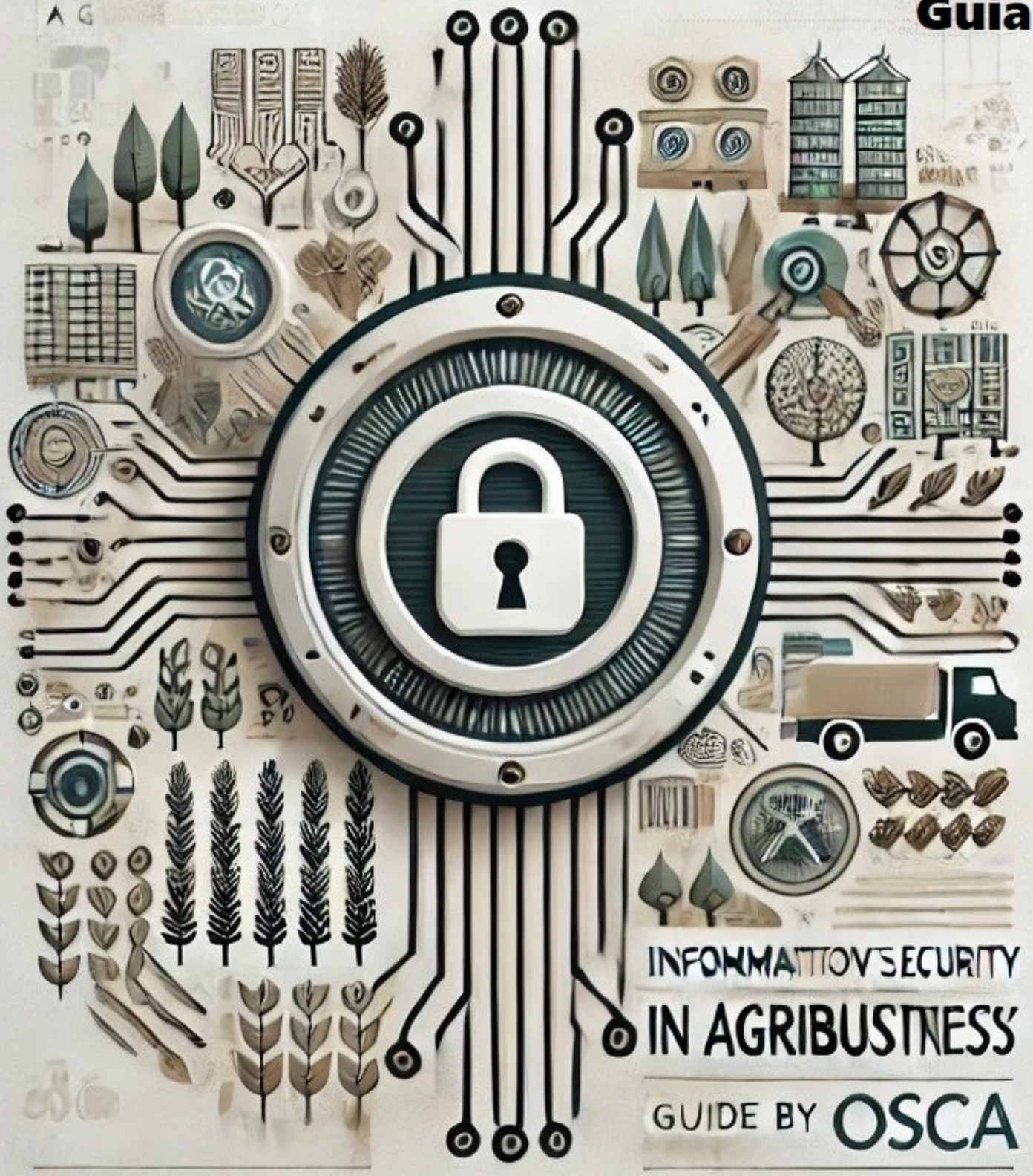
# SEGURANÇA CIBERNÉTICA NO AGRONEGÓCIO

**Guia**



INFORMATION SECURITY IN AGRIBUSINESS

GUIDE BY OSCA

**Dados Internacionais de Catalogação na Publicação (CIP)**
**(Câmara Brasileira do Livro, SP, Brasil)**

Guia de segurança cibernética no agronegócio [livro eletrônico] / organização Heleno do Nascimento Santos...[et al.]. -- Brasília, DF : Ed. dos Autores, 2024.
PDF

Outros organizadores: Helton Fabiano Garcia, João Souza Neto, Marcelo Silva Cunha, Marcus Peixoto, Paulo Henrique Rocha Latado.
Bibliografia.
ISBN 978-65-01-22689-7

1. Agricultura 2. Agronegócio 3. Agropecuária 4. Cibernética - Medidas de segurança 5. Internet - Medidas de segurança I. Santos, Heleno do Nascimento.II. Garcia, Helton Fabiano. III. Souza Neto, João. IV. Cunha, Marcelo Silva. V. Peixoto, Marcus. VI. Latado, Paulo Henrique Rocha.

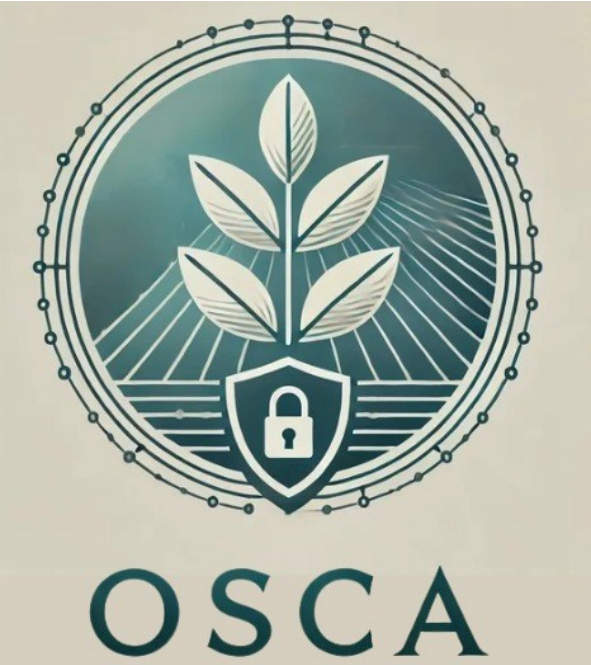
24-238571 CDD-005.8

**Índices para catálogo sistemático:**

1. Internet : Segurança cibernética : Processamento de dados 005.8

Eliane de Freitas Leite - Bibliotecária - CRB 8/8415

Este **GUIA DE SEGURANÇA CIBERNÉTICA NO AGRONEGÓCIO** faz parte da campanha mundial "**Outubro: mês de Conscientização sobre a Segurança Cibernética**" que o **OSCA** aderiu em prol do Agronegócio Brasileiro! Ocorreu ao longo do mês de outubro de 2024, inspirada pelas campanhas da Food and Ag-ISAC, Cybersecurity and Infrastructure Security Agency (CISA), National Cybersecurity Alliance e European Union Agency for Cybersecurity (ENISA).




Pesquisadores, Editores e Fundadores do **Observatório da Segurança Cibernética no Agronegócio - OSCA**:

- Heleno do Nascimento Santos, Dr.
- Helton Fabiano Garcia, MSc.
- João Souza Neto, Dr.
- Marcelo Silva Cunha, MSc.
- Marcus Peixoto, Dr.
- Paulo Henrique Rocha Latado, Engº

# PREFÁCIO

O agronegócio brasileiro vive uma era de profunda transformação digital. A adoção acelerada de tecnologias avançadas como agricultura de precisão, Internet das Coisas (IoT), Inteligência Artificial (IA) e automação tem impulsionado ganhos significativos de produtividade e eficiência em toda a cadeia produtiva. Do campo à mesa, sistemas digitais integrados gerenciam operações, monitoram cultivos, controlam maquinário e otimizam processos logísticos.

