#ESPAÇOCIBER

Orientações de cibersegurança para implementação de política de BYOD

1ª Edição | 2025

ANBIMA

Sumário

Sobre o Guia Técnico

Este Guia Técnico de Orientações de cibersegurança para implementação de política de BYOD – *Bring Your Own Device* é resultado do trabalho conjunto da ANBIMA – Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais com participantes de mercado reunidos no Grupo Consultivo de Cibersegurança. O material traz recomendações e orientações técnicas de segurança cibernética às organizações atuantes nos mercados financeiro e de capitais com o objetivo de contribuir para sua integridade e maior resiliência frente às crescentes ameaças cibernéticas.

O conteúdo deste documento não é vinculante para quaisquer organizações, associadas ou não à ANBIMA, e não se caracteriza, de nenhum modo, como elemento da autorregulação da Associação. O presente material reflete tão somente orientações técnicas, e, sob nenhuma hipótese, vincula as organizações e a ANBIMA a eventuais futuras discussões sobre o tema no âmbito da autorregulação.

O conteúdo deste documento também não deve ser interpretado de forma a contrariar, mitigar ou se opor a nenhum normativo da legislação, regulação[1] e autorregulação[2] aplicáveis às organizações participantes dos mercados financeiro e de capitais. Limitando-se, tão somente, a orientar técnicas para melhor consecução de atividades ao mercado.

[1] BRASIL. Resolução CMN Nº 4.893/2021. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4893>.
BRASIL. Resolução CVM Nº 35/2021. Disponível em: <https://conteudo.cvm.gov.br/export/sites/cvm/legislacao/resolucoes/anexos/001/resol035consolid.pdf>.

[2] ANBIMA. Regras e Procedimentos de Deveres Básicos. Disponível em: <https://www.anbima.com.br/data/files/1E/42/14/73/BB3EF810B99A0EF8B82BA2A8/Regras%20e%20Procedimentos%20de%20Deveres%20Basicos%20_vigente%20a%20partir%20de%2003.06.24_.pdf>.

Introdução

Este material complementa o disposto no **Guia de Cibersegurança ANBIMA**[3], que orienta as organizações para a definição de funções mínimas que visam garantir a eficácia de seu programa de segurança cibernética. Dentre elas, recomendações relacionadas ao estabelecimento de política de acesso de dispositivos aos ativos críticos da organização que considere:

i. Modelo de confiança zero para acesso de dispositivos às redes internas; e
ii. Regras e procedimentos específicos para utilização de dispositivos pessoais de colaboradores (BYOD), quando aplicável, que inclua no mínimo: controles para mitigar riscos identificados, critérios de responsabilização e procedimentos relacionados às situações de desligamento do colaborador.

A prática de BYOD – Bring Your Own Device tem se popularizado na rotina das organizações pelos benefícios que oferece. No entanto, permitir que colaboradores utilizem dispositivos pessoais para acessar ativos corporativos também traz desafios importantes. Confira exemplos não exaustivos a seguir.

BENFÍCIOS

- Dispositivos pessoais podem atender melhor às necessidades e preferências dos colaboradores
- Economia de recursos com a aquisição e manutenção de equipamentos
- O estabelecimento de política de BYOD auxilia na prevenção contra perda de dados (DLP – Data Loss Prevention)

DESAFIOS

- Dispositivos pessoais estão mais vulneráveis a ameaças cibernéticas
- Perda, danificação, roubo ou furto dos dispositivos pessoais podem comprometer a segurança da organização
- Diferentes modelos de dispositivos implicam em maior complexidade de gestão e monitoramento

Os diversos riscos à segurança associados à essa prática precisam ser adequadamente identificados e mitigados para que não comprometam o programa de segurança cibernética da organização. Neste sentido, são apresentadas na seção a seguir recomendações e orientações técnicas objetivas e não exaustivas para apoiar as organizações atuantes nos mercados financeiro e de capitais no desenvolvimento de políticas, regras e procedimentos de BYOD fundamentados na legislação, regulação e autorregulação aplicáveis e alinhados com padrões internacionais.

