Procedimento de Segurança de Acesso Físico

Histórico de versões

Data	Versão	Responsável
28/04/2024	1	Camila Andrade de Sena

1. Apresentação

O acesso físico às instalações da empresa é um aspecto crítico do gerenciamento de segurança para a Alura. Este procedimento descreve as etapas e diretrizes para controlar e gerenciar o acesso físico para garantir a segurança das pessoas, dos ativos e das informações confidenciais em conformidade com os padrões de governança, risco e conformidade (GRC).

Ao salvaguardar os pontos de entrada e saída, este protocolo visa proteger não só a segurança física das pessoas, mas também os bens e as informações sensíveis alojadas nas instalações. Portanto, as orientações contidas nesse documento devem ser entendidas e seguidas em todos os níveis hierárquicos da instituição.

2. Escopo

Esse procedimento define as práticas de segurança de acesso físico para a Alura. Este procedimento se aplica a todos os funcionários, visitantes e prestadores de serviços terceirizados que necessitem de acesso físico às instalações da instituição.

3. Objetivos

O objetivo deste procedimento é estabelecer uma estrutura segura para conceder, monitorar e revogar o acesso físico às instalações da Alura. Para que esse objetivo seja alcançado, são definidos os seguintes objetivos específicos:

a) segurança: implementar medidas robustas de controle de acesso físico para assegurar que apenas pessoas autorizadas tenham acesso às instalações, prevenindo tanto acessos indevidos internos quanto externos;
b) conformidade: garantir a conformidade com regulamentos, padrões e melhores práticas relevantes do setor para mitigar riscos legais e proteger a reputação da organização;
c) riscos: identificar e mitigar riscos potenciais associados a acesso não autorizado, violações e incidentes de segurança;
d) ativos de informação: proteger os ativos da empresa, informações confidenciais e propriedade intelectual contra acesso não autorizado ou roubo;

e) responsabilização: estabelecer responsabilização cara pela gestão e monitoramento das medidas de controle de acesso físico, promovendo a transparência e facilitando a prestação de contas em caso de investigação;
f) auditoria: monitorar continuamente os logs de acesso e realizar auditorias regulares para detectar anomalias, tentativas de acesso não autorizado ou atividades suspeitas;
g) treinamento e conscientização: realizar sessões de treinamento e programas de conscientização para educar os funcionários sobre políticas, procedimentos e protocolos de segurança de controle de acesso para promover uma cultura de segurança sólida e reduzir o risco de violações devido a falhas humanas;
h) plano de resposta a incidentes: desenvolver um plano de resposta a incidentes para abordar incidentes de segurança relacionados ao acesso físico, incluindo procedimentos para escalonamento, investigação e correção;
i) confiança: construir confiança entre as partes interessadas, incluindo funcionários, clientes e parceiros, demonstrando o compromisso de manter um ambiente seguro.

4. Público-alvo

A abrangência desse procedimento inclui:

a) departamento de segurança: encarregado de planejar, implementar e fazer cumprir as medidas de controle de acesso físico, garantindo a segurança efetiva das instalações;
b) gestão de instalações: responsável por supervisionar a manutenção e o funcionamento dos sistemas de controle de acesso e das barreiras físicas, assegurando sua operacionalidade contínua;
c) recursos humanos: responsável por fornecer informações essenciais para as permissões de acesso, incluindo o processo de integração, transferências e rescisões de funcionários, garantindo que as autorizações sejam atualizadas de acordo com as mudanças de status dos colaboradores;
d) funcionários: encarregados de seguir as políticas de controle de acesso estabelecidas, contribuindo para a segurança ao relatar quaisquer atividades suspeitas ou violações de segurança que possam comprometer a integridade das instalações ou dos dados.

5. Medidas de controle de acesso

5.1 Sistema de controle de acesso físico

Um sistema de controle de acesso físico se faz importante para regular o acesso à determinadas áreas da empresa. O sistema envolve:

a) cartões de acesso e leitores biométricos para funcionários;
b) sistema de gestão de visitantes para regular o acesso temporário. Isso inclui a criação de um processo específico para o acesso físico de visitantes, preferencialmente utilizando o Business Process Model and Notation (BPMN)

e compreendendo as etapas de solicitação de entrada, análise do pedido, criação de credenciais e providência de acesso;
c) câmeras de segurança em pontos de entrada e pontos estratégicos;
d) proteção de instalações em proporção com criticalidade ou importância.

5.2 Identificação

Estando definido o sistema de controle de acesso físico, a primeira fase do processo de controle de acesso é a identificação, a fase responsável por verificar e confirmar a identidade do usuário que solicita acesso às áreas protegidas. Nesta etapa, são realizados os seguintes métodos:

a) registro de usuários e criação de perfis de acesso;
b) atribuição de privilégios de acesso com base nas funções e responsabilidades do trabalho;
c) a identificação do usuário se dará por uma comparação entre as informações fornecidas durante o processo de autenticação e os dados registrados no sistema.

