Aprendizagem online segura

Guia para instituições educacionais da América Latina para proteger os dados digitais de seus estudantes em ambientes escolares

eon resilience lab by C Minds

BID

Aprendizagem online segura

Guia para instituições educacionais da América Latina para proteger os dados digitais de seus estudantes em ambientes escolares

Autoras: **Claudia May Del Pozo**, **Ana Victoria Martín del Campo Alcocer** e **Mariana Róo Rubí** (Eon Resilience Lab, C Minds).

Colaboradoras: **Constanza Gómez Mont** y **Daniela Rojas Arroyo** (C Minds); **Cristina Pombo** e **Natalia González Alarcón** (BID Setor Social); **Elena Arias** (BID Setor Educação).

https://www.iadb.org/

Índice

Agradecimentos

Por todas as colaborações, principalmente as contribuições de conhecimentos que ajudaram a fortalecer a pesquisa, agradecemos às pessoas que são membros de nosso Conselho Consultivo:

Ana Cecilia Pérez Rosales, Cofundadora e Codiretora, CAPA 8, Escuelas Ciberseguras (México); **Carla Vázquez Wallach**, Especialista em direito digital e fundadora da Legal + Innovation (México); **Cristina Martínez Pinto**, Fundadora e diretora do PIT Policy Lab (México); **Lucía Acurio**, Fundadora e diretora da Escuelas Digitales (Peru); **Priscila Gonsales**, Diretora Nacional da Educadigital (Brasil), e **Santiago Paz**, Especialista Setorial em Segurança Cibernética do Banco Interamericano de Desenvolvimento (BID) (regional).

Da mesma forma, expressamos nosso agradecimento aos entrevistados durante a investigação, pois suas perspectivas foram fundamentais para o enriquecimento do documento:

Andrew Young, Diretor de conhecimento do The Gov Lab (Estados Unidos); **Alejandro Morduchowicz**, Especialista Líder em Educação na Divisão de Educação do BID (regional); **Cecilia Hughes**, Chefa de Avaliação e Acompanhamento do Plan Ceibal (Uruguai); **Diego Russo**, Analista de Cibersegurança do Plan Ceibal (Uruguai); **Fernando Valenzuela,** Fundador da Global EdTech Impact Alliance (global); **Gabriela Castro,** Diretora do Departamento de Recursos Tecnológicos do Governo da Costa Rica (Costa Rica); **Leda Muñoz**, Diretora da Fundação Omar Dengo (Costa Rica); **Lindsey Barret**, Pesquisadora da Universidade de Georgetown, Fundo das Nações Unidas para a Infância (UNICEF) (Estados Unidos); **Lucía Acurio**, Presidente Executiva da Educatec (Peru); **Marcelo Cabrol,** Gerente do Setor Social do BID (regional); **Marcelo Pérez**, Especialista Líder em Educação na Divisão de Educação do BID (regional); **Miguel Brechner**, Especialista Líder em Educação na Divisão de Educação do BID (regional); **Monserrat Creamer**, Especialista em Educação (Equador); **Priscila Gonsales**, Diretora Nacional da Educadigital (Brasil), e **Víctor Giorgi**, Diretor Geral do Instituto Interamericano da Criança e do Adolescente da Organização dos Estados Americanos (OEA) (regional).

Pela inscrição ou participação na roda de conversa regional e seus importantes pontos de vista, agradecemos aos professores:

Carola Betzabé Huaringa Ospino (Peru), Enrique Castañeda Zuñiga (Peru), **Gabriela Pagliaso** (Argentina), **Graciela Pozzer** (Argentina), **Gloria Elizabeth Galeano Álvarez** (Paraguai), **Iris Peña** (Panamá), **Patricia Santanaria Guaminí** (Equador), **Roberto Antonio Carmona Caro** (Colômbia) e **Silvia Medina** (Argentina).

Além disso, um agradecimento a Juan Pablo Carsi Reyna, Cofundador e Codiretor da Capa 8, por atuar como revisor do documento. Por fim, um agradecimento especial aos nossos parceiros de divulgação da Pesquisa Regional, por terem aderido à proposta com tanto entusiasmo:

Enseña por México (Mexico), **Fundación Lewis Galindo** (Panamá), **Fundación Omar Dengo** (Costa Rica), **Fundación Quirós Tanzi** (Costa Rica) e **Profesoras Conversando** (Peru).

I. Introdução e contexto

1. Introdução

As instituições escolares têm sido tradicionalmente uma espécie de segundo lar dos estudantes, mas, como resultado da pandemia de COVID-19, elas se tornaram um espaço exclusivamente virtual. Nele, seja físico ou virtual, busca-se o bem-estar fisiológico, educacional e emocional dos alunos, tendo como centro um aspecto básico: a segurança. A proteção integral dos estudantes inclui os aspectos físicos e mentais, bem como a proteção de suas informações, tarefa que hoje deve ser estendida ao mundo digital.

Nos últimos dez anos (Arias Ortiz e Cristia, 2014), as instituições escolares têm visto avanços significativos na incorporação de tecnologias disruptivas nas salas de aula. Essa tendência acelerou-se (UNICEF, 2019) diante da situação grave que a América Latina e o mundo vivem: a pandemia de COVID-19, que representou um desafio para escolas e colégios que, em questão de semanas e em caráter de emergência, tiveram que migrar para as plataformas digitais para manter uma certa continuidade nos processos de ensino e aprendizagem. Como consequência da atividade online, surgiram (ONU, 2020) grandes quantidades de dados digitais de estudantes e professores que agora estão na nuvem[1]. Atualmente, os estudantes possuem dados nos sites das empresas, registros nas plataformas de administração para gestão educacional e contas nos serviços de streaming de áudio e vídeo.

Embora as instituições escolares tenham garantido com sucesso a proteção dos dados físicos de seus estudantes, neste momento, elas se deparam com um novo desafio: a proteção tanto de sua identidade quanto de sua pegada digitais em plataformas educacionais digitais. De acordo com uma pesquisa em sete países da região[2] realizada pelo Banco Interamericano de Desenvolvimento (BID) e o Laboratório de Resiliência Eon da C Minds para os fins deste Guia, constatou-se que 16,7% dos professores desconhecem os riscos que podem advir do fato de haver dados digitais de seus estudantes nas redes, e 43% dos professores não sabem se um ataque de segurança cibernética ou um vazamento de dados ocorreu em sua escola.

Essa mesma pesquisa revelou que apenas 19,5% das instituições de ensino solicitam autorização escrita ou digital dos pais ou responsáveis legais dos estudantes para o uso de plataformas e ferramentas digitais. Além disso, 53,12% dos professores não leem as políticas de privacidade quando começam a usar esse tipo de plataforma, o que implica que não sabem como os dados de seus estudantes (e os dos próprios professores) estão sendo utilizados.

1 De acordo com a ONU, a computação em nuvem implica o uso de recursos computacionais e de TIC que são proporcionados como um serviço pela Internet de localizações geograficamente diversas, utilizando-se uma infraestrutura compartilhada e redimensionável dinamicamente. Para mais informações, acesse: https://uncitral.un.org/es/cloud

2 Inclui 1304 respostas dos países a seguir: Brasil, Colômbia, Costa Rica, México, Peru, Panamá e Uruguai. Para mais informações, consulte o Anexo 1.

Considerando-se a atual inexistência de diretrizes e políticas públicas quanto ao tratamento responsável dos dados de crianças nos ambientes digitais escolares, torna-se de suma importância que cada escola priorize a transferência do cuidado dos dados obtidos do mundo físico para o digital. Os resultados da pesquisa revelaram que apenas 13,9% das instituições de ensino entram em contato com o aplicativo correspondente para deletar os dados de seus estudantes assim que deixam de usá-lo, o que significa que 86,1% não possuem procedimentos para a eliminação de dados, ou os professores não sabem se existe algum procedimento para isso.

Essa transição abrupta para o mundo digital deixou claro que professores e gestores precisam de toda a ajuda necessária para permitir a continuidade no ensino, sem comprometer a segurança dos dados de seus estudantes. 72,3% dos professores não têm formação (ou ela é insuficiente) em questões de privacidade de dados e uso responsável de plataformas e ferramentas digitais, o que significa que apenas 14,9% receberam formação regulatória ou consideram que foi suficiente.

Por isso, o Grupo BID[3] e o Laboratório de Resiliência Eón da C Minds[4] uniram esforços, no âmbito da iniciativa fAIr LAC[5], para elaborar e implementar o projeto Aprendizagem online segura, que nasceu com o objetivo de responder à necessidade urgente de proteção de dados digitais de crianças em ambientes educacionais. Como parte desse projeto, este Guia foi concebido para diretores e professores que buscam fortalecer a proteção dos dados de seus estudantes nas plataformas online que utilizam nas e para as instituições de ensino.

O Guia divide-se em duas seções: a seção teórica informativa, onde os riscos e conceitos relevantes são analisados para identificar os riscos enfrentados por instituições de ensino e colégios online, e a seção com recomendações de boas práticas, para que as instituições de ensino tenham as ferramentas para proteger os dados de estudantes e professores, uma vez que as instituições de ensino, mesmo quando contratam com terceiros o uso de plataformas educacionais na Internet, continuam sendo responsáveis pelo serviço educacional, enquanto as empresas são responsáveis pelo tratamento.

Nesse sentido, devem continuar cumprindo todas as prerrogativas, diretrizes e regulamentos conhecidos aplicáveis ao tratamento de dados, de acordo com a base legal, como:

- Manter os dados pessoais apenas pelo período estritamente necessário ao cumprimento da finalidade de sua utilização, estabelecendo-se prazos para a eliminação dos dados.
- Recolher dados adequados, pertinentes e limitados para os fins para os quais forem solicitados.
- Adotar medidas técnicas e organizacionais, como pseudonimização, criptografia de dados, garantia de confidencialidade, integridade, disponibilidade de sistemas, medidas de continuidade em caso de incidentes e processos de avaliação ou verificação periódica das medidas de segurança no processamento de dados.

3 Para mais informações, acesse https://www.iadb.org/es/acerca-del-bid/financiamiento-del-bid/financiamiento-del-bid%2C6028.html

4 Para mais informações, acesse https://www.cminds.co

5 fAIr LAC é uma parceria entre os setores público e privado, a sociedade civil e as universidades para incidir tanto na política pública como no ecossistema empreendedor na promoção do uso responsável e ético da IA. Mais informações em https://fairlac.iadb.org/es

2. Breve resumo do contexto na América Latina

Segundo o UNICEF-UNESCO (UNICEF, 2020), mais de 70% dos países da América Latina decidiram migrar para plataformas online de educação à distância de níveis básico e intermediário. Embora exista uma cultura de segurança na região (BID e OEA, 2020), é possível que, em vários casos, a urgência da adoção tecnológica não tenha permitido a implementação de diretrizes e protocolos de segurança cibernética.

Em termos de proteção de dados, a América Latina enfrenta desafios específicos no ambiente educacional. Somente no último ano, 67% das instituições de ensino foram vítimas de ataques cibernéticos[6], e apenas 44% (ESET, 2017) delas contam com medidas básicas de proteção. O levantamento regional revelou que apenas 5,8% dos professores sabem se sua instituição possui protocolos para casos de violação ou vazamento de dados; desse número, 25% dos professores desconhecem como esse protocolo é realizado.

Em contrapartida, de acordo com a Agência da União Europeia para a Cibersegurança (ENISA), 80% das instituições de ensino (OAS, 2020) da União Europeia contam com medidas básicas de proteção.

3. Metodologia

Para fazer um diagnóstico do estado, necessidades, desafios e oportunidades referentes à proteção de dados digitais de estudantes em âmbitos escolares na América Latina, além da pesquisa documental, foram realizadas três atividades no âmbito do projeto **Escolas seguras online**: (1) entrevistas individuais semiestruturadas, com 15 especialistas; (2) duas rodas de conversa regionais com professores de quatro países; e (3) uma pesquisa regional, da qual participaram aproximadamente 1.304 gestores e professores de sete países[7].

