ATUALIZAÇÃO DE ÁREA
1° SEMESTRE DE 2023

CIÊNCIAS BIOLÓGICAS, EXATAS E DA TERRA

https://www.nucleodoconhecimento.com.br/livros/ciencias-biologicas-exatas-e-da-terra/cie-bio-exa-ter-atu-are-1-sem-2023

DOI: 10.32749/nucleodoconhecimento.com.br/livros/3310

C569c

Ciências Biológicas, Exatas e da Terra: Atualização de Área - 1° semestre de 2023 [recurso eletrônico] / Organizadores Carla Viana Dendasck, [et al.]. – 1.ed. – São Paulo: CPDT, 2023. 67p.

Vários autores
Formato: ePUB
Incluir Bibliografia
ISBN: 978-65-996273-2-3

1. Ciências Biológicas, Exatas e da Terra 2. Atualização de Área 3.I. Dendasck, Carla Viana,

CDD:570
CDU:57

https://www.nucleodoconhecimento.com.br/livros/ciencias-biologicas-exatas-e-da-terra/ficha-catal-cie-bio-1-sem-2023

DOI: 10.32749/nucleodoconhecimento.com.br/livros/3313

EDITORIAL

https://www.nucleodoconhecimento.com.br/livros/ciencias-biologicas-exatas-e-da-terra/editorial-cie-bio-1-sem-2023

DOI: 10.32749/nucleodoconhecimento.com.br/livros/3318

Julio Rodrigues Alves

Luciane Farias Ribas

Maria Eduarda da Silva Souza

Milena Gaion Malosso

Ricardo de Oliveira Boaro

Sabrynna De Oliveira Brito

Yusdel Díaz Hernández

https://www.nucleodoconhecimento.com.br/livros/ciencias-biologicas-exatas-e-da-terra/editorial-cie-bio-1-sem-2023

DOI: 10.32749/nucleodoconhecimento.com.br/livros/3318

SUMÁRIO

https://www.nucleodoconhecimento.com.br/livros/ciencias-biologicas-exatas-e-da-terra/sumario-cie-bio-1-sem-2023

DOI: 10.32749/nucleodoconhecimento.com.br/livros/3321

APRESENTAÇÃO

Caro leitor, é com muita satisfação que a Revista Núcleo do Conhecimento compartilha com você mais um compilado de informações atuais e inovadoras na área das Ciências Biológicas.

Cada capítulo desse livro irá lhe proporcionar uma imersão no "velho mundo novo" da biologia de forma aplicada. Aqui, os autores trazem seu olhar científico e crítico sobre aspectos importantes e cotidianos da Ciência da Vida. Esta iniciativa visa difundir resultados e opiniões especializadas, compartilhar pensamentos e aproximar os membros da sociedade acadêmica e grupos de pesquisa.

Estamos certos de que todas as contribuições aqui reunidas serão valiosas para seus estudos e formação intelectual e profissional. Sinta-se convidado a interagir com os autores e demais leitores, além de divulgar este material.

Tenha uma boa leitura e bons estudos!

Cordialmente,

Prof Dr Sabrynna De Oliveira Brito

DOI: 10.32749/nucleodoconhecimento.com.br/livros/3324

DOI: 10.32749/nucleodoconhecimento.com.br/livros/3324

EXATAS E DA TERRA

GESTÃO CENTRALIZADA E AUTOMATIZADA DOS ACESSOS LÓGICOS

Ricardo de Oliveira Boaro

DOI: 10.32749/nucleodoconhecimento.com.br/livros/3341

RESUMO

Este estudo buscou apresentar as principais vantagens que a gestão centralizada de identidade pode trazer para uma empresa, independente do seu tamanho ou seguimento. A ideia é garantir o controle de acesso dos usuários nas aplicações e/ou recursos de forma automatizada e centralizada. Pois dessa forma, a instituição garante a segurança da informação, a conformidade aos itens de auditoria e medidas que impactam positivamente o negócio. Não iremos aprofundar na parte técnica, pois existem diversas soluções no mercado, onde cada empresa analisará a melhor que se adeque ao seu tipo.