[3] ANBIMA. Guia de Cibersegurança (3ª Edição – 2021). Disponível em: <https://www.anbima.com.br/data/files/34/B3/04/8F/D96F971013C70F976B2BA2A8/Guia%20de%20Ciberseguranca%20ANBIMA.pdf>.

1. Legislação e regulação

De forma não exaustiva, destacam-se a seguir normativos relacionados à segurança da informação e cibernética aplicáveis às organizações atuantes nos mercados financeiro e de capitais:

- **Resolução CMN Nº 4.893/2021[4]:** dispõe sobre a política de segurança cibernética e os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.
- **Resolução BCB Nº 498/2025[5]:** disciplina, no âmbito do Sistema Financeiro Nacional e do Sistema de Pagamentos Brasileiro, os requisitos, os procedimentos e as condições para o credenciamento de Provedor de Serviços de Tecnologia da Informação – PSTI.
- **Resolução CVM Nº 35/2021[6]:** define os requisitos mínimos do programa de segurança cibernética e da política de segurança da informação exigidos de intermediários de valores mobiliários.
- **Lei Nº 13.709/2018[7]:** Lei Geral de Proteção de Dados Pessoais (LGPD).
- **Resolução CD/ANPD Nº 2/2022[8]:** regulamento de aplicação da LGPD para agentes de tratamento de pequeno porte.
- **Resolução CD/ANPD Nº 15/2024[9]:** regulamento de comunicação de incidente de segurança.

2. Principais referências

Para elaboração deste material e fundamentação de suas recomendações e orientações técnicas de forma alinhada com padrões de segurança amplamente reconhecidos internacionalmente, as publicações descritas a seguir foram consultadas a título de referência. Não exaustivamente, estas referências podem ser utilizadas pelas organizações para complementar e aprofundar seu processo de implementação de políticas, regras e procedimentos de BYOD.

- **CIS – Center for Internet Security:** CIS Critical Security Controls (CIS Controls) v8.1 (2025)[10].
- **ISO – International Organization for Standardization:** ISO/IEC 27001 (2022)[11].
- **NIST – National Institute of Standards and Technology:** NIST Special Publication 800-207 – Zero Trust Architecture (2020)[12]; e NIST Special Publication 800-124r2 – Guidelines for Managing the Security of Mobile Devices in the Enterprise (2023)[13].

[4] BRASIL. Resolução CMN Nº 4.893/2021. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4893>
[5] BRASIL. Resolução BCB Nº 498/2025. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=498>
[6] BRASIL. Resolução CVM Nº 35/2021. Disponível em: <https://conteudo.cvm.gov.br/export/sites/cvm/legislacao/resolucoes/anexos/001/resol035consolid.pdf>.
[7] BRASIL. Lei Nº 13.709/2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>.
[8] BRASIL. Resolução CD/ANPD Nº 2/2022. Disponível em: <https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022>.
[9] BRASIL. Resolução CD/ANPD Nº 15/2024. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024>.
[10] CIS. CIS Critical Security Controls (CIS Controls) v8.1 (2022). Disponível em: <https://www.iso.org/standard/27001>
[11] ISO. Information security, cybersecurity and privacy protection — Information security management systems — Requirements (2022). Disponível em: <https://www.iso.org/standard/27001>
[12] NIST. NIST Special Publication 800-207. Zero Trust Architecture (2020). Disponível em: <https://doi.org/10.6028/NIST.SP.800-207>
[13] NIST. NIST Special Publication 800-124r2. Guidelines for Managing the Security of Mobile Devices in the Enterprise (2023). Disponível em: <https://doi.org/10.6028/NIST.SP.800-124r2>

Recomendações para implementação de política de BYOD

A implementação de política e programa eficaz de segurança cibernética pelas organizações, conforme discute a introdução deste documento, deve considerar o acesso de dispositivos a seus ativos críticos. Na hipótese de a organização permitir o acesso de dispositivos pessoais a esses ativos, é crucial que adote uma política de BYOD associada a práticas e rotinas de gestão, monitoramento e controle para identificar, avaliar e mitigar riscos, bem como para prevenir e tratar incidentes.