Para saber mais sobre a metodologia e essas colaborações, consulte o Anexo 1 deste Guia.

6 Consulte o Glossário para ver a definição de ciberataque.

7 Os países pesquisados foram: Brasil, Colômbia, Costa Rica, México, Panamá, Peru e Uruguai.

II. Cibersegurança na instituição escolar

Esta seção explora algumas questões cruciais sobre privacidade e segurança em plataformas educacionais digitais que professores e diretores podem enfrentar na transição digital dos ambientes educacionais. Conhecer estes conceitos ajuda a dar visibilidade aos riscos online relativos à proteção dos dados de seus estudantes e à importância dessa proteção.

1. O que são plataformas educacionais digitais?

Plataformas educacionais são programas da Internet[8] utilizados para conectar-se e comunicar-se com estudantes, professores, diretores e pais ou responsáveis da mesma organização escolar. Essas plataformas têm como objetivo oferecer uma experiência digital semelhante à de uma instituição de ensino. Por esse motivo, na maioria das vezes, incluem funções como ferramentas de comunicação interna (fóruns, chats e plataformas para videochamadas); funções de gestão de acesso, que permitem a cada usuário acessar apenas as áreas e funções que lhe correspondem, e os sistemas de avaliação (existem plataformas que permitem o carregamento e visualização das notas, e algumas até possuem avaliações automatizadas, entre outras funções).

2. O que acontece quando acessamos plataformas educacionais online? Existe um registro da atividade online de estudantes e professores?

Resumindo, cada vez que acessamos a Internet, geramos dados digitais que são registrados nos servidores utilizados pela plataforma que acessamos. Cada ação que realizamos online transforma-se em dados digitais. Todas as informações geradas como resultado da atividade online de uma pessoa ou, em outras palavras, todas as informações que existem na Internet sobre uma pessoa como resultado de sua atividade online são conhecidas como a pegada digital dessa pessoa.

Os dados provêm das pesquisas realizadas por uma pessoa, dos sites que ela visita e com os quais interage, e do uso de plataformas digitais. É importante que o corpo docente esteja ciente de que, ao transferir a educação para o mundo digital, está contribuindo para a criação e/ou crescimento das pegadas digitais de crianças, podendo incluir informações privadas, principalmente quando as plataformas retêm informações para traçar o perfil dos usuários e segmentá-los para fins comerciais ou outros.

8 A Internet é um sistema de comunicação entre milhões de dispositivos eletrônicos. A Internet é composta por dois atores principais: os servidores e os fornecedores.

3. Terceiros têm acesso às pegadas digitais de seus estudantes?

Plataformas de terceiros, determinados sites e plataformas Web, bem como vários aplicativos, muitas vezes coletam dados do usuário, mesmo de forma automática (LSE, 2021), às vezes sem notificar o usuário. Ao visitar sites ou usar aplicativos, existem cookies; trata-se de pequenos dados armazenados no computador do usuário que rastreiam e registram o que ele faz online, desde a análise de compras e renda até a previsão de comportamentos para desenvolver produtos ou melhorar produtos existentes com base em suas preferências.

Os cookies, juntamente com todo o ecossistema online que cruza as informações, permitem que terceiros externos acessem as pegadas digitais dos estudantes, se eles não forem cuidadosos com os sites que visitam ou com a forma em que compartilham as informações. Organizações do mundo todo exploraram as diretrizes sobre a devida gestão dos dados. Um recurso pioneiro no assunto é a "Gestão ética dos dados"[9] da fAIr LAC.

4. Por que a pegada digital de seus estudantes deve ser protegida?

Como espaço seguro, a instituição de ensino tem a obrigação de proteger os dados que, fisicamente, foram armazenados nas instituições. Obrigação que atualmente se estende aos dados digitais pessoais que fazem parte das pegadas digitais dos estudantes para protegê-los em termos de integridade e privacidade.

Uma vez que os professores utilizam plataformas educativas e recreativas para ministrar suas aulas, é importante saber que, além de utilizar os dados recolhidos pelos cookies para efeitos de melhoria da oferta, algumas dessas plataformas podem vender esses dados a empresas para personalizar a publicidade exibida online, de acordo com os interesses específicos de cada usuário, bem como para projetar produtos. Isso pode acontecer em sites e aplicativos usados por professores para ministrar suas aulas ou por estudantes em suas atividades escolares, sem saber quem tem acesso aos dados.

Usar plataformas de terceiros sem cautela pode levar à divulgação indevida de informações confidenciais, ou seja, dados privados, como o histórico socioeconômico ou a saúde mental e física de um aluno, podem tornar-se públicos. Recomendações de como ter o cuidado adequado são fornecidas abaixo.

9 Para mais informações, acesse: https://fairlac.iadb.org/es/gestion-etica-datos

5. Quais são os principais riscos enfrentados por estudantes, professores e diretores na educação digital?

Sete tipos comuns[10] de risco de *bullying* e violência que os estudantes podem enfrentar online são: *ciberbullying*, ameaças por e-mail, *flaming*, *outing*, *phishing*, assédio por externos e roubo de identidade.

A. Ciberbullying

O *ciberbullying* pode ser mais intenso que o *bullying* presencial: é o *bullying* que ocorre através de meios eletrônicos (e-mails pessoais ou escolares, chats em plataformas de videochamada, plataformas educacionais, redes sociais etc.). Na maioria dos casos, o *ciberbullying* permite o anonimato que os agressores não teriam na vida física, permitindo-lhes realizar ataques mais graves e contínuos que aqueles que os estudantes poderiam receber pessoalmente. As ameaças, a forma mais agressiva de *ciberbullying*, evidenciam o fato de que o destinatário sofrerá danos físicos ou sociais, a menos que cumpra as exigências do assediador.

B. *Ransomware*

Por outro lado, as instituições podem ser vítimas de *ransomware*, uma situação em que os cibercriminosos sequestram dados valiosos e extorquem dinheiro da pessoa ou instituição para obter ganho financeiro em troca dessas informações. De acordo com a Agência Federal de Investigação dos Estados Unidos (FBI), o ransomware é uma tendência crescente nas instituições educacionais (Governo dos Estados Unidos, 2020).

C. *Flaming*

Quando uma pessoa insulta ou agride outra pessoa em discussões exageradas ou acaloradas em um fórum online, pode ocorrer *flaming*, "assédio e ofensa levados a um nível extremo em público". Embora o controle seja relativamente simples nas plataformas escolares, é necessário considerar que esse risco pode existir em espaços fora do controle das instituições de ensino. O risco é maior se as instituições de ensino redirecionarem os estudantes para um espaço, meio ou plataforma que contenha uma seção de comentários aberta ao público, onde eles podem comentar anonimamente, como, por exemplo, quando a tarefa solicitada envolve assistir a um vídeo de uma plataforma externa à da instituição escolar.

D. *Outing*

Outing é o ato de divulgar informações compartilhadas em particular (por meio de e-mails, fotos, textos ou outras comunicações). O *outing* é especialmente doloroso quando feito no contexto de sexualidade ou orientação sexual, porque leva os adolescentes a publicarem, sem querer, informações privadas.

10 Seleção baseada no estudo da UNESCO, *School violence and bullying: global status report*, e no guia de telecomunicações do governo do México, Relatório Safe Kids Online Uruguai do UNICEF, entre outros documentos internacionais.

E. *Phishing*

Phishing é um ataque cibernético no qual o invasor se faz passar por uma pessoa ou entidade confiável, usando engenharia social e meios eletrônicos falsos para roubar dados privados, como, por exemplo, o número do cartão de crédito. Seu objetivo é fazer com que o destinatário acredite que a mensagem é algo que ele deseja ou precisa. Isso significa que é possível que uma pessoa se faça passar por estudante ou professor para enganar os alunos.

F. Assédio por estranhos

Como os estudantes têm uma forte presença online, é possível que pessoas de fora da instituição de ensino tenham acesso à comunicação com os estudantes e, consequentemente, assediem-nos. O assédio online é qualquer tipo de abuso que ocorra na Internet, facilitado pela tecnologia, como computadores, tablets, telefones celulares e outros dispositivos com acesso à Internet[11].

G. Usurpação ou simulação de identidade

No âmbito das questões tratadas neste Guia, roubo de identidade ou simulação é a criação de um perfil falso ou fazer-se passar por outra pessoa nas redes, dizendo coisas vergonhosas, obscenas ou perversas para gerar uma imagem negativa dela na Internet.

11 O assédio pode acontecer em qualquer local online que permita a comunicação digital, como redes sociais, mensagens de texto e aplicativos de mensagens, e-mail e mensagens privadas, chats online, comentários nos sites de transmissão ao vivo e chat de voz nos videogames, entre outros.

6. Qual é o risco de terceiros externos à instituição escolar acessarem os dados digitais dos estudantes e da equipe?

O fato de as plataformas digitais comercializarem os dados obtidos em atividades educacionais é, em várias ocasiões, ilegal e compromete a finalidade social do ensino. É alarmante que, para ter acesso à educação, uma criança ou adolescente seja constantemente vigiado ao compilar tantas informações privadas, íntimas e sigilosas, principalmente quando são utilizadas para bombardeios de propagandas que não têm nada a ver com atividades pedagógicas. Além disso, deve-se lembrar que, em alguns países e em certas circunstâncias, a publicidade dirigida especificamente a crianças é abusiva (OCDE, 1999) e, portanto, deveria ser ilegal[12].

O risco de escolas e colégios sofrerem ataques cibernéticos ou coleta de dados é alto, dadas as informações pessoais que gerenciam de estudantes, professores e toda a equipe de ensino. As instituições geralmente possuem dados de documentos de identidade, registros acadêmicos, históricos médicos, calendários com horários específicos e até dados financeiros e previdenciários, o que acarreta um alto risco de acesso e roubo de dados internos (ESET, 2017). De acordo com o relatório da ESET de 2017, o estudo da região com a análise mais recente, 67% dessas instituições na América Latina foram vítimas de pelo menos um ataque cibernético[13].

Nada disso é motivo para rejeitar a tecnologia. As instituições de ensino podem tomar medidas para mitigar os riscos derivados de sua operação no ambiente digital, bem como assumir responsabilidades pela segurança informática de sua organização.

Na próxima seção, discutiremos as práticas que podem ser implementadas para tornar as instituições de ensino online seguras.

12 Quase nenhum país da América Latina penaliza essa ação no âmbito de um Código legal. Um bom exemplo desse tipo de lei é a Lei de Proteção da Privacidade Online (COPPA) dos Estados Unidos, que se aplica à compilação online de informações pessoais por parte de pessoas ou entidades sob a jurisdição estadunidense.

13 De acordo com a Organização para a Cooperação e o Desenvolvimento Econômicos (OCDE), um ciberataque é uma tentativa ativa, maliciosa e deliberada feita por uma pessoa, grupo ou organização para invadir um sistema de informação de qualquer pessoa, instituição ou Estado.

III. Boas práticas que podem ser aplicada

As ações a seguir destinam-se a instituições de ensino e seus profissionais. Estas recomendações são baseadas nas melhores práticas internacionais e incluem todas as ferramentas existentes até o momento para que possam ser adotadas por instituições de ensino a fim de proteger os dados digitais de seus estudantes. Embora o Guia seja voltado principalmente para professores e pessoas em funções de gestão, ele também oferece ações que incluem os pais, mães ou responsáveis, e que também podem ser realizadas diretamente pelos estudantes.

A seguir, são apresentados os três atores que desempenham um papel na garantia da privacidade dos dados de menores em ambientes escolares e um breve panorama de suas responsabilidades. Esta sessão é dividida em três partes:

- • As decisões a serem tomadas e as boas práticas a serem adotadas pela diretoria em conjunto com a equipe pedagógica da instituição.
- • Boas práticas de transparência e comunicação constante de diretores e professores com pais, mães e estudantes.
- • Boas práticas para diretores, professores e estudantes.

