Norma de Áreas Seguras

Niva Tecnologia da Informação

www.nivati.com.br
SIG QUADRA 01 N° 985 SALAS 236 A 243 - CENTRO EMPRESARIAL PARQUE BRASILIA
- CEP: 70.610.410 - BRASILIA – DF TEL: (61) 3326-8673

ÍNDICE

1. OBJETIVOS

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

2. DOCUMENTOS DE REFERÊNCIA

2.1. ABNT NBR ISO/IEC 27002:2013 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a Gestão da Segurança da Informação.

2.2. ABNT NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de segurança – Sistemas de Gestão de Segurança da Informação – Requisitos.

2.3. Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018.

2.4. Lei de Acesso à Informação (LAI) 12.527 de 18/11/2011.

2.5. Política de Segurança da Informação – PSIC.

3. PAPÉIS E RESPONSABILIDADES

3.1. Responsáveis pela elaboração – **Dirigentes da NIVA**.

3.2. Público Alvo – todos os dirigentes, colaboradores, parceiros e fornecedores.

4. DIRETRIZES GERAIS

4.1. Perímetros da Segurança Física

4.1.1. Área Pública

4.1.1.1. Corresponde ao perímetro externo às dependências da **NIVA**, como, por exemplo:

4.1.1.1.1. Instalações prediais do edifício no qual a **NIVA** utiliza salas comerciais.

4.1.1.2. Por ser área pública, controles de segurança devem ser implementados para garantir que o acesso de pessoas por estas áreas, sejam devidamente autorizados.

4.1.1.3. 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.

4.1.2. Área Protegida

4.1.2.1. Corresponde às dependências do CPD.

4.1.2.2. 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.

4.1.2.3. As portas externas devem ser protegidas de forma apropriada contra acessos não autorizados, como, por exemplo, mecanismos de controle e travas.

4.1.2.4. 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.

4.1.2.5. 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.

4.1.2.6. Todas as portas de incêndio na área protegida devem possuir mecanismo para fechamento automático.

4.1.2.7. Devem ser afixados avisos (normalmente nas entradas, saídas e corredores de acesso), facilmente visíveis, contento aviso geral sobre o controle de acesso para as pessoas e alertando sobre as restrições ao acesso público, de tal forma que desestimule as invasões.

4.1.3. **Área de Segurança**

4.1.3.1. Incluem-se nesta classificação especial as áreas protegidas que contenham informações, dispositivos ou serviços imprescindíveis ao negócio, como, por exemplo:

4.1.3.1.1. Centro de Processamento de Dados (CPD).

4.1.3.1.2. Salas e armários com informações sensíveis associadas a interesses relevantes da **NIVA**.

4.1.3.1.3. Locais com equipamentos de conectividade (switches, roteadores, etc.), e;

4.1.3.1.4. Locais com infraestrutura de conectividade (quadro de telefonia, quadro de cabeamento, etc.).

4.1.3.2. É proibida a permanência de pessoas na área do CPD sem a devida autorização.

4.1.3.3. 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.

4.1.3.4. 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 desestimule as invasões.

4.2. Identificação das pessoas nas áreas da NIVA

4.2.1. Os usuários para terem acesso ao ambiente da **NIVA** devem ser previamente identificadas na recepção e, se possível, possuir um crachá de identificação.

4.2.2. O crachá deve ser colocado na parte frontal do colo do portador, devendo estar sempre visível a face com as informações de controle.

4.2.3. Crachás de visitantes não devem dar acesso a abertura das portas.

4.2.4. 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 **NIVA**.

4.2.5. Os terceiros que comprovadamente tiverem a necessidade de entrar diariamente nas dependências da **NIVA** podem receber crachás de identificação provisórios.

4.2.6. Exclusivamente para períodos de inatividade (finais de semanas, feriados, períodos noturnos, férias coletivas, etc) o acesso às instalações da **NIVA** somente será liberado após verificação se o nome do usuário consta na lista de pessoas autorizadas em período de inatividade.

4.2.7. Deve ser mantida relação atualizada de crachás perdidos, sumidos e furtados.

4.2.8. A perda, furto ou desaparecimento de crachás deve ser avisado imediatamente para atualização e distribuição da relação de crachás perdidos, sumidos e furtados.

4.2.9. É responsabilidade de todos evitar o uso de crachás fora das normas de segurança, devendo as irregularidades serem impedidas e avisadas imediatamente.

4.2.10. Para dirigentes e colaboradores a validade do crachá é indeterminada. O crachá deve ser devolvido em caso de encerramento de suas atividades na **NIVA**.

4.2.11. Para prestadores de serviço que executam atividades não previstas ou não rotineiras, é recomendado o uso do crachá de visitantes.

4.2.12. Os acessos aos ativos imprescindíveis da **NIVA** ocorrerão somente mediante autorização do colaborador responsável pelos mesmos.

4.2.13. Visitantes não podem ter acesso às estações de trabalho disponíveis na **NIVA** e não devem conectar equipamentos particulares na rede de computadores, salvo previamente autorizados.

4.2.13.1. De acordo com os interesses da **NIVA**, o visitante pode ter acesso somente às estações de trabalho configuradas para uso específico.

4.3. Segurança em instalações de processamento

4.3.1. 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.

4.3.2. 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.

4.3.3. 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.

4.3.4. 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.

4.3.5. As portas de entrada devem permanecer trancadas nos períodos de inatividade

4.4. Trabalhando em áreas de segurança

4.4.1. Os usuários só devem ter conhecimento da existência de informações ou de atividades dentro da área de segurança quando necessário.

4.4.2. 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.

4.4.3. 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.

4.4.4. 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.

4.4.5. 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.

4.5. Circuito Fechado de TV (CFTV)

4.5.1. A **NIVA** 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.

4.5.2. A **NIVA** realiza o armazenamento dos dados monitorados para fins administrativos e legais, bem como para colaborar com as autoridades em caso de investigação.

4.5.3. A **NIVA** deve fixar nos ambientes físicos em que haja o monitoramento por câmeras.

4.5.4. A **NIVA** 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.

4.5.5. 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.

4.5.6. Qualquer equipamento de gravação seja fotografia, vídeo, som ou outro tipo de equipamento só deve ser utilizado com autorização e finalidades permitidas conforme LGPD.

4.6. Em casos de quebra de Segurança da Informação por meio de recursos de informática, o Canal de Atendimento (suporte@nivati.com.br) deve ser imediatamente acionado para adotar as providências necessárias.

4.7. 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.

4.8. Dúvidas: Qualquer dúvida relativa a esta Norma deve ser encaminhada ao CSIC.