Esta revolução tecnológica, no entanto, traz consigo novos desafios e vulnerabilidades. À medida que as atividades agropecuárias se tornam cada vez mais dependentes de sistemas informatizados e conectados, cresce exponencialmente a exposição a riscos cibernéticos. Ataques como *ransomware*, roubo de dados, sabotagem de sistemas de controle industrial e fraudes eletrônicas emergem como ameaças concretas capazes de causar prejuízos financeiros, operacionais e reputacionais significativos.

Neste cenário, a segurança cibernética deixa de ser uma preocupação restrita aos departamentos de TI para se tornar um imperativo estratégico para todo o setor. Proteger a infraestrutura digital, os dados sensíveis e a propriedade intelectual passa a ser tão vital quanto salvaguardar as colheitas ou o rebanho.

Este guia representa um esforço pioneiro para conscientizar e orientar os profissionais do agronegócio brasileiro sobre as melhores práticas de segurança cibernética. Elaborado por especialistas que aliam profundo conhecimento tanto do setor agrícola quanto de tecnologia da informação, o documento oferece recomendações práticas e acessíveis para mitigar riscos e construir resiliência digital.

As orientações aqui contidas são essenciais para que o agronegócio brasileiro possa colher os frutos da transformação digital de forma segura e sustentável. Que este guia sirva como um farol, iluminando o caminho para um futuro em que inovação tecnológica e segurança caminhem lado a lado, garantindo a competitividade e a continuidade dos negócios no campo.

Guilherme Soria Bastos Filho

Coordenador do Centro de Estudos do Agronegócio da FGV

# Observatório da Segurança Cibernética no Agronegócio - OSCA

O **Observatório da Segurança Cibernética no Agronegócio - OSCA** - foi criado por seis pesquisadores em 1º de maio de 2024, após mais de um ano de estudos sobre o tema, com o objetivo de promover a consciência situacional sobre segurança cibernética no agronegócio brasileiro. Seis meses depois, contamos com inúmeros posts e mais de 780 seguidores no LinkedIn.

O **OSCA** é formado pela junção de esforços voluntários oriundos das áreas de agricultura e governança e segurança cibernética, vocacionados para a área de pesquisa e entusiastas por buscar e compartilhar conhecimento. O objetivo é pesquisar questões relacionadas, divulgar informações sobre segurança cibernética e colaborar em eventos e campanhas de conscientização, principalmente por meio das redes sociais, tendo iniciado pelo LinkedIn.

Em poucos mais de um semestre, o **OSCA** já alcançou importantes resultados. O **OSCA** aderiu à campanha global de segurança, como organização campeã da "*Cybersecurity Awareness Month 2024*", promovido pela *National Cybersecurity Alliance* (NCA). Veja nosso post alusivo ao fato.

O **OSCA** também publicou o decálogo de segurança cibernética no agronegócio, o qual serviu de insumo para a confecção do presente Guia.

Além disso, o **OSCA** tem se mostrado ativo na comunicação e alerta de incidentes cibernéticos e vulnerabilidades envolvendo o setor de agronegócio, como ataques de *phishing* e *ransomware*, para auxiliar o agronegócio brasileiro a perceber, compreender e enfrentar ameaças cibernéticas.

Cabe um destaque para a séria questão do déficit de mão de obra especializada em segurança cibernética. Diante desse grave problema o **OSCA** publicou post intitulado "Proposta de um Plano de Ensino de Segurança Cibernética no Agronegócio Brasileiro". As Escolas de Ciências Agrárias do Brasil precisam prover competências (C.H.A.V.) em segurança cibernética para os profissionais do Agronegócio do futuro.

O **OSCA** também colabora na organização de eventos de segurança cibernética para o agronegócio, como no Seminário "Segurança Cibernética no Campo: protegendo a agropecuária do futuro", que ocorreu no dia 7 de novembro de 2024, no Auditório Jonas Pinheiro do Ministério da Agricultura e Pecuária - MAPA, em Brasília. Evento presencial e online, oferecido pela ENAGRO, contando com palestrantes nacionais e internacionais.

# SIGLAS

| | |
|---|---|
| 2FA | *Double-factor authentication* (autenticação em duplo fator) |
| 5W2H | *What? When? Where? Why? Who? How? How Much?* |
| ABNT | Associação Brasileira de Normas Técnicas |
| ANPD | Autoridade Nacional de Proteção de Dados |
| CERT.br | Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil |
| CGI.br | Comitê Gestor da Internet no Brasil |
| CIS | *Center for Internet Security* |
| CISA | *Cybersecurity and Infrastructure Security Agency* |
| CISO | *Chief Information Security Officer* |
| CVM | Comissão de Valores Mobiliários |
| ENAGRO | Escola Nacional de Gestão Agropecuária |
| ENISA | *European Union Agency for Cybersecurity* |
| FBI | *Federal Bureau of Investigation* |
| IBM | *International Business Machines Corporation* |
| IA | Inteligência Artificial |
| ID | Identificador do Usuário |
| IEC | *International Electrotechnical Commission* |
| IoT | Internet das Coisas |
| IREs | *Isolated Recovery Environment* |
| ISAC | *Information Sharing and Analysis Center* |
| ISACA | *Information Systems Audit and Control Association* |
| ISO | *International Organization for Standardization* |
| IT | *Information Technology* (Tecnologia da Informação) |
| MAPA | Ministério da Agricultura e Pecuária |
| MFA | *Multi-factor authentication* (autenticação em múltiplos fatores) |
| NBR | Norma Brasileira Regulamentadora |
| NCA | *National Cybersecurity Alliance* |
| NCIRP | *The National Cyber Incident Response Plan* |
| NCSC | *The National Cyber Security Centre* |
| NIC.br | Núcleo de Informação e Coordenação do ponto BR |
| NIST | *National Institute of Standards and Technology* |

# SIGLAS

| | |
|---|---|
| OSCA | Observatório da Segurança Cibernética no Agronegócio |
| OT | *Operational Technology* (Tecnologia Operacional) |
| PIN | *Personal Identification Number* |
| PPSI | Programa de Privacidade e Segurança da Informação |
| PRIAC | Plano de Resposta a Incidentes e Ataques Cibernéticos |
| SP | *Special Publication* |
| TI | Tecnologia da Informação |
| TIC | Tecnologia da Informação e Comunicações |
| TO | Tecnologia Operacional |
| UTFPR | Universidade Técnica Federal do Paraná |

# ÍNDICE

# PRÁTICAS DE SEGURANÇA CIBERNÉTICA NO AGRONEGÓCIO

Os temas para as práticas de Segurança Cibernética apresentadas neste Guia foram inspirados e complementados do relatório "*Farm-to-Table Ransomware Realities: Exploring the 2023 Ransomware Landscape and Insights for 2024*" da Food and Ag-ISAC a quem nominamos e agradecemos.

## I - SEJA ÚNICO COM SENHAS (INCOMUNS MESMO)!

Escolha boas senhas para a autenticação (*login*) nos sistemas da Propriedade Rural e/ou Agroindustrial, inclusive pessoais.

É realmente uma **QUESTÃO VITAL!**

**USE SENHAS PARA TUDO!**

De acordo com a norma internacional vigente, NIST SP 800-63B (em inglês), recomenda-se utilizar senhas exclusivas contendo uma combinação de ao menos 8 caracteres, números e caracteres especiais. Utilize também letras maiúsculas e minúsculas.