Gestor(a) (Ge)	Professor(a) (Pr)	Pais ou responsáveis (Es)
• Principal responsável pela gestão escolar. • Desempenha um papel central na articulação da comunidade educacional. • Sua função é liderar e facilitar uma série de processos dentro da instituição de ensino.	• Oferece ensino e atendimento em sala de aula. • Orienta os estudantes em seu processo de aprendizagem. • Fornece informações relevantes e oportunas.	• Líderes no processo de aprendizagem do estudante. • Transmitem valores. • Preocupam-se com a educação integral de seus filhos, incluindo o plano de proteção digital.

As recomendações para as seguintes ações compartilhadas são codificadas por cores, dependendo do ator responsável por implementá-las ou segui-las. As recomendações terão uma etiqueta laranja para gestores, amarela para professores e verde para pais ou responsáveis/estudantes.

1. Decisões a serem tomadas e boas práticas a serem adotadas pela diretoria e pela equipe pedagógica da instituição

Esta seção inclui cinco subseções que ajudarão os grupos de gestão a estabelecer uma boa governança de dados dentro de sua instituição.

Ge			A. Atribuir a uma pessoa ou grupo de pessoas, conforme necessário, a responsabilidade de zelar pelo cumprimento das tarefas estabelecidas.

O direito à proteção da privacidade no que diz respeito aos dados digitais do estudante começa com seu tratamento responsável, conhecendo-se o ciclo que os dados seguem em todas as suas fases e identificando-se quem pode utilizá-los ou processá-los, para quê e por quê.

A instituição de ensino pode proteger a privacidade da comunidade educacional, tendo clareza em relação às plataformas utilizadas e nomeando os responsáveis por: a) cada uma das fases (coleta, armazenamento, uso, acesso e eliminação) dos dados digitais e b) usar plataformas Web próprias da instituição de ensino, bem como externas.

O(a) diretor(a):

a. Distribui entre seus funcionários as responsabilidades pela gestão dos dados digitais dos estudantes, professores e toda a equipe da instituição de ensino. Também pode considerar a abertura de novas vagas para tratar da privacidade. Pode ser um(a) oficial de privacidade, como, por exemplo, um(a) especialista em gestão de dados.

b. Estabelece processos de uso, seleção e controle de plataformas Web e aplicativos que são utilizados no ambiente escolar, tanto para ministrar aulas online quanto para apoiar atividades educacionais dos estudantes a fim de reforçar conhecimentos, desenvolver habilidades, aprender brincando etc.

c. Continua aprendendo para exercer uma governança institucional correta sobre os dados. Por esse motivo, é aconselhável estudar recursos que proponham como dimensionar o impacto de uma organização por meio do uso de tecnologia, como o recurso "Gestão ética dos dados"[14] da fAIr LAC.

d. Conta com protocolos ou diretrizes sobre o uso adequado das tecnologias da informação e da comunicação por professores, gestores e administradores.

14 Para mais informações, acesse: https://fairlac.iadb.org/es/gestion-etica-datos

O relatório *Cost of a Data Breach Report 2020*, realizado pelo Instituto Ponemon em conjunto com a IBM, destaca que o tempo médio que uma organização leva para identificar e conter uma violação de dados em todo o mundo é de 280 dias. Na América Latina, o tempo médio é de 328 dias, o que confirma que as organizações que não possuem controles que permitam detectar incidentes de segurança em tempo suficientemente hábil não terão a capacidade de responder e contê-los.

Essa situação é evidente nas instituições de ensino, que, por não possuírem mecanismos de monitoramento suficientes que lhes permitam identificar uma violação de dados ou um ciberataque em andamento, de forma alguma podem afirmar que eles não estão acontecendo e, na melhor das hipóteses, poderiam apenas argumentar que não estavam cientes.

Ge			B. Implementar sistemas de segurança em dispositivos para evitar vazamentos de dados ou acessos não autorizados (confira os exemplos no Anexo 2).

Uma das formas de prevenir a violação da privacidade dos estudantes, bem como de toda a comunidade educacional cujos dados a instituição de ensino coleta e utiliza, é por meio da adoção de sistemas de segurança nos dispositivos utilizados para fins educacionais. Para isso, é necessário:

a. Considerar a possibilidade de destinar recursos à instalação dos referidos sistemas de segurança, visto que pode ser necessário estipular um orçamento (confira o Anexo 2 para conhecer alguns dos sistemas e ferramentas de segurança cibernética que podem ser implementados na instituição de ensino).

b. Considerar outras práticas simples que melhorarão a segurança e a proteção da privacidade:

   i. Certificar-se de contar com e promover boas práticas de acesso, de forma que seja utilizado um mecanismo que permita a identificação dos estudantes, como higienização de senhas e autenticação em dois fatores ou duas etapas (ver Anexo 3). Evitar processos de autenticação que envolvam o uso de biometria (reconhecimento facial ou impressão digital), pois não é proporcional aos fins escolares. As senhas dos e-mails e das plataformas das escolas são as chaves para a vida digital. Tomar as medidas adequadas para ter uma senha forte é fundamental para proteger os dados dos estudantes e equipes de ensino (INCIBE, 2016)[15].

   ii. Algumas plataformas permitem que o aplicativo seja configurado de acordo com as políticas de senha da entidade educacional.

15 Há também outras boas práticas cíclicas na Seção 3: Boas práticas para equipes de ensino, professores e estudantes, na página 19.

Ge			C. Criar um plano para gerenciar a comunicação de uma violação de dados ou acesso não autorizado.

Além das práticas adequadas de identificação, avaliação e gestão de riscos, e das políticas de prevenção e mitigação referentes aos dados digitais, também é aconselhável traçar um plano de resposta em caso de contingências que inclua protocolos que permitam garantir a continuidade dos negócios e que seja capaz de lidar com uma violação de segurança e responder a um ataque cibernético e suas consequências.

Informações relevantes podem ser encontradas nos cinco pontos a seguir.

? Como saber se houve vazamento de dados e como reagir?

Perceber um vazamento é difícil, pois geralmente ele é feito silenciosamente. Um elemento essencial para detectar e responder em tempo hábil a um incidente de segurança é o monitoramento da segurança cibernética, que deve dar visibilidade aos eventos que ocorrem na infraestrutura tecnológica da instituição, como, por exemplo, suas redes, suas plataformas virtuais ou seus aplicativos, ou seja, que tenha a capacidade de detectar e monitorar os diferentes elementos que coletam, processam, resguardam ou transmitem informações sigilosas da comunidade educacional e dos sistemas ou plataformas que suportam e permitem o trabalho educacional (para mais informações, veja o Anexo 2).

Caso a instituição de ensino tenha sofrido um incidente cibernético, não se deve presumir automaticamente que houve uma violação de dados; e, caso tenha ocorrido uma violação, ela pode ou não ser notificada. Isso dependerá dos quadros regulamentares de cada país.

Um exemplo de padrão de regulamentação de proteção de dados é o Regulamento Geral de Proteção de Dados (RGPD) da União Europeia. Em geral, para que uma violação seja notificada à autoridade de controle, deve haver um risco provável para os indivíduos (por exemplo, roubo de dados da folha de pagamento, que pode levar a perdas financeiras).

Antes de entrarmos em mais detalhes sobre as principais características de uma violação de dados, um breve resumo é compartilhado abaixo:

1. Uma violação de dados evolui rapidamente e requer uma resposta igualmente rápida para evitar mais perdas.

2. Existem muitas partes interessadas, o que torna a comunicação um elemento-chave de qualquer plano de preparação para enfrentar violações de dados.

3. A privacidade, identidade ou interesses financeiros dos funcionários da escola, pais ou responsáveis e estudantes podem ser comprometidos em uma violação de dados. É responsabilidade do centro do ensino proteger as partes interessadas.

4. Quando se trata de relatar uma violação de dados (dependendo da região), dispõe-se de 72 horas para informá-la ao órgão regulador. Aqui, o tempo é tudo.

5. Sem um plano, coloca-se em risco a comunidade e a reputação da escola.

O que fazer se houver um vazamento de bancos de dados com informações confidenciais?

É importante agir o mais rápido possível (INCIBE, 2012) durante todo o protocolo. Esta tabela indica a resposta imediata a um incidente. O Anexo 4 apresenta um protocolo geral para prevenção e para evitar situações de urgência e emergência.

Ações	Passo a passo
1. Buscar a detecção precoce do incidente sempre que possível, para iniciar imediatamente o protocolo de ação correspondente (confira o protocolo de resposta a incidentes no Anexo 4).	a. Determinar que dados são afetados e sua quantidade. b. Estabelecer a causa do vazamento, seja ela de origem técnica ou humana.
2. Realizar o processo de avaliação inicial do incidente assim que as informações acima forem conhecidas e determinar as etapas a serem seguidas.	c. Determinar ações para encerrar o vazamento e evitar novos vazamentos. d. Traçar o plano de comunicação do incidente e dos afetados, somente se necessário, conforme os dados comprometidos. e. Fazer uma estimativa do impacto: danos à reputação, legais, financeiros ou outros.
3. Executar o plano de ação.	f. Terminar a violação de segurança por meio da desconexão de um serviço ou sistema, dependendo da origem do vazamento de dados. g. Caso os dados tenham sido publicados, localizar onde foram publicados e tomar as medidas necessárias para solicitar sua imediata exclusão. Informar o incidente aos professores, estudantes e pais e mães. Em caso de vazamento de dados sigilosos, informar, também, que dados foram afetados, para que as ações de segurança correspondentes possam ser tomadas.

O que fazer se houver uma invasão indesejada em uma sala de aula virtual?

Junto com o aumento da utilização de plataformas de videoconferência, que passaram a funcionar como salas de aula virtuais devido à suspensão das aulas presenciais devido à COVID-19, também surgiu o denominado Zoombombing (Conselho Escolar Conejo Valley, 2020), no qual pessoas indesejadas entram em sessões virtuais e mostram conteúdo impróprio

(pornográfico ou racista, por exemplo), independentemente da presença de menores. Aqui estão algumas maneiras de evitar o risco e, caso se materialize, mitigá-lo.

Prevenção	Mitigação
- Usar uma plataforma de videoconferência que permita ajustes de segurança. - Certificar-se de que a videoconferência seja privada por meio de uma senha de reunião ou sala de espera para permitir a entrada manualmente. - Não compartilhar o link ou ID da reunião publicamente, como, por exemplo, em redes sociais. De preferência, gerar uma senha única para cada reunião. - Configurar a sessão para que apenas uma pessoa designada possa compartilhar a tela. Assim, se um usuário indesejado entrar, não poderá exibir nenhum vídeo ou imagem na tela principal. - Realizar simulações periodicamente na escola. Assim, pode-se garantir que todos os professores estejam preparados para o caso de uma pessoa indesejada entrar em sua aula online.	- Assim que for identificado que existe uma pessoa indesejada na sessão virtual, o anfitrião ou a pessoa designada para controlar as permissões em uma videochamada deverá expulsar o intruso o mais rápido possível. - Para remover pessoas indesejadas, algumas plataformas permitem remover participantes indesejados da sessão. No menu *Participantes*, posicione o cursor sobre o nome do participante que deseja excluir, para que sejam exibidas várias opções de ações a serem realizadas, como *Excluir*. Clique para tirá-lo da sessão. - Se demorar para identificar a pessoa indesejada, é recomendável encerrar a videochamada.

Como informar os pais, mães e os estudantes afetados quando ocorrer uma violação de segurança?

As violações de segurança podem prejudicar a imagem da instituição escolar, além de colocar em risco estudantes e professores. Em caso de vazamento de dados sigilosos, é importante notificar os pais, mães e os estudantes, informando-os sobre os dados afetados, para que possam tomar as ações de segurança correspondentes (confira a base do protocolo de notificação de incidentes no Anexo 5).

