

A decorative graphic consisting of several overlapping, wavy horizontal lines in shades of white and light blue, spanning the width of the page and separating the header from the main content area.

# Política de Segurança da Informação com Fornecedores

## ÍNDICE

1. OBJETO.....	3
2. ABRANGÊNCIA .....	3
3. RESPONSABILIDADES.....	3
4. SISTEMÁTICA DE EXECUÇÃO.....	3
4.1. <i>DUE DILIGENCE</i> .....	4
4.2. SEGURANÇA NOS ACORDOS COM FORNECEDORES.....	4
4.3. MONITORAMENTO E REVISÃO DE SERVIÇOS DE FORNECEDORES .....	4
4.4. GERENCIANDO MUDANÇAS NOS SERVIÇOS DOS FORNECEDORES.....	5
4.5. COMPUTAÇÃO EM NUVEM .....	5
5. PENALIDADES.....	6

## 1. OBJETO

A Política de Segurança da Informação com fornecedores é o documento que orienta e estabelece as diretrizes corporativas do Grupo Forship para a proteção das informações da empresa na relação com fornecedores.

## 2. ABRANGÊNCIA

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

## 3. RESPONSABILIDADES

Gestores

- Exigir de seus fornecedores o cumprimento da política.
- Conscientizar fornecedores críticos.
- Reportar qualquer risco ou desvio.

DTI - Diretoria de TI

- Avaliar riscos de segurança da informação e *due diligence* em fornecedores.
- Determinar ações e controles.
- Auxiliar no gerenciamento de mudanças de fornecedores, assim como encerramento de contrato.

Comitê de Segurança da Informação

- Determinar requisitos para relacionamento com fornecedor.

## 4. SISTEMÁTICA DE EXECUÇÃO

Em geral, os requisitos de segurança da informação variam de acordo com o tipo de relação contratual que existe com cada fornecedor e os bens ou serviços entregues.

No entanto, geralmente se aplica o seguinte:

- Os requisitos e controles de segurança da informação devem ser documentados formalmente em um acordo contratual que pode fazer parte ou um adendo ao contrato principal.
- Acordos de não divulgação (NDA) separados devem ser usados quando houver um nível mais específico de controle sobre o contrato de confidencialidade.
- A *due diligence* deve ser exercida na seleção e aprovação de novos fornecedores críticos antes que os contratos sejam firmados.
- As disposições de segurança da informação em vigor nos fornecedores existentes (onde a *due diligence* não foi realizada como parte da seleção inicial) devem ser claramente compreendidas e melhoradas quando necessário.
- O acesso remoto por fornecedores deve ser feito por meio de métodos aprovados que estejam em conformidade com nossas políticas de segurança da informação.
- O acesso às informações do Grupo Forship deve ser limitado, sempre que possível, de acordo com a necessidade comercial clara.

- Princípios básicos de segurança da informação, como privilégio mínimo, segregação de funções e defesa em profundidade, devem ser aplicados.
- Espera-se que o fornecedor exerça controle adequado sobre as políticas e procedimentos de segurança da informação usados pelos subcontratados que desempenham um papel na cadeia de abastecimento de entrega de bens ou serviços para o Grupo Forship.
- O Grupo Forship terá o direito de auditar as práticas de segurança da informação do fornecedor e, quando apropriado, dos subcontratados.
- A gestão de incidentes e planos de contingência devem ser implementados com base nos resultados de uma avaliação de risco.
- Treinamento de conscientização será realizado por ambas as partes do acordo, com base nos processos e procedimentos definidos.

A seleção dos controles necessários deve ser baseada em uma avaliação de risco abrangente, considerando os requisitos de segurança da informação, o produto ou serviço a ser fornecido, sua criticidade para a organização e as capacidades do fornecedor.

#### 4.1. DUE DILIGENCE

Antes de contratar um fornecedor, é responsabilidade do Grupo Forship exercer a *due diligence* para chegar a um entendimento tão completo quanto possível da abordagem de segurança da informação e dos controles que a empresa possui.

Isso é particularmente importante quando os serviços de computação em nuvem estão envolvidos, visto que devem ser levadas em conta questões legais sobre a localização e o armazenamento de dados pessoais.

#### 4.2. SEGURANÇA NOS ACORDOS COM FORNECEDORES

Uma vez que um fornecedor potencial tenha sido avaliado positivamente com a *due diligence*, os requisitos de segurança da informação do Grupo Forship devem ser refletidos por escrito no acordo contratual celebrado. Este acordo deve considerar a classificação de qualquer informação a ser processada pelo fornecedor (incluindo qualquer mapeamento necessário entre as classificações do Grupo Forship e aquelas em uso dentro do fornecedor), requisitos legais e regulamentares e quaisquer controles de segurança adicionais que sejam necessários.

Para prestadores de serviços em nuvem, as funções e responsabilidades de segurança da informação devem ser claramente definidas em áreas como *backups*, gerenciamento de incidentes, avaliação de vulnerabilidade e controles criptográficos.

Deve-se obter aconselhamento jurídico adequado para garantir que a documentação contratual seja válida no país ou países em que será aplicada.

Para aqueles fornecedores que não foram sujeitos a uma avaliação de segurança da informação antes de um acordo ser feito, um processo de avaliação deve ser realizado a fim de identificar quaisquer melhorias necessárias.

