Política de segurança da informação

2.1 GESTÃO DE INFORMAÇÃO

Rua Prof. José Leite e Oiticica, 530
Vila Gertrudes - 04705-080
São Paulo, SP - Brasil
T +55 (11) 4040 3514
www.cba-design.com/latam

cba B+G

Sumário

Rua Prof. José Leite e Oiticica, 530
Vila Gertrudes - 04705-080
São Paulo, SP - Brasil
T +55 (11) 4040 3514
www.cba-design.com/latam

1. Objetivo

Esta política estabelece diretrizes para a gestão segura das informações, visando proteger dados sensíveis e confidenciais contra acessos não autorizados, vazamentos, alterações indevidas ou perdas. A política abrange classificação da informação, uso aceitável, armazenamento, transporte, descarte, retenção, e continuidade da informação em casos de incidente ou desastre.

2. Abrangência

Aplica-se a todos os colaboradores, parceiros, prestadores de serviço e quaisquer terceiros que, de alguma forma, tenham acesso às informações da empresa, independentemente do meio de armazenamento ou transmissão.

3. Diretrizes

3.1. Classificação da Informação

Classificamos as informações sensíveis ou privadas de acordo com sua fonte. Aplicamos essa classificação nos nossos sistemas de gestão de arquivos, o que direciona o controle de permissionamento.

3.2. Uso Aceitável de Ativos

Os ativos de informação (computadores fornecidos, dispositivos BYOD, sistemas, e-mail corporativo, nuvem) são utilizados exclusivamente para fins profissionais. Essa normativa é passada para os colaboradores no momento do onboarding e reforçada em nossos contratos de trabalho e BYOD.

O uso de dispositivos pessoais segue diretrizes específicas da política de BYOD, que especifica a separação dos perfis de trabalho e de uso pessoal na máquina do indivíduo. A CBA B+G possui acesso administrativo no perfil de trabalho, com o objetivo de aplicar as restrições de segurança, assim como auditar o uso desses perfis.

É proibido o compartilhamento de senhas, acesso a conteúdos impróprios ou não relacionados às atividades da empresa usando dispositivos ou contas fornecidas.

3.3. Armazenamento e Transporte Seguro

Todos os sistemas utilizados pela CBA B+G passam por uma avaliação prévia de segurança, com foco na estrutura, armazenamento e retenção de dados. Apenas são adotadas soluções que estejam em conformidade com nossas políticas de governança e privacidade da informação.

As informações sensíveis são armazenadas exclusivamente em ambientes controlados por administradores de sistemas, com proteção por mecanismos de criptografia e controle de acesso. O transporte desses dados ocorre por canais seguros, como conexões TLS 1.2 ou superiores, redes VPN e sistemas que utilizam autenticação forte.

Todos os colaboradores são orientados a armazenar arquivos apenas em equipamentos configurados pela empresa, utilizando seus perfis de trabalho e os softwares corporativos de gestão de arquivos fornecidos.

Arquivos hospedados em servidores físicos (colocation) e ambientes virtuais (como Microsoft 365) seguem os mesmos critérios de segurança descritos nesta política, garantindo a integridade e a confidencialidade da informação em todos os meios de armazenamento.

3.4. Descarte e Retenção de Dados

Documentos físicos ou digitais são descartados de maneira segura: trituramos os documentos no caso de papel, usamos de software de limpeza segura para mídias eletrônicas e reforçamos a exclusão de dados em softwares e ferramentas no encerramento de contas.

O prazo de retenção dos dados respeita as exigências legais e contratuais, sendo aplicadas rotinas de revisão periódica.

3.5. Política de Mesa e Tela Limpa

Orientamos que, ao se ausentar do ambiente de trabalho (mesmo remoto), os colaboradores bloqueiem suas telas e não deixem suas anotações expostas a terceiros no seu ambiente de trabalho de forma que Documentos físicos contendo dados sensíveis sejam guardados em local seguro ao final do expediente.

Orientamos que os usuários tenham cautela com a abertura de documentos sensíveis em ambientes de trabalho compartilhados, como escritórios ou coworkings.

3.6. Continuidade da Informação

A continuidade de informação é fundamental para mantermos o fluxo de trabalho em um ambiente remoto. Nossa estrutura, processos e ferramentas são focados em garantir a proteção de dados críticos em situações de falha técnica, desastres ou indisponibilidades. Os principais pilares são:

3.7. Papéis e responsabilidades definidos

Possuímos um managing partner responsável pela continuidade da informação, responsável por coordenar o plano de resposta em casos de incidentes. Temos também um time de tecnologia com competência, acessos e responsabilidade para restabelecer o fluxo de informação.

3.8. Backup Automatizado e Distribuído

Garantimos cópias de segurança dos dados em múltiplos ambientes (Microsoft 365, Google Cloud, servidores em colocation), com rotinas automatizadas e armazenamento segregado entre produção e arquivo morto.

Recuperação Rápida

Nossos processos priorizam a capacidade de restaurar informações com agilidade, minimizando impactos em caso de falhas ou perdas. As políticas de restauração são testadas e documentadas.

Alta Disponibilidade dos Sistemas Críticos

Soluções em nuvem e servidores locais possuem configuração redundante, quando aplicável, para manter os serviços essenciais ativos mesmo durante manutenções ou incidentes.

Parceiros e prestadores de serviços

Contratamos serviços de suporte técnico e atendimento prioritário das ferramentas mais importantes para o nosso fluxo de trabalho, com SLAs estabelecidos.

O processo de continuidade de informação é detalhado no nosso Plano de Continuidade da Segurança da Informação (PCSI).

3.9. Gestão de Ativos

Todos os ativos de informação são identificados, inventariados e monitorados, de acordo com a nossa política de gestão de equipamentos. Quaisquer mudanças, manutenções ou descarte de ativos são bloqueadas por padrão e devem seguir processo formal de autorização e registro. O usuário deve solicitar a mudança para o time de tecnologia, que realiza o procedimento para garantir a integridade do equipamento e continuidade do seu funcionamento.

3.10. Criptografia

O tráfego de informações confidenciais entre usuários, sistemas e serviços externos deve ocorrer via protocolos criptografados, como TLS 1.2/1.3 ou AES 256 bits. Chaves de criptografia são gerenciadas e armazenadas de forma segura.

4. Responsabilidades

Head de informação: Definir, revisar e evoluir os processos referentes à gestão de informação na CBA B+G. Responder tecnicamente pelo nível de adesão dos termos dessa política na empresa.

Área de Tech support: Implementar os controles técnicos para garantir o cumprimento desta política. Monitorar a aplicação da política e revisar periodicamente seu conteúdo.

5. Penalidades

O descumprimento desta política poderá acarretar em medidas disciplinares conforme previsto no regulamento interno, incluindo advertência, suspensão e, em casos mais graves, desligamento.

6. Controle de alterações

Versão	Data	Quem	Anotações
2	04/02/2025	Luis Bartolomei	Aprovação
1	03/12/2024	Thiago Ramiro	Criação