Política de segurança da informação

2.6 AUDITORIA E CONTROLE

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 os princípios e práticas para auditoria, verificação e controle contínuo da conformidade com as políticas de segurança da informação. Visa garantir a efetividade dos controles técnicos e administrativos implementados, apoiar a gestão de riscos e demonstrar aderência a requisitos legais, contratuais e normativos.

2. Abrangência

Aplica-se a todos os sistemas, processos, colaboradores, terceiros e recursos tecnológicos envolvidos no tratamento de informações da empresa, incluindo ambientes internos, em nuvem e infraestrutura em colocation.

3. Diretrizes

3.1. Coleta e Retenção de Logs

Mantemos a coleta de logs nos sistemas críticos para garantir rastreabilidade e segurança. Registramos eventos como autenticações, acessos privilegiados, falhas, alterações de configuração e movimentações de dados. Sempre que possível, os logs são armazenados de forma centralizada, com proteção contra alterações e acesso não autorizado, e são mantidos por, 3 meses para fins de auditoria e investigação.

3.2. Monitoramento

Adotamos uma abordagem de monitoramento contínuo com base nas ferramentas de auditoria integradas aos ambientes que utilizamos, como Microsoft 365, Google Cloud Platform e AWS. O time de tech support acompanha eventos relevantes, como acessos privilegiados, alterações de configuração e movimentações de dados sensíveis, por meio dos logs nativos dessas plataformas. Priorizamos a análise dos registros dos sistemas mais críticos, com foco na identificação de comportamentos suspeitos, acessos fora do padrão e outras anomalias operacionais.

3.3. Relatórios de Controle

Estamos estruturando um processo de emissão periódica de relatórios de conformidade que evidenciem nossa aderência às políticas internas de segurança da informação e aos requisitos legais, como a LGPD. A intenção é que esses relatórios sejam compartilhados com a alta gestão e lideranças das áreas críticas, acompanhados de registros objetivos e, quando necessário, recomendações para correções e melhorias.

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

3.4. Testes e Simulações de Incidentes

Pretendemos implementar uma rotina anual de testes e simulações de incidentes de segurança, como falhas operacionais, vazamentos de dados ou ataques cibernéticos, com o objetivo de avaliar a eficácia dos nossos procedimentos e preparar o time para diferentes cenários. Esses exercícios serão documentados, analisados e utilizados como base para planos de ação e ajustes nos protocolos de resposta.

3.5. Auditorias Internas

Estamos definindo um cronograma de auditorias internas de segurança da informação, que permitirá revisar periodicamente políticas, processos e controles técnicos. A prioridade será dada a áreas com maior exposição a riscos ou que passaram por mudanças recentes. As auditorias poderão ser conduzidas pelo time de tech support ou com apoio de especialistas externos, garantindo uma visão independente e estruturada.

3.6. Auditorias Externas e Requisições Contratuais

Atendemos às demandas de auditorias externas e exigências contratuais, sempre que necessário. Nesses casos, prezamos pela transparência, expondo e estado atual da nossa maturidade no processo de evolução em segurança de informação. Disponibilizamos evidências de controles, registros de logs e cópias de políticas internas, respeitando os acordos de confidencialidade estabelecidos com cada parte.

4. Responsabilidades

Head de informação: Desenvolver e implementar os mecanismos de auditoria e relatórios para a alta gestão.

Tech support: Manter a coleta e integridade dos logs; acompanhar eventos suspeitos; aplicar testes de incidente; emitir relatórios e viabilizar auditorias.

Alta gestão: Apoiar a realização de auditorias e garantir que os planos de ação derivados sejam implementados.

Colaboradores: Apoiar auditorias quando envolvidos e seguir os procedimentos definidos pela empresa.

5. Penalidades

A obstrução de auditorias, o fornecimento de informações falsas ou a alteração indevida de registros de log serão tratados com rigor e podem levar à aplicação de medidas disciplinares, incluindo desligamento ou responsabilização civil/penal, conforme o caso.

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