Em que casos informar as autoridades?

Se a violação de segurança em questão violar gravemente dados pessoais que possam afetar a integridade do estudante, será necessário comunicar o incidente às "forças e órgãos de segurança, sejam locais, regionais ou nacionais, dependendo do cenário. Por outro lado, será feita a denúncia do incidente e demais ações que venham a surgir a partir da coordenação da solicitação de informações pelas forças e órgãos de segurança" (INCIBE, 2012).

É necessário, também, levar em consideração a possibilidade de informar os órgãos e autoridades correspondentes que possam ter poderes derivados das informações vazadas, como, por exemplo, oficiais de proteção de dados (Arias Ortiz e Cristia, 2014) nomeados em órgãos governamentais, a área correspondente do Ministério da Educação ou conforme estabelecido na legislação de cada país.

Ge			D. Selecionar as ferramentas permitidas para a comunicação digital entre professores e estudantes (diretrizes do diretor).

As instituições educacionais exigem produtos e serviços de terceiros que são indispensáveis para a educação online. No entanto, na medida do possível, é responsabilidade da instituição de ensino assegurar que os produtos e serviços que decida utilizar contem com as devidas proteções para os dados de seus estudantes, ou seja, que disponham de garantias suficientes para aplicar medidas técnicas e organizacionais adequadas, de forma que o tratamento dos dados esteja de acordo com o quadro regulamentar cabível.

Quais seriam os critérios de seleção de uma plataforma em termos de privacidade e segurança?

Antes de utilizar qualquer serviço tecnológico, sejam plataformas, sites ou aplicativos, com os estudantes ou envolvendo seus dados, é necessário ler os Termos e Condições de Uso e a Política de Privacidade[16], ou, se for o caso, o contrato firmado, e garantir a existência de certas garantias, como estas:

- Os dados serão processados apenas de acordo com as instruções da instituição escolar.
- Os dados não serão usados para finalidades diferentes das acordadas.
- As medidas de segurança para proteção dos dados serão detalhadas.
- Os dados serão devolvidos ou apagados assim que o contrato ou a utilização da plataforma finalizar.

Apesar da linguagem jurídica ou técnica que esses documentos digitais costumam utilizar, aceitá-los antes de utilizar um serviço é semelhante a assinar um contrato que envolve certas obrigações e até cede certos dados, e, portanto, é necessário que os pais, mães ou responsáveis e os professores tenham conhecimento do que está envolvido no uso de um serviço. O Anexo 6 contém diversas questões que facilitarão a leitura dos Termos e Condições de Uso e da Política de Privacidade para destacar os critérios que devem ser levados em consideração na seleção de serviços tecnológicos para uso escolar e garantir a proteção da privacidade e segurança dos dados digitais de seus estudantes.

Quais são as plataformas e ferramentas de comunicação autorizadas pela instituição escolar?

Uma vez que os critérios ideais de seleção de um serviço digital para uso escolar tenham sido revistos, recomenda-se que a instituição de ensino elabore uma lista oficial das plataformas e ferramentas de comunicação autorizadas entre professores e estudantes (confira no Anexo 7 uma análise das plataformas existentes). Essa lista seria pública, para que todos da comunidade educacional (pais, mães, professores e estudantes) saibam quais são as plataformas e aplicativos permitidos e limitem os estudantes a utilizarem apenas esses serviços tecnológicos, o que permitirá à instituição de ensino ter um melhor controle da proteção dos dados

16 O conteúdo de aviso de privacidade varia de país para país. É necessário verificar o regulamento nacional antes de aceitar os termos e condições.

digitais dos estudantes, bem como da gestão do risco, caso danos sejam gerados.

Além disso, os pais e responsáveis devem receber informações básicas, claras e concisas sobre os termos e características dos serviços contratados, as finalidades do tratamento dos dados e as políticas de privacidade e proteção dos referidos prestadores. A necessidade de um novo consentimento dependerá de cada legislação, pois alguns pais ou responsáveis podem não saber claramente quais são os dados relativos a seus filhos que podem ser coletados ou deduzidos através das plataformas, nem como eles podem ser utilizados.

Ge			E. Adaptar o regulamento da instituição de ensino para incluir questões digitais.

Como o uso de plataformas digitais está imerso na rotina escolar, é importante incluir tópicos específicos no regulamento da instituição de ensino, para que haja diretrizes claras e um espaço digital seguro possa começar a ser criado para seus estudantes, bem como para todos os funcionários da escola. O Anexo 8 fornece sugestões de seções que podem ser incluídas nos regulamentos da escola em relação a questões digitais.

É importante que esses regulamentos estabeleçam regras e penalidades para os estudantes que se envolverem em atividades como ciberbullying, outing ou flaming, antes que qualquer incidente ocorra.

2. Boas práticas de transparência e comunicação constante de diretores e professores com pais, mães e estudantes

Embora seja importante que a instituição de ensino conte com todas as medidas possíveis para proteger a segurança e privacidade dos dados digitais de seus estudantes, também é uma tarefa que exige comunicação constante e transparência com toda a comunidade de ensino, inclusive os estudantes, pais e mães, em relação à coleta, uso, armazenamento, tratamento e eliminação de seus dados. Para isso, podem ser adotadas as seguintes boas práticas, que permitirão que a comunidade educacional se mantenha informada de forma pertinente e faça a diferença no uso e tratamento ético dos dados.

Ge	Pr		A. Exigir assinatura (física ou digital) do regulamento: atualizado com tópicos digitais pelos pais ou responsáveis dos estudantes menores de idade e pelos estudantes maiores de 18 anos. Recomenda-se uma assinatura geral do diretor e uma por sala de aula por parte do professor.

Carta de notificação aos pais e mães

Além de dispor do regulamento escolar atualizado sobre questões digitais, este deve integrar os protocolos de emergência para que pais ou responsáveis e estudantes se mantenham informados. Utiliza-se um protocolo para selecionar as plataformas Web e aplicativos para uso no ambiente escolar, sendo aconselhável contar com uma lista oficial dessas plataformas e aplicativos. Também é importante destacar a questão da notificação e consentimento quando se trata de dados digitais. Para usar plataformas Web e aplicativos que requeiram dados dos estudantes, recomenda-se que haja uma carta de notificação aos pais e mães sobre que tipos de dado digital as ferramentas tecnológicas que seus filhos utilizarão em qualquer atividade escolar coletam.

Contar com uma análise prévia das plataformas Web e aplicativos autorizados pela instituição escolar facilitará tomar ciência dos detalhes dos dados digitais que são coletados para notificá-los aos pais e mães. O Anexo 9 contém uma proposta de carta de notificação para esses casos.

Formação contínua e campanha de informação sobre o assunto

Adquirir habilidades para habitar um mundo digital não é mais um assunto opcional. Tanto professores como estudantes exigem capacitação constante sobre os riscos relacionados aos dados digitais que esse mundo traz. É aconselhável estabelecer prazos (mensais, semestrais ou anuais) para uma formação contínua da equipe pedagógica (diretores, professores e estudantes), incluindo sessões de informação para pais e mães com o objetivo de conscientizá-los sobre a importância de proteger os dados digitais.

Essa formação pode ser reforçada com uma estratégia de comunicação sobre questões de proteção dos dados digitais que convidem à reflexão e informem sobre os riscos e como mitigá-los. O Anexo 10 oferece recursos de apoio para administradores e professores na realização de atividades e oficinas com estudantes e seus pais e mães.

Uma estratégia de comunicação cujo objetivo seja informar sobre a importância de proteger os dados digitais é um passo importante na conscientização em relação ao assunto. Uma campanha informativa dessa natureza deve ser dirigida aos estudantes, pais e mães, pois estes desempenham um papel importante no acompanhamento da aprendizagem dos filhos, uma vez que o uso digital aumentou com a transição para a virtualidade promovida pela COVID-19 (UNICEF, 2020b). O Anexo 11 menciona os temas relevantes para a realização de uma campanha de informação sobre o assunto.

Depois de receber o treinamento, os estudantes devem ser capazes de:

1. Reconhecer um e-mail que não seja institucional.
2. Evitar conversar na Internet com estranhos.
3. Respeitar os outros em espaços virtuais.
4. Reconhecer quando não devem compartilhar informações em plataformas não autorizadas.
5. Saber como reconhecer um site que contém informações legítimas.

3. Boas práticas para gestores, professores e estudantes

No Item III, 1, são abordadas recomendações para decisões de alto nível a serem tomadas pelos diretores. As recomendações a seguir são ações direcionadas a esse pessoal, bem como aos professores e estudantes.

Ge	Pr	Es	
			Certifique-se de que os diretores, professores e estudantes adotem as melhores práticas regulares em dispositivos para uso escolar.

Além das boas práticas dentro da instituição escolar e aquelas destinadas a informar estudantes e seus pais e mães, há uma série de práticas cíclicas que se recomenda ter em mente ao navegar online. São práticas simples de realizar em escolas e colégios, mas também é necessário convidar estudantes e seus pais e mães a realizá-las como medidas de proteção dos dados digitais.

Abaixo estão as melhores práticas cíclicas referentes à navegação digital, plataformas Web e aplicativos para uma maior proteção dos dados.

Atualizar sistemas operacionais e programas instalados

Manter os sistemas operacionais e aplicativos dos aparelhos da escola ou colégio atualizados, assim como os antivírus e as versões dos navegadores, pois as atualizações costumam incluir mudanças importantes que melhoram o desempenho e a segurança dos computadores. Muitos deles fazem isso automaticamente; é apenas uma questão de aceitar essa atualização quando notificada. Por isso, a comunidade escolar, professores, estudantes, pais e mães também devem ser informados sobre a importância de fazer isso em computadores pessoais, telefones celulares e tablets usados por estudantes e professores em casa (Governo do México, 2020).

Fazer cópias de segurança

A realização de cópias de segurança regulares dos dados é uma medida que deve ser ampliada (INCIBE, 2017) em todas as instituições de ensino. Isso permitirá recuperar os dados em caso de perda.

Para fazer cópias de segurança, é necessário:

- Identificar os dados que precisam ser preservados.
- Estabelecer a frequência dos processos de cópia e contar com dispositivos de armazenamento.
- Controlar o acesso aos dispositivos de armazenamento de cópias.

Alterar senhas

Além de definir senhas fortes (ver Anexo 3), recomenda-se alterá-las periodicamente, uma vez que os hackers têm formas de desencriptá-las e, portanto, a alteração geralmente oferece uma maior proteção. Por isso, nas instituições de ensino, é importante estabelecer um período de renovação de senhas, principalmente nos sites ou serviços que contenham dados de estudantes.

Excluir histórico e cookies

Sabendo-se que os cookies armazenam dados sobre a nossa navegação na Internet, é aconselhável excluí-los quando terminarmos de usar o navegador ou marcar uma data para excluí-los periodicamente.

- Se algum site estiver aberto, a combinação de teclas Ctrl + Shift + Del abre diretamente a janela para limpar os dados de navegação.
- Outra forma de excluir esses dados depende do navegador usado. As recomendações encontram-se no Anexo 5.

Verificar se o endereço de e-mail indica "HTTPS"

O protocolo de transferência de hipertexto (Hypertext Transfer Protocol Secure ou HTTPS, na sigla em inglês), um protocolo de Internet que protege as conexões dos usuários em sites, pode ser adotado, para que a experiência online seja segura e privada. Isso envolve várias etapas que podem ser exploradas neste site[17].

