Afya FACULDADE
PORTO NACIONAL · TO

Ebsco

Biblioteca Nossa Senhora das Mercês

1 Base de Dados EBSCO

A Afya Faculdade de Porto nacional através de sua mantenedora possui contrato com a Base de Dados EBSCO. Esse contrato é renovado anualmente e a verba para manutenção é inclusa em orçamento no centro de custo da Biblioteca. A EBSCO é a fornecedora líder de bancos de dados de pesquisa, gerenciamento de assinaturas de periódicos eletrônicos e pacotes eletrônicos, desenvolvimento de coleções de livros e gerenciamento de aquisições e um importante fornecedor de tecnologia de biblioteca.

1.1 Academic Search Complete

A Academic Search™ Complete possui uma vasta coleção de periódicos eletrônicos em texto completo, oferecendo aos usuários acesso a conteúdo acadêmico em diversas áreas do conhecimento. Realize suas pesquisas e encontre os resultados confiáveis dos mais prestigiados autores através da caixa de busca nesta página.

1.2 Fonte Acadêmica

Esta base de dados multidisciplinar fornece extensa cobertura em texto completo de conteúdos acadêmicos em língua portuguesa. É uma coleção de periódicos do Brasil e de Portugal em rápido crescimento, destinada a tornar a pesquisa acadêmica prontamente disponível em formato PDF.

1.3 Medline Ultimate

A MEDLINE Ultimate oferece aos profissionais médicos e pesquisadores acesso a conteúdo em texto completo baseado em evidências e revisado por pares contendo ainda mais das principais revistas biomédicas. Também oferece mais cobertura de periódicos internacionais do que qualquer outra base de dados MEDLINE.

2 Acessos à Base de Dados

2.1 Acesso Presencial

O acesso presencial também está disponível nas dependências da Biblioteca da Instituição, onde os usuários contam com o suporte da equipe técnica especializada para a orientação quanto ao uso das bases de dados e demais recursos informacionais.

1. **EBSCO**

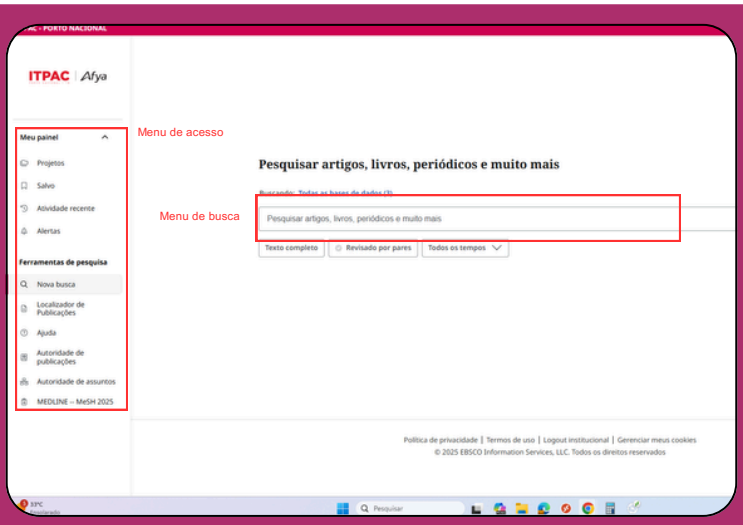
A EBSCO é uma empresa líder global na área de informação, especializada em fornecer soluções de acesso a conteúdo digital para instituições como universidades, escolas, bibliotecas e hospitais. A EBSCO oferece um vasto catálogo de bases de dados com artigos de periódicos, livros e outros tipos de conteúdo, abrangendo diversos temas e áreas de conhecimento.

