

Norma de Procedimentos e Responsabilidades Operacionais

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 definir regras de operação segura e correta dos recursos de informática da **Alsar**.

- **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.
- Norma de Classificação da Informação.
- Política de Segurança da Informação – PSIC.
- Termo de compromisso e responsabilidade de acesso por virtual *private network* – VPN.

- **PAPÉIS E RESPONSABILIDADES**

- Responsáveis pela elaboração – **Dirigentes da Alsar**.
- Público Alvo – Canal de atendimento – Suporte TI.

- **DIRETRIZES GERAIS**

- Os procedimentos operacionais devem ser formalmente documentados e mantidos atualizados.
- O suporte deve homologar e aprovar as alterações ocorridas nos procedimentos operacionais.
- Os procedimentos operacionais devem conter as instruções necessárias para a execução das atividades.
- **Controle de mudanças operacionais**
- As mudanças no ambiente tecnológico da **Alsar** devem ser previamente avaliadas quanto aos requisitos de segurança da informação e comunicação.
- Durante a realização da mudança devem ser adotados procedimentos que possibilitem a identificação e o registro dos seguintes quesitos:
 - Descrição da mudança.
 - Relação dos recursos de informática envolvidos.
 - Relação dos Usuários envolvidos e afetados.

- Responsável por executar a mudança.
- Após a mudança no ambiente tecnológico da **Alsar**, o suporte deve garantir que toda a documentação dos recursos de informação envolvidos seja imediatamente atualizada.
- Quando houver alterações no ambiente tecnológico na **Alsar** ou nos procedimentos operacionais, os usuários envolvidos devem ser formalmente notificados.
- As alterações devem ser avisadas antecipadamente aos usuários, de forma a evitar perda de integridade, confidencialidade e disponibilidade das informações que estão sendo manipuladas.
- **Segregação de função e de ambiente**
- O suporte deve manter os ambientes de desenvolvimento, homologação e produção.
- No ambiente de produção somente devem existir as versões homologadas e finais dos *softwares* utilizados pela **Alsar**.
- Os *softwares* em desenvolvimento e homologação devem ser processados em ambiente distinto do ambiente de produção.
- O acesso ao ambiente de produção deve ser diferente do acesso ao ambiente de desenvolvimento. Os usuários devem usar diferentes senhas para esses ambientes e as telas de abertura devem exibir mensagens de identificação apropriadas.
- A área de desenvolvimento deve receber senhas para acesso ao ambiente de produção de forma controlada, a fim de proceder ao suporte dos sistemas desse ambiente. Deve haver controle que garanta a alteração das senhas após o uso.
- **Separação do ambiente de desenvolvimento, homologação e produção**
- Os sistemas em desenvolvimento e teste devem ser processados em ambiente seguro, estável e separados do ambiente de produção.
- O pessoal de desenvolvimento deve receber senhas para acesso ao ambiente de produção de forma controlada, a fim de proceder ao suporte dos sistemas desse ambiente. Deve haver controles que garantam a alteração das senhas após o uso.
- O ambiente de produção pode oferecer acesso externo via conexão segura (VPN).
- Os ambientes de homologação só podem ter conexão externa se o mesmo tiver integração com outros sistemas externos. A solicitação deve ser formal, monitorada, controlada e ter conexão segura.
- Os usuários que utilizarem de acesso remoto devem ter ciência e assinar Termo de compromisso e responsabilidade de acesso por virtual *private network* – VPN.
- 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.