A política de BYOD, ou documento análogo, é fundamental para estabelecer requisitos mínimos a serem observados para que os colaboradores possam utilizar seus dispositivos pessoais para acessar ativos da organização. Por outro lado, é importante que os colaboradores estejam devidamente informados e consintam com o acesso a recursos e informações de seus dispositivos pessoais pela organização para realização de práticas e rotinas de segurança.

Nesse sentido, estão dispostas a seguir recomendações e orientações técnicas, alinhadas com padrões de segurança amplamente reconhecidos internacionalmente, que visam apoiar as organizações no desenvolvimento de políticas, regras e procedimentos de BYOD, dispostas nos seguintes tópicos:

1. Governança e conformidade

Este tópico aborda os componentes essenciais a serem considerados pelas organizações na implementação de política de BYOD, ou documento análogo, visando garantir o uso seguro e responsável de dispositivos pessoais para acessar ativos corporativos.

Recomendações:

1.1. Estabelecer política de BYOD, ou documento análogo, considerando:

a. Adotar modelo de confiança zero para o acesso de dispositivos pessoais aos ativos corporativos, considerando:

i. Conceder acesso de dispositivos pessoais aos ativos corporativos apenas quando necessário; e
ii. Não presumir confiança em nenhum dispositivo ou usuário.

b. Adotar regras e procedimentos que não contrariem, mitiguem ou se oponham:

i. À legislação, regulação e/ou autorregulação aplicáveis; e
ii. A nenhum elemento do programa, das políticas e/ou regras e procedimentos de segurança da informação e cibernética da organização, conforme aplicável.

c. Definir termo de uso de dispositivos pessoais para acesso a ativos da organização, ou documento análogo, considerando, conforme aplicável e de forma não exaustiva:

i. Definir clara e objetivamente colaboradores elegíveis à utilização de dispositivos pessoais para acesso a ativos da organização e, consequentemente, contemplados pelo termo de uso, ou documento análogo;
ii. Na hipótese de o colaborar optar por utilizar seus dispositivos pessoais para acessar ativos da organização, descrever clara e objetivamente os controles e acessos franqueados à organização em decorrência dessa opção, destacando as funções, informações, dados, mídias e arquivos abrangidos;
iii. Descrever clara e objetivamente os potenciais impactos ao dispositivo pessoal de procedimentos, rotinas e controles para mitigação de riscos realizados pela organização, por exemplo, com relação ao desgaste do aparelho e ao comprometimento do espaço de armazenamento, do processamento ou da velocidade de conexão;
iv. Definir clara e objetivamente o que é permitido e proibido no uso de dispositivos pessoais para acessar ativos da organização;
v. Estabelecer procedimentos para o colaborador informar e manter atualizada a organização acerca dos dispositivos pessoais a partir dos quais acessa os ativos corporativos;
vi. Estabelecer requisitos mínimos para acesso, reprodução, tratamento, transporte, compartilhamento e descarte de dados da organização através de dispositivos pessoais, abrangendo a utilização de redes corporativas de dados e de computação em nuvem;
vii. Estabelecer requisitos mínimos para acesso à rede mundial de computadores (internet), abrangendo o uso de conexão sem fio e de redes públicas ou privadas;
viii. Estabelecer requisitos mínimos para a instalação e atualização de aplicativos e aplicações (softwares) nos dispositivos pessoais utilizados para acessar ativos da organização;
ix. Estabelecer procedimentos e requisitos mínimos para acesso e conexão (login) a ambientes digitais corporativos por meio de dispositivos pessoais, abrangendo procedimentos e requisitos específicos para usuários administradores;
x. Definir critérios para ativação de ferramenta de rede privada virtual (VPN – Virtual Private Network);
xi. Estabelecer procedimentos para o colaborador reportar casos de perda, danificação, roubo ou furto dos dispositivos pessoais utilizados para acessar ativos da organização;