1.2. Site:

Site oficial da IES

Aba biblioteca

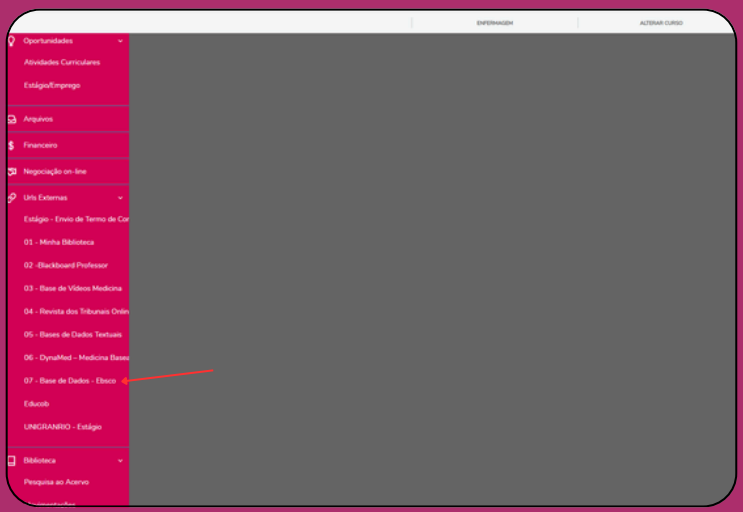
Aba Ebsco



Página inicial Ebsco

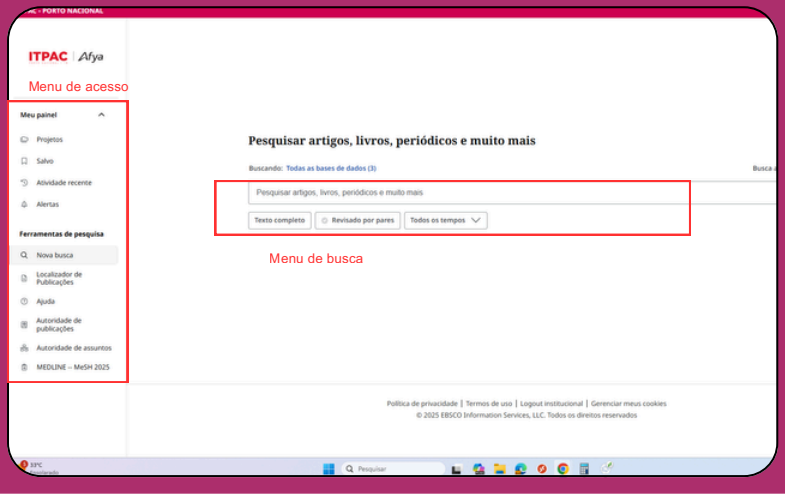
Acesso pelo portal do aluno

Portal do aluno:



Página inicial portal do aluno

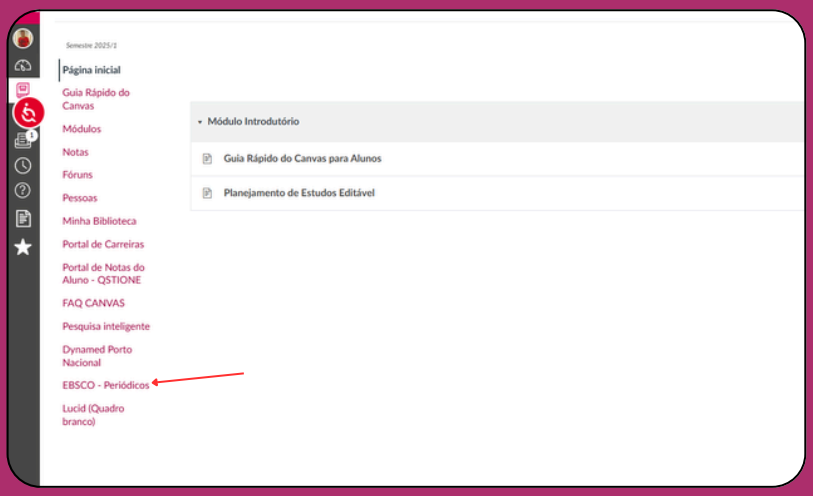
Coluna lateral de menu

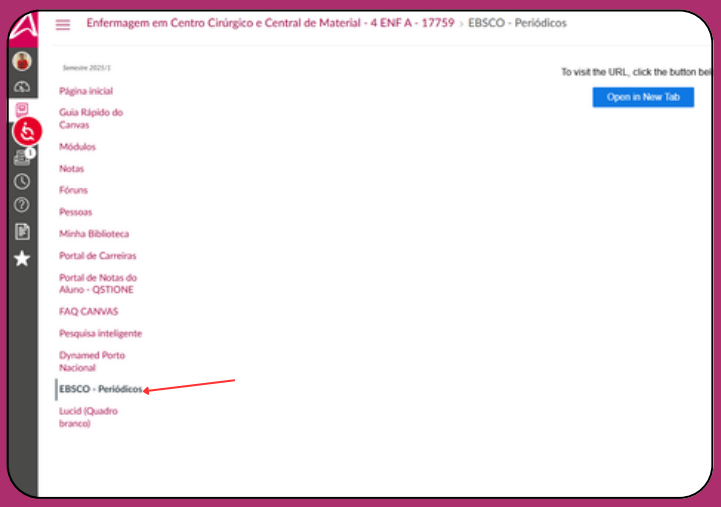


Canvas

Acesso pelo canvas

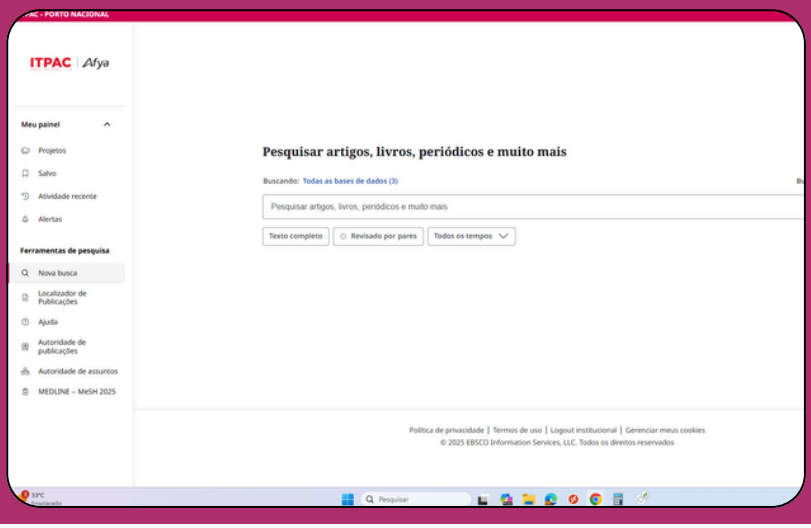
Canvas





Página inicial Ebsco

Página inicial Ebsco



EBSCO

EIS Segurança da Informação e Sistema de Gestão de Privacidade

Uma Publicação da EBSCO Information Services (EIS)