Outra boa opção é uma senha longa - uma senha frase - composta de várias palavras, números e caracteres especiais, tornando-as mais longas e mais complexas do que as senhas.

Sempre utilize senhas robustas para os sistemas "missão crítica" da propriedade.

Em verdade, o ideal é que a Agroempresa possua uma "Política de Senhas" vigente, implantada e de conhecimento dos funcionários operadores de sistemas.

Os cibercriminosos contam com o fato de que muitas pessoas usam a mesma senha para todas as suas contas, ou usam senhas muito simples como, p.ex. "senha", "12345678" (números sequenciais), "00000000" (números repetidos), "asdfg" (sequência do teclado), "mimosa", "margarida", "soja2024", 19121998 (data de nascimento), e por aí vai. Aí o "jogo" fica fácil para o crime cibernético!

Boas práticas na gestão de senhas:

- prefira senhas longas (15 caracteres);
- troque periodicamente;
- proteja a senha da conta de e-mail;
- se anotar as senhas, guarde-as com segurança, longe do equipamento;
- considere usar um gerenciador de senhas.

O que deve ser evitado:

- senhas com elementos facilmente identificáveis por possíveis atacantes hackers / cibercriminosos;
- reuso de senha para os sistemas distintos da propriedade. Assim, o comprometimento de uma senha não permitirá que o atacante tenha acesso a outros sistemas;
- manter senhas padrão (*default*) dos fabricantes dos equipamentos / ativos de software e hardware tão logo sejam conectados à rede da propriedade.

Ao escolher suas senhas, também evite:

- nomes do usuário, próprios ou de famílias;
- identificador do usuário (ID), mesmo com caracteres embaralhados;
- nome de membros da família ou de amigos íntimos;
- nomes de pessoas ou lugares em geral;
- nomes de animais de estimação;
- local e datas de nascimento;
- feriado favorito;
- algo relacionado ao time de futebol favorito;
- nome do sistema operacional ou da máquina que está sendo utilizada;
- números de telefone, de cartão de crédito, de carteira de identidade ou de outros documentos pessoais;
- placas ou marcas de carro;
- palavras que constam de dicionários em qualquer idioma;
- letras ou números repetidos;

- letras seguidas do teclado do computador (ASDFG, YUIOP);
- objetos ou locais que podem ser vistos do local de trabalho.

E por que não adotar esses dados?

Simplesmente porque um atacante pode coletar dados conhecidos da vítima, usando engenharia social, para compor uma bancada de dados (*Rainbow Tables*) para tentar quebrar a sua senha, por força bruta.

Seguem fontes complementares de informações para inspirá-los na **Arte de Criar e Gerenciar Senhas** mais seguras para sistemas agrícolas expostos à Internet:

- Cert.br: Cartilha de Segurança para Internet - Fascículo Senhas;
- TCU: Boas práticas em segurança da informação, pág. 20.

Em inglês:

- Food and Ag-ISAC: *Farm-to-Table Ransomware Realities*;
- NCSC, Inglaterra: Cyber security for farmers, pág. 9.

A família de normas NIST SP 800-63 encontra-se em revisão pela comunidade.

Esta norma é parte integrante de uma série de 4 volumes, que hoje se encontra em revisão.

A nova proposta acrescenta também a recomendação de dar preferência a senhas de tamanho mais longo, 15 caracteres, podendo ser formada por uma combinação de palavras, ou senha frase, mantendo ou melhorando a segurança da senha contra ataques e, ao mesmo tempo, facilitando a sua memorização.

- https://pages.nist.gov/800-63-3/
- https://pages.nist.gov/800-63-4/

Em breve o OSCA trará as novidades afetas ao uso no nosso setor: Agronegócio Digital.

Senhas robustas é preciso!

**Conscientizar é preciso!**

**PROTEJA NOSSO MUNDO!**

# II - IMPLEMENTE MFA - Autenticação Multifator!

MFA (*Multi-factor authentication*) é um procedimento de segurança para verificar a identidade de um usuário por meio de duas ou mais formas de autenticação, antes de conceder acesso a uma conta ou sistema. Uma forma de implementar MFA é usando 2FA, autenticação em duas etapas.

Basicamente, o 2FA exige uma segunda forma de verificação, além da senha, que serve como primeiro fator. Isso geralmente envolve um código enviado para seu e-mail ou um aplicativo de autenticação.

O objetivo do 2FA é oferecer autenticação mais robusta. Veja a questão do ponto de vista do atacante. Agora ele precisa comprometer dois fatores para ter acesso indevido à conta da vítima. Então, mesmo que a senha seja comprometida, o atacante não conseguirá entrar na conta sem o 2FA. Logo, a medida é capaz de reduzir risco de comprometimento de contas e acessos não autorizados.

**E por que isso é importante?**

Segundo o relatório "*2024 Data Breach Investigations Report*" o roubo de identidades figura entre as principais preocupações relacionadas a crimes cibernéticos.

De acordo com o relatório publicado pelo FBI em 2023, intitulado "*Internet Crime Report*", o roubo de identidade gerou prejuízos de mais de US$ 126 milhões.

Além disso, a Estratégia de Segurança Cibernética 2023 - 2030 publicada pelo governo australiano reconhece que o roubo de identidade pode ter consequências devastadoras para as empresas e os indivíduos. Vítimas podem passar dias ou semanas com seus sistemas inoperantes tentando recuperar suas identidades roubadas, enfrentando perdas financeiras e operacionais significativas.

**E como implementar 2FA?**

Os fatores de autenticação são baseados em três tipos:

| | |
|---|---|
| • O que se/você sabe: | geralmente é representado por uma senha ou PIN. |
| • O que se/você tem: | em geral, um *token* de segurança ou um aplicativo autenticador. |
| • O que se/você é: | biometria, como impressão digital, reconhecimento facial. |

A adoção de 2FA está alinhada com boas práticas de segurança nacionais, como a família de normas da ABNT NBR ISO/IEC 27.000 e internacionais, como NIST SP 800-63, mencionado no primeiro post, sobre senhas, dessa campanha.

Em resumo, o MFA/2FA representa camada extra de segurança colaborando para proteger contas e informações contra ameaças. Implementá-lo é uma das melhores práticas de segurança, para usuários e organizações.

Vídeo explicativo no YouTube Autenticação Multifator (MFA) da Minds.digital.

Fique seguro!

**Conscientizar é preciso!**

**PROTEJA NOSSO MUNDO!**

## III - CUIDADO COM O *PHISHING*: NÃO MORDA A ISCA!

### Você sabe o que é *Phishing*?

Segundo a Cartilha de Segurança para Internet do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (Cert.br e Nic.br) trata-se de uma armadilha digital comumente encaminhada por e-mail, para ludibriar vítimas, com o objetivo de auferir vantagens, como comprometer senhas de usuários, infligir prejuízos financeiros e roubar informações sensíveis, que podem ser vendidas.

As estatísticas apontam *Phishing* como o principal vetor de ataque. O relatório anual "*Cyber Security Breaches Survey 2024*" publica pesquisas sobre violações de segurança cibernética no Reino Unido. Nas últimas edições, 2021, 2022 e 2023, *Phishing* permanece como, nos termos dos relatórios, "de longe o tipo mais comum de ataque".

Conforme matéria intitulada "3,5 milhões de brasileiros vítimas de *phishing*" publicada na revista CISO Advisor, recente levantamento da consultoria Redbelt Security revelou que ao menos 3,5 milhões de brasileiros foram vítimas de *phishing* em 2023. Estima-se aumento mínimo de 30% para 2024.