5.3 Autenticação

Após a fase de identificação, o próximo passo no processo de controle de acesso é a autenticação, onde as credenciais fornecidas pelo usuário são verificadas para confirmar sua identidade. Esta etapa envolve:

a) verificação da legitimidade das credenciais por métodos de autenticação, como senhas, cartões de acesso, tokens ou biometria;
b) validação da identidade do usuário.

5.4 Autorização

Após a autenticação bem-sucedida, o usuário passa para a fase de autorização, onde são concedidos os privilégios de acesso de acordo com as permissões associadas ao seu perfil de usuário. Este processo inclui:

a) definição de privilégios de acesso para áreas e atividades específicas da empresa de acordo com perfil de acesso;
b) autorização do usuário de acordo com as suas permissões individuais.

6. Práticas recomendadas

Para maior eficiência do processo, recomenda-se a adoção das seguintes recomendações:

6.1 Revisões de acesso

a) revisões regulares das permissões de acesso para garantir o alinhamento com as funções e responsabilidades atuais;
b) realização das revisões de acordo com as necessidades organizacionais.

6.2 Monitoramento e registros

a) todos os acessos, tanto bem-sucedidos quanto malsucedidos, devem ser registrados pelos sistemas de controle de acesso;
b) os registros devem incluir informações como data, hora, identidade do usuário, local de acesso e resultado da tentativa (sucesso ou falha).

6.3 Gerenciamento de riscos

a) realização de avaliações periódicas de risco para identificar potenciais vulnerabilidades no controle de acesso físico às instalações da empresa;
b) desenvolver estratégias de mitigação para abordar as vulnerabilidades identificadas, incluindo melhorias nos sistemas de controle de acesso, reforço da segurança física das instalações, revisão de políticas e procedimentos de segurança, bem como investimentos em tecnologias de segurança adicionais;
c) implementar e monitorar continuamente as estratégias de mitigação para avaliar sua eficácia e identificar possíveis novas vulnerabilidades.

6.4 Treinamento e conscientização

a) realizar treinamento abrangente para os funcionários sobre as medidas de segurança física adotadas pela empresa, incluindo os procedimentos de controle de acesso;
b) promover campanhas de conscientização para educar os funcionários sobre a importância de aderir às políticas de controle de acesso;
c) informar regularmente os funcionários sobre as práticas recomendadas de segurança através de diversos canais de comunicação, como e-mails, intranet, cartazes e reuniões;
d) realizar exercícios periódicos de simulação de situações de segurança, incluindo simulações de evacuação, testes de resposta a emergências e cenários de intrusão simulados.

6.5 Protocolo de resposta a incidentes

a) definição de procedimentos de travamento para ameaças iminentes à segurança, como intrusões não autorizadas, ataques ou outras emergências;
b) definição de procedimentos de evacuação para situações de emergência que representem um risco para a segurança física dos funcionários, clientes ou visitantes;
c) acionamento de notificações de emergência em caso de incidentes graves que exijam uma resposta de emergência, podendo ser feitas por meio de sistemas de alarme, mensagens de texto, e-mails ou sistemas de megafone, dependendo da gravidade e urgência da situação;
d) definição de protocolo de resposta incluindo diretrizes claras sobre como coordenar e colaborar com as autoridades competentes, como polícia, bombeiros ou equipes de resgate, em caso de incidentes de segurança que exijam intervenção externa;

e) realizar uma avaliação do protocolo de resposta para identificar quaisquer áreas de melhoria ou ajustes necessários após cada incidente de segurança.

6.6 Revisão

a) revisar o presente procedimento de maneira periódica, com uma frequência definida de acordo com as necessidades da empresa e os requisitos regulamentares;
b) a avaliação durante o processo de revisão pode incluir a análise de incidentes de segurança anteriores, feedback dos funcionários, auditorias de segurança e revisões de conformidade;
c) comunicar de forma clara todas as atualizações ou revisões feitas no procedimento de acesso físico para todas as partes interessadas relevantes;
d) atualizar os processos de treinamento de acordo;
e) documentar e arquivar adequadamente todas as revisões e atualizações feitas no procedimento de acesso físico.

7. Referências

ABNT NBR ISO/IEC 27001:2022. Segurança da informação, segurança cibernética e proteção da privacidade — Sistemas de gestão de segurança da informação – Requisitos. Rio de Janeiro: ABNT, 2022.

ABNT NBR ISO/IEC 27002:2022. Segurança da informação, segurança cibernética e proteção da privacidade — Controles de segurança da informação. Rio de Janeiro: ABNT, 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018.