Março 2026

Tabela de Conteúdo

Introdução

A EBSCO Information Services (EBSCO) é a maior divisão da EBSCO Industries, uma grande corporação privada com sede em Birmingham, Alabama, EUA. A EBSCO possui operações globais diversificadas e atua como uma subsidiária integral. Embora muitos aspectos da EBSCO sejam operados de forma independente, sua área de Tecnologia trabalha em conjunto com a organização-mãe para obter alavancagem e economias de escala.

A EIS conta com equipes de profissionais altamente experientes em Segurança da Informação e Compliance. Os membros da equipe de Segurança da Informação da EIS são especialistas em diversas áreas, incluindo, mas não se limitando a: Segurança da Informação e Privacidade, Normas Regulatórias, Engenharia de Operações de Segurança, Engenharia de Gestão de Identidade e Acesso, treinamento e desenvolvimento de produtos ágeis e Arquitetura e Design de Cloud.

Os produtos de pesquisa da EBSCO, incluindo EBSCOhost, EBSCO Discovery Service, DynaMed, Marketplace e CINAHL, são hospedados principalmente na AWS região US East (Região 1), localizada na região norte da Virgínia. Para hospedagem do FOLIO, Locate, OpenRS e Panorama, a EBSCO oferece opções em múltiplas regiões da AWS e pode hospedar os dados na região AWS escolhida pelo cliente.

O GOBI é hospedado em um data center local em Contoocook, New Hampshire, EUA, enquanto a nova plataforma de pedidos de livros MOSAIC é hospedada na AWS região US East (Região 1). O EBSCONet é hospedado no data center da EBSCO Industries em Birmingham, Alabama, EUA, com migração planejada para o Amazon Web Services. O EBSCOLearning, que inclui LearningExpress e Accel, é hospedado na AWS regiões US East (Região 1) e US West (Região 2), em Oregon.

Aplicabilidade

Esse documento técnico é aplicável para os seguintes serviços:

- Serviços de Administração e Configuração (EBSCOadmin, EBSCO Experience Manager, EBSCO Configuration Manager, IAM)
- Serviços de Criação de Website para Bibliotecas (STACKS)
- Sistemas de Gestão de Bibliotecas (FOLIO, LOCATE, OpenRS)
- Panorama
- Library Aware
- EBSCONet, EBSCO Marketplace
- GOBI Library Solutions

- Serviços de Descoberta e Bases de Dados de Pesquisa (EBSCO Discovery Service (EDS), EBSCOhost, EBSCO Host Mobile, EDS API)
- Serviços de Periódicos e Pacotes Eletrônicos (Global Knowledgebase, EBSCO Publishing Knowledgebase)
- Serviços de Vinculação de Holdings (Holdings Manager, Full Text Finder, Publication Finder, HoldingsIQ, LinkIQ, and Usage Consolidation)
- Gestão de Recursos Eletrônicos (Flipster, eBooks, EBSCOhost Collection Manager ECM)
- EBSCOLearning (LearningExpress, Accel)
- EBSCO Health (CINAHL, Patient Education Reference Center, Nursing Reference Center, Nursing Reference Center Plus, Continuing Medical Education (CME))
- Produtos de Conhecimento em Saúde (Dynamed, Dynamic Health, Dynamedex, Dyna AI, Dynamed Decisions, MyHealth Decisions)

Segurança da Informação e Política de Privacidade

A EBSCO implementou um Sistema de Gestão de Segurança da Informação e Privacidade (ISPMS) em conformidade com as normas internacionais de segurança da informação e privacidade, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 e ISO/IEC 27701. Essas normas definem os requisitos para um ISPMS baseado em melhores práticas reconhecidas internacionalmente.

Essas políticas se aplicam a sistemas, pessoas e processos que compõem os sistemas de informação da organização, incluindo membros do conselho, diretores, colaboradores, fornecedores e outras partes terceiras que tenham acesso aos sistemas da EIS. Um princípio fundamental do Sistema de Gestão de Segurança da Informação e Privacidade da EIS é que os controles implementados são orientados pelas necessidades do negócio e são comunicados regularmente a todos os colaboradores por meio de reuniões de equipe e documentos informativos.

A operação do ISPMS traz diversos benefícios para o negócio, incluindo:

- Proteção dos dados de clientes e usuários
- Garantia do fornecimento de produtos e serviços aos clientes
- Conformidade com requisitos legais e regulatórios

A EBSCO mantém certificação nas normas ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 27017 e ISO/IEC 27018 para assegurar a adoção eficaz das melhores práticas de segurança da informação e privacidade. Esse programa é validado por um organismo certificador independente (Registered Certification Body – RCB), responsável por auditorias externas à EIS. O certificado hospedado externamente (#1737791-6) pode ser consultado no link indicado.

