Política de Segurança da Informação e Segurança Cibernética

Janeiro | 2025

1. INTRODUÇÃO

A empresa depende em grande parte da tecnologia para conduzir seu negócio, atendendo às suas necessidades operacionais, comerciais e estratégicas. Os sistemas de informação, a infraestrutura tecnológica, os arquivos de dados e as informações internas ou externas são considerados ativos importantes da empresa. Com a finalidade de acompanhar as boas práticas das organizações globais e as exigências dos órgãos reguladores, dos próprios clientes e dos sócios, é necessário que as informações sejam armazenadas, conduzidas e processadas em ambiente seguro e que todos os colaboradores compartilhem da responsabilidade pelos processos de segurança utilizados para controlar a integridade, a disponibilidade e a confidencialidade dos ativos de informação da empresa.

A definição e a implementação de uma Política de Segurança de Informação e de Segurança Cibernética são passos essenciais para estabelecer objetivos, funções, ações, mecanismos de delegação e responsabilidades pelos processos de segurança da informação, segurança cibernética e controles internos, de modo a preservar e até mesmo incrementar a expressiva vantagem competitiva que a empresa possui e deseja manter em relação ao mercado, qual seja o uso de recursos avançados de tecnologia da informação. Enfim, essa Política estabelece os fundamentos de segurança da informação e segurança cibernética para toda a empresa e, em especial, para as áreas de TI Suporte, TI Sistemas e Gerência Administrativa e é de onde as normas, padrões, orientações e procedimentos de segurança da informação e de segurança cibernética derivam.

2. ABRANGÊNCIA

A Política de Segurança da Informação e de Segurança Cibernética abrange os seguintes itens:

- A segurança de todas as informações da empresa, acessadas, processadas, utilizadas, transportadas ou armazenadas em qualquer meio, de tecnologia ou de sistema. Vale ressaltar que todas as informações, mesmo aquelas aparentemente de menor importância são um ativo da empresa e assim devem ser devidamente protegidas conforme descrito na Política.
- Todo colaborador, interno ou externo, de todos os níveis, que acesse qualquer ambiente da empresa e/ou gere, processe, utilize ou armazene as informações da empresa, em qualquer tecnologia, local ou meio.
- Todos os sistemas e aplicativos existentes na empresa, sejam os localizados nas áreas de negócios ou aqueles utilizados como apoio administrativo, ou qualquer outro que auxilie as atividades da empresa ou que manipule transporte ou armazene suas informações.
- Todas as instalações onde estão localizados os ativos de informação da empresa.
- Todo o acesso físico ou lógico a qualquer equipamento, tecnologia, meio de comunicação ou processo utilizado na aquisição, criação, utilização, armazenamento, transporte, manipulação, eliminação ou descarte de qualquer informação da empresa.
- Todos os dispositivos de comunicação interna e externa em uso pela empresa e seus colaboradores no exercício de suas atividades profissionais.

3. ESTRUTURA DO COMITÊ DE SEGURANÇA

A empresa possui um Comitê de Segurança para atuar na segurança da informação e na segurança cibernética, composto pelo Security Officer, Gerente de TI Suporte, Gerente de TI Sistemas, Gerente Jurídica, Diretor de Risco e Diretor Administrativo, que tem como responsabilidades:

- Aprovar o programa de conscientização dos colaboradores quanto à segurança da informação e segurança cibernética.
- Aprovar os controles a serem utilizados para garantir a segurança das informações e a segurança cibernética.
- Aprovar e revisar a política e normas de segurança e responsabilidades correspondentes.
- Acompanhar os indicadores de segurança e incidentes reportados e deliberar sobre a aplicação ou não de penalidades sobre as violações ocorridas na Política de Segurança.
- Monitorar mudanças significativas na exposição dos ativos de informação a ameaças.
- Elaborar e dar manutenção à Política, às normas e aos procedimentos de segurança, assim como metodologias e padrões utilizados.
- Assessorar as áreas de TI Suporte e TI Sistemas e os gerentes das demais áreas na proteção de seus bens de informação.
- Desenvolver, manter e implementar programas de treinamento e de conscientização dos colaboradores sobre a Política de Segurança da Informação e da Segurança Cibernética, como ela está estruturada e os principais conceitos.
- Participar na homologação de novos produtos de segurança para a empresa.
- Participar nos planejamentos anuais de segurança, considerando as diversas áreas da empresa e seus planos específicos, para definir as estratégias, alocar os recursos tecnológicos, financeiros, humanos e priorizar os investimentos, aprovando o plano de segurança.
- Assegurar a implementação dos elementos do programa de segurança em todas as áreas e dependências da empresa, abrangendo atividades de negócios, de retaguarda e de apoio administrativo.
- Garantir que toda norma e procedimento de segurança formalizados estejam aderentes à Política da Segurança da Informação e da Segurança Cibernética e possuam procedimentos que possibilitem a verificação de seu cumprimento.
- Assegurar que exista um processo apropriado para informar os incidentes e violações de segurança e que seja utilizado por todos os colaboradores, independentemente dos recursos de tecnologia.
- Definir as principais funções e responsabilidades quanto à segurança da informação e à segurança cibernética para toda a organização.
- Avaliar a adequação e acompanhar a implementação dos controles de segurança da informação e segurança cibernética específicos para novos sistemas e serviços.
- Garantir a consistência do conhecimento e das experiências de segurança da informação e de segurança cibernética da empresa.
- Auxiliar nas decisões no tocante à segurança da informação e à segurança cibernética da empresa.
- Assegurar uma ação rápida no evento de incidentes de segurança mantendo contato com autoridades de segurança, entidades regulamentadoras, operadores de telecomunicações e prestadores de serviços de informações.
- Dirimir dúvidas de Prepostos, relacionadas à questões de segurança da informação, segurança cibernética e à esta Política.