**E por que *Phishing* pode se tornar uma tremenda dor de cabeça?**

Clicar em links indevidos é a maneira mais comum de infecção por *Phishing*. O link pode levar à instalação de softwares maliciosos, capazes de danificar ou roubar dados da vítima. Pode haver redirecionamento para sítios falsos projetados pelo atacante para coletar informações da vítima, como nomes de usuário, senhas ou dados bancários. O atacante pode obter acesso indevido ao dispositivo da vítima, permitindo monitorar atividades ou roubar informações sensíveis, bem como escalonar privilégios de acesso dentro do dispositivo ou mesmo na rede da vítima

**E por que *Phishing* é tão popular?**

Simplesmente porque é tentador e lucrativo! O relatório do *Federal Bureau of Investigation* (FBI), denominado "*Internet Crime Report*", 2023, alerta que perdas relacionadas a comprometimento de e-mails podem ser superiores a US$ 2,9 bilhões, estimativa superior ao relatório de 2022, cuja previsão foi de US$ 2,7 bilhões.

**Certo, mas eu tenho soluções de segurança da minha empresa. Estou seguro então?**

O relatório "*Phishing Benchmark Global Report*", da Fortra e Microsoft, alerta que soluções de tecnologia podem não ser suficientes para garantir proteção contra *Phishing* e destaca a importância de ações educativas com os colaboradores para promover e fortalecer cultura de segurança na organização.

Vale também acessar o fascículo *Phishing* e Outros Golpes - Cartilha de Segurança para Internet e ainda o Guardião Cibernético 6.0 para mais informações.

**Conscientizar é Preciso!**

**PROTEJA NOSSO MUNDO!**

# IV - ATUALIZE SEU AMBIENTE!

A atualização tem como objetivo identificar e corrigir falhas que possam ser usadas por invasores para comprometer a segurança de um sistema. Desta forma, organizações conseguem proteger suas informações e dados sensíveis contra-ataques cibernéticos, reduzindo a exposição a riscos que possam prejudicar suas operações. Ou seja, diminuir a sua superfície de ataque.

A aplicação de correções ("*patch management*") visa corrigir vulnerabilidades existentes e identificadas pelos fabricantes.

Falando agora em uma linguagem simples. "O que acontece quando se encontra um buraco na cerca da fazenda?" "Você não precisa consertá-la?" Então, vulnerabilidade para a cerca pode ser um buraco que precisa ser corrigido. E quando a cerca foi consertada, podemos dizer que a correção foi aplicada ("*patch*") e a fazenda (sistema) está protegida.

E por que esse assunto é importante?

Segundo o relatório publicado pela agência de cibersegurança europeia "*ENISA Threat Landscape, 2024*", foi registrado significativo aumento de 26,35% na variação anual de vulnerabilidades identificadas: 33.524, de jul/23 a jul/24, contra 24.690, de jul/22 a jul/23.

O mesmo relatório destaca a necessidade de aplicar correções, priorizando as vulnerabilidades classificadas como 'altas' ou 'críticas'. Prática essencial para proteger um Agronegócio contra ataques. Em muitos casos, vulnerabilidades podem apresentar um ponto de entrada mais acessível para cibercriminosos.

Preocupa também o comportamento pré-assintótico da curva de vulnerabilidades cumulativas, evidenciado no relatório IBM "*X-Force Threat Intelligence Index 2022*".

Sendo assim, a correção de vulnerabilidades é fundamental para:

- Prevenir ataques cibernéticos: ao corrigir falhas antes que possam ser exploradas, age-se de forma preventiva, para impedir que invasores "passem pela cerca";
- Reduzir riscos: identificar vulnerabilidades possibilita a priorização de ações, permitindo que as mais críticas sejam tratadas rapidamente;

- Atender normas e regulamentos: muitas legislações e normas de segurança exigem que as empresas mantenham processos de gestão de vulnerabilidades;
- Proteger dados, inclusive pessoais e sensíveis à organização: contribui-se para a proteção de informações classificadas e pessoais, vazamentos e comprometimento.

Em resumo, fiquem de olho na sua cerca! Rompeu? Precisa consertar!

É assim no espaço cibernético.

Atualizar é Preciso!

**Conscientizar é preciso!**

**PROTEJA NOSSO MUNDO!**

## V - FAÇA BACKUP DE ARQUIVOS E TESTE (PERIODICAMENTE)!

Para você do agronegócio, uma pergunta básica. Você coloca todos os ovos na mesma cesta?

Sim? Vamos falar sobre isso.

*Backups* são arquivos, equipamentos, dados e procedimentos disponíveis para uso em caso de falha ou perda, se os originais forem destruídos ou estiverem fora de serviço, segundo o glossário de termos publicado pela ISACA.

A disponibilidade dos dados é um dos pilares da segurança da informação, e sem *backups*, a perda de dados pode causar prejuízos significativos. Sendo assim, é imprescindível que o processo de backup ocorra de maneira periódica e programada.

A importância do *backup* reside na proteção de dados e na continuidade de negócios. Ele é essencial para garantir que informações possam ser recuperadas, em situações de falhas, erros humanos ou ataques, como *ransomware*. Neste último caso, o ciclo de vida de ataque por *ransomware* já foi analisado pelo OSCA. Veja os posts:

- Ciclo de Vida de Ataque de Ransomware - Parte 1 e
- Ciclo de Vida de Ataque de Ransomware - Parte 2.

Segundo o relatório publicado pelo Gartner, "*How to Recover From a Ransomware Attack Using Modern Backup Infrastructure*", um backup preparado contra *ransomware* vai além das simples cópias de segurança:

- Incorporação de tecnologias avançadas como backups imutáveis que não podem ser alterados ou excluídos, mesmo que o sistema principal seja comprometido;
- Adoção de ambientes de recuperação isolados (IREs) para preservar dados separados fisicamente ou logicamente do restante da rede, prevenindo que sejam acessados ou corrompidos por *ransomware*;
- Recursos de análise de anomalias e inteligência artificial para detectar padrões de comportamento suspeitos nos dados de backup, garantindo que a restauração não reintroduza o malware no sistema.

A expectativa é de mitigar riscos de perda ou alteração indevida de dados, bem como de assegurar que dados possam ser recuperados em caso de incidentes, além de definir ponto de recuperação em caso de desastre.

Agora você já sabe. Deixe seus ovos em cestas separadas!

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (Cert.br e Nic.br) fornece essas ótimas cartilhas e apresentação, em português:

- *Backup*;
- Fascículo *Backup*; e
- Apresentação *Backup*.

Façam o *download* e distribuam para os funcionários da fazenda.

Implantem uma **Política de Backup**!

O Modelo de Política de Backup, do PPSI é uma boa fonte.

Fazer backup e Testar é preciso!

**Conscientizar é preciso!**

**PROTEJA NOSSO MUNDO!**

# VI - SEGMENTE SUAS REDES!

Mas, o que é isso, segmentação?

Vamos explicar por uma analogia do campo.

*Na minha infância, visitava meus avôs que moravam numa colônia de imigrantes no interior do Paraná. Pequena fazenda. Sem água encanada. Banheiro à base de fossa seca.*

*Gostava de visitar a "criadeira", onde ficavam os pintinhos para dar "quirera". Acho que falei certo, porque era o termo que ouvia do meu avô, com um sotaque bem carregado. Ambiente de madeira, conjugado com misto de simplicidade e improviso.*

*Um dia soube que o local foi visitado por uma espécie de raposa do campo à procura de alimentos. Aproveitou um ponto fraco na estrutura para invadir o espaço. O estrago foi grande.*

*Na ocasião, lembro-me de ter imaginado se o estrago poderia ser um pouco menor se o ambiente fosse dividido. Devia ter uns 8 anos. Era introvertido, mas muito imaginativo. Então a conversa foi comigo mesmo. E a vida seguiu.*

Segmentação é isso! Separar a "criadeira" em vários ambientes.

