Omni
Soluções Financeiras

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA PÚBLICA

Omni
Soluções Financeiras

ÍNDICE

1. OBJETIVO

Esta Política define os princípios e diretrizes estabelecidos pela OMNI (Omni S.A.- Crédito, Financiamento e Investimento, instituição líder do Conglomerado Prudencial) para assegurar a disponibilidade, a integridade e a confidencialidade dos seus dados e dos seus sistemas de informação.

2. ABRANGÊNCIA

Aplicável a todo o Conglomerado Prudencial OMNI (“Omni”) e empresas controladas, bem como a todos os colaboradores, executivos, prestadores de serviços e fornecedores (no Brasil e no Exterior), que tenham acesso à dados e informações, sejam no âmbito cibernético, seja no formato eletrônico ou no formato físico.

3. DIRETRIZES

3.1. Treinamento e Conscientização

Todos os colaboradores, prestadores de serviços e fornecedores devem participar e apoiar o treinamento de segurança e requisitos de conscientização da Omni.

3.2. Cooperação entre organizações

Devem ser estabelecidos e mantidos contatos com as autoridade, órgãos reguladores e grupos de segurança, para compartilhamento de conhecimento e assistência, conforme apropriado.

3.3. Condutas de Segurança da Informação

3.3.1. Uso aceitável de ativos

Todos os colaboradores e prestadores de serviços e fornecedores devem cumprir com as normas de uso aceitável.

3.3.2. Uso aceitável dos sistemas de informação

Todos os usuários dos sistemas de informação são obrigados a utilizar os sistemas de maneira legalmente responsável.

Nos computadores e redes da Omni, somente devem ser instalados software e hardware licenciados e aprovados pelos times de TI.

3.3.3. Direito de busca e monitoramento

A direção da Omni reserva-se o direito de monitorar, inspecionar e/ou pesquisar constantemente os seus sistemas de informação.

3.4. Classificação da Informação

Toda informação da Omni deve ter um responsável principal para:

- Determinar como a informação pode ser usada.
- Classificar e rotular qualquer informação que ele tenha criado ou sob a sua responsabilidade.

- Estabelecer os controles adequados de segurança da informação, entre outras atribuições.

Entre as responsabilidades do proprietário da informação está a necessidade de garantir a classificação adequada entre os níveis estabelecidos pela Omni.

3.5. Gestão de Riscos

A Omni estabelece um processo de gestão de riscos de segurança da informação visando mitigar os riscos identificados nos processos considerados críticos da empresa.

3.6. Gerenciamento de vulnerabilidades

Devem ser realizadas análises de vulnerabilidades nos ativos e sistemas de processamento da Omni.

3.7. Inventário de ativos

Deve ser mantido inventário atualizado dos ativos de informação da Omni contendo recursos de hardware, software, aplicações de negócio, equipamentos de rede, recursos humanos, instalações físicas e itens relevantes para a Omni, como prestadores de serviços e fornecedores.

3.8. Transferência das informações

A transferência eletrônica ou física de informações entre a Omni e prestadores de serviços e fornecedores deve ser controlada da maneira planejada para assegurar a sua proteção e armazenamento adequado.

3.9. Gerenciamento nas comunicações e operações

3.9.1. Documentação dos procedimentos operacionais

Os processos e procedimentos, para administrar e executar as operações de segurança e controle da Omni devem ser documentados e mantidos para promover a coerência com o ambiente operacional da empresa.

3.9.2. Gerenciamento de mudanças

Modificações e aperfeiçoamentos dos sistemas de informação da Omni devem ser administrados através do processo controlado de gerenciamento de mudanças.

3.9.3. Monitoramento e registro (log) do sistema

A Omni deve desenvolver e manter um processo para monitorar e capturar informações, relacionadas à interação entre os usuários e ativos de informação.

3.9.4. Monitoramento de uso do sistema

A Omni deve desenvolver procedimentos para o monitoramento da segurança das atividades relacionadas a eventos de log.

3.9.5. Estação de trabalho sem monitoração

Os computadores devem solicitar a autenticação no início da sessão, e ficar protegidos por um bloqueio de tela ou encerramento automático quando ociosos ou não sendo usados.

3.9.6. Proteção de intrusão e gerenciamento de incidentes

As responsabilidades e procedimentos estabelecidos devem ser projetados para evitar, detectar, atuar e resolver os incidentes que possam afetar a confidencialidade, disponibilidade ou integridade dos sistemas, informações ou processos de negócio da Omni.

3.9.7. Processo de resposta a incidentes

Processos e procedimentos devem ser estabelecidos para responder às violações de segurança, eventos e incidentes anormais ou suspeitos, com o objetivo de minimizar o dano aos ativos de informação e permitir a identificação e punição de seus autores.

3.9.8. Software de antivírus e código malicioso

Os controles de detecção e prevenção, projetados para proteger a Omni contra software de código malicioso e vírus, devem ser instalados em todos os ativos relacionados à informação da empresa.

3.9.9. Identificação e operação

Os usuários devem comunicar de imediato às áreas de TI, sobre qualquer vírus ou código malicioso detectado em computador da rede ou dispositivo relacionado.