1. INTRODUÇÃO

Muitas empresas possuem sua gestão de identidade sendo realizadas nas pontas de cada aplicação e/ou recursos, trazendo a necessidade de ter profissionais especialistas em cada ponta para realizar o ciclo de vida do usuário, além de ser uma atividade realizada de forma manual, podendo trazer inconsistências entre as bases (da aplicação com a do RH).

Com base nesse problema enfrentado pelas empresas, a gestão centralizada de identidade apresenta uma forma mais ágil, segura e confiável para as instituições, não importando seu tamanho ou seu seguimento, realizarem as administrações dos acessos (criações, atualizações e exclusões de usuários).

Com a gestão centralizada de identidade não é mais necessária uma equipe especializada em gestão em cada aplicação e/ou recurso, pois essas ações serão realizadas de forma automatizadas através de um único “orquestrador”.

Também traz um grande ganho operacional devido ao tempo de cada execução. Além de estar compliance junto a base de RH e aos itens normalmente exigidos pelas

DOI: 10.32749/nucleodoconhecimento.com.br/livros/3341

Auditorias externas e internas, onde o acesso será realizado apenas por usuários ativos na empresa e respectivas autorizados.

Esse estudo irá apresentar os principais pontos sobre a gestão de acesso centralizada e automatizada, onde será possível entender o grande benefício que essa solução traz para a intuição.

2. GESTÃO DO ACESSO LÓGICO

2.1 ACESSO LÓGICO

A tecnologia é o principal ator quando falamos de acesso lógico. Acesso lógico é conhecido como todos os acessos que o usuário (colaborador, cliente, parceiros, fornecedores...) realizam nos recursos de informática, como acessar uma aplicação (SAP como exemplo), um banco de dados, um e-mail corporativo, um servidor ou qualquer outro recurso de rede corporativa.

Sendo assim, tudo que gera recurso de informática serão considerados acesso lógicos.

Normalmente encontramos 2 tipos de acessos corporativos, um é o acesso lógico e o outro é o acesso físico. Esse segundo, trata dos acessos fisicamente nas dependências da instituição, como exemplo: portarias, roletas, salas de reunião, estacionamentos entre outros espaços físicos que a empresa possui.

Devido aos diversos seguimentos, existem empresas que possuem usuários apenas com acesso físico, não sendo necessário que esse usuário acesse qualquer recurso de informática. Um bom exemplo disso é a classe de serviços gerais, onde o empregado (ou parceiros, caso seja um serviço terceirizado) precisa apenas do acesso físico (acesso nas instalações da empresa) para realizar suas atividades, não acessando nenhum recurso de informática (exemplo, ler um e-mail corporativo).

De outro modo, existem empresas que possuem usuários apenas com acesso lógico, um bom exemplo disso são os consultores externos que por algum motivo realizam as atividades temporárias da sua própria instalação, não sendo necessário acessar a instalação corporativa da empresa contratante.

https://www.nucleodoconhecimento.com.br/livros/ciencias-biologicas-exatas-e-da-terra/gestao-centralizada-e-automatizada

DOI: 10.32749/nucleodoconhecimento.com.br/livros/3341

Esses acessos deverão ser muito bem controlados, para que seja haja acessos indevidos ou desnecessários, com esse pequeno controle a empresa mitiga um risco muito grande.

Normalmente esse controle é de responsabilidade da equipe de Recursos Humanos, onde está o contrato dos usuários.

2.2 CONTROLE DE ACESSO LÓGICO

Para realizar o controle de acesso lógico é necessário um conjunto de passos e medidas, além de um casamento de hardware e software para a proteção e controle das informações. Também é muito importante um recurso de segurança da informação para garantir que somente pessoas autorizadas possa gerenciar esse controle.