Uma definição clara dos requisitos de segurança da informação dentro da EIS é aplicada e

mantida tanto nos processos internos quanto no relacionamento com clientes externos, garantindo que todas as atividades do programa de segurança e privacidade estejam focadas no cumprimento desses requisitos. Requisitos legais, regulatórios e contratuais também são documentados e incorporados aos processos de planejamento de produtos. Requisitos específicos relacionados à segurança de sistemas ou serviços novos ou modificados são definidos durante a fase de design de cada projeto.

A política de privacidade da EBSCO pode ser consultada aqui.

Controle de Acesso

O controle de acesso aos ativos de informação da EBSCO é uma parte fundamental de uma estratégia de segurança em camadas (defense-in-depth). A equipe de segurança da informação da EIS atua para proteger a confidencialidade, integridade e disponibilidade dos dados classificados, garantindo a implementação de um conjunto abrangente de controles físicos e lógicos.

A política de controle de acesso da EIS é projetada considerando os requisitos de negócio e de segurança da informação da organização, sendo revisada regularmente para assegurar que permaneça adequada.

O conceito de **Privilégio Mínimo (Least Privilege Access)** é aplicado em todos os controles de acesso da EIS. A equipe de segurança da informação da EBSCO trabalha para garantir que esse princípio seja seguido em todos os sistemas de informação da empresa. A autenticação de dois fatores é utilizada para o acesso dos colaboradores da EIS, juntamente com parâmetros de senha alinhados às melhores práticas do mercado, incluindo comprimento mínimo, requisitos de complexidade, rotatividade de senhas, bloqueio automático, entre outros.

A EBSCO conta com uma equipe dedicada de gestão de identidade e acesso, que atua em conjunto com a organização para garantir a segregação de funções entre o provisionamento de acessos e a gestão dos sistemas. Também seguimos um processo abrangente de aprovação de acessos privilegiados.

Segurança de IA

Na EBSCO, estamos comprometidos em seguir os princípios de pesquisa responsável como base para o uso de Inteligência Artificial (IA).

A EBSCO reconhece a importância da confiança e busca desenvolver tecnologias de IA que complementem, e não substituam, a expertise humana no processo de pesquisa. Com um forte compromisso com o desenvolvimento responsável de IA, nossos processos e tecnologias são fundamentados em dados confiáveis e na garantia da precisão do conteúdo.

Um aspecto central da filosofia de IA da EBSCO é a transparência. Estamos comprometidos com a identificação clara de conteúdos gerados por IA e com a

disponibilização de recursos de IA explicável. Isso permite que os usuários compreendam como os sistemas chegam aos resultados, promovendo uma tomada de decisão mais informada e o uso responsável da tecnologia. A EBSCO acredita que, ao priorizar transparência e explicabilidade, pode capacitar os usuários a avaliar criticamente e utilizar de forma eficaz as ferramentas de IA em suas atividades de pesquisa.

Em essência, a EBSCO busca ser uma referência no desenvolvimento responsável de IA no setor de pesquisa. Ao seguir práticas de pesquisa reconhecidas globalmente e priorizar precisão, transparência e supervisão humana, trabalhamos para garantir que a IA atue como uma ferramenta valiosa para pesquisadores, contribuindo para o avanço do conhecimento e da descoberta.

Gerenciamento de Ativos

A EBSCO mantém um inventário atualizado e preciso dos ativos associados a todas as instalações de processamento de informação. A EIS possui um catálogo de dados abrangente que identifica riscos dentro da organização. Essas atividades são coordenadas por membros das equipes de Segurança da Informação e de Governança, Risco e Compliance (GRC).

A EBSCO garante o cumprimento de todos os requisitos legais e regulatórios ao considerar a sensibilidade dos dados. Além disso, mantém um inventário completo de todos os ativos físicos, como estações de trabalho e servidores que prestam serviços aos clientes. A EIS assegura que todos os requisitos de segurança da informação sejam cumpridos ao longo de todo o ciclo de vida dos ativos físicos.

Gerenciamento de Disponibilidade

A EIS busca garantir ambientes de alta disponibilidade para seus clientes, tanto em data centers locais quanto na nuvem AWS. O status atual dos serviços da EBSCO pode ser consultado aqui.

Os requisitos de disponibilidade das instalações de processamento de informação são definidos em conjunto com os responsáveis pelos sistemas e outras partes interessadas, devendo ser iguais ou superiores aos seguintes padrões:

- Os serviços são projetados para que o carregamento das páginas ocorra, em média, em até 5 segundos ou menos.
- Disponibilidade ponta a ponta dos serviços (SLA esperado de 99,9% de uptime, equivalente a menos de 9 horas de indisponibilidade por ano).
- Objetivo de Tempo de Recuperação (RTO) máximo de 10 minutos para sistemas críticos, ou seja, os sistemas devem ser restabelecidos em até 10 minutos após um incidente que afete a disponibilidade.
- Objetivo de Ponto de Recuperação (RPO) mínimo de 8 horas para sistemas críticos, ou seja, os sistemas críticos devem ser copiados (backup) pelo menos uma vez a cada 8 horas, garantindo que, em caso de restauração, os dados não tenham mais de 8 horas de defasagem.

