as medidas corretivas adotadas.

- Evidência: Relatórios de incidentes e planos de ação corretiva.

b) Auditorias Passadas: Avaliar os resultados de auditorias de segurança anteriores.

- Evidência: Relatórios de auditoria de terceiros.

4. Reputação e Confiabilidade

a) Referências de Clientes: Obter e revisar referências de clientes atuais e anteriores.

   a. Evidência: Testemunhos de clientes e estudos de caso.

b) Reputação no Mercado: Avaliar a reputação do fornecedor no mercado através de análises de mercado e feedback de clientes.

a. Evidência: Relatórios de análise de mercado e feedback de clientes.

5. Requisitos Legais e Regulatórios

a) Conformidade Legal: O fornecedor deve estar em conformidade com todas as leis e regulamentações aplicáveis, como GDPR, LGPD, HIPAA, etc.

- Evidência: Relatórios de conformidade e auditorias legais.

b) Políticas de Privacidade: Avaliar as políticas de privacidade e proteção de dados do fornecedor.

- Evidência: Documentação de políticas de privacidade e proteção de dados.

6. Políticas e Procedimentos Internos

a) Políticas de Segurança: Avaliar a abrangência e eficácia das políticas de segurança da informação do fornecedor.

- Evidência: Cópias das políticas de segurança e relatórios de conformidade.

b) Planos de Continuidade de Negócios: O fornecedor deve possuir planos de continuidade de negócios robustos e testados.

- Evidência: Documentação dos planos de continuidade de negócios e registros de testes.

7. Gestão de Riscos

a) Identificação e Avaliação de Riscos: O fornecedor deve ter processos para identificar, avaliar e mitigar riscos de segurança da informação.

- Evidência: Relatórios de avaliação de riscos e planos de mitigação.

b) Monitoramento Contínuo: O fornecedor deve implementar processos de monitoramento contínuo para identificar e responder a ameaças.

- Evidência: Relatórios de monitoramento e incidentes.

ANEXO B – CHECKLIST DE AVALIAÇÃO DE FORNECEDORES

CRITÉRIO	SUBCRITÉRIOS	EVIDÊNCIAS NECESSÁRIAS	PONTUAÇÃO MÁXIMA	PONTUAÇÃO OBTIDA
Conformidade com Normas de Segurança	ISO/IEC, NIST, PCI-DDI, SOC, outras certificações para a área de atuação do fornecedor.	Certificados de Conformidade;	20	
Capacidade Técnica	Infraestrutura de Segurança, Gestão de Acessos	Relatórios técnicos, Documentação de políticas	20	
Histórico de Segurança	Histórico de Incidentes, Auditorias Passadas	Relatórios de incidentes, Relatórios de auditoria	15	
Reputação e Confiabilidade	Referências de Clientes, Reputação no Mercado	Testemunhos, Relatórios de análise de mercado	15	
Requisitos Legais e Regulatórios	Conformidade Legal, Políticas de Privacidade	Relatórios de conformidade, Documentação de políticas	10	
Políticas e Procedimentos Internos	Políticas de Segurança, Planos de Continuidade de Negócios	Cópias das políticas, Documentação de planos	10	
Gestão de Riscos	Identificação e Avaliação de Riscos, Monitoramento Contínuo	Relatórios de avaliação, Relatórios de monitoramento	10	