O acesso lógico tem as funções de identificar, autenticar e autorizar os usuários no acesso a recursos computacionais. Com isso, é necessário um controle de ciclo de vida do usuário (criação, atualização e exclusão) muito robusto. A integração entre o departamento pessoal e a equipe responsável pelo controle nas aplicações, deve ser claro e constante, para que o acesso seja liberado ou excluído com base no status do usuário.

A proteção aos recursos computacionais (aplicações, e-mail, banco de dados...) deve estar sempre baseado na atividade de cada usuário, todos os usuários deverão acessar apenas o que for pertinente a sua função.

Normalmente as empresas utilizam um identificar único e intransferível (ID) para a autenticação e autorização nos recursos computacionais, esses acessos são realizados através desse ID e da senha pessoal do usuário. Dependendo do tipo de acesso, empresas podem e utilizamos outros recursos a mais para mitigar possíveis riscos, um bom exemplo é o 2º fator de autenticação (token) ou um sistema de biometria.

2.3 IMPORTÂNCIA DO CONTROLE DE ACESSO

O controle de acesso aos recursos computacionais inclui desde aplicações (das mais simples como mais críticas com o SAP ou um CRM) até as mais altas permissões em um banco de dados ou servidores corporativo.

Então, caso tenha alguma falha ou falta de controle, códigos fontes, base de dados, arquivos podem sofrer acessos indevidos.

https://www.nucleodoconhecimento.com.br/livros/ciencias-biologicas-exatas-e-da-terra/gestao-centralizada-e-automatizada

DOI: 10.32749/nucleodoconhecimento.com.br/livros/3341

Acessos não autorizados ao código fonte pode ser utilizado para alterar funções ou parar seu funcionamento. Acessos não autorizados em base de dados podem expor informações de clientes e trazer problemas sérios na imagem da empresa.

- ✓ A implantação de um controle de acesso lógico é muito importante, porque garante:
- ✓ Apenas usuários autorizados e ativos tenham acesso aos recursos;
- ✓ Os usuários tenham acesso apenas os recursos realmente necessários;
- ✓ O acesso a recursos críticos pode ser monitorado, restritos a poucas pessoas e possui mais fatores de autenticação (uso de token, biometria...);
- ✓ Usuários de férias ou licença ficam temporariamente bloqueados;
- ✓ Uso adequado de uma politica de senha;

3.CENTRALIZAÇÃO DA GESTÃO DE IDENTIDADE

3.1 CONCEITO DA CENTRALIZAÇÃO

Algumas empresas realizam seu controle aos acessos lógicos de forma descentralizada, que significa que para cada atividades de criação, atualização ou exclusão de acesso, o Administramos realizará as funções diretamente no respectivo recurso.

A centralização dessas administrações é um passo muito grande para a empresa, pois todas as pontas serão tratadas a partir de um único orquestrador.

Para entender um pouco mais, a figura abaixo apresenta um cenário sem a centralização e outra com a centralização.

Percebam a melhora e toda a cadeia de gestão de acesso, a centralização é incluir todos os controles e um único recurso, normalmente chamado de serviço de diretório corporativo.

Isso é simplificação da gestão de acesso, centralizando a administrações dos usuários no mesmo repositório, por meio de interface unificada.

https://www.nucleodoconhecimento.com.br/livros/ciencias-biologicas-exatas-e-da-terra/gestao-centralizada-e-automatizada

DOI: 10.32749/nucleodoconhecimento.com.br/livros/3341

3.2 PROCESSO DA CENTRALIZAÇÃO

Um projeto de centralização de gestão de acesso lógico é algo que pode ser complexo por envolver diversos sistemas, tecnologias diferentes. Pode também demandar uma equipe especialista em gerenciamento de identidade e segurança da informação.

Um controle de identidade centralizado permite determinar permissões de acesso por meio da definição de dispositivo, cargo, localização e políticas de segurança. Assim, os profissionais podem bloquear o acesso a aplicações e dados que estejam fora das regras definidas. Esses sistemas podem ser ainda mais bem aproveitados com bons mecanismos de autenticação, como senhas fortes e fator duplo.