Há um cuidado contínuo para garantir que essas metas de disponibilidade e confiabilidade sejam mensuráveis e compreendidas em toda a organização. Procedimentos e ferramentas são implementados para registrar a disponibilidade de todos os serviços-chave com metas definidas.

As estatísticas de disponibilidade são publicadas como parte do ciclo de relatórios gerenciais e refletem os objetivos mencionados. Os mecanismos de cálculo da disponibilidade ponta a ponta são transparentes, garantindo entendimento comum sobre como os indicadores são obtidos.

A EBSCO ou seus provedores de serviço também monitoram a disponibilidade dos componentes essenciais que suportam os serviços, permitindo análise adequada em caso de incidentes.

Quando uma meta não é atingida, são fornecidas explicações sobre as causas e as ações corretivas planejadas. Informações sobre disponibilidade podem ser consultadas em status.ebsco.com, onde os clientes também podem se inscrever para receber notificações em caso de interrupções.

Indisponibilidades planejadas são comunicadas a todos os clientes. Em caso de interrupções não planejadas, a EBSCO ou seus provedores se esforçam para manter clientes e usuários informados sobre o status e os prazos estimados para restauração dos serviços.

Todas as solicitações de mudança são avaliadas quanto ao impacto na disponibilidade dos produtos e serviços, dentro de processos robustos de gestão de mudanças. As equipes internas trabalham para garantir que os níveis de disponibilidade definidos sejam mantidos durante a implementação de alterações nos ambientes de produção.

Plano de Backup

A EBSCO trabalha diligentemente para garantir que recursos e planos de contingência suficientes sejam implementados e testados regularmente. Isso é alcançado por meio da implantação de recursos em vários data centers locais (on-premise) e seus equivalentes virtuais nas Zonas de Disponibilidade (AZ) da AWS. Essa abordagem diversificada de hospedagem de recursos garante redundância e tolerância a falhas, minimizando o impacto de possíveis interrupções.

Para proteger os dados dos clientes e assegurar a continuidade dos negócios, implementamos uma estratégia robusta de backup e recuperação. Para otimizar e automatizar os processos de backup, utilizamos tecnologias avançadas para ativos na AWS e on-premise. Esses serviços gerenciam e agendam backups para nossos recursos físicos de computação e recursos da AWS, como instâncias EC2, volumes EBS e bancos de dados RDS.

Nossa estratégia de recuperação é projetada para minimizar o tempo de inatividade e a perda de dados para nossos clientes. Definimos métricas claras de Recovery Time Objective (RTO) e Recovery Point Objective (RPO) para orientar os procedimentos de recuperação. Também mantemos um ambiente “pilot light” (standby ativo) em regiões e Zonas de Disponibilidade separadas, permitindo redirecionar rapidamente o tráfego e

escalar os recursos em caso de uma grande interrupção.

Nosso plano abrangente de recuperação de desastres é bem documentado, descrevendo procedimentos passo a passo para restaurar dados e aplicações. Testes regulares garantem que nossos processos de recuperação atendam às metas definidas de RTO e RPO. Além disso, monitoramos continuamente nossos sistemas e contamos com mecanismos de alerta para detectar e responder proativamente a possíveis problemas.

Uma filosofia central da EBSCO é evitar eventos disruptivos ao projetar redundância e resiliência em todas as operações. Fazemos isso estabelecendo instalações geograficamente e tecnicamente diversas e redundantes, além de realizar testes regulares de cenários de “failover” de backup. Esses testes são realizados, no mínimo, uma vez por ano. Nenhuma intervenção do cliente é necessária para gerenciar os backups.

Plano de Continuidade de Negócios

Os planos de Continuidade de Negócios da EBSCO são integrados e interdependentes. Eles são orientados para planos de ação simples que guiam a gestão e os colaboradores na resposta adequada durante eventos que interrompem os negócios, garantindo comunicação eficaz, eficiência e execução. O sucesso da EIS depende da sustentabilidade desses esforços. Assim, buscamos incorporar princípios e práticas de continuidade de negócios em toda a organização, integrando-os aos procedimentos operacionais padrão.

O Plano de Continuidade de Negócios estabelece a estratégia da EBSCO para o gerenciamento de recursos e a manutenção das operações em caso de desastre ou possível interrupção de serviços. Esse plano é aprovado pela alta administração e revisado anualmente, bem como sempre que ocorrem mudanças significativas no ambiente.

A EBSCO realiza múltiplos testes por ano em seus diversos sistemas e planos que fazem parte da abordagem geral de continuidade de negócios. A cultura de melhoria contínua da EIS permite a adoção de ações com base nos resultados de cada teste.

A EBSCO já demonstrou com sucesso a resiliência desse programa em situações de emergência severas, incluindo enchentes, tornados, furacões e interrupções em instalações locais. Essas preparações permitiram a continuidade das operações e a prestação de serviços sem impacto aos clientes. Embora tenhamos orgulho disso, permanecemos vigilantes para garantir que nossos produtos continuem a atender nossos clientes, independentemente de quaisquer eventos extraordinários. A EIS também adotou amplamente ferramentas baseadas em nuvem em toda a organização e aproveita extensivamente as capacidades de força de trabalho remota.