3.9.10. Segregação de funções

As funções e responsabilidades incompatíveis devem ser separadas, para minimizar a possibilidade de acesso ou uso indevido.

3.9.11. Segregação de ambientes

Os ambientes de desenvolvimento, testes e produção devem ser segregados.

3.9.12. Planejamento de capacidade

Os ativos relacionados à informação da Omni devem contar com a capacidade e recursos adequados.

3.9.13. Backup e retenção

A Omni deve garantir periodicamente backups dos ativos de informação, para propósitos de recuperação operacional, assim como estar em conformidade com os procedimentos de continuidade operacional e de recuperação de desastres e que tais backups sejam retidos, de acordo com os requisitos de negócios e regulatórios.

3.9.14. Controles criptográficos

Controles criptográficos devem ser utilizados quando uma informação precisa ser protegida baseada na sua classificação e o ambiente onde é armazenada ou através do qual é transmitida não é seguro.

3.9.15. Segurança de Rede

A Omni deve providenciar os recursos de segurança de rede, de acordo com o grau mais adequado para a natureza dos dados sendo transmitidos.

3.9.16. Uso de senha de acesso

A Omni provê um sistema adequado para gerenciamento de senhas de acesso e de sistemas respeitando os requisitos de complexidade, tamanho mínimo e histórico de senhas.

3.10. Acesso aos sistemas

Todo usuário dos serviços de informação da Omni deve utilizar uma identificação exclusiva, para autenticação e atribuição das responsabilidades individuais. Há necessidade de autorização documentada para que a identificação do usuário seja emitida.

3.11. Sistema de gerenciamento de senhas

Os usuários aprovados e autorizados pela Omni a utilizar os sistemas, redes, aplicativos e a informação ali contida, são responsáveis pela proteção de suas respectivas senhas. As senhas de usuários devem permanecer confidenciais, não devendo, em hipótese alguma, ser compartilhadas, enviadas ou divulgadas de qualquer outra maneira.

3.12. Desenvolvimento, manutenção e aquisição de novos sistemas e aplicações

As considerações de segurança devem ser incluídas em todas as fases do ciclo de vida do desenvolvimento dos sistemas, especialmente para assegurar que as políticas de segurança da Omni sejam abordadas em tempo hábil e com eficiência de custos.

3.13. Acesso remoto

Todos os usuários, inclusive prestadores de serviços e fornecedores, com acesso remoto aos sistemas da Omni, são responsáveis pela segurança da conexão a todos os sistemas e recursos de informação da empresa.

3.14. Ambiente em nuvem

Devem ser cumpridas as diretrizes de segurança da informação afim de garantir a disponibilidade, confidencialidade e integridade das informações da Omni quando estiverem armazenadas, disponibilizadas e acessíveis em ambiente Cloud (Nuvem).

3.15. Terceirização e aquisição

Os acordos ou contratos de terceirização devem incluir os requisitos da Omni para administração de seus ativos de informação, de acordo com a Política de Segurança da Informação.

3.16. Conformidade com requisitos legais e contratuais

São avaliados internamente o cumprimento dos requisitos de segurança, legais, regulamentares e contratuais aplicáveis às suas respectivas práticas de negócio, através dos procedimentos projetados para apoiar e monitorar a conformidade daqueles requisitos.

3.17. Gestão de dados privados

A Omni deve garantir a privacidade dos dados coletados pelos sistemas de informação, de maneira que se compartilhados a prestadores de serviços e fornecedores e que impliquem na identificação pessoal do indivíduo, este deve ser previamente comunicado para autorizar como proprietário da informação.

Todas as informações coletadas e recebidas são utilizadas de acordo com a necessidade indicada na sua solicitação para prestação de serviços e existem controles implementados para proteger as informações contra acesso não autorizado ou processamento indevido.

3.18. Pessoal e provisão de recursos

As considerações relativas à segurança que apoiam os requisitos da Omni devem ser endereçadas através da descrição das responsabilidades do cargo da equipe, ou informadas de acordo com o trabalho a ser executado.

3.18.1. Acordo de confidencialidade

O colaborador deve ler, entender e atuar de acordo com os termos contratuais importantes e aplicáveis a sua posição. Para prestadores de serviços e fornecedores o acordo de confidencialidade deve constar no contrato entre as partes.

3.19. Gestão de Continuidade de Negócios

A Omni deve proteger adequadamente os seus ativos, informações e processos de negócio críticos contra os efeitos de falhas e desastres de grandes proporções, através do desenvolvimento e implantação de uma estratégia abrangente de continuidade de negócios.

3.20. Gestão de Terceiros

A Omni reserva-se o direito de auditar as atividades e práticas de acesso destes terceiros nos contratos aplicáveis. A Omni reserva-se o direito de realizar essa auditoria, incluindo inspeções on-site em prazos razoáveis de negócio.

4. DISPOSIÇÕES GERAIS

4.1. Prazo

O prazo de atualização desta Política é de 01 (um) ano ou em data anterior, caso necessário.

5. DIVULGAÇÃO DO CONTEÚDO

Esta versão deve ser utilizada para publicação nos veículos de comunicação externa da Omni, alinhada com a Política de Segurança da Informação oficial interna.