Segmentação de redes é a divisão em várias sub-redes, onde os segmentos podem funcionar de forma relativamente independente e o tráfego entre eles pode ser controlado por dispositivos como firewalls ou roteadores. A segmentação é fundamental como medida protetiva. Inclusive contra *ransomware*.

Mas o que é *ransomware* mesmo? O OSCA já elaborou dois posts bem interessantes sobre análise do ciclo de vida de ataque por *ransomware*. Veja os posts:

- Ciclo de Vida de Ataque de Ransomware - Parte 1 e
- Ciclo de Vida de Ataque de Ransomware - Parte 2.

O relatório publicado pelo Gartner, "*How to Recover From a Ransomware Attack Using Modern Backup Infrastructure*", esclarece que a segmentação é medida fundamental para reduzir possibilidades de que o malware se espalhe para outras partes da rede. Se um segmento é comprometido, se estiver isolado, pode impedir que outro não o seja, como forma de minimizar impacto

do ataque. Mesmo raciocínio se aplica a uma invasão e na tentativa de movimentação lateral pelo atacante.

A Food and Ag-ISAC recomenda ao Agronegócio no seu relatório intitulado "*Farm-to-Table Ransomware Realities: Exploring the 2023 Ransomware Landscape and Insights for 2024*":

***"garanta a segmentação de suas redes (como manufatura/produção da rede de negócio) a fim de limitar / mitigar o risco operacional caso haja interrupção".***

Já a matéria "*Segmentação de redes pode evitar disseminação de ransomware*" da revista Security Leaders, por ocasião do *ransomware* WannaCry em 2017, ajuda a entender a disrupção desses ataques.

Entendeu o que é segmentação? Separe a sua "criadeira".

Segmentar é preciso!

**Conscientizar é preciso!**

**PROTEJA NOSSO MUNDO!**

## VII - TENHA UM PLANO DE RESPOSTA A INCIDENTES E ATAQUES CIBERNÉTICOS!

**Ataque Cibernético ao Agro?**

*"A pergunta não é mais 'SE' serei atacado,*

*. . .*

*mas 'QUANDO' serei atacado"!*

Frase instigante da Drª Christa Hoffmann, Agrônoma e Profª de Agricultura Digital da Universität Hohenheim na Alemanha e primeira presidente da GIL - Sociedade alemã de Informática na Agricultura, Silvicultura e Indústria Alimentícia, em coluna intitulada "Safety First".

Dessa forma, ter Resiliência Cibernética e estar preparado é uma

**QUESTÃO DE SOBREVIVÊNCIA!**

Ter em vigor, e testar, um Plano de Resposta a Incidentes e Ataques Cibernéticos - PRIAC, em especial para *ransomware*, vai ajudar a empresa do Agro a recuperar e restaurar suas operações de forma mais rápida e efetiva.

O NIST define um PRIAC como "a documentação de um conjunto predeterminado de instruções ou procedimentos para detectar, responder e limitar as consequências de ataques cibernéticos maliciosos contra o(s) sistema(s) de informação de uma organização".

Este Plano deve, no estilo 5W2H, prever: notificar e acionar o time de resposta; avaliar o incidente e a necessidade de comunicar à ANPD, CVM, etc.; conter e erradicar; recuperar; fazer as lições aprendidas; e documentar.

A matéria intitulada "A Importância de um Plano de Resposta a Ataques Cibernéticos" da revista digital TI Inside contextualiza bem essa necessidade.

Referências que podem inspirar o Agronegócio a construir o seu PRIAC:

- o Guia "Computer Security Incident Handling Guide" - NIST SP 800-61 Rev. 2, do NIST americano, é a principal referência mundial para a construção de PRIACs;
- a norma ABNT NBR ISO/IEC 27.035-1 - Gestão de Incidentes de Segurança da Informação é basilar;
- o "Guia de Resposta a Incidentes de Segurança da Secretaria de Governo Digital", do PPSI do Governo Federal, é uma boa referência;
- a agência CISA apresenta o "The National Cyber Incident Response Plan - NCIRP", norte-americano;
- a agência ENISA, da comunidade europeia, dispõe uma série de informações sobre resposta a incidentes para download.

Infelizmente, ataques cibernéticos bem sucedidos contra a Propriedade Rural e/ou Agroindustrial irão ocorrer.

**ESTEJAM PREPARADOS!**

Planejar a "Resposta a Incidentes e Ataques Cibernéticos" é preciso!

**Conscientizar é preciso!**

**PROTEJA NOSSO MUNDO!**

## VIII - CRIPTOGRAFE SEUS ARQUIVOS SENSÍVEIS!

Você conhece a velha brincadeira do telefone com fio e latas?

Pois é, e se essa comunicação pudesse ser ouvida de forma sorrateira por um terceiro? Nessa brincadeira, bastaria estar por perto. No mundo digital, precisamos proteger a informação com criptografia.

Vamos explicar.

A cadeia de dados sensíveis no Agronegócio é importante e longa: como dados de cooperados, funcionários, clientes e fornecedores; de propriedade intelectual, e financeiros. Vitais para as empresas. Além disso, a conformidade com regulamentos de proteção de dados é uma obrigação para evitar violações legais e prejuízos à reputação.

A criptografia é um dos principais métodos de proteção de dados, tanto em trânsito quanto locais. Ela mitiga o risco de comprometimento dos dados e é fundamental para atender às exigências regulatórias que visam proteger informações sensíveis.

A falta de criptografia pode expor a empresa a ataques, onde dados sensíveis podem ser extraídos sem que a organização perceba. Além disso, dispositivos físicos roubados ou ataques a parceiros podem comprometer informações críticas. Erros de gestão de dados e falhas humanas também são uma fonte comum de vazamentos de dados, causando graves impactos nos negócios.

É a raposa à espreita dos seus dados.

Qual a solução?

A criptografia serve para proteger suas informações e documentos mais sensíveis, incluindo informações de clientes, fornecedores, colaboradores e cooperados, informações de identificação pessoal e e-mails. Na prática, uma organização possui informações com diferentes níveis de criticidade e classificação.

O CIS (*Center for Internet Security*) v8 é conjunto de 18 práticas recomendadas de segurança cibernética, criado para ajudar organizações a proteger seus sistemas e dados contra ameaças cibernéticas. É organizado de forma a ser mais adaptável a tecnologias modernas, como a nuvem e o trabalho remoto, e pode ser aplicado em diferentes tipos de organizações, independentemente do tamanho, inclusive para o setor de agronegócio.

Não à toa, o controle 3 – proteção de dados, prevê nada menos do que 4 das suas 14 medidas protetivas, especificamente falando de criptografia em diferentes aspectos. Criptografia de dados em dispositivos de usuário final (3.6); em mídias (3.9); em trânsito (3.10); localmente (em repouso) (3.11).

Essa ênfase acaba sendo reflexo da necessidade do uso da criptografia para manter os seus dados protegidos.

E no caso da brincadeira de fio e latas, é uma forma de assegurar uma bate-papo seguro.

Agora você já sabe. Criptografe seus dados!

Criptografar os dados sensíveis é preciso!

**Conscientizar é preciso!**

**PROTEJA NOSSO MUNDO!**

## IX - COMPARTILHAR É CUIDAR!

Grupos de *ransomware* compartilham conhecimento uns com os outros e “Congressos Hackers” já ocorreram pelo mundo.

