Política de segurança da informação

2.4 GESTÃO DE INFRAESTRUTURA

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

Estabelecer diretrizes para garantir a operação segura, resiliente e eficiente da infraestrutura de tecnologia da informação, incluindo servidores físicos (colocation), redes, serviços em nuvem, mecanismos de backup, controle de acesso, proteção lógica e monitoramento.

2. Abrangência

Esta política aplica-se a todos os ambientes de infraestrutura utilizados pela empresa, como datacenter em colocation, serviços do Microsoft 365, redes corporativas (incluindo VPN), soluções de segurança, estações de trabalho e dispositivos móveis.

3. Diretrizes

3.1. Segurança Física e Lógica

O acesso físico ao ambiente de colocation é restrito e controlado por meio de credenciais e agendamento prévio, conforme determinado na política de gestão de equipamentos. Todo acesso a sistemas, servidores e dispositivos segue a política de gestão de acessos, com autenticação multifator e segregação de funções.

3.2. Gestão de Ambientes em Nuvem

A segurança dos ambientes em nuvem utilizados pela empresa: Microsoft 365 (Exchange, SharePoint, OneDrive), Google Cloud Platform (GCP) e Amazon Web Services (AWS) é gerenciada de forma contínua pelo time de tech support, em conjunto com fornecedores especializados. Todos os ambientes adotam modelos de controle de acesso baseados em papéis, com segregação por área, função e nível de criticidade da informação.

As configurações de segurança de todas as plataformas digitais são revisadas periodicamente para garantir a conformidade com as políticas internas e exigências contratuais. Também são implementadas políticas de retenção e rastreamento de dados, além de mecanismos de alerta e auditoria de atividades incomuns, visando antecipar riscos e proteger informações sensíveis. A gestão desses ambientes contempla ainda criptografia nativa, autenticação multifator e monitoramento integrado aos sistemas de auditoria e resposta a incidentes.

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

3.3. Backup e Restauração

Nossa estrutura de backup e restauração que contempla os ambientes utilizados para a gestão de arquivos e informação (365, GCP e AWS). Os arquivos operacionais são organizados em dois níveis principais: drives individuais com permissões específicas por usuário e drives compartilhados para armazenamento de arquivos quentes utilizados colaborativamente entre times. Dados consolidados e materiais de referência são armazenados no servidor local, com gestão de acesso feita por perfil e função. Após seu ciclo ativo, os documentos passam por um processo de higienização e são enviados para o Google Cloud Platform (GCP), onde são armazenados em camadas de cold storage para arquivamento seguro e de longo prazo.

Todos os ambientes de armazenamento de informação (Microsoft 365, AWS, GCP e servidor local) contam com mecanismos de backup e restauração incluídos em sua configuração padrão ou contratada. Isso garante a redundância e recuperação de arquivos em caso de falha técnica, exclusão acidental ou incidentes de segurança. O time de tech support realiza monitoramento contínuo e testes periódicos de restauração para assegurar a integridade dos dados armazenados e a efetividade dos procedimentos de recuperação.

3.4. Disponibilidade e Continuidade

Os ambientes em nuvem (Microsoft 365, Google Cloud Platform e AWS) operam sob contratos com SLA robustos e contam com recursos nativos de continuidade, como failover automático, replicação entre zonas e restauração rápida de dados. Já o servidor em colocation oferece redundância de energia, discos e rede, além de gerenciamento remoto via iDRAC, o que permite atuação imediata mesmo em casos de indisponibilidade física. Essa combinação de arquitetura garante resiliência operacional e recuperação ágil em casos de falhas ou interrupções. Esses serviços essenciais em nuvem estão cobertos por SLAs robustos e planos de continuidade.

3.5. Proteção contra Ameaças

Os dispositivos Windows contam com o Kaspersky Endpoint Security corporativo, enquanto os dispositivos Apple operam com proteções nativas ativadas e integradas a políticas de controle remoto. A infraestrutura é protegida por firewalls ativos, tanto nos ambientes em nuvem quanto no servidor físico, com regras segmentadas e atualizadas periodicamente. Nossos ambientes em nuvem contam com proteções contra ataques DDoS configuradas nos provedores. Adicionalmente, são aplicadas práticas preventivas contra vazamentos de dados, e a empresa está avaliando soluções de Data Loss Prevention (DLP) para aprimorar o monitoramento e controle da informação sensível.

3.6. Patching e Atualizações

A gestão de atualizações de segurança é conduzida de forma contínua pelo time de tech support. Sistemas operacionais, softwares e firmware do servidor Dell são atualizados conforme cronograma definido, com aplicação de patches críticos priorizada. Ambientes em nuvem recebem atualizações automatizadas dos provedores (Microsoft, GCP, AWS), enquanto os ativos locais são validados em ambiente de homologação antes da atualização em produção, garantindo estabilidade e segurança.

Sistemas operacionais, servidores e softwares recebem atualizações regulares de segurança conforme cronograma definido.

3.7. Monitoramento e Alertas

Toda a infraestrutura da empresa é monitorada de forma proativa, com ferramentas automatizadas que acompanham métricas de performance, disponibilidade e segurança. Logs relevantes de atividades, autenticações e eventos de sistema são mantidos em conformidade com as políticas de auditoria e utilizados para investigação e resposta a incidentes. O servidor Dell PowerEdge conta com recursos nativos de diagnóstico e alertas via iDRAC, enquanto os ambientes em nuvem se integram com sistemas de notificação e auditoria centralizados (como o Microsoft 365 Audit Log e o Cloud Audit Logs do GCP). Esse ecossistema garante visibilidade contínua e resposta ágil a qualquer anomalia.

4. Responsabilidades

Head de informação: Revisar políticas, auditar configurações e validar planos de backup e continuidade.

Tech support: Garantir a implementação técnica dos controles, atualizações e monitoramento.

Todos os Colaboradores: Usar os recursos de forma segura, reportar anomalias e seguir as diretrizes estabelecidas.

5. Penalidades

O descumprimento desta política pode resultar em restrições de acesso, advertência formal ou medidas disciplinares, conforme o código de conduta da empresa..

6. Controle de alterações

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

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