Norma de Procedimentos e Responsabilidades Operacionais

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

Esta Norma tem por objetivo definir regras de operação segura e correta dos recursos de informática da **NIVA**.

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. Norma de Classificação da Informação.

2.6. Política de Segurança da Informação – PSIC.

2.7. Termo de compromisso e responsabilidade de acesso por virtual *private network* – VPN.

3. PAPÉIS E RESPONSABILIDADES

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

3.2. Público Alvo – Canal de atendimento – Suporte TI.

4. DIRETRIZES GERAIS

4.1. Os procedimentos operacionais devem ser formalmente documentados e mantidos atualizados.

4.2. O suporte deve homologar e aprovar as alterações ocorridas nos procedimentos operacionais.

4.3. Os procedimentos operacionais devem conter as instruções necessárias para a execução das atividades.

4.4. Controle de mudanças operacionais

4.4.1. As mudanças no ambiente tecnológico da **NIVA** devem ser previamente avaliadas quanto aos requisitos de segurança da informação e comunicação.

4.4.2. 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.

4.4.3. Após a mudança no ambiente tecnológico da **NIVA**, o suporte deve garantir que toda a documentação dos recursos de informação envolvidos seja imediatamente atualizada.

4.4.4. Quando houver alterações no ambiente tecnológico na **NIVA** ou nos procedimentos operacionais, os usuários envolvidos devem ser formalmente notificados.

4.4.5. As alterações devem ser avisadas antecipadamente aos usuários, de forma a evitar perda de integridade, confidencialidade e disponibilidade das informações que estão sendo manipuladas.

4.5. Segregação de função e de ambiente

4.5.1. O suporte deve manter os ambientes de desenvolvimento, homologação e produção.

4.5.2. No ambiente de produção somente devem existir as versões homologadas e finais dos *softwares* utilizados pela **NIVA**.

4.5.3. Os *softwares* em desenvolvimento e homologação devem ser processados em ambiente distinto do ambiente de produção.

4.5.4. 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.

4.5.5. 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.

4.6. Separação do ambiente de desenvolvimento, homologação e produção

4.6.1. Os sistemas em desenvolvimento e teste devem ser processados em ambiente seguro, estável e separados do ambiente de produção.

4.6.2. 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.

4.6.3. O ambiente de produção pode oferecer acesso externo via conexão segura (VPN).

4.6.4. 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.

4.6.5. Os usuários que utilizarem de acesso remoto devem ter ciência e assinar Termo de compromisso e responsabilidade de acesso por virtual *private network* – VPN.

4.7. 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.

4.8. 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.

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