Devemos, também, compartilhar uns com os outros para nos ajudarmos mutuamente. O relacionamento com empresas semelhantes pode nos ajudar a nos manter informados sobre um cenário adverso em constante mudança/evolução para que possamos nos defender apropriadamente.

Converse com seus funcionários, colegas e parceiros sobre segurança cibernética. Compartilhe informações sobre as ameaças que você identifica para que eles possam estar mais bem preparados e pergunte o que identificam para que você possa estar mais bem preparado.

Compartilhe “Guias” e “Boas Práticas” com seus funcionários e pares, capacite-os, para conscientizá-los sobre como podem proteger seu agronegócio. As Cartilhas do Cert.br / Nic.br / Cgi.br trazem boas práticas sobre Segurança da Informação e Cibernética.

**Deixe bem claro para seus funcionários que você leva a Segurança Cibernética a sério e espera que eles façam o mesmo! Cada colaborador é uma parte crítica da sua equipe de segurança e, muitas vezes, sua primeira linha de defesa.**

Em Gestão do Conhecimento, define-se uma Comunidade de Práticas como “um grupo de pessoas que compartilham uma preocupação, um conjunto de problemas, ou uma paixão sobre um assunto, e que aprofundam seu conhecimento e domínio nesta área interagindo em uma base contínua”.

Uma ISAC (*Information Sharing and Analysis Center*) é uma Comunidade de Práticas. São organizações sem fins lucrativos que proveem um recurso central para a coleta e compartilhamento de informações sobre ameaças cibernéticas entre os setores privado e público.

A ENISA oferece um excelente Guia para a criação de ISACs.

São competências de uma ISAC sobre Segurança Cibernética:

- Compartilhar informações sobre:
    - incidentes;
    - ameaças;
    - vulnerabilidades;
    - mitigações;
    - consciência situacional;
    - melhores práticas;
    - análises estratégicas;
- Análise;
- Construção de Confiança;
- Construção de Competências;
    - análise de vulnerabilidade e ameaças;
    - treinamentos;
    - exercícios.

São razões para criação de uma ISAC:

- Setor privado:
    - estabelecer cooperação;
    - prover acesso a conhecimento e experiências;
    - networking;
    - fazer parte do grupo de “pressão dos pares”;
    - economia de dinheiro;
- Regulações internacionais;
- Setor público:
    - conhecimento a respeito do nível de segurança em setores críticos;
    - possibilidade do estabelecimento de um único ponto de coordenação;
    - melhor conhecimento sobrem as necessidades do setor privado

A Food and Ag-ISAC, fundada em maio de 2023, é a ISAC do Setor de Infraestrutura Crítica de Alimentos e Agricultura dos Estados Unidos.

Diante de um Agro pujante e em forte processo de digitalização, responsável por alimentar 213 milhões de cidadãos e por quase ¼ do PIB do Brasil, não restam muitas dúvidas:

O Agronegócio brasileiro precisa criar sua própria ISAC para sua proteção contra os crescentes ataques cibernéticos!

Compartilhar é preciso!

Cuidar é preciso!

**Conscientizar é preciso!**

**PROTEJA NOSSO MUNDO!**

# X - SIGA O OSCA

Para fortalecer a Segurança Cibernética no Agronegócio brasileiro, é fundamental que empresas do Agronegócio e seus profissionais se conscientizem sobre os riscos envolvidos e adotem boas práticas de proteção de dados, informações, sistemas, equipamentos, maquinários, ativos corporativos e de software, etc.

O setor de Agricultura e de Alimentos, para o governo norte-americano, é considerado como um dos 16 setores cujos ativos, sistemas e redes, sejam físicos ou virtuais, são considerados tão vitais que sua incapacitação ou destruição teria um efeito debilitante sobre a segurança propriamente dita, a segurança econômica nacional, a saúde ou a segurança pública nacional, ou qualquer combinação disso, https://www.fda.gov/food/food-defense-initiatives/food-and-agriculture-sector-and-other-related-activities.

A adesão à campanha global de Conscientização sobre a Segurança Cibernética é uma das iniciativas promovidas pela OSCA com o objetivo de auxiliar o agronegócio brasileiro a lidar com este cenário desafiador. A campanha buscou inspirar e orientar o setor a adotar medidas de segurança mais robustas, acompanhando as melhores práticas recomendadas por entidades de referência, como a Cybersecurity and Infrastructure Security Agency (CISA), Food and Ag-ISAC, National Cybersecurity Alliance e a European Union Agency for Cybersecurity (ENISA).. O alinhamento com esses padrões internacionais representa um passo importante para preparar o setor agropecuário nacional contra ciberataques cada vez mais sofisticados.

Ao longo deste mês de conscientização, o OSCA reforçou a importância de seguir as recomendações e acompanhar os conteúdos informativos sobre segurança cibernética que serão disponibilizados.

O compartilhamento de informações e a aplicação de melhores práticas são as principais armas para proteger o agronegócio brasileiro de ameaças cibernéticas.

Resumo da campanha OSCA: “**Outubro: mês de Conscientização sobre a Segurança Cibernética no Agronegócio Brasileiro**”.

Contribua para um ambiente digital mais seguro e esteja preparado para os desafios de um mundo cada vez mais conectado e interdependente.

E conscientizar é preciso. Esse é justamente o trabalho promovido pelo OSCA!!

Seguir o OSCA é Preciso!

Não deixe de acompanhar nossos posts sobre segurança cibernética!!

Fique seguro!

**Conscientizar é preciso!**

**PROTEJA NOSSO MUNDO!**

## GLOSSÁRIO DE TERMOS

Cabem aqui algumas definições de termos empregados neste Guia e no mundo da Segurança Cibernética.

Procuramos utilizar aqui uma diversidade de fontes de Glossários de Termos, em português e inglês, para que os gestores e operadores dos sistemas digitais do Agronegócio tenham boas fontes para consulta e estudo.

O "**Glossário de Terminologias das Publicações de Segurança Cibernética e Privacidade**" do *National Institute of Standards and Technology*[1] (NIST, 2024) define como:

- **Ameaça Cibernética (Ciber Ameaça)** - qualquer circunstância ou evento com o potencial de impactar negativamente as operações de uma organização (incluindo missão, funções, imagem ou reputação), ativos organizacionais, indivíduos, outras organizações, ou uma nação utilizando sistemas de informações por meio de acesso não autorizado, destruição, divulgação/revelação, modificação de informações, e/ou negação de serviços;
- **Ataque Cibernético (Ciber Ataque)** - qualquer tipo de atividade maliciosa que tenha a intenção de coletar, causar disrupção, negar, degradar ou destruir recursos de sistemas de informações ou a própria informação;
- **Espaço Cibernético (Ciber Espaço)** - um domínio global dentro do ambiente de informações consistindo de redes interdependentes de infraestruturas de sistemas de informação incluindo a Internet, redes de

[1] Glossário de Terminologias das Publicações de Segurança Cibernética e Privacidade do NIST - https://csrc.nist.gov/glossary

telecomunicações, sistemas de computadores e processadores e controladores integrados;

- **Incidente Cibernético (Ciber Incidente)** - um conjunto de ações tomadas durante o uso de um sistema ou rede de informações que resultem em um efeito adverso, real ou potencial, em um sistema ou rede de informações e/ou na própria informação armazenada e trafegada por eles;
- **Resiliência Cibernética (Ciber Resiliência)** - a capacidade de antecipar, resistir, recuperar de, e adaptar-se a situações adversas, tensões, ataques, ou comprometimento em sistemas que usam ou são habilitados por recursos cibernéticos; e
- **Segurança Cibernética (Ciber Segurança)** - a capacidade de proteger e defender o uso do Espaço Cibernético de ciberataques.

