DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO PARA FORNECEDORES

cooxupé

SUMÁRIO

1. **OBJETIVO** 3
2. **DEFINIÇÕES** 3
3. **CONFORMIDADE** 3
4. **GESTÃO DE RECURSOS HUMANOS** 3
5. **GESTÃO DE ATIVOS** 4
6. **CONTROLE DE ACESSO** 4
7. **SEGURANÇA FÍSICA** 5
8. **GESTÃO DE OPERAÇÕES** 5
9. **CONTINUAÇÃO DE NEGÓCIOS E RECUPERAÇÃO DE DESASTRES** 6
10. **RESPOSTA A INCIDENTES E NOTIFICAÇÃO DE VIOLAÇÃO** 6

1. Objetivo

Esta diretriz de Segurança da Informação tem por finalidade definir as regras e princípios a serem adotados aos fornecedores da COOXUPÉ, para garantir a proteção das informações disponibilizadas pela COOXUPÉ, incluindo dados pessoais e dados pessoais sensíveis.

São levadas em consideração a segurança dos sistemas de informação dos fornecedores e suas infraestruturas que estão relacionados com os serviços prestados à COOXUPÉ e havendo necessidade, será enviado um questionário sobre o ambiente e a segurança da informação do fornecedor.

2. Definições

A classificação deste documento é considerada “pública”, devendo ser compartilhada com os fornecedores e prestadores de serviços da COOXUPÉ.

Documentos Relacionados
PROCEDIMENTO DE SEGURANÇA E PRIVACIDADE DE FORNECEDORES DE PRODUTOS E SERVIÇOS

3. Conformidade

Esta diretriz está sujeita a atualização semestral ou anual, conforme a necessidade das readequações internas da COOXUPÉ. Cabe ao fornecedor acessar o site www.cooxupe.com.br (*Menu Governança e Transparência)* para certificar as atualizações e revisões da mesma.

4. Gestão de Recursos Humanos

a) CONSCIENTIZAÇÃO SOBRE PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO é de extrema importância que os colaboradores dos fornecedores da COOXUPÉ acessem programas de conscientização em segurança e/ou proteção de dados e receber atualizações periódicas sobre conscientização. A Educação em segurança deve ser um processo contínuo afim de mitigar e reduzir riscos.

b) DESLIGAMENTO OU SUBSTITUIÇÃO DE COLABORADOR(ES) DO FORNECEDOR: em caso de desligamento ou substituição de colaborador(es) do fornecedor designado(s) para prestar serviços à COOXUPÉ, o fornecedor deverá comunicar à COOXUPÉ, imediatamente e por escrito, do desligamento e/ou substituição do(s) colaborador(es), para que o direito de acesso do(s) ex-colaborador(es) seja devidamente removido e/ou atualizado. Caso necessário, ficará o fornecedor responsável por devolver à COOXUPÉ, documentos de propriedade intelectual, estação de trabalho, celulares e/ou qualquer ativo que a COOXUPÉ tenha compartilhado com o fornecedor”.

5. Gestão de Ativos

a) Caso o fornecedor for armazenar, processar, compartilhar, divulgar, integrar ativos, informações e dados pertencentes a COOXUPÉ, o mesmo receberá um questionário com as questões técnicas sobre segurança da informação, proteção de dados e segurança cibernética, para avaliação dos ativos do fornecedor, podendo resultar em questionamentos por parte da COOXUPÉ, caso exista alguma dúvida ou divergência das informações preenchidas no FORMULÁRIO DE AVALIAÇÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE COOXUPÉ.

b) Todo o ativo do fornecedor que for necessário se conectar internamente na rede de dados da COOXUPÉ (exceto via VPN), deverá ser inspecionado e instalado o software de antivírus e proteção avançada utilizados pela COOXUPÉ.

c) O ativo da COOXUPÉ que for compartilhado com o fornecedor não poderá ser compartilhado com terceiros, salvo ressalva e de conhecimento da COOXUPÉ e/ou área responsável pelo processo, através de formalização de compartilhamento.

d) O fornecedor deve manter os ativos de seus ambientes que contenham dados/informações da COOXUPÉ protegidos, seguindo procedimentos, normas e práticas de segurança da informação.

e) Fica sob a responsabilidade do fornecedor a adoção de procedimentos que comuniquem anomalias ou incidentes nos ativos em que os dados e informações da COOXUPÉ, incluindo dados pessoais e dados pessoais sensíveis, estiverem sendo armazenados, compartilhados, divulgados, processados ou visualizados.

f) Ao término dos serviços prestados para a COOXUPÉ, o ativo de propriedade intelectual, incluindo dados pessoais e dados pessoais sensíveis que foram compartilhados podem estar sujeitos a descarte, com processos de formalização evidenciando a exclusão dos mesmos.