Precauções ao usar computadores compartilhados

Os computadores compartilhados podem ser encontrados em diferentes tipos de ambiente: um computador compartilhado em residências, instituições educacionais e até mesmo em livrarias públicas ou cibercafés. Para usá-los com segurança e sem compartilhar acidentalmente informações confidenciais com usuários que continuam seu uso, é recomendado:

- Nunca salvar senhas que são preenchidas automaticamente nem pressionar "lembrar".
- Sempre encerrar a sessão em todos os sites que tiver acessado.
- De preferência, usar o "modo de navegação anônima".
- Evitar usar computadores compartilhados para realizar procedimentos que envolvam o uso de informações pessoais ou confidenciais (transferência bancária, formulários de centros médicos etc.).

Implementar o controle parental

Uma ferramenta que pode ajudar na segurança de crianças online é o controle parental, que serve para cuidar da navegação na Internet, afastando-as de conteúdos inadequados. Os

17 Para mais informações, acesse: https://developers.google.com/search/docs/advanced/security/https?hl=es

implementadores desse controle (professores, pais, mães ou responsáveis) podem bloquear determinados sites e categorias de informações, além de restringir os downloads. Este último ponto aumenta a segurança do dispositivo contra softwares maliciosos (também conhecidos como malwares) e vírus. É especialmente recomendado para menores de 14 anos (Grupo Ático, 2020).

Alguns controles parentais podem rastrear conversas em vários sites, ajudando, assim, a combater o ciberbullying.

Usar redes Wi-Fi com segurança

Com as aulas online, a recomendação de aplicar medidas de segurança da rede na casa dos estudantes torna-se ainda mais urgente. Garantir que a rede Wi-Fi exija uma senha sempre que um novo dispositivo se conectar pela primeira vez ajudará a evitar que usuários não autorizados entrem na conexão (Governo da Espanha, 2021).

Ao mesmo tempo, é recomendável evitar o uso de redes Wi-Fi públicas para compartilhar conteúdo sigiloso, uma vez que outros dispositivos conectados à mesma rede podem capturar as informações transmitidas.

Anexos

Anexo 1. Metodologia

1. Pesquisa regional para professores

No âmbito das atividades de pesquisa deste projeto, foi elaborada a Pesquisa regional sobre a perspectiva de professores(as) e diretores(as) de instituições de ensino sobre a proteção de dados dos estudantes. A pesquisa buscou entender o nível de informação que professores e diretores têm sobre a questão da privacidade dos dados de crianças em ambientes escolares. Mais de 100 professores de sete países latino-americanos foram entrevistados[18]. Essa é a única pesquisa do gênero na região e serviu de recurso para a seleção do conteúdo relevante deste Guia.

Total de entrevistados:
1304 professores

México, **323 respostas**
Costa Rica, **207 respostas**
Panamá, **159 respostas**
Colômbia, **323 respostas**
Peru, **245 respostas**
Brasil, **18 respostas**
Uruguai, **29 respostas**

Nota importante: sempre que a pesquisa regional é mencionada neste texto, faz-se referência à Pesquisa regional sobre a perspectiva de professores(as) e diretores(as) de instituições de ensino sobre a proteção de dados dos estudantes.

2. Conversa com professores e diretores latino-americanos

Foi realizado uma roda de conversa com professores da Argentina, Equador, México e Peru para entender os desafios que enfrentaram na transição digital, suas experiências e preocupações, a fim de integrá-los a este Guia. Os participantes podem ser encontrados na seção Agradecimentos, no início do documento.

3. Entrevistas com especialistas em educação, sistema educacional e questões de privacidade na América Latina

Como parte do projeto ***Escolas Seguras Online***, 15 entrevistas foram realizadas com especialistas em educação, sistema educacional e questões de privacidade na América Latina e internacionalmente, para aprendermos sobre as melhores práticas, desafios atuais e considerações de alto nível. Os participantes são mencionados na seção Agradecimentos, no início do documento.

18 Total de entrevistados: 1304 professores, distribuídos assim: Brasil, 18 respostas; México, 323 respostas; Colômbia, 323 respostas; Costa Rica, 207 respostas; Panamá, 159 respostas; Peru, 245 respostas, e Uruguai, 29 respostas.

Anexo 2. Recomendações de sistemas e ferramentas de segurança cibernética

a) Segurança cibernética organizacional

1. Monitoramento preventivo[19]

O monitoramento da segurança cibernética pode ser entendido como um processo-chave na detecção em tempo hábil de ameaças cibernéticas e violações de dados, a fim de responder antes que causem danos ou interrupções em maior escala. É importante que a instituição de ensino decida se realizará esse processo internamente ou se contratará o apoio de um terceiro especializado.

Em ambos os casos, a instituição deve garantir que o pessoal responsável tenha:

- Clareza sobre seu papel, funções e o tempo necessário para a realização dessa atividade.
- Treinamento suficiente para a interpretação de eventos a fim de determinar a gravidade dos incidentes de segurança.
- Treinamento próprio do fabricante da solução de monitoramento escolhida (se aplicável).
- Processos e protocolos claramente definidos, descritos e implementados para notificar, dimensionar e responder a um incidente de segurança cibernética.
- Suporte do fabricante em caso de falha na solução ou consultoria sobre dúvidas dos eventos que forem identificados.

Em qualquer uma das opções acima, é importante fazer uma seleção adequada da solução de monitoramento de segurança cibernética. A seguir, alguns critérios que devem ser levados em consideração:

- Visibilidade em tempo real.
- Priorização de ameaças.
- Análises de dados.
- Notificações automáticas.
- Alimentação por fontes de inteligência.
- Integração com outras plataformas de rede ou segurança.
- Criação de uma base do protocolo de resposta a incidentes.

Antes de compartilhar informações com terceiros, é importante que as instituições educacionais considerem as práticas de dados dos provedores de serviços para manter a confidencialidade e segurança dos dados e impedir o acesso ou uso não autorizado das informações. É

19 Esta seção foi redigida com inputs da Capa 8, Escolas Ciberseguras. Para mais informações, acesse: https://capa8.com/

importante que esses terceiros consigam manter a confidencialidade e segurança das informações, principalmente no que se refere aos dados de menores. Por sua vez, recomenda-se que a instituição de ensino firme contratos de privacidade de dados com terceiros que tenham acesso a eles, conforme indicado na Lei de Proteção à Privacidade Online para Crianças (COPPA - Children's Online Privacy Protection Act dos Estados Unidos).

b) Segurança cibernética técnica

1. Proteção na conexão de rede: firewall para todos os equipamentos de uso escolar

Recomenda-se ativar funcionalidades de proteção, como firewalls, incorporadas aos sistemas operacionais mais comuns. Um firewall é a primeira linha de defesa contra um ataque de rede e protege o computador contra programas mal-intencionados ou invasores que tentam se conectar a ele remotamente. Além disso, permite estabelecer regras para indicar quais conexões de rede devem e não devem ser aceitas.

Sistemas operacionais como Windows, Mac[20] ou Linux incluem firewalls gratuitos.

2. Proteção dos dispositivos: antivírus

É importante instalar e atualizar um antivírus em todos os dispositivos eletrônicos, pois é a única forma de detectar e destruir um vírus; ele pode ser encontrado no computador, se o conteúdo tiver sido baixado da Internet.

- Dois antivírus não implicam mais segurança e, por isso, é recomendável investir em um antivírus que ofereça garantias de segurança consideráveis.
- Ao instalar e atualizar o antivírus, é recomendável baixá-lo do site oficial, nunca de um site de origem duvidosa.

20 As equipes que utilizam Mac contam com firewalls de alto rendimento e, por esse motivo, pode-se pensar (SAIGAL, 2020) que não é necessário fazer o download, mas é recomendável ter uma proteção dupla.

Anexo 3. Protocolo de boas práticas de acesso: higiene de senhas e autenticação em dois fatores

De acordo com o Escritório de Segurança do Internauta (OSI - Oficina de Seguridad del Internauta) do Instituto Nacional de Ciberseguridad (INCIBE) da Espanha, existem quatro características para que as senhas sejam as mais seguras possíveis.

Recomenda-se que as senhas sejam:

1. **Secretas.** Compartilhar senhas com outras pessoas viola a segurança das informações, pois outra pessoa teria acesso a elas.

2. **Fortes.** Uma senha com medidas fortes protege a nossa privacidade em maior grau, pois dificulta o acesso de outra pessoa. De acordo com o OSI do INCIBE[21], a senha deve:

   - Conter pelo menos oito caracteres.
   - Não conter o seu nome ou nome de usuário, nem a escola onde você estuda ou trabalha, mesmo que só parcialmente.
   - Não conter palavras do dicionário.
   - Não incluir informações pessoais: data e/ou local de nascimento, número do documento de identidade, número de telefone, datas especiais etc.
   - Não ser formada com números e/ou letras adjacentes no teclado.
   - Conter caracteres de cada um dos seguintes grupos: letras maiúsculas, letras minúsculas, números e caracteres especiais.

3. **Únicas para cada site ou serviço.** Usar a mesma senha para todos os sites ou serviços que utilizamos implica uma maior vulnerabilidade da nossa privacidade, pois, se alguém decifrar a senha, isso permitirá o acesso a todas as nossas contas. Basta fazer uma ligeira variação com base na senha de cada site, para que não seja muito difícil memorizá-las.

4. **Alteradas periodicamente.** Uma vez que os hackers têm formas de descobrir as senhas, é aconselhável alterá-las periodicamente. No caso de instituições de ensino, é especialmente importante estabelecer um período de renovação das senhas nos sites ou serviços que contenham dados de estudantes.

Além disso, sempre que possível, é recomendável usar a verificação ou autenticação em duas etapas ou a autenticação multifator (MFA, na sigla em inglês). Trata-se de um sistema de segurança que requer mais de uma forma de autenticação para verificar a legitimidade de uma transação. O objetivo da MFA é criar uma defesa em camadas e tornar mais difícil para uma pessoa não autorizada acessar um alvo, como uma localização física, um dispositivo eletrônico, uma rede ou um banco de dados. Em outras palavras, se um dos fatores estiver comprometido ou for quebrado, o invasor ainda tem pelo menos mais uma barreira para romper antes de entrar com sucesso no alvo.

21 Para mais informações, acesse: https://www.osi.es/es/actualidad/blog/2013/12/05/creando-contrasenas-robustas

Em particular, a autenticação em duas etapas fornece mais proteção contra acessos não autorizados a uma conta, uma vez que, além da senha, um código deve ser inserido. Esse código chega por e-mail, gerado em um aplicativo, ou por mensagem de texto SMS para o celular do usuário, dependendo da escolha do usuário no processo de estabelecimento da autenticação em duas etapas. Você também pode selecionar se deseja usar a MFA apenas para acessar uma conta usando um novo dispositivo ou de vez em quando. Alguns serviços permitem a verificação em duas etapas em seus serviços[22].

Geralmente, a MFA combina duas ou mais credenciais independentes: o que o usuário sabe (senha), o que o usuário possui (token de segurança) e o que o usuário é (verificação biométrica), conforme exemplificado na tabela a seguir:

Algo que eu saiba	Algo que eu tenha	Algo que eu seja
Uma senha: - Um número de telefone - Uma data de nascimento - Um endereço - Nome de qualquer animal de estimação	Token de segurança ou senha enviada por: - SMS - Mensagem por aplicativo - E-mail	Dados biométricos[23]: - Identificação facial - Identificação de impressão digital - Outros

Mais informações em "Tudo o que você precisa saber sobre senhas"[24] do INCIBE.

22 Para mais informações, acesse: https://www.google.com/landing/2step/?hl=es_419#tab=how-it-works

23 São as propriedades físicas, fisiológicas, comportamentais ou traços de personalidade. São atribuíveis apenas a uma pessoa e são mensuráveis.

24 Para mais informações, acesse: https://www.incibe.es/sites/default/files/contenidos/blog/antes-pyme-con-contrasenas-fuertes-que-sencillas/infografia-contrasenas-para-pymes.png

Anexo 4. Base do protocolo de resposta a incidentes

Existem vários tipos de incidente cibernético que podem ocorrer em uma instituição escolar. A resposta a ser dada dependerá da legislação de cada país, mas o "Esquema Nacional de Segurança de Gestão de Incidentes Cibernéticos"[25] é uma referência avançada que pode ser tomada como base para a resposta.

