

Norma de Áreas Seguras

Alsar Tecnologia em Redes

Classificação Pública

ÍNDICE

1.	<u>OBJETIVOS</u>	3
2.	<u>DOCUMENTOS DE REFERÊNCIA</u>	3
3.	<u>PAPÉIS E RESPONSABILIDADES</u>	3
4.	<u>DIRETRIZES GERAIS</u>	3

- **OBJETIVOS**

- Esta Norma tem por objetivo instituir regras de proteção para as instalações físicas da **Alsar** visando a prevenção de acessos físicos não autorizados e danos nas instalações.

-

- **DOCUMENTOS DE REFERÊNCIA**

- ABNT NBR ISO/IEC 27002:2013 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a Gestão da Segurança da Informação.
- ABNT NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de segurança – Sistemas de Gestão de Segurança da Informação – Requisitos.
- Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018.
- Lei de Acesso a Informação (LAI) 12.527 de 18/11/2011.
- Política de Segurança da Informação – PSIC.

-

- **PAPÉIS E RESPONSABILIDADES**

- Responsáveis pela elaboração – **Dirigentes da Alsar**.
- Público Alvo – todos os dirigentes, colaboradores, parceiros e fornecedores.

-

- **DIRETRIZES GERAIS**

- **Perímetros da Segurança Física**

- **Área Pública**

- Corresponde ao perímetro externo às dependências da **Alsar**, como, por exemplo:
- Instalações prediais do edifício no qual a **Alsar** utiliza salas comerciais.
- Por ser área pública, controles de segurança devem ser implementados para garantir que o acesso de pessoas por estas áreas, sejam devidamente autorizados.
- O edifício deve possuir pessoa ou equipe responsável pela segurança patrimonial predial, no mínimo em todas as portarias que permitam o acesso do público às salas comerciais e em instalações que armazenem ou processem informações ou recursos críticos.

- **Área Protegida**

- Corresponde às dependências do CPD.
- Deve ser localizada de forma a evitar o acesso do público, com indicações mínimas do seu propósito, tanto fora quanto dentro das dependências, da presença de atividades de processamento de informação.
- As portas externas devem ser protegidas de forma apropriada contra acessos não autorizados, como, por exemplo, mecanismos de controle e travas.
- Uma área de recepção ou outro meio de controle de acesso físico à área protegida deve ser usado. O acesso deve ser restrito apenas ao pessoal autorizado.
- Barreiras físicas devem, se necessário, ser estendidas da laje do piso até a laje superior para prevenir acessos não autorizados ou contaminação ambiental como as causadas por fogo e inundações.
- Todas as portas de incêndio na área protegida devem possuir mecanismo para fechamento automático.
- Devem ser afixados avisos (normalmente nas entradas, saídas e corredores de acesso), facilmente visíveis, contendo aviso geral sobre o controle de acesso para as pessoas e alertando sobre as restrições ao acesso público, de tal forma que desestime as invasões.

- **Área de Segurança**

- Incluem-se nesta classificação especial as áreas protegidas que contenham informações, dispositivos ou serviços imprescindíveis ao negócio, como, por exemplo:
- Centro de Processamento de Dados (CPD).
- Salas e armários com informações sensíveis associadas a interesses relevantes da **Alsar**.
- Locais com equipamentos de conectividade (switches, roteadores, etc.), e;
- Locais com infraestrutura de conectividade (quadro de telefonia, quadro de cabeamento, etc.).
- É proibida a permanência de pessoas na área do CPD sem a devida autorização.
- Barreiras e perímetros adicionais para controlar o acesso físico podem ser necessários em áreas com diferentes requisitos de segurança dentro de um mesmo perímetro de segurança.
- Devem ser afixados avisos (normalmente na respectiva porta), facilmente visíveis, alertando sobre as restrições ao acesso às áreas de segurança, indicando que somente pessoal autorizado pode entrar e de tal forma que desestime as invasões.