xii. Estabelecer procedimentos para o colaborador reportar incidentes, situações suspeitas ou tentativas de ataques aos dispositivos pessoais utilizados para acessar ativos da organização;
xiii. Estabelecer procedimentos de descarte adequado ou desconexão de dispositivos pessoais utilizados para acessar ativos da organização, abrangendo a situação de desligamento do colaborador;
xiv. Descrever situações elegíveis à revogação de acesso e apagamento remoto de dados corporativos pela organização, abrangendo a situação de desligamento do colaborador;
xv. Definir responsabilidades individuais e corresponsabilizações aos colaboradores relacionadas ao uso dos dispositivos pessoais para acesso a ativos da organização;
xvi. Prever entre as responsabilidades individuais dos colaboradores que estes devem agir de forma ética, zelando pela segurança da informação e cibernética e em conformidade com o que define políticas, regras e procedimentos da organização;
xvii. Definir medidas disciplinares para situações de não conformidade ou violação do termo de uso pelos colaboradores; e
xviii. Exigir que os colaboradores consintam com o termo de uso, ou documento análogo, por exemplo através de assinatura (quando aplicável, assinatura digital).

d. Estabelecer procedimentos e rotinas para identificação e gestão de dispositivos pessoais utilizados para acessar ativos da organização, considerando, conforme aplicável e de forma não exaustiva, as recomendações contidas no tópico 2 desta seção deste documento.

e. Estabelecer procedimentos e rotinas para identificação e avaliação de riscos associados à utilização de dispositivos pessoais para acessar ativos da organização, considerando, conforme aplicável e de forma não exaustiva, as recomendações contidas no tópico 3 desta seção deste documento.

f. Estabelecer práticas e controles para mitigar riscos identificados associados à utilização de dispositivos pessoais para acessar ativos da organização, considerando, conforme aplicável e de forma não exaustiva, as recomendações contidas no tópico 4 desta seção deste documento.

g. Implementar ações e rotinas de conscientização e treinamento de colaboradores com relação às práticas de BYOD, de forma específica ou integrando ações e rotinas já estabelecidas, considerando:

i. Garantir que os colaboradores tenham acesso e saibam como consultar o termo de uso de dispositivos pessoais para acesso a ativos corporativos e a política de BYOD da organização, ou documentos análogos;
ii. Garantir que os colaboradores compreendam suas responsabilidades individuais e corresponsabilizações ao optarem pelo uso de dispositivos pessoais para acessarem ativos da organização;
iii. Garantir que os colaboradores compreendam a abrangência dos controles e acessos franqueados à organização em decorrência da opção pela utilização de dispositivos pessoais para acessar ativos corporativos;

iv. Garantir que os colaboradores compreendam os potenciais impactos que práticas e controles para mitigação de riscos realizados pela organização podem gerar ao dispositivo pessoal;
v. Garantir que os colaboradores estejam capacitados para realizar e conheçam os procedimentos estabelecidos no termo de uso de dispositivos pessoais para acesso a ativos da organização;
vi. Disponibilizar e manter atualizados materiais e recursos, bem como promover ações e oferecer experiências que contribuam para o aumento do nível de conhecimento dos colaboradores com relação aos elementos da política de BYOD da organização (ou documento análogo), aos riscos associados a esta prática, aos tipos de ameaças cibernéticas e técnicas utilizadas para promover ataques e às medidas de segurança que podem ser incorporadas à rotina para mitigar os riscos;
vii. Estimular a incorporação de práticas de segurança no uso de dispositivos pessoais pelos colaboradores para acessar ativos corporativos e atitudes éticas, que zelem pela segurança da informação e cibernética e a conformidade com as políticas, regras e procedimentos da organização;
viii. Promover exercícios de verificação de assimilação de conhecimentos relacionados à prática de BYOD e da capacitação para realização dos procedimentos estabelecidos no termo de uso de dispositivos pessoais para acesso a ativos da organização; e
ix. Implementar, conforme aplicável, as recomendações e orientações técnicas contidas no guia técnico ANBIMA *Orientações para o treinamento de colaboradores em cibersegurança*[14].