A resposta a um incidente cibernético compreende várias fases, conforme mostrado neste gráfico:

Ciclo de vida de la Respuesta a Ciberincidentes

1. **A fase de preparação** consiste no estabelecimento de protocolos (Anexo 1) e monitoramento (Anexo 2).
2. **A fase de detecção**, análise e identificação começa pela classificação do ataque cibernético com base em seis critérios principais:

    a. Tipo de ataque[26].
    A periculosidade de um ataque pode variar de 1 a 5, onde 1 é baixo e 5 é grave, conforme mostrado na tabela:

Nivel	Peligrosidad
1	BAJO
2	MEDIO
3	ALTO
4	MUY ALTO
5	CRÍTICO

25 Para mais informações, acesse https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html

26 Para saber mais sobre a classificação de periculosidade, recomendamos consultar a página 12 do Esquema Nacional de Segurança de Gestão de Incidentes Cibernéticos.

b. Origem da ameaça.

c. Perfil dos usuários afetados (ou seja, quem foi afetado. Por exemplo, apenas alunos, professores, todos os funcionários etc.).

d. Número e tipos de sistemas afetados[27].

e. Impacto e possíveis consequências.

f. Requisitos legais e regulamentares (dependem de cada país).

3. **A fase de contenção, mitigação e recuperação** pode ser vista neste anexo e no Anexo 5.

4. **A fase de atividade pós-ataque cibernético** requer a avaliação do processo globalmente e a geração de um registro com detalhes do incidente, como:

    a. Resumo das ações realizadas para conter o incidente cibernético, erradicar o incidente e recuperar os sistemas afetados.

    b. Impacto do incidente cibernético, medido em tipologia das informações ou sistemas afetados, possível interrupção das aulas ou de qualquer outro serviço escolar, tempo e custos próprios e de terceiros até a retomada do funcionamento normal das atividades escolares, perdas econômicas (se aplicável) e danos à reputação associados.

Um dos incidentes cibernéticos que mais ameaçam a privacidade e a segurança dos estudantes é o vazamento de dados. Para lidar com um vazamento de dados, além do protocolo para fornecer uma resposta geral a incidentes cibernéticos, deve haver um protocolo de prevenção de resposta a incidentes.

A seguir, uma descrição de como pode ser elaborado esse tipo de protocolo de vazamento de dados com base em um Guia do INCIBE[28] (2012).

27 Para saber mais sobre a classificação dos ciberataques, recomendamos consultar a página 8 do *Guia de Cibersegurança*.

28 Para mais informações, acesse: https://www.incibe.es/extfrontinteco/img/File/intecocert/Formacion/EstudiosInformes/guia_gestion_fuga_informacion.pdf

Fase	Descrição
Fase inicial	• Detecção do incidente • Alerta do incidente no âmbito interno • Início do protocolo determinado pela equipe
Fase de lançamento	• Reunião da equipe de crise designada internamente • Relatório inicial da situação • Coordenação das primeiras ações e estabelecimento da causa do vazamento • Determinação das próximas etapas
Fase de avaliação	• Avaliação inicial do incidente • Preparação de um relatório preliminar
Fase de análise	• Reunião da equipe de crise designada • Apresentação do relatório preliminar • Determinação das principais ações • Atribuição de tarefas e planejamento
Fase de contenção	• Execução de todas as ações do plano. Pode incluir o estabelecimento de canais de comunicação com as pessoas afetadas pelo incidente e a localização dos dados (caso tenham sido divulgados publicamente).
Fase de acompanhamento e estabilização	• Avaliação dos resultados do plano • Gestão de outras consequências • Relatório completo para compartilhar com a comunidade educacional, professores, pais e mães de estudantes afetados pelo incidente • Aplicação de medidas e melhorias • Restabelecimento da atividade com novas medidas de segurança

Caso os dados afetados tenham sido publicados, o INCIBE recomenda:

- Identificar onde os dados foram divulgados, bem como o tipo e a quantidade de dados.
- Coletar as notícias que foram feitas sobre isso na mídia.
- Analisar as reações que ocorreram em relação ao incidente.

Anexo 5. Base do protocolo de notificação do incidente aos pais e mães

Uma vez iniciado o protocolo de ação devido a falhas de segurança dos dados na instituição de ensino, é importante informar as pessoas cujos dados foram afetados: estudantes, pais e mães.

Recomenda-se realizar as seguintes ações (INCIBE, 2012):

- Relatar o incidente e especificar quais dados foram violados. Assim, poderão ser tomadas as ações apropriadas, como alterações de senhas, bloqueios de contas ou o que for necessário, dependendo do caso.

- Estabelecer um canal de comunicação formal com os pais e mães para esclarecer todas as dúvidas, bem como oferecer recomendações e acompanhamento do protocolo e do andamento da remediação do incidente pela instituição de ensino.

    - É importante oferecer recomendações específicas, caso seja necessário tomar medidas para mitigar os efeitos que a violação de segurança pode causar
    - Recomenda-se que a comunicação seja feita por e-mail ou telefone

- Comunicar a devida solução da violação de segurança e as medidas que serão seguidas para evitar que ela se repita

- Rever os manuais de uso dos dados pessoais no país onde ocorreu o incidente para fazer valer as medidas legais, caso necessário

Anexo 6. Protocolo para selecionar plataformas e ferramentas de comunicação adequadas

De acordo com o Guia para professores sobre privacidade de dados de estudantes[29] (Connect Safely, 2016) e o Guia de proteção de crianças e adolescentes contra o uso de tecnologias nas escolas[30] (Dados Estudantis), algumas questões norteadas são apresentadas a seguir para avaliar se um serviço de tecnologia, seja uma plataforma, site ou aplicativo, protege os dados digitais de seus estudantes. Muitas destas perguntas podem ser respondidas por meio da leitura dos Termos ou Condições de Uso e da Política de Privacidade do serviço; portanto, sua revisão intencional e cuidadosa é de vital importância para determinar se seu uso é adequado.

Antes de começar a utilizar qualquer plataforma com os seus estudantes, é importante revisar as opções de privacidade e segurança que ela oferece e personalizar as funções de acordo com o uso escolar que se requer desse serviço, de forma a garantir a melhor proteção possível.

Perguntas guiadas para avaliação da plataforma

Observação: Nem todas estas questões precisam ser resolvidas necessária e vigorosamente em um curto período, mas são um guia para iniciar uma melhor gestão dos dados escolares.

- O serviço coleta informações de identificação pessoal do aluno?
    - » É importante saber exatamente como e quais dados o serviço coleta.
- O serviço compromete-se a não compartilhar informações do aluno além do necessário para o serviço educacional[31]?
    - » Por exemplo, você mantém as informações com terceiros ou vende dados? Este último ponto precisaria estar explícito.
    - » Os dados coletados e usados pelo serviço devem estar relacionados à finalidade e à funcionalidade do serviço. Por exemplo, se a plataforma for para fins educacionais, não deve solicitar informações sobre dados de saúde.
- O serviço cria perfis de seus estudantes fora dos objetivos educacionais especificados?
    - » A criação de perfis fora dos objetivos autorizados não é recomendada.
    - » Novamente, os dados coletados e usados pelo serviço devem estar relacionados ao propósito e à funcionalidade do serviço.
- O serviço indica quem é o responsável pela gestão dos dados armazenados na empresa prestadora do serviço?

29 Para mais informações, acesse (em inglês): https://www.connectsafely.org/wp-content/uploads/2016/05/Educators-Guide-Data-.pdf

30 Para mais informações, acesse (em português): https://www.dadosestudantis.org.br/modulo06.html

31 É importante avaliar quais dados a escola considera relevantes e quais ela está proibida de coletar. Esse critério deve ser considerado pela instituição de ensino, sempre alinhado ao regulamento de cada país.

  - » O controlador ou operador é o responsável pelo tratamento dos dados recolhidos, armazenados e utilizados por um serviço tecnológico, e é responsável por sua utilização indevida e pelas violações da privacidade.
  - » Sempre que houver uma opção possível no serviço tecnológico em questão, recomenda-se que a instituição de ensino seja a responsável pelo tratamento dos dados.
- Os pais, mães ou responsáveis, bem como a instituição de ensino, têm acesso aos dados digitais que o serviço coleta e armazena?
  - » Para ter visibilidade dos dados utilizados, os pais, mães ou responsáveis devem ter acesso a esses dados.
- Quando você termina de usar o serviço, seja cancelando a conta ou excluindo o aplicativo, o serviço exclui todos os dados do aluno coletados e gerados?
  - » Recomenda-se que os dados coletados sejam excluídos assim que o serviço deixar de ser utilizado, bem como saber com antecedência por quanto tempo os dados ficam armazenados.
- O serviço exibe publicidade aos usuários (estudantes) no site ou aplicativo utilizado?
  - » Em relação à publicidade, recomenda-se evitar que os anúncios exibidos sejam baseados em dados dos estudantes, ou seja, que funcionem por meio de segmentação comportamental, pois isso significaria que o serviço rastreia o comportamento dos estudantes online e coleta dados além do necessário para o atendimento educacional de interesse da instituição escolar.
  - » É importante prestar atenção aqui, principalmente nos serviços que não são projetados especificamente para ser ferramentas educacionais.
- O serviço compromete-se a fornecer segurança adequada para os dados que coleta e armazena?
  - » Um serviço que usa criptografia é recomendado ao fazer cópias de segurança ou transmitir dados. A criptografia de dados é uma camada de proteção que aumenta o nível de segurança.
- O serviço declara que sua política de privacidade pode ser alterada sem aviso prévio?
  - » Um alerta dessa natureza indicaria que seu uso em instituições de ensino não é recomendado, uma vez que o consentimento para a coleta e uso dos dados do aluno deve ser solicitado em todos os momentos. Uma mudança repentina das políticas de privacidade de um serviço não permitiria que ele fosse monitorado adequadamente.
- Existem comentários ou artigos sobre o serviço que são preocupantes?
  - » Você precisa pesquisar o que foi dito sobre o serviço antes de usá-lo com os seus estudantes.

Anexo 7. Análise de plataformas e ferramentas de comunicação com estudantes

A seguir, faremos uma análise das opções oferecidas, em termos de privacidade e segurança de dados digitais, por diversas plataformas e aplicativos que são frequentemente utilizados na educação, tenham ou não sido concebidos especificamente para a educação.

1. Recursos de segurança e privacidade a serem analisados para escolher serviços de videochamada para aulas online

Recomenda-se garantir que o serviço tenha as seguintes características:

- Selecionar os contatos que deseja adicionar um por um antes de iniciar uma chamada de vídeo. Por exemplo, neste video[32], o INCIBE explica como usar uma determinada plataforma com segurança.
- Escolher se deseja ou não compartilhar informações sobre sua atividade na plataforma.
- Bloquear os usuários, se um comportamento incomum for observado.
- Ajustar as permissões dos diversos canais de comunicação da plataforma, de modo que fiquem restritos aos diferentes grupos de pessoas selecionados. Esta opção permite que as mensagens públicas sejam apenas as pertinentes para que todos os estudantes as vejam, mantendo-se em canais de comunicação específicos as que dizem respeito a determinados estudantes.
- Selecionar quem tem acesso ao conteúdo do documento compartilhado e que tipo de acesso têm (por exemplo, se podem editar ou apenas visualizar).
- Verificar as permissões dos aplicativos inclusos na plataforma.
- Atribuir permissões específicas como anfitrião.
- Habilitar a função sala de espera, que permite à pessoa que estiver como anfitriã da reunião dar acesso a participantes mediante autorização (houve casos em que foram publicadas senhas de videoconferências que eram vulneráveis, e isso permitiu o ingresso de pessoas não autorizadas).
- Proteger a sala de reunião virtual com uma senha [33](Zoom, 2020).
- Desativar a opção de compartilhamento de tela.
- Utilizar criptografia de ponta a ponta.
- Ativar o recurso "Knock Knock", que permite que o usuário veja o vídeo de quem está chamando antes mesmo de atender à ligação.
- Aceitar ou recusar o link[34] de convite antes de iniciar uma conversa com alguém (Protect Young Eyes).
- Controlar se outras pessoas podem encontrar os membros da plataforma por número de telefone ou endereço de e-mail.