#### 4.3. MONITORAMENTO E REVISÃO DE SERVIÇOS DE FORNECEDORES

Para concentrar os recursos nas áreas de maior necessidade, os fornecedores serão categorizados com base em uma avaliação de seu valor para a organização.

O desempenho dos fornecedores estratégicos será monitorado regularmente de acordo com uma combinação de relatórios produzidos pelo fornecedor em relação ao contrato e análises produzidas internamente.

Sempre que possível, uma verificação cruzada frequente será feita entre os relatórios do fornecedor e aqueles criados internamente, a fim de garantir que os dois apresentem uma imagem consistente do desempenho do fornecedor.

#### 4.4. GERENCIANDO MUDANÇAS NOS SERVIÇOS DOS FORNECEDORES

##### 4.4.1. Mudanças no Contrato

Mudanças nos serviços prestados pelos fornecedores estarão sujeitas ao processo de gestão de mudanças do Grupo Forship. Esse processo inclui o requisito de avaliar quaisquer implicações de mudanças na segurança da informação, para que a eficácia dos controles seja mantida.

Em todos os momentos, o grau de risco para o negócio deve ser gerenciado e, se possível, minimizado.

##### 4.4.2. Encerramento de Contrato

O seguinte processo será seguido para o fim agendado do contrato, o fim antecipado do contrato ou a transferência do contrato para outra parte:

- O término do contrato será solicitado por escrito nos termos acordados.
- A transferência para outra parte deve ser planejada como um projeto e devem ser seguidos os procedimentos de controle de mudança apropriados.
- Uma avaliação do risco para a organização deve ser realizada antes de encerrar ou transferir o contrato, e os planos de contingência devem ser implementados.
- Quaisquer implicações orçamentais devem ser incorporadas no modelo financeiro.

Os vários aspectos de rescisão de um contrato devem ser cuidadosamente considerados no momento da negociação do contrato inicial.

#### 4.5. COMPUTAÇÃO EM NUVEM

É política do Grupo Forship na área de computação em nuvem que:

- Os dados pertencentes ao Grupo Forship só serão armazenados nos serviços em nuvem com a permissão prévia da DTI.
- A avaliação de risco apropriada deve ser realizada em relação ao uso proposto ou contínuo de serviços em nuvem, incluindo todo o entendimento dos controles de segurança da informação implementados pelo CSP.
- A *due diligence* deve ser conduzida antes da inscrição em um provedor de serviços em nuvem para garantir que os controles apropriados estejam em vigor para proteger os dados. Será dada preferência a fornecedores que sejam certificados pela ISO/IEC 27001 e que cumpram os princípios dos códigos de prática ISO/IEC 27017 e ISO/IEC 27018 para serviços em nuvem.
- Acordos de nível de serviço e contratos com provedores de serviços em nuvem devem ser revisados, compreendidos e aceitos antes da inscrição no serviço, incluindo questões de LGPD/GPDR.
- As funções e responsabilidades por atividades como *backups*, *patches*, gerenciamento de *log*, proteção contra *malware* e gerenciamento de incidentes devem ser acordadas e documentadas antes do início do serviço em nuvem.
- Devem ser estabelecidos procedimentos para garantir que as atividades irreversíveis no ambiente de nuvem (por exemplo, exclusão de servidores virtuais, encerramento de

um serviço de nuvem ou restauração de *backups*) estejam sujeitas a controles adequados para evitar erros. A supervisão por uma segunda pessoa devidamente qualificada deve fazer parte de tais procedimentos.

- A localização dos dados armazenados com o CSP deve ser entendida e a base jurídica aplicável estabelecida, levando em conta o país cuja lei se aplica ao contrato.
- A autenticação multifator deve ser usada para acessar todos os serviços em nuvem.
- O *log* de auditoria deve estar disponível para permitir que o Grupo Forship entenda as formas pelas quais esses dados estão sendo acessados e para identificar se algum acesso não autorizado ocorreu.
- Os dados confidenciais armazenados em serviços em nuvem devem ser criptografados usando tecnologias e técnicas aceitáveis. Sempre que possível, as chaves de criptografia serão mantidas pelo Grupo Forship e não pelo fornecedor.
- As políticas do Grupo Forship para a criação e gerenciamento de contas de usuário serão aplicadas aos serviços em nuvem.
- Devem ser feitos *backups* de todos os dados armazenados na nuvem. Isso pode ser realizado diretamente pelo Grupo Forship ou sob contrato com o provedor de serviços em nuvem.
- Todos os dados do Grupo Forship devem ser removidos dos serviços de nuvem em caso do contrato ser encerrado por qualquer motivo.

Em geral, os requisitos de segurança da informação variam de acordo com o tipo de relação contratual que existe com cada fornecedor e os bens ou serviços entregues.

## 5. PENALIDADES

O descumprimento das diretrizes desta Política, mesmo que por mero desconhecimento, sujeitará o infrator a sanções administrativas, incluindo a aplicação de advertência verbal ou escrita, demissão por justa causa ou rescisão contratual, bem como sujeitará o infrator às demais penalidades administrativas, cíveis e penais previstas na legislação brasileira.

É dever de todo colaborador comunicar ao Gestor a ocorrência de incidente que afete a segurança da informação, que por sua vez escalará a Diretoria Executiva para análise quando assim for necessário.