4. RESPONSABILIDADES E PROCEDIMENTOS

4.1. Quanto à Política de Segurança da Informação e à Segurança Cibernética

Todos os sócios, administradores, funcionários, estagiários e colaboradores ("Prepostos") devem observar e garantir a aplicação das políticas, normas e procedimentos de segurança determinados pela empresa. Para tanto, todos devem assinar o Termo de Responsabilidade, no qual assumem tal responsabilidade, quando ingressarem ou iniciarem suas atividades na empresa.

Todos são responsáveis individualmente pelos equipamentos de tecnologia que utilizam ou gerenciam. Tal compromisso é formalizado através da assinatura do referido Termo de Responsabilidade.

Todas as informações quando impressas devem ser acompanhadas e retiradas imediatamente das impressoras.

A empresa designou um Diretor responsável pela Política de Segurança Cibernética e pela execução do plano de ação e de resposta a incidentes.

4.2. Quanto à Confidencialidade das Informações

As informações da empresa devem ser classificadas como Confidenciais ou Não Confidenciais.

Nenhum Preposto pode revelar a terceiros quaisquer informações referentes aos demais colaboradores, tais como, endereço, telefone, função, dentre outras, assim como informações referentes a clientes, tais como, identidade, informações pessoais, investimentos dentre outras.

Nenhuma informação confidencial da empresa pode ou deve ser discutida em locais inapropriados como locais públicos ou locais fechados com a presença de terceiros ou pessoas não diretamente relacionadas com o assunto ou sem autorização de acesso e conhecimento dessa informação.

4.3. Quanto ao uso do E-mail, Chat (Teams) e Internet

Para ter acesso a Suite de email e colaboração da empresa, o uso de autenticação em duas etapas é obrigatório.

Todas as mensagens enviadas via correio eletrônico e chat são consideradas como comunicação formal da empresa. Dessa forma, seu conteúdo deve ser ponderado, antes de sua emissão.

Não é permitida a utilização de linguagens ou imagens impróprias, obscenas ou de baixo calão na composição de mensagens.

O uso do correio eletrônico e do chat devem ser destinados somente para as atividades relacionadas ao negócio da empresa. Atividades como envio de correntes, engajamento em qualquer atividade ilegal, imprópria ou não ética, fotos, piadas, estórias ou qualquer tipo de áudio/vídeo de tais naturezas são terminantemente proibidas.

As informações armazenadas ou enviadas por meio dos computadores da empresa não são consideradas privadas, podendo ser abertas pela empresa quando for julgado necessário, sem que isso configure invasão de privacidade.

Preferencialmente não se deve encaminhar e-mails ou chats com discussões internas para o meio externo.

O acesso à Internet somente deve ser realizado para finalidades relacionadas aos interesses e assuntos profissionais da empresa.

É permitida a realização de download de arquivos de sites da Internet desde que esteja relacionado aos interesses e assuntos profissionais da empresa, e que os sites sejam de confiança inquestionável.

- Mensagem de Ausência Temporária (Out of Office)

Em caso de ausência do escritório, o Preposto deverá programar sua caixa de mensagens para o envio automático de mensagem de ausência temporária. A programação no Outlook é feita clicando em Settings (Configurações) - Conta – Respostas Automáticas.

Não é permitido colocar nomes, telefones e e-mails de outros prepostos. O texto deverá ser padronizado, da seguinte forma:

"Estarei ausente do escritório no período de [data] a [data]. Em caso de urgência, por favor, entre em contato com xxxxx@opportunity.com.br."