32 Para mais informações, acesse https://www.youtube.com/watch?v=ys3k1yEPevo&feature=youtu.be

33 Para mais informações, acesse https://blog.zoom.us/es/keep-uninvited-guests-out-of-your-zoom-event/

34 Para mais informações, acesse (em inglês) https://protectyoungeyes.com/apps/google-duo-parental-controls/

Recomendações gerais para videochamadas

A Agência de Segurança Nacional dos Estados Unidos (NSA, na sigla em inglês) publicou um guia de segurança para plataformas de videoconferencia[35] que inclui os seguintes critérios de avaliação principais em termos de segurança e privacidade (Kaspersky, 2020):

- Utiliza serviço criptografado de ponta a ponta, limitando a possibilidade de outras pessoas espionarem a chamada?
- Utiliza verificação em múltiplas etapas, uma opção que protege de forma efetiva as contas dos usuários?
- A tecnologia em que se baseia é de código aberto, que pode ser inspecionada, sendo, portanto, considerada mais segura que o software proprietário, impossível de inspecionar?
- A ferramenta compartilha informações com terceiros ou parceiros?
- Os usuários poderão excluir com segurança os dados do serviço e de seus repositórios quando precisarem (tanto o cliente quanto no lado do servidor)?

Embora todas as plataformas de videoconferência tenham algumas oportunidades para melhorar sua segurança, seria ideal usar aquelas que fornecem as medidas de proteção mais adequadas para uso por parte dos e das estudantes. Além disso, recomenda-se acompanhar seu uso com boas práticas que aumentem a segurança e proteção de estudantes e professores na plataforma:

- Compartilhar o link com os e as estudantes alguns minutos antes de iniciar a aula online por meio de canal previamente autorizado
- Evitar compartilhar o link em fóruns públicos, onde é possível perder o controle de quem pode vê-lo e usá-lo
- Atribuir um responsável da instituição de ensino (o professor, por exemplo) para controlar quem acessa a videoconferência, bem como as permissões para compartilhar tela, usar microfones e vídeos
- Evitar compartilhar informações pessoais por meio de chats em salas de videoconferência
- Usar a opção de gravar as sessões apenas quando necessário, pois cada país possui seus protocolos de utilização de imagens
- Em caso de gravação, avisar sempre os estudantes ou seus pais e mães, se for o caso.

2. Outros recursos de segurança e privacidade de plataformas e aplicativos Web para uso por professores e estudantes

Recomenda-se garantir que a plataforma ou aplicativo possa:

- Escolher uma verificação ou autenticação em duas etapas e métodos alternativos para verificar a identidade de quem ingressa na plataforma

35 Para mais informações, acesse https://www.zdnet.com/article/heres-the-nsas-guide-for-choosing-a-safe-text-chat-and-video-conferencing-service/

- Personalizar as informações exibidas no perfil individual
- Estabelecer preferências sobre o histórico e anúncios publicitários por meio da seção de dados e personalização
- Gerenciar os contatos no menu Configurações da conta, seguido de Contatos e informações compartilhadas, o que permite adicionar somente os contatos selecionados e, além disso, bloquear aqueles que não forem reconhecidos ou apresentarem comportamento incomum na plataforma
- Oferecer a opção de enviar mensagens públicas ou no chat privado, o que permite gerenciar em qual canal compartilhar uma determinada informação
- Editar as permissões para acessar, editar, baixar ou visualizar qualquer um dos documentos que forem compartilhados com os estudantes
    - Os documentos possuem um histórico de edições, para que o professor identifique as edições e usos que os estudantes fazem do documento
- Garantir o acesso à plataforma apenas para os usuários com permissão
- Estabelecer restrições de permissão sobre certas informações para estudantes não designados. Por exemplo, as notas de cada estudante só poderão ser visualizadas em sua própria conta
- Ter controle sobre quais informações são exibidas em cada perfil
- Definir funções dentro da plataforma sobre quem tem permissões específicas para baixar documentos
- Estabelecer que os usuários que entram na plataforma se identifiquem por meio da função forcelogin[36].

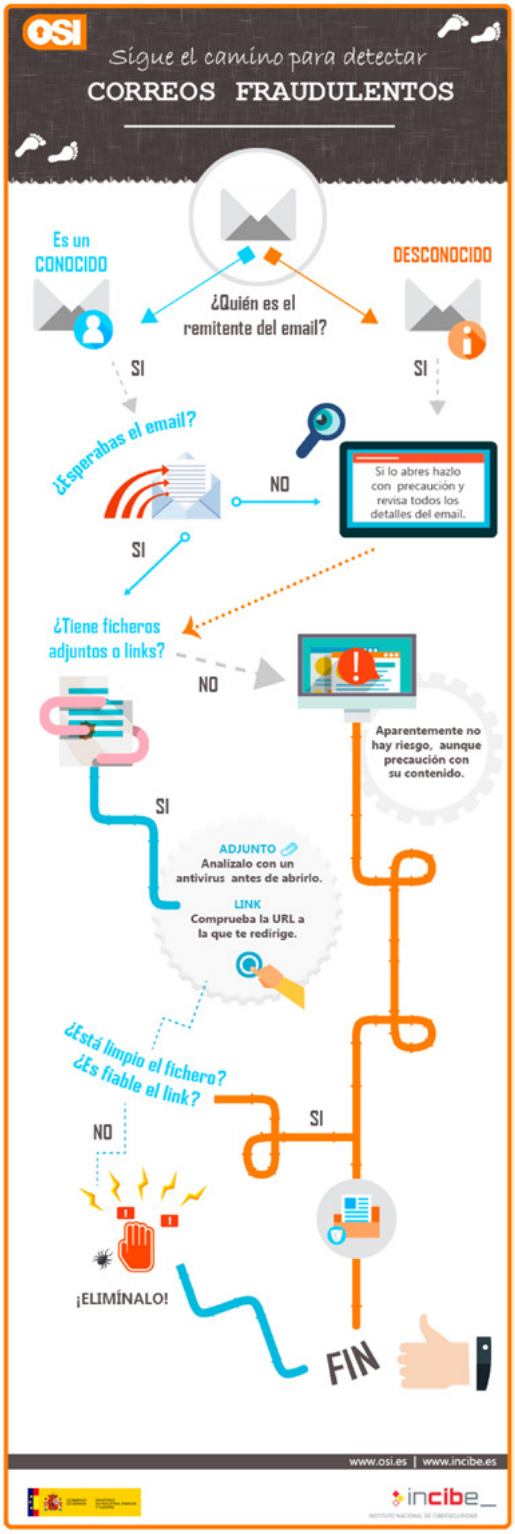
36 Em criptografia, um ataque de força bruta é quando um atacante envia muitas senhas ou frases com a esperança de acabar adivinhando uma combinação. O atacante testa sistematicamente todas as senhas e frases possíveis até encontrar a certa. Alternativamente, o atacante pode tentar adivinhar o código que normalmente é criado a partir da senha, utilizando uma função de derivação de códigos. (Fuente: Adleman, Leonard M.; Rothemund, Paul W.K.; Roweis, Sam; Winfree, Erik (June 10–12, 1996). On Applying Molecular Computation to the Data Encryption Standard. *Proceedings of the Second Annual Meeting on DNA Based Computers*. Princeton University).

3. Ameaças por e-mail

Para evitar e mitigar ameaças por e-mail, o ideal é que a instituição de ensino forneça à sua equipe pedagógica, de gestão e aos estudantes uma conta de e-mail para uso estritamente institucional. Como acontece com qualquer plataforma ou aplicativo Web, é recomendado:

- Usar uma senha forte, alterá-la regularmente e, se possível, com autenticação em duas etapas
- Incorporar, sempre que possível, tecnologias anti-malware e verificação de links no serviço de e-mail

Além disso, deve-se ter cuidado com e-mails desconhecidos recebidos, pois existem e-mails fraudulentos e maliciosos que podem colocar em risco a segurança dos dados ou conter vírus. O gráfico a seguir fornece informações para detectar e-mails fraudulentos (OSI, 2015)



4. Cuidado com o uso de redes sociais

Como integrante do corpo docente de uma instituição, é preferível não utilizar as redes sociais para atividades online com os estudantes, pois são plataformas abertas a quem quiser entrar, não um sistema fechado no qual se possa controlar a privacidade e segurança dos integrantes (neste caso, alunos). Recomenda-se, também, orientar os estudantes a não utilizarem um e-mail institucional para gerar uma conta nas redes sociais, pois sua identidade pode ser rastreada, ou o estudante pode perder o acesso à conta de e-mail.

Anexo 8. Sugestões de seções sobre o uso de plataformas digitais em regulamentos escolares

Estas são algumas das seções que sugerimos que sejam incluídas na regulamentação sobre questões digitais, desde o uso de plataformas e aplicativos Web até o comportamento durante as atividades de educação online:

1. Plataformas e aplicativos oficiais da Internet para uso educacional na instituição, como aqueles utilizados para:
    a. Suporte para aulas
    b. Videoconferências
    c. Comunicação entre professores e estudantes (sugere-se, também, estabelecer um cronograma para sua realização)
    d. Comunicação entre a equipe de diretoria, professores e pais e mães (sugere-se, também, estabelecer um cronograma para isso)

2. Especificações sobre:
    a. Os comportamentos exigidos durante as aulas online, tanto de professores como de estudantes (por exemplo, ligar ou não a câmera)
    b. Permissões para gravar, fotografar e compartilhar a sessão educacional por videoconferência
    c. O tipo de plataforma educacional autorizada para atividades escolares
    d. A responsabilidade de cada indivíduo de garantir que os arquivos compartilhados estejam livres de vírus
    e. As consequências de um ataque cibernético interno (OEA, s.d.)

Anexo 9. Proposta de carta de notificação aos pais e mães (inclui informações sobre o assunto)

Antes de redigir a carta de notificação, é necessário analisar a legislação de proteção de dados do país em questão para garantir o cumprimento dos termos e condições necessários.

Como a legislação varia de um país para o outro, é preciso primeiro consultar os requisitos nacionais referentes a avisos de privacidade. Esta carta é apenas um exemplo.

CARTA DE NOTIFICAÇÃO AOS PAIS OU RESPONSÁVEIS (Governo do México)37

[CIDADE E DATA]

[PESSOA E INSTITUIÇÃO ÀS QUAIS É ENDEREÇADA]

Declaro que tenho conhecimento da inclusão de questões digitais nos regulamentos da instituição de ensino e do protocolo de plataformas Web de uso escolar em [NOME DA INSTITUIÇÃO], e que isso implica a coleta, utilização e armazenamento de dados do meu filho ou da minha filha [NOME], de [IDADE] anos de idade, atualmente cursando o [NÚMERO DO ANO] ano.

ASSINATURA, NOME E DADOS DE IDENTIFICAÇÃO DO PAI, MÃE OU RESPONSÁVEL

_____
PAI

_____
MÃE

NA AUSÊNCIA DOS PAIS, O NOME E ASSINATURA DE QUEM ESTÁ EXERCENDO O PODER FAMILIAR OU TUTORIA.

_____

37 Para mais informações, acesse: https://www.gob.mx/cms/uploads/attachment/file/453174/Carta-autorizaci_n_Padre-o-tutor.pdf

Anexo 10. Sugestão de estratégia de comunicação para discutir privacidade com diretores, administradores, professores, estudantes e pais e mães (recursos)

Dentro das atividades escolares, podem ser realizadas campanhas de informação para conscientizar sobre a questão dos riscos e a importância da proteção dos dados digitais.