h. Estabelecer procedimentos de contingência para tratamento de incidentes de segurança da informação e cibernética envolvendo dispositivos pessoais de colaboradores com acesso aos ativos da organização, de forma específica ou integrando documentos e políticas da organização já estabelecidos (por exemplo, relacionados à continuidade de negócios), considerando:

i. Definir e descrever táticas e medidas de contingência específicas e adequadas para as diferentes ameaças e vulnerabilidades que podem envolver os dispositivos pessoais utilizados para acessar os ativos corporativos;
ii. Definir critérios e processos de ativação das táticas e medidas de contingência definidas, indicando responsáveis pela realização de cada etapa;
iii. Identificar e avaliar o incidente, buscando mensurar sua extensão e implementar as táticas e medidas adequadas para recuperação e mitigação dos impactos;
iv. Proteger as evidências do incidente e adotar as medidas cabíveis com relação à privacidade e proteção de dados e de comunicação do incidente às autoridades e autarquias competentes, conforme aplicável;
v. Definir situações elegíveis à revogação temporária ou definitiva dos acessos do dispositivo pessoal a ativos da organização, à desconexão completa e ao apagamento remoto de dados corporativos;

[14] ANBIMA. Orientações para treinamento de colaboradores em cibersegurança (2024). Disponível em: <https://www.anbima.com.br/data/files/67/25/31/3D/483B49100054FA49B82BA2A8/Orientacoes_treinamento_de_colaboradores_em_ciber.pdf>

vi. Garantir o adequado tratamento do incidente e recuperação dos padrões de segurança antes de retomar os acessos de um dispositivo pessoal sujeito à revogação temporária de acessos; e
vii. Implementar, conforme aplicável, as recomendações e orientações técnicas contidas no guia técnico ANBIMA *Orientações para cibersegurança na gestão de continuidade de negócios*[15].

i. Estabelecer procedimentos de revisão e atualização periódicos da política de BYOD, ou documento análogo, para garantir conformidade e eficácia, considerando:

i. Definir colaboradores e/ou equipes responsáveis pela manutenção da política de BYOD, ou documento análogo, incluindo a realização dos procedimentos de revisão e atualização;
ii. Definir fluxo de aprovações e validações necessárias para implementação da revisão e atualização;
iii. Estabelecer prazos regulares para realização dos procedimentos de revisão e atualização periódicos não superiores a 2 (dois) anos, abrangendo situações que exijam adaptação dos cronogramas estabelecidos, por exemplo em decorrência de atualizações em leis ou regulações aplicáveis;
iv. Estabelecer procedimentos de notificação dos colaboradores acerca de revisões e atualizações realizadas, abrangendo medidas para obtenção de consentimentos quando necessário;
v. Garantir que a política de BYOD, ou documento análogo, esteja em conformidade com a legislação, regulação e autorregulação vigentes;
vi. Investir os melhores esforços para manter a política de BYOD, ou documento análogo, alinhada aos principais padrões de segurança reconhecidos internacionalmente; e
vii. Investir os melhores esforços para manter a política de BYOD, ou documento análogo, atualizada com relação ao desenvolvimento tecnológico e à evolução de ameaças à segurança da informação e cibernética.

2. Identificação e gestão de dispositivos

Este tópico aborda elementos mínimos, e não exaustivos, a serem considerados pelas organizações na implementação de rotinas e procedimentos para identificação e gestão dos dispositivos pessoais utilizados para acessar os ativos corporativos, observáveis pelas equipes responsáveis pela segurança da informação e cibernética.