Hoje existem diversos fornecedores e consultorias que prestam todo o suporte necessário, pois cada empresa deverá analisar a melhor solução. O ideal é utilizar soluções que seja como um canivete suíço, tendo suporte a diversos protocolos e facilidade em customizar todos conectores.

Como primeiro passo e muito importante é levantar e avaliar o ambiente atual da empresa:

- ✓ Aval e comprometimento dos gestores.
- ✓ Número de aplicações e suas versões, importante avaliar se possuem suporte do fornecedor;
- ✓ Funcionamento de cada aplicação, levantando a documento e informações sobre integração ou federações relacionado a autenticação e autorização (levamento dos protocolos);
- ✓ Número e versão dos bancos de dados;
- ✓ Número e versão dos servidores;
- ✓ Análise da politica de acesso e senha de cada recurso;

Conhecendo todo seu legado, ficará mais fácil no levamento do requisito para a aquisição da solução de gerenciamento centralizado.

Muita atenção na aquisição e na arquitetura da solução adotada, lembre-se que toda a gestão de acesso estará sendo gerenciada por essa solução, sendo altamente necessário implantação distribuídas (de preferencias em cyber data center diferente) para caso haja falha em um o outro possa assumir de forma transparente, garantindo 100% a continuidade do negócio.

https://www.nucleodoconhecimento.com.br/livros/ciencias-biologicas-exatas-e-da-terra/gestao-centralizada-e-automatizada

DOI: 10.32749/nucleodoconhecimento.com.br/livros/3341

Após a escolha e implantação, o ideal é iniciar as integrações com os recursos mais críticos. Nessa está de implantação é altamente recomendado a análise e certificação da equipe de Segurança da Informação.

Assim fica fácil para os administradores criarem políticas que se adequem a cada negócio, seguindo exigências de compliance e outros requisitos de segurança da informação, e os funcionários podem ter acesso mais fácil e rápido para a continuidade das suas funções.

3.3 IMPORTÂNCIA DA CENTRALIZAÇÃO

Mesmo que a criação de um projeto de gestão de identidades de acesso possa ser complexo à primeira vista, são vários os benefícios alcançados, como:

- ✓ Redução na complexidade na gestão de acesso;
- ✓ Melhoria na segurança da informação;
- ✓ Redução de falhas na gestão de acesso;
- ✓ Os processos se tornam mais rápidos, ganho na agilidade das concessões;
- ✓ Diminuição de custos, não será mais necessário administradores nas pontas;
- ✓ Consulta facilitada da informação de acesso;

Com ela, é possível controlar todo o acesso e os privilégios em uma única console, podendo habilitar indicadores, emissões de relatórios, logs das concessões e rastreamento completo do que cada funcionário possui, podendo ter auditorias rápidas como o que cada usuário está acessando, hora e dia dos acessos entre outras diversas possibilidade relacionado a Segurança da Informação.

Isso é simplificação do gerenciamento de acesso, centralizando a administração dos usuários no mesmo repositório, por meio de interface unificada.

Gerencia de forma centralizada facilita muito o processo de auditoria e governança, com um login único para todos as aplicação e/ou recurso da empresa, significando muito mais agilidade e facilidade no monitoramento de atividades suspeitas, utilizando envios de alertas e auditoria de acesso.

Todo o processo de manutenção do acesso torna-se mais eficiente e ágil. A equipe e o usuário têm um acesso mais simplificado e otimizado. Essa solução evita a perda de tempo que ocorre com a descentralização, já que há a necessidade de buscar dados por outros meios para a liberação do acesso.

https://www.nucleodoconhecimento.com.br/livros/ciencias-biologicas-exatas-e-da-terra/gestao-centralizada-e-automatizada

DOI: 10.32749/nucleodoconhecimento.com.br/livros/3341

Sendo assim, toda a cadeia de concessão de acesso sofre benefícios importantes, além de algumas atividades sofrerem diminuição de ações, como o reset de senha, isso porque com a centralização, a senha do usuário passa a ser única entre as aplicações e/ou recursos, fazendo com o que o usuário não precise de uma senha para cada acesso e com políticas diferenciadas.