Criptografia

Os produtos da EBSCO utilizam HTTPS e TLS 1.2/1.3 para proteger a transmissão de dados dos usuários para nossos sistemas. Dentro dos nossos sistemas, dados sensíveis dos clientes são protegidos por padrão com criptografia AES 256.

A área de Segurança da Informação da EBSCO estabelece requisitos para o uso de técnicas de criptografia por meio da implementação desta política. Ela é aplicada para a proteção de dados sensíveis em repouso, em trânsito, em uso ou quando exigido por contrato. Os controles e procedimentos relacionados às diversas áreas onde criptografia e outras técnicas criptográficas são necessárias estão em conformidade com leis federais e internacionais, sendo aderentes ao padrão FIPS 140-2.

Nenhuma intervenção do cliente é necessária para a criptografia dos dados dentro da plataforma da EBSCO.

Responsabilidade de Controle do Cliente

Os clientes da EBSCO, em consulta ou com o apoio da nossa equipe de suporte, são responsáveis por configurar a autenticação para nossos serviços. Eles também são responsáveis por notificar a EBSCO sobre configurações ou ajustar o acesso aos serviços via Single Sign-On (SSO), garantindo que o acesso aos bancos de dados da EBSCO seja removido quando um usuário deixar a instituição correspondente. A EBSCO é responsável pelos demais controles de segurança dentro de sua plataforma.

Nenhuma ação do cliente é necessária para garantir a sincronização de relógio dentro da nossa plataforma.

Para mais informações sobre as opções de autenticação da EBSCO, consulte a documentação correspondente.
https://www.ebsco.com/sites/g/files/nabnos191/files/acquiadam-assets/Authentication-Solutions-Guide.pdf

Segurança de Recursos Humanos

Verificações adequadas de antecedentes são realizadas para todos os colaboradores antes da contratação. Os contratos de trabalho, incluindo aqueles com profissionais terceirizados, especificam requisitos relevantes de segurança da informação e privacidade, incluindo o compromisso de cumprir as políticas da EBSCO. Isso inclui acordos abrangentes de uso aceitável e confidencialidade, que devem ser reconhecidos por todos os colaboradores.

Todos os colaboradores com acesso aos sistemas da EBSCO são obrigados a realizar treinamentos de conscientização em segurança e privacidade duas vezes por ano. Treinamentos específicos por função também são exigidos para determinados colaboradores e contratados, com nível de detalhamento adequado às suas responsabilidades.

Resposta a Incidentes

O plano de resposta a incidentes (IRP) da EIS define os procedimentos a serem seguidos e as ações apropriadas a serem tomadas durante as diferentes fases de uma resposta a incidentes, caso ocorra algum evento. O plano estabelece essas fases, as respostas correspondentes e a abordagem para coleta e implementação de lições aprendidas. Ele também assegura o nível de disponibilidade de recursos que os clientes exigem e

esperam.

O IRP da EIS inclui procedimentos para limitar o impacto de qualquer incidente de segurança e prevê as comunicações necessárias, tanto para clientes quanto internamente, detalhando o ocorrido. A EIS está comprometida em garantir que todos os requisitos de reporte, legais e regulatórios sejam atendidos. Diversas partes interessadas em toda a organização — incluindo operações de segurança, governança, risco e conformidade, o escritório do CIO e a alta administração — possuem papéis definidos dentro do IRP da EBSCO.

Os incidentes são tratados por meio de um processo definido, com cenários comuns previamente mapeados para as equipes. Após cada incidente, são conduzidas análises de lições aprendidas, e os planos de resposta e runbooks são atualizados com base nesses aprendizados.

Caso ocorra uma violação de dados, a EBSCO notificará os clientes em até 72 horas após a confirmação da violação de dados do cliente. Quando aplicável, a empresa também cumprirá as leis vigentes relacionadas à notificação de autoridades públicas ou do público em geral.

Se os clientes suspeitarem de uso indevido da plataforma da EBSCO, devem entrar em contato pelo e-mail: eis_compliance@ebsco.com

Registro e monitoramento

A EBSCO possui uma equipe de Operações de Segurança responsável pelo registro (logging) e monitoramento do ambiente interno, abrangendo todos os produtos dentro do seu escopo e limites. Atualmente, não é oferecida integração com sistemas de logging de segurança dos clientes.

A empresa mantém um SOC (Security Operations Center) operando 24 horas por dia, 7 dias por semana, gerenciado por meio de um sistema de monitoramento de eventos e incidentes de segurança (SIEM). A equipe de operações de segurança, em conjunto com um provedor externo de SIEM e recursos automatizados, analisa alertas para identificar anomalias nos sistemas.

A Política de Logging e Monitoramento da EIS define procedimentos para configurar e gerenciar logs internos, com o objetivo de monitorar o uso dos sistemas e garantir a segurança e integridade dos ativos de informação da EIS e dos clientes. Essa política se aplica a todos os indivíduos e sistemas dentro da EIS, incluindo colaboradores, fornecedores e terceiros com acesso aos sistemas.