De acordo com o "**Glossário de Segurança da Informação**" do Gabinete de Segurança Institucional da Presidência da República[2] (BRASIL GSIPR, 2024):

- **Criptografia**, é arte de proteção da informação, por meio de sua transformação em um texto cifrado (criptografado), com o uso de uma chave de cifragem e de procedimentos computacionais previamente estabelecidos, a fim de que somente o(s) possuidor(es) da chave de decifragem possa(m) reverter o texto criptografado de volta ao original (texto pleno). A chave de decifragem pode ser igual (criptografia simétrica) ou diferente (criptografia assimétrica) da chave de cifragem; e
- **Terrorismo Cibernético (Ciber Terrorismo)** é definido como crime cibernético perpetrado por razões políticas, religiosas ou ideológicas, contra qualquer elemento da infraestrutura cibernética com os objetivos de: provocar perturbação severa ou de longa duração na vida pública; causar danos severos à atividade econômica, com a intenção de intimidar a população; forçar as autoridades públicas ou uma organização a executar, tolerar, revogar ou a omitir um ato; ou abalar ou destruir as bases políticas, constitucionais, econômicas ou sociais de um Estado, organização ou empresa.

[2] Glossário de Segurança da Informação do GSI/PR - https://www.gov.br/gsi/pt-br/ssic/glossario-de-seguranca-da-informacao-1

***Backups***, conforme o "**Glossário de Termos**" da ISACA[3], são arquivos, equipamentos, dados e procedimentos disponíveis para uso em caso de falha ou perda, se os originais forem destruídos ou estiverem fora de serviço.

**Crime Cibernético (Ciber Crime)** é definido por **Gordon e Ford**[4] (2006, p. 2) como qualquer crime que seja facilitado ou cometido usando um computador, rede, ou dispositivo de hardware, e o FBI complementa como uma questão complexa e global, envolvendo criminosos e nações-estados, visando comprometer redes, causar disrupção de infraestruturas críticas e roubar dinheiro e propriedade intelectual.

Definições de **Ataques Cibernéticos** mais comuns em organizações do Agronegócio (antes, dentro e depois da porteira):

- ***Data Breach*** **(violação de dados)**[5] - é o termo utilizado para designar um incidente resultante de um vazamento, violação, fuga ou exposição de dados (incluindo informação sensível relacionada com organizações ou simples detalhes pessoais de indivíduos, e.g., informação médica). Relaciona-se diretamente com os resultados de outras ciberameaças.
- ***Malware***[6] - é abreviação de *software* malicioso. Projetado para se infiltrar, danificar ou obter informações de um sistema de computador sem o consentimento do proprietário. O malware geralmente inclui vírus de computador, *worms*, cavalos de Tróia, *spyware* e *adware*. O *spyware* é geralmente usado para fins de marketing e, como tal, não é malicioso, embora geralmente seja indesejado. Contudo, o *spyware* pode ser utilizado para recolher informações para roubo de identidade ou outros fins claramente ilícitos.
    - ***Worm***[7] - em computação, *worm* ou *computer worm* (do inglês que significa, literalmente, "verme" ou "verme de computador") é um programa independente (*standalone*), do tipo *malware*, que se replica com o objetivo de se espalhar para outros computadores. Geralmente, usa uma rede de computadores para se espalhar, ou mesmo unidades USB, contando com falhas de segurança no computador de destino para acessá-lo. Alguns *worms* também se alastram por mensagens de e-mail, criando anexos maliciosos e os enviando para as listas de contato da conta invadida. Ele usará

[3] Glossary of Terms English-Brazilian Portuguese da ISACA- https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/glossary/isaca-glossary-english-portuguese_mis_por_0615.pdf.
[4] On the definition and classification of cybercrime - https://www.researchgate.net/publication/220673373_On_the_Definition_and_Classification_of_Cybercrime.
[5] Glossário de Termos de Cibersegurança do Centro Nacional de Cibersegurança de Portugal - https://www.cncs.gov.pt/pt/glossario.
[6] Glossary of Terms English-Brazilian Portuguese da ISACA - https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/glossary/isaca-glossary-english-portuguese_mis_por_0615.pdf.
[7] Wikipédia: Worm - https://pt.wikipedia.org/wiki/Worm.

esta máquina como hospedeiro para varrer e infectar outros computadores.

- ***Spyware***[8] - em computação, um *spyware* (em português: programa espião ou software mal-intencionado) é um tipo de programa automático intruso (ou *malware*) destinado a infiltrar-se em um sistema de computadores e *smartphones*, para coletar informações pessoais ou confidenciais do usuário de forma ilícita (espião) (furto), e encaminhar para uma entidade externa via Internet para fins maliciosos, ou análise de marketing e financeiros.
- ***Adware***[9] - em computação, um *adware* (do inglês *advertisement* = "anúncio", e software = "programa") é qualquer programa de computador que executa automaticamente e exibe uma grande quantidade de anúncios sem a permissão do usuário. As funções do *adware* servem para analisar os locais de Internet que o usuário visita e lhe apresentar publicidade pertinente aos tipos de bens ou serviços apresentados lá.

- **Negação de Serviços (DoS ou DDos)**[10] - o ataque de negação de serviço (também conhecido como DoS, acrônimo em inglês de *Denial of Service*), é um ataque virtual que tenta tornar os recursos de um sistema indisponíveis para os seus usuários. Alvos típicos são servidores *web* e *websites*, estes possuem um limite de solicitações de usuários que serão respondidas simultaneamente, o ataque DDos (*Distributed* DoS) envia um excesso de solicitações que leva os alvos à sobrecarga, tentando tornar as páginas hospedadas indisponíveis na rede.
- ***Phishing***[11] - trata-se de uma armadilha digital comumente encaminhada por e-mail, para ludibriar vítimas, com o objetivo de auferir vantagens, como comprometer senhas de usuários, infligir prejuízos financeiros e roubar informações sensíveis, que podem ser vendidas.
- ***Ransomware***[12] - é um artefato malicioso que ameaça restringir acesso a um sistema. Os dados são criptografados e o acesso é bloqueado até que o pagamento de um resgate (*ransom*) seja recebido em troca da promessa de normalização do acesso, com o compartilhamento de chaves de descriptografia à vítima. *Ransom* significa “resgate”.

[8] Wikipédia: *Spyware* - https://pt.wikipedia.org/wiki/Spyware.
[9] Wikipédia: *Adware* - https://pt.wikipedia.org/wiki/Adware.
[10] Wikipédia: Ataque de negação de serviço - https://pt.wikipedia.org/wiki/Ataque_de_nega%C3%A7%C3%A3o_de_servi%C3%A7o.
[11] Cartilha de Segurança para Internet, Versão 4.0 do NIC.br - https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf
[12] *Blueprint for Ransomware Defense* da ISACA - McCABE - https://www.isaca.org/resources/white-papers/2023/blueprint-for-ransomware-defense

# REFERÊNCIAS DO GLOSSÁRIO

BRASIL GSI PR. **Glossário de Segurança da Informação do GSI/PR**. 2024. Disponível em < https://www.gov.br/gsi/pt-br/ssic/glossario-de-seguranca-da-informacao-1 >. Acessado em 01.11.2024.

BRASIL NIC.BR. **Cartilha de Segurança para Internet**, Versão 4.0 . São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em < https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf >. Acessado em 01.11.2024.

GORDON, S. & FORD. R. On the definition and classification of cybercrime. **Journal in Computer Virology**, 2, 13-20, 2006. Disponível em < https://www.researchgate.net/publication/220673373_On_the_Definition_and_Classification_of_Cybercrime >. Acessado em 01.11.2024.