4. AUTOMATICAÇÃO DA GESTÃO DE IDENTIDADE

4.1 CONCEITOS DA AUTOMATIZAÇÃO

Esse é um processo de complementa e fecha todos o clico relacionado a gerenciamento centralizado de identidade, pois trata-se da automatização do processo de concessão/manutenção do acesso.

Significa que cada concessão, alteração de perfil e até mesmo retirada do acesso, serão realizados de forma automatizadas, sem qualquer intervenção manual. Todo o start é realizado por eventos onde diversos drivers poderão tomar as ações necessárias.

O ponto de partida deverá ser sempre as bases de RH, pois é nela que estar o verdadeiro status funcional do usuário, seja ativo, férias ou até mesmo de licença médica. Com base nesse status, os acessos poderão ser bloqueados de desbloqueados de forma on-line. Garantindo que somente usuários ativos tenham acesso nos ativos da empresa.

Será necessário criar comunicações entre cada ativo, para que toda a comunicação ocorra (sempre criptografada) de maneira simples e com garantia de entrega (integridade).

4.2 PROCESSO DA AUTOMATIZAÇÃO

Para que a processo seja centralizado e automatizado, será necessário buscar ferramentas próprias para essas atividades, ferramentas que irão auxiliar e realizar toda essa cadeia de atividades.

Chamamos de solução de IDM (Identity Management) e IAM (Identity Access Management – mais atual), onde hoje disponibilizamos de diversos grandes fornecedores (como IBM, Oracle, Microsoft, Microfocus entre outras) e até mesmo versões gratuitas. Todas elas com o intuito de gerenciar o clico de vida do usuário de forma automatizadas.

https://www.nucleodoconhecimento.com.br/livros/ciencias-biologicas-exatas-e-da-terra/gestao-centralizada-e-automatizada

DOI: 10.32749/nucleodoconhecimento.com.br/livros/3341

Seguem alguns dos principais passos que serão necessários para a implantação da automatização:

- ✓ Criação de um time especialista em IAM.
- ✓ Estude da melhor solução, olhando sempre para os ativos que sua empresa possui.
- ✓ Conheça bem os softwares que serão implantando.
- ✓ Escolha um sistema (fornecedor) com gestão fácil de entendimento.
- ✓ Busque um sistema (fornecedor) com suporte bem avaliado.
- ✓ Estude de cada protocolo de comunicação.
- ✓ Inclua o time de segurança da informação e arquitetura no projeto.
- ✓ Estude de infraestrutura, sempre com redundância e backup (solução robusta).
- ✓ Estabeleça claramente os objetivos.
- ✓ Mantenha os gestores e equipes envolvidos no processo.
- ✓ Criar uma gestão de perfis.

Por mais que a solução para a gestão corporativa automatize boa parte das funções do clico de vida do usuário, ainda existe a necessidade de se ter uma equipe comprometida no processo. Um time treinado e conhecedor da solução como um todos, seja para realizar o suporte como também para realizadas as novas integrações das aplicações que a empresa adquire ao longo da vida.

4.3 IMPORTÂNCIA DA AUTOMATIZAÇÃO

A implantação de um IDM/IAM traz benefícios de agilidade no processo de solicitação, aprovação e concessão de acessos. Como todo o processo será realizado de forma automatizada, o risco de concessões errôneas dendê a diminuir e até mesmo zerar, pois toda a cadeia de concessão será baseada no status funcional do usuário e aprovação gerencial para aquele acesso.