A política exige a ativação de mecanismos de auditoria em todos os equipamentos relevantes, registrando eventos-chave, tentativas de acesso e alterações nos sistemas. Também determina a revisão periódica desses logs, considerando fatores como criticidade do negócio e sensibilidade das informações. Além disso, enfatiza a proteção dos dados de log por meio de permissões rigorosas, arquivamento e backups diários.

Adicionalmente, a EBSCO trata do registro de falhas (fault logging), exigindo a investigação de falhas reportadas para garantir a integridade dos controles de segurança. Também assegura a sincronização dos relógios dos sistemas para permitir investigações precisas de incidentes e o registro adequado das atividades de administradores.

Sanitização e descarte de mídias

A EBSCO estabeleceu diretrizes para métodos seguros de sanitização e destruição de mídias, com o objetivo de proteger contra a divulgação não autorizada de informações sensíveis durante a realocação ou descarte desses materiais.

Além disso, muitos produtos e serviços da EIS são hospedados na Amazon Web Services, que segue diversos frameworks de segurança e privacidade, bem como requisitos associados para o descarte adequado de mídias. Todas as mídias que aguardam sanitização ou descarte são tratadas e armazenadas como contendo “informações confidenciais”, em conformidade com as diretrizes vigentes. A sanitização ou destruição dessas mídias é realizada exclusivamente por equipes de suporte de TI da EBSCO, pela área de Segurança da Informação ou por fornecedores licenciados de descarte seguro.

As atividades de sanitização ou destruição de mídias são registradas e mantidas por, no mínimo, um ano, incluindo as seguintes informações:

- Descrição da mídia
- Data da sanitização ou destruição
- Nome do responsável ou fornecedor que executou o processo
- Método de sanitização ou destruição utilizado

Os discos rígidos passam por um processo que inclui desmagnetização (degaussing), trituração e, posteriormente, esmagamento.

Contratos e acordos de serviço com fornecedores também preveem que a EIS possa sanitizar, destruir, criptografar ou reter mídias removíveis antes de devolver equipamentos ao fornecedor, independentemente do motivo.

Segurança de Rede

O modelo de segurança de rede da EBSCO adota uma abordagem de Defesa em Profundidade (Defense-in-Depth), com múltiplas camadas de controle para proteção dos sistemas.

Esses controles incluem, mas não se limitam a:

- Regras de negação por padrão (Default Deny) em roteadores de borda (Edge Routers)
- Conjuntos de regras de negação por padrão em firewalls
- Arquiteturas segmentadas, incluindo camadas de aplicação, apresentação, sessão e back-end
- Uso de Web Application Firewalls (WAFs) nas camadas segmentadas apropriadas

Essa abordagem em camadas reduz a superfície de ataque e aumenta a resiliência contra ameaças, garantindo que múltiplos mecanismos de segurança atuem de forma complementar dentro da infraestrutura da EBSCO.

Segurança Física

A EBSCO está comprometida em garantir a segurança de seus colaboradores, contratados e ativos, tratando a segurança física como uma prioridade. A EIS possui um conjunto abrangente de controles de segurança física que asseguram a proteção adequada de seus data centers e escritórios. O acesso a esses ambientes é restrito apenas ao pessoal necessário, sendo todo acesso registrado e revisado para identificar possíveis anomalias.

Além disso, a EBSCO contrata a Amazon Web Services para fornecer segurança de nível mundial em seus data centers hospedados. Para mais informações sobre a segurança física em ambientes hospedados na AWS, recomenda-se consultar a documentação específica da plataforma, disponível aqui.

Considerações de Privacidade

A EBSCO construiu um ambiente em conformidade com as principais regulamentações de privacidade. Isso inclui, entre outras, o General Data Protection Regulation (GDPR), a UK Data Protection Act, a California Consumer Privacy Act (CCPA), a California Privacy Rights Act (CPRA), a Family Educational Rights and Privacy Act (FERPA), a Children's Online Privacy Protection Act (COPPA), a Health Insurance Portability and Accountability Act (HIPAA), a Virginia Consumer Data Protection Act, a Personal Information Protection and Electronic Documents Act, o Privacy Act 1988, a Lei Geral de Proteção de Dados, a Connecticut Data Privacy Act, a Colorado Privacy Act, a Utah Consumer Privacy Act e a Protection of Personal Information Act.

A equipe de Governança, Risco e Conformidade da EBSCO revisa regularmente novas leis de privacidade à medida que são implementadas, garantindo que seus produtos permaneçam em conformidade com as legislações aplicáveis nos locais onde são armazenados.

A EBSCO atua como operadora (processor) das informações fornecidas diretamente pelos clientes ou contidas no produto de hospedagem FOLIO.

Além disso, a empresa permite que usuários criem contas para personalizar sua experiência de pesquisa. Nesse caso, a EBSCO atua como controladora conjunta (joint controller) dessas informações. Isso significa que foram implementadas funcionalidades que permitem aos usuários exercer seus direitos de privacidade — incluindo visualizar, modificar e excluir seus dados pessoais — diretamente no módulo de autoatendimento da conta ou por meio do contato com privacy@ebsco.com

Nenhuma ação é exigida do administrador institucional do cliente para que esses direitos sejam exercidos.