No texto acima, "xxxxx" deverá ser o nome do grupo do departamento ou um nome de grupo criado especialmente para períodos de férias. Entre em contato com a área de Tecnologia para maiores informações.

- Padrão de E-mails | Tipologia e Assinatura

Consulte o Manual de Orientação aos Funcionários – MOF.

4.4. Quanto ao uso de senhas

Todas as senhas devem ser individuais e mantidas confidenciais pelos seus proprietários e não devem ficar expostas para consulta nem serem anotadas em papel ou em qualquer outro local. Os usuários são responsáveis por todas as atividades realizadas com seus logins e senhas.

Não devem ser utilizadas senhas de fácil adivinhação como, por exemplo, data de aniversário, nome, sobrenome, dentre outras. As senhas devem ter de mínimo 6 caracteres para sistemas e, para logon na rede, um mínimo de 8 caracteres, sendo compostas por caracteres alfabéticos, numéricos, e caracteres especiais (!@#$%, por exemplo). As senhas antigas não devem ser reutilizadas após sua expiração.

Os eventos de login e alteração de senhas devem ser auditáveis e rastreáveis.

4.5. Quanto ao Acesso às Dependências da empresa

É vedado o acesso de visitantes às dependências da empresa sem identificação na recepção, sendo que o acesso dos visitantes aos salões de trabalho deve ser permanentemente acompanhado pelo Preposto responsável pela visita. Estão incluídos como visitantes os prestadores de serviços, Prepostos de empresas de auditoria ou órgãos reguladores e prestadores de serviço de manutenção de software.

Os Prepostos não devem divulgar aos visitantes, em qualquer hipótese, as senhas de ingresso às dependências da empresa.

É vedado o acesso de visitantes às mesas de trabalho, mesmo na presença de um Preposto. Entretanto, casos excepcionais podem ser previamente analisados e aprovados pelo Diretor responsável pela área.

Os trabalhos de visitantes deverão ser desenvolvidos em salas de reuniões e na presença do Preposto responsável pela visita na empresa, mesmo nos fins de semana.

4.6. Quanto ao reporte de incidentes

Os Prepostos também são responsáveis por reportar quaisquer incidentes de segurança ocorridos e imediatamente comunicá-los ao Comitê de Segurança, fornecendo todas as informações solicitadas pelo Comitê.

Os incidentes ocorridos no ambiente de tecnologia da empresa não devem ser divulgados a terceiros ou outras partes que não estejam diretamente envolvidas com o incidente.

O não reporte dos incidentes de segurança ocorridos por parte dos Prepostos implicará em uma violação de segurança e o responsável estará sujeito às penalidades previstas nesta Política.

5. VIOLAÇÕES

São consideradas violações à Política de Segurança da Informação e de Segurança Cibernética as seguintes situações, não se limitando às mesmas:

- Quaisquer ações ou situações que possam expor a empresa à perda financeira e de imagem, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos de informação.
- Uso indevido de dados corporativos, divulgação não autorizada de informações ou de segredos comerciais ou outras informações sem a permissão expressa da empresa.
- Uso de dados, informações, equipamentos, software, sistemas ou outros recursos tecnológicos, para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos internos e externos, da ética ou de exigências de organismos reguladores da área de atuação da empresa.
- A não comunicação imediata ao Comitê de Segurança de quaisquer violações ou atitudes anormais de que porventura um Preposto venha a tomar conhecimento ou chegue a presenciar.
- O não cumprimento de qualquer norma desta Política de Segurança da Informação e de Segurança Cibernética.

6. PENALIDADES

A violação desta Política é considerada falta grave, podendo ser aplicadas penalidades de acordo com a deliberação do Comitê de Segurança, como segue:

- Advertência pelo Comitê de Segurança.
- Aplicação de ações disciplinares.
- Término ou cessão do contrato de prestação de serviço ou relação comercial.
- Processo civil ou criminal.

7. PROCEDIMENTOS DE SEGURANÇA

O Comitê de Segurança desenvolveu e aprovou normas e procedimentos internos de segurança, a serem observados principalmente pelas áreas de TI Suporte, TI Sistemas e Gerência Administrativa, de forma a garantir a segurança da informação, segurança cibernética e da empresa como um todo.

Os procedimentos de segurança estão anexos a esta Política de Segurança e poderão ser disponibilizados pelo Security Officer, nas situações e para os fins que este ou o Comitê de Segurança entender cabíveis.

Os procedimentos de segurança somente podem ser alterados pelo Comitê de Segurança e serão revisados anualmente por tal Comitê.

* * *