[15] ANBIMA. Orientações para Cibersegurança na Gestão de Continuidade de Negócios (2024). Disponível em: <https://www.anbima.com.br/data/files/03/74/D7/D3/A94749107AF1F649EA2BA2A8/Orientacoes_ciberseguranca_na_continuidade_de_negocios.pdf>

Recomendações:

2.1. Implementar rotinas e procedimentos para identificação dos dispositivos pessoais utilizados para acessar os ativos da organização, considerando:

a. Garantir a manutenção e eficácia do procedimento definido na política de BYOD, ou documento análogo, para o colaborador informar e manter atualizada a organização acerca dos dispositivos pessoais a partir dos quais acessa os ativos corporativos.

b. Estabelecer critérios e procedimentos para aprovação da conexão de dispositivos pessoais aos ativos corporativos e para seu registro.

c. Manter inventário atualizado de dispositivos pessoais utilizados para acessar os ativos corporativos e verificá-los com frequência para identificar elementos estranhos à organização.

2.2. Implementar rotinas e procedimentos de gestão dos dispositivos pessoais utilizados para acessar ativos da organização, considerando:

a. Avaliar a adoção de soluções de gestão de mobilidade empresarial (EMM – Enterprise Mobility Management), incluindo ferramentas de gerenciamento de dispositivos móveis (MDM – Mobile Device Management), que permitem a aplicação de políticas e controles de segurança, a instalação de atualizações e a remoção de dados corporativos para os casos aplicáveis.

3. Identificação e avaliação de riscos

Este tópico aborda elementos mínimos, e não exaustivos, a serem considerados pelas organizações na implementação de rotinas e procedimentos para identificação e avaliação dos riscos, ameaças e vulnerabilidades associados ao uso de dispositivos pessoais para acessar ativos corporativos, observáveis pelas equipes responsáveis pela segurança da informação e cibernética.

Recomendações:

3.1. Implementar rotinas e procedimentos para identificação e avaliação dos riscos, ameaças e vulnerabilidades associados ao uso de dispositivos pessoais para acessar ativos da organização, considerando:

a. Monitorar os dispositivos pessoais para detectar anomalias, incluindo a implementação de soluções de defesa contra ameaças móveis (MTD – Mobile Threat Defense), abrangendo minimamente a identificação de:

i. Aplicativos maliciosos;
ii. Ataques de rede (e.g. man-in-the-middle); e
iii. Configurações inseguras.

b. Implementar procedimentos para avaliação de aplicativos moveis (Vetting), incluindo, conforme aplicável, testagem de segurança (MAST – Mobile Application Security Testing), abrangendo minimamente a identificação de:

   i. Vulnerabilidades;
   ii. Comportamentos que violem políticas de privacidade; e
   iii. Uso indevido de dados sensíveis.

c. Avaliar implementar soluções de registro e monitoramento de atividades para detectar a comportamentos suspeitos ou maliciosos.

d. Auditar periodicamente os dispositivos pessoais para avaliar a eficácia dos controles e das políticas de segurança.

4. Controles para mitigar riscos identificados

Este tópico aborda elementos mínimos, e não exaustivos, a serem considerados pelas organizações na implementação de práticas e controles de segurança para mitigação dos riscos identificados associados ao uso de dispositivos pessoais para acessar ativos corporativos, observáveis pelas equipes responsáveis pela segurança da informação e cibernética.

Recomendações:

4.1. Implementar práticas e controles de segurança para mitigação dos riscos identificados associados ao uso de dispositivos pessoais para acessar ativos corporativos, considerando:

a. Implementar soluções de controle de acesso gerenciado, abrangendo minimamente:

   i. Exigir autenticação multifator (MFA – Multi-Factor Authentication) para acesso a ativos corporativos a partir de dispositivos pessoais, destacadamente para acesso remoto a ativos críticos;
   ii. Garantir que o acesso seja concedido com base no Princípio do Menor Privilégio, prevendo a concessão de permissões e acessos estritamente necessários para o desempenho de funções legítimas, conforme aplicável;
   iii. Definir critérios específicos para acesso com base nos diferentes contextos, tais como localização, horário e tipo de dispositivo utilizado;
   iv. Adotar políticas de senha segura e definir critérios para bloqueio de acesso após tentativas falhas; e
   v. Implementar procedimentos específicos relacionados à situação de desligamento do colaborador, incluindo a revogação de acessos e desconexão completa do dispositivo.