6. Controle de Acesso

a) O fornecedor deve manter um nível de controle de acesso aceitável em seus ambientes que contenham dados/informações da COOXUPÉ.

b) Os acessos aos ativos da COOXUPÉ deverão ser efetuados por métodos de autenticação, que terão rastreamento de logs de acessos por parte da COOXUPÉ, em casos que houver tratamentos de dados, os acessos aos ativos COOXUPÉ deverão seguir itens de segurança específicos que serão pré-acordados.

c) Todos os acessos aos ativos do fornecedor que mantém dados e informações da COOXUPÉ devem ser monitorados pelo mesmo.

d) O fornecedor deve manter controles de acesso em seus ativos e processos para seus colaboradores, terceiro e/ou organizações que prestam serviços a ele, referente a prestação de serviços a COOXUPÉ.

e) Identificar individualmente todos os colaboradores ou organizações que sejam ou estiverem sobre responsabilidade do fornecedor que prestam serviços a COOXUPÉ.

f) Utilizar métodos de autenticação satisfatórios aos colaboradores da COOXUPÉ que acessam os ativos do fornecedor.

g) Todas as contas de serviços que serão utilizadas em sistemas e/ou plataformas do fornecedor deverão ser repassadas e seus direitos de acessos definidos juntamente com o departamento de TI da COOXUPÉ.

h) Exclusão de contas padrões de sistemas, processos e ativos após a implantação do projeto.

i) Manter seus ativos atualizados e manter controles e recursos para mitigar acessos e tentativas indevidas.

j) Controlar por perfil os acessos dos colaboradores aos ativos do fornecedor, ou seja, ter acesso somente aos dados e informações necessários para a realização do seu trabalho.

k) Efetuar a guarda de credenciais de acessos fornecidos pela COOXUPÉ, não permitindo o seu compartilhamento, salvo exceções acordadas com ambas as partes.

l) O fornecedor deve manter os logs de acessos, seja para integrações entre sistemas, acessos de colaboradores da COOXUPÉ em sua plataforma, bem como logs de armazenamento, processamento e compartilhamento de ativos pertencentes a COOXUPÉ, para posteriores análises e averiguações, caso seja necessário.

m) Os acessos ao ambiente COOXUPÉ por parte dos colaboradores, terceiros ou organização que são de responsabilidade dos fornecedores ocorrerão por VPN e usuário nomeado.

7. Segurança Física

a) O fornecedor deve manter medidas de segurança física apropriadas para proteção dos sistemas de computação, utilizando softwares e hardwares com nível de segurança adequados para proteger os ativos contratados, bem como manter medidas de proteção contra desastres ambientais, quedas de energia e outro intemperes, de acordo com os riscos relevantes aos processos que impactam no negócio da COOXUPÉ.

b) O fornecedor dever se comprometer a não deixar em exposição papéis, mídias removíveis, credenciais de acesso e/ou outros meios que contenham ativos da COOXUPÉ.

c) Proteger por controles de acessos apropriados o(s) datacenter(s) que contém ativos da COOXUPÉ, a fim de garantir que apenas o pessoal autorizado seja capaz de acessa-lo.

8. Gestão de Operações

a) Para toda transferência de ativo que contenha dados e informações da COOXUPÉ não é recomendado o uso de plataformas públicas/não corporativa, afim de evitar exposição de dados.

b) Recomenda-se que o fornecedor valide as configurações de ativos que contenham dados e/ou informações da COOXUPÉ, afim de evitar vazamentos e exposições indevidas de dados e/ou

informações.

c) Quando houver necessidade de o fornecedor compartilhar, armazenar, processar, integrar processos e sistemas que contenham ativos da COOXUPÉ, a equipe de segurança da informação em conjunto com o fornecedor avaliará os requisitos de segurança e se necessários, adequações no processo podem ocorrer.

d) O fornecedor deve manter a proteção contra exposição de dados, ataques e tentativas de intrusão das plataformas que contenham dados da COOXUPÉ.

e) O fornecedor deve utilizar mecanismos de proteção de intrusão a ataques web (Firewall de aplicação) e softwares que geram alertas automaticamente para a equipe de resposta a incidentes cibernéticos.

f) Utilizar solução antivírus atualizada nos dispositivos dos colaboradores do fornecedor que irão prestar serviços a COOXUPÉ para prevenir perda de dados e tentativas de intrusão.

9. Continuação de Negócios e Recuperação de Desastres

a) O fornecedor deve manter um plano de continuidade de negócios e recuperação de desastres que aborde a disponibilidade e integridade do sistema e/ou serviço contratado.

b) Implementar redundância aos ativos de suporte do fornecedor do sistema contratado pela COOXUPÉ para manter a disponibilidade acordada.

c) O fornecedor deve adotar processo e políticas de backup dos ativos que armazenam informações da COOXUPÉ.

d) O fornecedor informará via questionário o RTO (Tempo de recuperação) e RPO (Objetivo de ponto de recuperação), visando a recuperação e disponibilidade dos ativos que contenham dados e/ou informações da COOXUPÉ, conforme contratação.

10. Resposta a Incidentes e Notificação de Violação

a) O fornecedor deve manter um programa de resposta a incidentes testado, que será funcional a responder incidentes que envolvam dados da COOXUPÉ. Informar a COOXUPÉ caso seja descoberta alguma falha e vulnerabilidade nos ativos, seja de seus colaboradores, de terceiros ou organizações que contenham dados da COOXUPÉ, bem como ativos que fornecem acessos aos dados da COOXUPÉ.

b) A menos que a notificação seja atrasada pelas ações ou demandas de uma autoridade legal, o fornecedor informará a COOXUPÉ imediatamente sobre qualquer acesso ilegal ou aquisição, uso ou divulgação não autorizados de seus dados que ocorreram no sistema e/ou serviço contratado.

c) O fornecedor deve tomar as medidas para mitigar a causa de qualquer violação de dados da COOXUPÉ, e tomará medidas corretivas para evitar futuras violações de dados.

d) Caso o incidente afete colaboradores, cooperados e outros que tenham envolvimento com a COOXUPÉ, o fornecedor na medida do possível, será o responsável pelo fornecimento das informações sobre a natureza e as consequências da violação de dados que sejam razoavelmente

solicitadas para permitir que a COOXUPÉ notifique indivíduos afetados, agências governamentais e/ou agências de crédito.