ISACA. **Glossary of Terms English-Brazilian Portuguese**. 2015. Disponível em < https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/glossary/isaca-glossary-english-portuguese_mis_por_0615.pdf >. Acessado em 01.11.2024.

McCABE, E. **Blueprint for Ransomware Defense**. [S. l.]: ISACA, 2023. Disponível em < https://www.isaca.org/resources/white-papers/2023/blueprint-for-ransomware-defense >. Acessado em 01.11.2024.

NIST. **Glossary terms and definitions**. Last updated: February 26, 2024. Disponível em < https://csrc.nist.gov/glossary >. Acessado em 01.11.2024.

PORTUGAL. **Glossário de Termos de Cibersegurança**. Centro Nacional de Cibersegurança de Portugal. Disponível em < https://www.cncs.gov.pt/pt/glossario/ >. Acessado em 01.11.2024.

WIKIPÉDIA. **WIKIPÉDIA A enciclopédia livre**. Disponível em < https://pt.wikipedia.org/ >. Acessado em 01.11.2024.

# OUTUBRO 2024: MÊS DE CONSCIENTIZAÇÃO SOBRE A SEGURANÇA CIBERNÉTICA NO AGRONEGÓCIO BRASILEIRO

## POSTS DA CAMPANHA 2024 NA PÁGINA LINKEDIN DO OSCA

**I - SEJA ÚNICO COM SENHAS (INCOMUNS MESMO)!**

https://lnkd.in/ekRkb3dH

**II - IMPLEMENTE MFA - Autenticação Multifator!**

https://lnkd.in/dJ3acfpy

**III - CUIDADO COM O *PHISHING*: NÃO MORDA A ISCA!**

https://lnkd.in/dXU4NhJ7

**IV - ATUALIZE SEU AMBIENTE!**

https://lnkd.in/da-F44T8

**V - FAÇA BACKUP DE ARQUIVOS E TESTE (PERIODICAMENTE)!**

https://lnkd.in/dZrvcgYW

**VI - SEGMENTE SUAS REDES!**

https://lnkd.in/d2yteYdu

**VII - TENHA UM PLANO DE RESPOSTA A INCIDENTES E ATAQUES CIBERNÉTICOS!**

https://lnkd.in/d_FSsnG8

**VIII - CRIPTOGRAFE SEUS ARQUIVOS SENSÍVEIS!**

https://lnkd.in/djpnpnR9

**IX - COMPARTILHAR É CUIDAR!**

https://lnkd.in/depENXBG

**X - SIGA O OSCA!**

https://lnkd.in/daTA_Nv2

# OUTUBRO 2024: MÊS DE CONSCIENTIZAÇÃO SOBRE A SEGURANÇA CIBERNÉTICA NO AGRONEGÓCIO BRASILEIRO

## INSTITUIÇÕES PARCEIRAS DO OSCA NA CAMPANHA 2024

O Observatório da Segurança Cibernética no Agronegócio - OSCA agradece a adesão e a colaboração tempestiva dessas instituições públicas e privadas (nominadas em ordem cronológica) na difusão da campanha "**Outubro: mês de Conscientização sobre a Segurança Cibernética no Agronegócio Brasileiro**" para o Agro nacional (antes, dentro e depois da porteira). Boas Práticas de Segurança Cibernética foram disseminadas a fim de despertar a Consciência Situacional do setor para os Riscos Cibernéticos.

GRUPO PUBLIQUE

PRESENÇA TOTAL NO AGRO

FALA CAMIÃO!

A PRATELEIRA DE CIMA

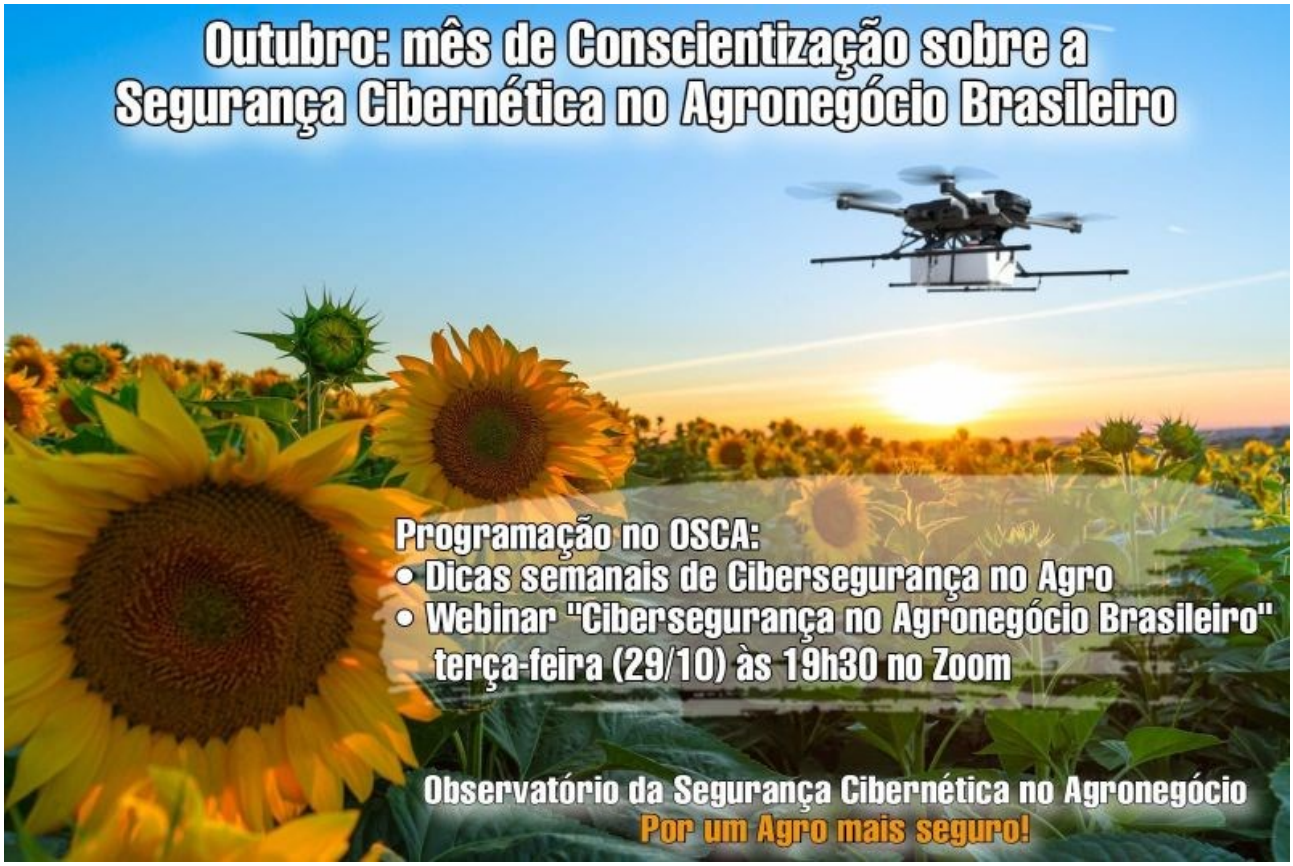
OBSERVATÓRIO DA AGROPECUÁRIA BRASILEIRA

MAPA
MINISTÉRIO DA AGRICULTURA E PECUÁRIA

UTFPR
UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
CAMPUS MEDIANEIRA

AGRICULTURA, PECUÁRIA E ABASTECIMENTO

MINAS GERAIS
GOVERNO DIFERENTE. ESTADO EFICIENTE.




ISBN: 978-65-01-22689-7

CBL

9 786501 226897

# OSCA