Considerações de Privacidade para Localização de Dados na União Europeia (EU Data Locality)

A EBSCO oferece opções de hospedagem na União Europeia para uso com Folio, Locate e OpenRS, a fim de atender aos requisitos de residência de dados de clientes localizados na UE. Para outros produtos, as informações são hospedadas nos Estados Unidos; no entanto, a empresa cumpre o General Data Protection Regulation (GDPR) e aderiu ao EU/US Data Privacy Framework, que regula transferências internacionais de dados com base em uma decisão de adequação da Comissão Europeia. Além disso, seu contrato padrão inclui Cláusulas Contratuais Padrão (SCCs), que cobrem transferências internacionais de dados caso o EU/US Data Privacy Framework seja invalidado pelas autoridades europeias.

Para clientes com requisitos de residência de dados, a EBSCO oferece opções para evitar que dados pessoais sejam transferidos para os Estados Unidos. Ao criar uma conta MyEBSCO via Single Sign-On (SSO), a instituição ou biblioteca controla quais dados são compartilhados com a EBSCO. O requisito mínimo é um identificador único (que pode ser pseudonimizado), enquanto nome, sobrenome e e-mail são opcionais.

Além disso, para clientes europeus que utilizam ferramentas de pesquisa da EBSCO (como EBSCOhost e EBSCO Discovery Service), mas não contratam Folio/Locate, é oferecida integração com o OpenAthens, um serviço de federação de identidade hospedado no Reino Unido. Nesse caso, também é possível utilizar identificadores pseudonimizados para os dados transferidos aos EUA.

O Single Sign-On baseado em Security Assertion Markup Language (SAML) pode ser configurado para limitar as informações pessoais compartilhadas durante o processo de autenticação. Isso garante que dados sensíveis permaneçam dentro dos limites de TI da organização cliente, ao mesmo tempo em que permite acesso seguro às aplicações SaaS da EBSCO. Para isso, os produtos da EBSCO podem ser configurados com mapeamento e filtragem de atributos no SAML SSO.

O SAML SSO utiliza “assertions” para transmitir atributos do usuário (como nome e e-mail) para um provedor de serviços (SP) durante a autenticação nos produtos e serviços da

EBSCO. Durante a fase de implementação e configuração, identificadores sensíveis (como nomes reais) podem ser substituídos por identificadores opacos, específicos da organização e não considerados sensíveis pelo cliente. Em outros casos, determinados dados podem simplesmente não ser compartilhados com a EBSCO, o que pode ser feito com pouca ou nenhuma perda de funcionalidade dos produtos.

Desenvolvimento Seguro

A EBSCO possui um programa abrangente de desenvolvimento seguro, com controles em etapas (gates) para garantir que todo o código seja revisado e testado contra as principais vulnerabilidades do OWASP Top 40 e outros defeitos antes de ser promovido para produção.

Além disso, é necessária a aprovação de pessoal autorizado dentro do pipeline de implantação de código antes que qualquer alteração seja levada ao ambiente de produção.

Como parte do processo de gestão de mudanças, a EBSCO exige que as equipes de desenvolvimento avaliem o impacto na privacidade e na segurança de mudanças significativas, como alterações na coleta de dados.

Teletrabalho

Muitos colaboradores da EBSCO têm a opção de trabalhar remotamente (teletrabalho). Como resultado, a empresa implementou um conjunto completo de controles para garantir a segurança dos dados nesse contexto.

A política de mesa limpa (clear desk) e tela limpa (clear screen) da EBSCO se aplica a todos os colaboradores em trabalho remoto. Além disso, há controles para criptografar e apagar remotamente (remote wipe) os dispositivos de trabalho, garantindo a proteção dos dados em estações utilizadas fora do ambiente corporativo.

O acesso remoto à rede interna da EBSCO é protegido por meio de VPN segura, com autenticação de dois fatores (2FA). A prevenção de acessos não autorizados a partir de redes inseguras é considerada de extrema importância.

Em caso de desligamento, por qualquer motivo, todos os equipamentos fornecidos devem ser devolvidos à EBSCO.

Gerenciamento de Fornecedor

Os relacionamentos da EBSCO com fornecedores são baseados em um entendimento claro das expectativas e requisitos relacionados à segurança da informação. Esses requisitos são documentados e enfatizam a importância de manter e evoluir continuamente a eficácia dos controles implementados, a fim de reduzir riscos organizacionais e garantir a segurança e a privacidade das informações dos clientes.

O programa de due diligence de fornecedores da EBSCO é baseado nas normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022, com foco em áreas específicas de acordo

com os requisitos de segurança da EIS. A empresa realiza Avaliações de Impacto à Proteção de Dados (DPIA) em todos os fornecedores e, quando aplicável, envia questionários de due diligence.

Os subprocessadores da EBSCO possuem certificações SOC 2 Tipo 2 e/ou ISO 27001, e esses relatórios de auditoria são revisados regularmente pela equipe de conformidade da EIS para garantir que os controles adotados pelos subprocessadores atendam aos rigorosos padrões da organização.