Principais ganhos ao implantar uma gestão centralizada e automatizada:

- ✓ A solução traz garantias de itens relacionados a auditoria, compliance, governança, segurança da informação, processo, politicas e normas legais (como exemplo a SOX – Sarbanes Oxley).

https://www.nucleodoconhecimento.com.br/livros/ciencias-biologicas-exatas-e-da-terra/gestao-centralizada-e-automatizada

DOI: 10.32749/nucleodoconhecimento.com.br/livros/3341

- ✓ A solução traz um aumento de produtividade, uma vez que a tecnologia consegue eliminar atividades manuais, ultrapassadas, lentas e complexas. Tornando mais rápido e intuitiva.
- ✓ A solução traz uma redução de custos, pois a incidência de erros, repetições e burocracias é reduzido com a automatização.
- ✓ A solução traz um controle de qualidade, a automatização estabelece padrões para cada atividade, criando uma linha produtiva ininterrupta, totalmente interligadas.
- ✓ A solução traz agilidade, eliminação de equipe administrativas nas pontas para cada aplicação (sendo necessário apenas uma equipe especialista em IDM/IAM).

A automatização do gerenciamento de acesso (clico de vida do usuário) é um movimento alinhado com o futuro e com a tecnologia, que é uma grande aliada das empresas.

5. CONSIDERAÇÕES FINAIS

Nas últimas décadas, as empresas vêm adquirindo mais e mais softwares, aplicações, recursos para facilitar o dia a dia, aumentar a produtividades, informatizar um setor, buscar novas formas de interagir com o cliente entre outros diversos motivos dependendo de cada setor e seguimento.

Muitas empresar sofrem com o número de aplicações e como controlar tudo isso, pois o risco de vazamento de informações pode causar impactos irreparáveis para a marca.

Controlar um enorme número de equipes é um desafio muito grande para qualquer gestor de TI, ainda mais equipe de super acessos administrando base de aplicações como SAP, CRM´s, bases de cliente...

Empresas que possuem um turnover (rotatividade) elevando, se preocupam com as respectivas retiradas de acessos dos ex-colaboradores, porque o risco é muito grande, além da falta de compliance junto a política da empresa e segurança da informação.

Esses são alguns pontos que muitas empresas possuem ou possuíam antes de implantar um gerenciamento centralizado de identidade, nesse sentido, modernizar setores com a ajuda de sistema deve ser prioridade para qualquer gestor atualmente, pois,

https://www.nucleodoconhecimento.com.br/livros/ciencias-biologicas-exatas-e-da-terra/gestao-centralizada-e-automatizada

DOI: 10.32749/nucleodoconhecimento.com.br/livros/3341

desse modo, é possível potencializar o desempenho e ter um negócio mais competitivo, estratégico e inteligente.

A gestão de identidade de acesso se trata do conceito da criação de uma identidade digital única e intransferível para cada um usuário. Essa gestão é importante para qualquer corporação que busca se manter no mercado de maneira atuante e com crescimento gradativo.

O sistema de gestão consegue promover mais eficiência ao trabalho e pode torná-lo mais produtivo, isso porque fornece mais agilidade nos procedimentos. Ele também reduz a possibilidade de erros.

Ao implantar um sistema de gestão, é possível de um único lugar conseguir obter tudo o que está acontecendo dentro da empresa.

Espero ter ajudado, de forma simples, no entendimento e importância dessa mudança nas empresas, um passo longo mais muito importante a ser tomado. Não é fácil, mais depois de implantado o ganho é astronômico e infinito, pois toda a cadeia torna muito mais fácil.

INFORMAÇÕES SOBRE O AUTOR:

Ricardo de Oliveira Boaro

Pós-graduação em Tecnologia - Governança e Gestão da Tecnologia da Informação.
ORCID: https://orcid.org/0009-0009-9333-5718.

https://www.nucleodoconhecimento.com.br/livros/ciencias-biologicas-exatas-e-da-terra/gestao-centralizada-e-automatizada

DOI: 10.32749/nucleodoconhecimento.com.br/livros/3341