Política de segurança da informação

2.3 GESTÃO DE EQUIPAMENTOS

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

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 define os requisitos para o uso, proteção e descarte seguro de equipamentos utilizados para acessar, processar, armazenar ou transmitir informações da empresa. Visa garantir a integridade, confidencialidade e disponibilidade das informações por meio do controle adequado dos dispositivos físicos utilizados nas operações.

2. Abrangência

Aplica-se a todos os equipamentos corporativos (como notebooks e servidores), bem como a dispositivos pessoais autorizados para uso profissional (BYOD), incluindo smartphones e computadores usados em regime remoto.

3. Diretrizes

3.1. Uso Autorizado e Inventário

Todos os equipamentos corporativos são inventariados, com número de série, modelo, responsável e status atualizados. O controle dos equipamentos é feito por um sistema que registra os dados dos equipamentos, guarda todo o histórico de movimentações e usuários. Esse sistema é alimentado apenas pelos membros da equipe de tech support.

Equipamentos pessoais só podem ser utilizados mediante autorização formal e conforme diretrizes da política de BYOD. Qualquer equipamento utilizado deve ser configurado pelo time de tecnologia para atender os padrões de segurança de informação e de acessos. O uso dos equipamentos fornecidos pela CBA B+G é exclusivo para atividades relacionadas ao trabalho.

Todos os colaboradores assinam o Contrato de comodato de bem móvel para execução de atividade profissional ao receberem equipamentos da empresa. Todos os termos relevantes ao uso dos equipamentos estão contemplados nesse contrato.

3.2. Política de BYOD (Bring Your Own Device)

O BYOD é uma metodologia de trabalho, cujo propósito é trazer maior flexibilidade aos profissionais para que possam utilizar seus equipamentos ou dispositivos eletrônicos pessoais preferenciais também no ambiente corporativo. Para que isso aconteça temos estabelecida a política de BYOD, que tem como objetivo garantir a segurança e integridade da infraestrutura tecnológica e a segurança das informações envolvidas na execução dos trabalhos.

Os profissionais devem concordar com os termos e condições estabelecidos nesta política para poder utilizar os recursos disponibilizados pela CBA B+G, tais como, acesso à rede interna, plataformas de trabalho colaborativas nas nuvens e softwares de trabalho ou gestão. A CBA B+G reserva-se os direitos de fiscalizar e revogar os acessos aos profissionais que não cumprirem os termos e procedimentos descritos nesta política, a qual estabelece as diretrizes da CBA B+G para o uso de equipamentos ou dispositivos eletrônicos pessoais preferenciais, por profissionais, para os fins relacionados aos trabalhos contratados, seja qual for a modalidade de contratação.

A política de BYOD é assinada por todos os colaboradores no onboarding.

3.3. Configuração Segura e Gerenciamento

Todos os notebooks corporativos são entregues com configurações mínimas de segurança aplicadas, de acordo com o sistema operacional:

Dispositivos Apple (macOS):

São configurados com FileVault ativado para criptografia de disco, firewall ativado, atualizações automáticas do sistema habilitadas e exigência de senha de acesso.

Sempre que possível, são incluídos em solução de gerenciamento remoto compatível com macOS, permitindo rastreamento e bloqueio em caso de perda ou roubo.

Dispositivos Windows:

São protegidos com a solução corporativa Kaspersky Endpoint Security, com proteção em tempo real, firewall ativo e atualizações automáticas habilitadas.

Os discos são criptografados com BitLocker ou solução equivalente, conforme compatibilidade do equipamento.

3.4. Equipamentos em Colocation

O servidor em colocation está localizado em ambiente controlado, com acesso físico limitado a profissionais autorizados. A configuração do servidor segue boas práticas de segurança, incluindo controle de acesso ao sistema operacional, atualizações regulares e criptografia de dados sensíveis.

A infraestrutura local da empresa conta com servidores DELL, com recursos nativos de segurança, como Secure Boot, TPM 2.0 (Trusted Platform Module) e firmware assinado digitalmente, que garantem a integridade do sistema e da cadeia de inicialização. A confidencialidade das informações armazenadas é reforçada por criptografia em nível de disco e controle de acesso lógico segmentado. Já a alta disponibilidade é suportada por fontes redundantes, tolerância a falhas e gerenciamento remoto via iDRAC9, permitindo ações corretivas mesmo em casos de indisponibilidade física. Com isso, o servidor atende aos pilares fundamentais da segurança da informação: confidencialidade, integridade e disponibilidade.

3.5. Transporte e Armazenamento Seguro

Todo o transporte de entrega e recolhimento de equipamentos é coordenado pelo time de tech support, que conta com fornecedores de logística com sistemas de seguro e rastreabilidade para essa operação.

As nossas políticas de comodato instituem que equipamentos fora da sede devem ser transportados com cuidado e não devem ser deixados em locais públicos sem supervisão. Documentos sensíveis não devem ser armazenados localmente em dispositivos móveis sem criptografia.

3.6. Descarte Seguro

Equipamentos que serão descartados ou realocados tem todos os dados removidos com ferramentas de limpeza segura. Quando a remoção dos dados envolve riscos à confidencialidade, recomenda-se a destruição física de discos rígidos e mídias.

4. Responsabilidades

Tech support: Manter o inventário atualizado; configurar e monitorar os dispositivos corporativos; garantir a aplicação das políticas de segurança em equipamentos BYOD autorizados; supervisionar o descarte seguro.

Colaboradores: Zelar pela conservação dos equipamentos; seguir as diretrizes de segurança; comunicar imediatamente perda, furto ou mau funcionamento de qualquer dispositivo usado em atividades da empresa.

5. Penalidades

O descumprimento desta política poderá acarretar medidas disciplinares, conforme previsto em contrato ou regulamento interno, incluindo advertência, bloqueio de acesso ou desligamento, conforme a gravidade.

6. Controle de alterações

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