b. Implementar procedimentos de gerenciamento de dados, abrangendo minimamente:

   i. Adotar soluções de criptografia de dados em repouso e em trânsito;
   ii. Empregar soluções de rede privada virtual (VPN) para conexões remotas seguras; e

iii. Implementar soluções de segregação de dados pessoais e corporativos, incluindo, conforme aplicável, adoção de contenção de dados (containers), perfis de trabalho e/ou virtualização; e
iv. Implementar procedimentos específicos relacionados à situação de desligamento do colaborador, incluindo a remoção e/ou apagamento remoto de dados corporativos.

c. Implementar procedimentos de proteção do colaborador e do dispositivo pessoal utilizado para acessar ativos da organização, abrangendo minimamente:

i. Integrar as soluções de defesa contra ameaças móveis (MTD) e de gestão de mobilidade empresarial (EMM) para ações automatizadas de mitigação;
ii. Instalar e manter soluções de segurança como antivírus, firewall e proteção contra phishing nos dispositivos pessoais;
iii. Implementar mecanismos de detecção de jailbreak nos dispositivos pessoais utilizados para acesso a ativos corporativos, revogando o acesso ou desconectando dispositivos que apresentem sinais de modificação não autorizada;
iv. Adotar políticas de sandboxing para aplicativos móveis instalados nos dispositivos pessoais, conforme aplicável; e
v. Garantir a atualização de aplicativos e aplicações instalados nos dispositivos pessoais, destacadamente com relação à instalação de patches de segurança mais recentes, e definir critérios para bloqueio de acesso a dispositivos desatualizados.

Dicas adicionais

A política de BYOD, ou documento análogo, deve ser cuidadosamente elaborada para equilibrar a flexibilidade e a conveniência do uso de dispositivos pessoais com a necessidade de proteger os dados e a infraestrutura corporativa. Nesse sentido, além das recomendações dispostas na seção anterior deste documento, estão listadas a seguir dicas adicionais para apoiar as organizações na mitigação de riscos e na promoção de uma cultura de segurança na utilização de dispositivos pessoais para acesso aos ativos corporativos.

PROTEÇÃO FÍSICA DOS APARELHOS

Orientar colaboradores que utilizam dispositivos pessoais para acessar ativos corporativos para a adequada proteção física dos aparelhos (e.g. não deixar desacompanhados em locais públicos), especialmente em viagens, para evitar danos, perdas e furtos.

CUIDADOS NO COMPARTILHAMENTO

Orientar colaboradores para o compartilhamento seguro de dispositivos pessoais utilizados para acessar ativos corporativos com outras pessoas, visando evitar que terceiros realizem condutas que coloquem em risco a segurança do colaborador e da organização.

PLANO DE COMUNICAÇÃO

Orientar colaboradores acerca do tráfego e compartilhamento seguro de dados corporativos, em conformidade com políticas, regras e procedimentos da organização, abrangendo o uso de plataformas de troca de mensagens.

Para se aprofundar nos tópicos relacionados à segurança da informação e cibernética, consulte nossa página especial, acessando o QR CODE ao lado.

