

CYBER NEWS

O Boletim Informativo Oficial de Gestão de Riscos em Terceiros



NESTA EDIÇÃO

GESTÃO DE CONTAS DE USUÁRIOS

GERENCIAMENTO DE CONTROLE DE ACESSOS

MELHORES PRÁTICAS

- ✓ Gestão de Contas de Usuários
- ✓ Gerenciamento de Controle de Acessos

CONCLUSÃO

Neste Volume vamos explicar sobre Gestão de Contas de Usuários e Gerenciamento de Controle de Acessos, como se interligam e a sua importância para Segurança da Informação.

Gestão de Contas de Usuários

A gestão de contas de usuários é o processo de criar, manter, monitorar e excluir contas de usuários em um sistema, rede ou organização.

O objetivo é garantir que cada usuário tenha o nível apropriado de acesso aos recursos, mantendo a segurança, organização e eficiência, para que não tenha contas desatualizadas, senhas fracas e acessos indevidos que podem abrir brechas para ataques cibernéticos, vazamentos de dados e prejuízos operacionais de riscos de má gestão, como:

- Acesso indevido a informações confidenciais;
- Contas órfãs (de ex-colaboradores) sendo exploradas;
- Privilégios excessivos sem necessidade operacional;
- Incidentes de segurança por compartilhamento de credenciais.

Para tanto, iremos apresentar boas práticas, que as empresas devem ter para se manterem protegidas.

Mas antes de falarmos de boas práticas de gestão de contas de usuários sem citar gerenciamento de controle de acessos, pois esses temas são inseparáveis quando falamos sobre Segurança e Administração de Sistemas, como será demonstrado.

Gerenciamento de Controle de Acesso

O gerenciamento de controle de acesso é o processo de garantir que apenas usuários autorizados possam acessar determinados recursos, sistemas ou dados, e que esse acesso ocorra de forma apropriada ao seu papel ou função, sendo necessário possuir:

- Componentes fundamentais como autenticação, para verificar se o usuário é quem diz ser. Exemplos: Senhas; Autenticação multifator (MFA); Biometria.
- Autorização para definir que o usuário pode fazer após ser autenticado. Exemplo: funcionário do RH pode acessar dados de folha de pagamento, mas não os sistemas de TI.
- Auditoria e monitoramento, para registrar e analisar o uso dos acessos para detectar comportamentos suspeitos ou violações de políticas.
- Ter em mente o princípio do menor privilégio, para que cada usuário possua apenas os acessos estritamente necessários para realizar suas tarefas.

Melhores Práticas

Gestão de Contas de Usuários

A gestão eficaz de contas de usuários é essencial para garantir a segurança, a conformidade e a eficiência operacional em qualquer empresa. Aqui estão algumas boas práticas que a sua empresa pode adotar:

- Criação Controlada de Contas - Toda nova conta deve ser criada mediante solicitação formal e com aprovação do gestor responsável.
- Princípio do Menor Privilégio - Conceda apenas os acessos estritamente necessários para a função desempenhada.
- Revisão Periódica de Acessos - Realize auditorias regulares para identificar acessos desnecessários ou inconsistentes.
- Desativação Imediata de Contas Inativas ou de Ex-colaboradores - Sempre que alguém deixar a empresa ou mudar de função, revise os acessos imediatamente.
- Política de Senhas Fortes - Senhas devem ser complexas, únicas e trocadas regularmente.
- Proibição do Compartilhamento de Contas - Contas são pessoais e intransferíveis. Cada colaborador deve ter seu próprio login.

Gerenciamento de controle de acessos

O gerenciamento de controle de acessos garante que apenas pessoas autorizadas tenham acesso aos recursos certos, no momento certo, e pelas razões certas. Aqui estão as melhores práticas para implementar um controle de acessos eficaz:

- Princípio do Menor Privilégio - conceder apenas os acessos mínimos necessários para execução da função.
- Segregação de Funções - evitar que um mesmo usuário execute funções conflitantes dentro de processos críticos.
- Acesso baseado em papéis - utilizar perfis de acesso baseados em cargos e responsabilidades.
- Revalidação periódica de acessos críticos - verificar regularmente se os acessos concedidos ainda são pertinentes.
- Monitoramento e registro de acessos - utilizar logs para registrar e auditar atividades de acesso em sistemas sensíveis.

Conclusão

Lembre-se de perguntar “Quem acessa o que, quando e o motivo?”

- Se não for possível responder essas perguntas com clareza, a empresa tem um risco.

Então, manter-se atualizados sobre as melhores práticas de segurança é crucial para proteger sua empresa. Fique atento aos próximos boletins para mais dicas!