1. Equipes (diretores, administradores, professores)

- A formação em questões de uso ético e responsável das ferramentas digitais para a educação, de forma a garantir a privacidade e a segurança dos dados digitais dos estudantes, requer, idealmente, a formação das equipes de diretoria, administrativas e pedagógicas que utilizem tecnologias para a educação.

Recursos virtuais úteis com informações pertinentes para professores

- Série de vídeos informativos sobre segurança cibernética[38] produzida pelo INCIBE. Inclui vídeos curtos e interativos em contexto escolar, úteis para treinamentos sobre o assunto.
- Kit de conscientização sobre segurança cibernética[39] criado pelo INCIBE. Inclui material gráfico, leituras, apresentações acompanhadas de informações e um teste de avaliação.

2. Estudantes

Recursos virtuais úteis para uso escolar com estudantes:

Os recursos a seguir são atividades de apoio à conscientização sobre o tema que podem ser realizadas em sala de aula entre professores e estudantes:

- Oficina para professores e estudantes sobre "dados inteligentes[40]. Inclui a apresentação de uma série de atividades simples para realizar com os estudantes e um guia para os professores sobre como realizar a apresentação.
- Atividade que incentiva o aprendizado de diretrizes simples de segurança cibernética[41] em plataformas educacionais online. Inclui um questionário que pode ser respondido no site.

38 Para mais informações, acesse https://itinerarios.incibe.es/

39 Para mais informações, acesse https://www.incibe.es/protege-tu-empresa/blog/actualizate-ciberseguridad-el-nuevo-kit-concienciacion

40 Para mais informações, acesse https://en.datasmartkids.com/recursos

41 Para mais informações, acesse https://www.is4k.es/educadores/test-plataformas-educativas-online

3. Pais, mães ou responsáveis

- A transição das aulas para o modo digital destacou a importância do trabalho dos pais e mães no acompanhamento da aprendizagem online dos estudantes (UNICEF, 2020), enfatizando a necessidade de ampliar a campanha de comunicação ou disponibilizar sessões informativas sobre proteção dos dados digitais dos estudantes.
- Recomenda-se que a instituição de ensino estabeleça os canais de comunicação adequados da diretoria e dos professores com os pais e mães, para envio de relatórios sobre o assunto, recursos ou convites para sessões de informação (se possível).

Recursos virtuais úteis com informações pertinentes para os pais e mães:

- Ferramentas de apoio e informações destinadas a pais e mães[42] para la sensibilización acerca del tema, en el portal de Internet Segura For Kids.

42 Para más información, ver https://www.is4k.es/de-utilidad/recursos/material-de-difusion-para-centros-educativos

Anexo 11. Pontos para compartilhar em uma campanha de informação

Em uma campanha de informação, os seguintes aspectos podem ser compartilhados:

- Importância da proteção dos dados digitais
  - » Direito das crianças à privacidade e a importância do consentimento
- Riscos à privacidade e à segurança relacionados aos dados digitais e suas consequências:
  - » Ataque/hackeamento
  - » Vazamento de dados
  - » Rastreamento de atividade online
  - » Venda de dados
- Medidas de segurança do dispositivo:
  - » Firewall
  - » Antivírus
- Importância da implementação de práticas para maior proteção dos dados das crianças:
  - » Criação de senhas fortes
  - » Leitura dos termos e políticas de privacidade em plataformas e aplicativos Web antes de começar a usá-los
  - » Configurações de privacidade de acordo com seu uso
  - » Realização de práticas cíclicas

Glossário[43]

- **Antivirus**: um programa que ajuda a proteger os dispositivos contra a maioria dos vírus, worms, cavalos de Troia e outros tipos de malware que podem infectar os dispositivos.
- **Ciberataque**: conjunto de ações ofensivas contra sistemas de informação, como bancos de dados, redes de computadores etc., destinadas a danificar, alterar ou destruir instituições, pessoas ou empresas.
- **Criptografia ponta a ponta**: nas comunicações (chats, por exemplo), significa que as mensagens são seguras e que apenas o remetente e o destinatário podem ler seu conteúdo.
- **Cookies**: arquivos que o nosso navegador guarda, onde são armazenadas pequenas quantidades de dados utilizados pelos servidores dos sites que visitamos para guardar diversos tipos de informação que nos identificam quando tornamos a visitá-los.
- **Cópia de segurança**: ferramenta destinada ao armazenamento de dados ou informações com o objetivo de poder recuperá-los em caso de perda acidental ou intencional.
- **Dados pessoais**: informações de qualquer tipo que podem ser utilizadas para identificar, contatar ou localizar uma pessoa.
- **Malware**: software projetado intencionalmente para prejudicar um computador, servidor, cliente ou rede de computadores.
- **Sistema operacional**: software que coordena e direciona todos os serviços e aplicativos utilizados pelo usuário em um computador.

43 O glossário se baseia no Guia de Cibersegurança da Secretaria de Telecomunicações (Governo do México, 2020).

Fontes consultadas e referências

Arias Ortiz, Elena e Julián Cristia. (2014). El BID y la tecnología para mejorar el aprendizaje: ¿Cómo promover programas efectivos? ("O BID e a tecnologia para aprimorar o aprendizado: como promover programas eficazes?") Washington, D.C.: Banco Interamericano de Desenvolvimento. https://publications.iadb.org/publications/spanish/document/El-BID-y-la-tecnología-para-mejorar-el-aprendizaje-how-promover-programas-efectivos.pdf

Bojalil, Paulina e Carlos Vela-Treviño. (2019). Despuntan las reformas en materia de protección de datos en América Latina ("As reformas de proteção de dados na América Latina destacam-se"). BID: 12 de fevereiro. https://blogs.iadb.org/conocimiento-abierto/es/proteccion-de-datos-gdpr-america-latina/

Agência de Segurança Cibernética e Infraestrutura. (2021). Ransomware reference materials for K-12 school and school district IT staff ("Materiais de referência de ransomware para escolas de ensino fundamental e médio e equipes de TI do distrito escolar"). Governo dos Estados Unidos. https://www.cisa.gov/ransomware-reference-materials-k-12-school-and-school-district-it-staff

Comunicações. (2020). Guía de ciberseguridad para el uso de redes y dispositivos de telecomunicaciones ("Guia de segurança cibernética para o uso de redes e dispositivos de telecomunicações"). México: Ministério das Comunicações e Transportes. https://drive.google.com/file/d/13z_PWUQvycbLTzVMAWbKjfTO4l6l2ZRX/view

Distrito escolar unificado de Conejo Valley. (s.d.) https://www.conejousd.org

Contreras, Belisario (coord.). (2020). Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y el Caribe ("Segurança cibernética. Riscos, avanços e perspectivas na América Latina e no Caribe"). Washington, D.C.: BID e OEA. https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

ESET. (2017). Eset Security Report Latin America 2017. https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf

González, Yolanda (2020). Control parental y seguridad de los menores en Internet ("Controle parental e segurança de menores na Internet"). Madrid: Grupo Ático 34. 4 de junho.https://protecciondatos-lopd.com/empresas/parental-control/#Because_is_so_important_controlar_el_control_que_que_ven_our_children_on_internet

Instituto Nacional de Biossegurança. (2012). Gestión de fuga informática ("Gestão de vazamentos de computador"). Espanha: Ministério da Indústria, Energia e Turismo. Leão (Espanha): INCIBE. https://www.incibe.es/extfrontinteco/img/File/intecocert/Formacion/EstudiosInformes/guia_gestion_fuga_informacion.pdf

Instituto Nacional de Biossegurança. (2016). Guía de almacenamiento seguro de la información ("Guia de armazenamento seguro de informações"). Leão (Espanha): INCIBE. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_almacenamiento_seguro_metad_0.pdf

Instituto Nacional de Biossegurança. (2017). Dispositivos móviles personales para uso profesional (BYOD). Una guía de aproximación para el empresario ["Dispositivos móveis pessoais para uso comercial (BYOD). Um guia de abordagem para o empreendedor"]. Leão (Espanha): INCIBE. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_dispositivos_moviles_metad.pdf

Ponemon Institute, IBM. (2020) Cost of a Data Breach Report 2020 ("Relatório de Custo de uma Violação de Dados 2020"). USOS: IBM. https://www.ibm.com/security/data-breach

Kaspersky (2020) Cyber Security Risks: Best Practices for Working from Home and Remotely ("Riscos de segurança cibernética: Melhores práticas para trabalhar em casa e remotamente"). https://www.kaspersky.com/resource-center/threats/remote-working-how-to-stay-safe

OCDE. (1999). Online Advertising and Marketing Directed Toward Children ("Publicidade e marketing online voltados para crianças"). Documentos de Economia Digital da OCDE, nº 46. Paris: Publicação da OCDE. https://www.oecd-ilibrary.org/science-and-technology/online-advertising-and-marketing-directed-toward-children_236506677507;jsessionid=uI9s3Ad_5jvO3P3PVgII_uIU.ip-10-240-5-52

Oficina de Seguridad del Internauta. (2013). Creando contraseñas robustas ("Criação de senhas fortes"). 5 de dezembro. https://www.osi.es/es/actualidad/blog/2013/12/05/creando-contrasenas-robustas

Organização dos Estados Americanos. (s.d.). Reglamento de uso del aula virtual ("Regulamentação do uso da sala de aula virtual"). portal.oas.org/LinkClick.aspx?fileticket=nCougUTRFpk=&tabid=1905

Organização dos Estados Americanos. (2020). Educación en ciberseguridad. Planificación del futuro mediante el desarrollo de la fuerza laboral ("Educação em segurança cibernética. Planejamento para o futuro por meio do desenvolvimento da força de trabalho"). Washington: OEA. www.oas.org/es/sms/cicte/docs/20200925-ESP-White-Paper-Educacion-en-Ciberseguridad.pdf

Saigal, Rahul. (2020). Does Your Mac Really Need a Firewall? What You Need to Know ("Seu Mac realmente precisa de um firewall? O que você precisa saber"). MUO. 25 de fevereiro.

https://www.makeuseof.com/tag/mac-really-need-firewall/

The London School of Economics and Political Science. (2020). My data and privacy online. A toolkit for young people ("Meus dados e privacidade online. Um kit de ferramentas para jovens"). Londres: LSE. https://www.lse.ac.uk/my-privacy-uk/for-educators

UNESCO. (2017). International Symposium on School Violence and Bullying: from Evidence to Action ("Simpósio Internacional sobre Violência Escolar e Bullying: da Evidência à Ação"). Seul: UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000246970

UNICEF. (2020). Mamás y papás deben apoyar el aprendizaje de las y los adolescentes en el hogar ("Os pais ou responsáveis devem apoiar a aprendizagem dos adolescentes em casa"). Bolívia: UNICEF. https://www.unicef.org/bolivia/historias/mamás-y-papás-deben-apoyar-el-aprendizaje-de-las-y-los-adolescentes-en-el-hogar

UNICEF. (2019). Preparación y respuesta educativa. Respuesta de UNICEF a los desafíos de educación en América Latina y el Caribe durante el COVID-19 ("COVID-19: Preparação e resposta educacional. Resposta do UNICEF aos desafios da educação na América Latina e no Caribe durante a COVID-19"). Panamá: Unicef. https://www.unicef.org/lac/en/covid-19-education-preparedness-and-response

Nações Unidas. (2020). Policy Brief. Education during COVID-19 and beyond ("Resumo de Política. Educação durante o COVID-19 e além"). Nova York: UMA. https://www.un.org/development/desa/dspd/wp-content/uploads/sites/22/2020/08/sg_policy_brief_covid-19_and_education_august_2020.pdf


eon
resilience lab
by C Minds


BID
Melhorando vidas