#ESPAÇOCIBER

Glossário

GLOSSÁRIO	
TERMOS	**DEFINIÇÃO**
BYOD	Utilização de dispositivos pessoais de colaboradores acessar ativos da organização (Bring Your Own Device).
Containers	Prática que visa isolar aplicações e seus componentes em ambientes controlados e padronizados.
DLP	Prevenção contra perda de dados (Data Loss Prevention).
EMM	Gestão de mobilidade empresarial (Enterprise Mobility Management).
Firewall	Sistema que controla o tráfego de rede com base em regras de segurança.
Jailbreak	Processo de remoção das restrições impostas pelo fabricante de um dispositivo móvel, permitindo acesso irrestrito ao sistema operacional.
LGPD	Lei Geral de Proteção de Dados Pessoais (Lei Nº 13.709/2018).
Man-in-the-Middle (MitM)	Um ataque onde o adversário se posiciona entre o usuário e o sistema para poder interceptar e alterar os dados que trafegam entre eles.
MAST	Testagem de Segurança de Aplicativos Móveis (Mobile Application Security Testing).
MDM	Gerenciamento de dispositivos móveis (Mobile Device Management).
MFA	Autenticação multifator (Multi-Factor Authentication).
Modelo de confiança zero (Zero Trust, ZT)	Conjunto de paradigmas de segurança cibernética que elimina a confiança implícita em usuários, dispositivos ou redes, mesmo que estejam dentro do perímetro corporativo ou previamente autenticados.
MTD	Defesa contra ameaças móveis (Mobile Threat Defense).
Phishing	Uma técnica para tentar adquirir dados sensíveis, tais como números de contas bancárias, através de uma solicitação fraudulenta por e-mail ou num website, em que o perpetrador se faz passar por uma empresa legítima ou pessoa respeitável.
Princípio do Menor Privilégio	Diretriz de segurança que estabelece que cada usuário, processo ou sistema deve operar com o mínimo de permissões necessárias para realizar suas funções legítimas (Least Privilege).
Sandboxing	Um ambiente de execução restrito e controlado que impede que softwares potencialmente maliciosos, como códigos móveis, acessem recursos do sistema além daqueles para os quais estão autorizados.
Vetting	Verificação, avaliação e validação de idoneidade de indivíduos ou sistemas para acesso a informações sensíveis ou ambientes protegidos.
VPN	Ferramenta de rede privada virtual (Virtual Private Network).

Expediente

GUIA TÉCNICO

Orientações de cibersegurança para implementação de política de BYOD

Gerência de Representação de Distribuição de Produtos de Investimentos
Luiz Henrique de Carvalho

Redação
Augusto Brisola

Divulgação
Paula Lepinski

Presidência
Carlos André

Diretoria
Adriano Koelle, Andrés Kikuchi, Aquiles Mosca, Carlos Takahashi, César Mindof, Eduardo Azevedo, Eric Altafim, Fernanda Camargo, Fernando Rabello, Flavia Palacios, Giuliano De Marchi, Gustavo Pires, Julya Wellisch, Pedro Rudge, Roberto Paolino, Roberto Paris, Rodrigo Azevedo, Sergio Bini, Sergio Cutolo, Teodoro Lima e Zeca Doherty

Comitê Executivo
Amanda Brum, Eliana Marino, Francisco Vidinha, Guilherme Benaderet, Lina Yajima, Marcelo Billi, Soraya Alves, Tatiana Itikawa, Thiago Baptista e Zeca Doherty

Grupo Consultivo de Cibersegurança
Adonai Bernardes, Ana Paula Godoy, Anderson Mota, Denise Ornellas, Fabio Nacajune, Frederico Neres, Hanna Ki, Ismar Marcos Leite, Joao Paulo Santos, Jorge Matsumoto, José Silva, Kenia Carvalho, Leonardo Alonso, Lilian Celeri, Luiz Leme, Mauricio Corrêa, Patrik Lemos, Rodrigo Fusco, Simone de Grandis e William Borges

Endereço

Rio de Janeiro
Praia de Botafogo, 501 - 704, Bloco II, Botafogo,
Rio de Janeiro, RJ - CEP: 22250-911
Tel.: (21) 2104-9300

São Paulo
Av. Doutora Ruth Cardoso, 8501, 21º andar, Pinheiros
São Paulo, SP - CEP: 05425-070
Tel.: (11) 3471-4200
www.anbima.com.br