- **Identificação das pessoas nas áreas da Alsar**
- Os usuários para terem acesso ao ambiente da **Alsar** devem ser previamente identificadas na recepção e, se possível, possuir um crachá de identificação.
- O crachá deve ser colocado na parte frontal do colo do portador, devendo estar sempre visível a face com as informações de controle.
- Crachás de visitantes não devem dar acesso a abertura das portas.
- A data, o horário de entrada e de saída e a identificação dos visitantes devem ser registrados pelos colaboradores responsáveis pela recepção e entrada no perímetro físico da **Alsar**.
- Os terceiros que comprovadamente tiverem a necessidade de entrar diariamente nas dependências da **Alsar** podem receber crachás de identificação provisórios.
- Exclusivamente para períodos de inatividade (finais de semanas, feriados, períodos noturnos, férias coletivas, etc) o acesso às instalações da **Alsar** somente será liberado após verificação se o nome do usuário consta na lista de pessoas autorizadas em período de inatividade.
- Deve ser mantida relação atualizada de crachás perdidos, sumidos e furtados.
- A perda, furto ou desaparecimento de crachás deve ser avisado imediatamente para atualização e distribuição da relação de crachás perdidos, sumidos e furtados.
- É responsabilidade de todos evitar o uso de crachás fora das normas de segurança, devendo as irregularidades serem impedidas e avisadas imediatamente.
- Para dirigentes e colaboradores a validade do crachá é indeterminada. O crachá deve ser devolvido em caso de encerramento de suas atividades na **Alsar**.
- Para prestadores de serviço que executam atividades não previstas ou não rotineiras, é recomendado o uso do crachá de visitantes.
- Os acessos aos ativos imprescindíveis da **Alsar** ocorrerão somente mediante autorização do colaborador responsável pelos mesmos.
- Visitantes não podem ter acesso às estações de trabalho disponíveis na **Alsar** e não devem conectar equipamentos particulares na rede de computadores, salvo previamente autorizados.
- - De acordo com os interesses da **Alsar**, o visitante pode ter acesso somente às estações de trabalho configuradas para uso específico.
-
- **Segurança em instalações de processamento**
- Devem-se levar em consideração as possibilidades de dano causado por fogo, inundações, explosões, manifestações civis e outras formas de desastres naturais ou causados pelo homem, as regulamentações e padrões de segurança e saúde. Também deve tratar qualquer ameaça originada em propriedades vizinhas, como, por exemplo, vazamento de água de outras áreas, quando forem definidos os controles de segurança para estas dependências.

- Portas e janelas devem ser mantidas fechadas quando não utilizadas e devem ser instaladas proteções extras, principalmente quando essas portas e janelas se localizarem em andar térreo.
- Sistemas de detecção de intrusos devem ser instalados por profissionais especializados e testados regularmente, de forma a cobrir todas as portas e janelas acessíveis. As áreas desocupadas devem possuir um sistema de alarme que permaneça sempre ativado.
- Equipamentos de contingência e meios magnéticos de reserva devem ser guardados a uma distância segura para evitar danos que podem se originar em um desastre na área protegida.
- As portas de entrada devem permanecer trancadas nos períodos de inatividade
- **Trabalhando em áreas de segurança**
- Os usuários só devem ter conhecimento da existência de informações ou de atividades dentro da área de segurança quando necessário.
- Essas áreas devem estar fechadas e trancadas adequadamente de forma a impedir acessos não autorizados. Áreas de segurança desocupadas devem ser mantidas fisicamente fechadas e verificadas periodicamente.
- Somente devem ter acesso às áreas de segurança os usuários imprescindíveis para a realização dos trabalhos rotineiros ou de manutenção, mediante autorização de funcionário responsável.
- Deve-se evitar trabalho sem supervisão nas áreas de segurança tanto por razões de segurança como para prevenir oportunidades para atividades maliciosas. O pessoal de serviços de suporte terceirizados deve ter acesso restrito às áreas de segurança somente quando suas atividades o exigirem. Esse acesso deve ser autorizado e monitorado.
- Materiais combustíveis ou perigosos devem ser guardados de forma segura a uma distância apropriada de uma área de segurança. Suprimentos volumosos, como material de escritório, não devem ser guardados em uma área de segurança, a menos que sejam necessários.
-
- **Circuito Fechado de TV (CFTV)**
- A **Alsar** monitora seus ambientes físicos, por meio de câmeras, com a finalidade de proteção de seu patrimônio, de sua reputação e daqueles com quem se relaciona.
- A **Alsar** realiza o armazenamento dos dados monitorados para fins administrativos e legais, bem como para colaborar com as autoridades em caso de investigação.
- A **Alsar** deve fixar nos ambientes físicos em que haja o monitoramento por câmeras.
- A **Alsar** deve possuir um circuito fechado de televisão (CFTV) para monitorar todas as dependências da empresa, principalmente aqueles que armazenam informações Restritas e Confidenciais ou Recursos de TIC.

- Todos os acessos a arquivos de gravação seja fotografia, vídeo, som ou outro tipo deve ser registrado com a data e hora (Padrão GMT-3) e a identificação da pessoa que obteve o acesso.
- Qualquer equipamento de gravação seja fotografia, vídeo, som ou outro tipo de equipamento só deve ser utilizado com autorização e finalidades permitidas conforme LGPD.
- Em casos de quebra de Segurança da Informação por meio de recursos de informática, o Canal de Atendimento (suporte@alsar.com.br) deve ser imediatamente acionado para adotar as providências necessárias.
- Esta norma entra em vigor a partir da data de sua divulgação e sua revisão deve ocorrer em intervalos planejados, pelo menos anualmente, ou sempre que existirem alterações das regras acima expostas.
- Dúvidas: Qualquer dúvida relativa a esta Norma deve ser encaminhada ao CSIC.