Orientações para Compartilhamento de **Informações de Incidentes Cibernéticos**

ANBIMA

Sumário

Introdução

Público-alvo

Esta publicação destina-se aos Grupos de Resposta a Incidentes de Segurança (CSIRTs), administradores de redes e sistemas, especialistas em segurança cibernética, responsáveis pela privacidade de informações, equipes de suporte técnico, responsáveis pela segurança da informação (CISOs) e tecnologia da informação (CIOs), e todos os demais interessados na atividade de compartilhamento de informações sobre incidentes cibernéticos.

Compartilhamento de informações

Enfrentar as ameaças cibernéticas e seus danos representam um desafio complexo e em constante evolução para as instituições financeiras. A troca de informações entre pares de mercado, via grupos de compartilhamento, é umas das iniciativas de destaque no enfrentamento dessas ameaças – e requisito regulatório disposto às instituições financeiras pela Resolução 4.893 do CMN e aos intermediários pela Resolução CVM 35. A prática envolve basicamente duas questões: (i) onde compartilhar; e (ii) o que compartilhar. A primeira trata das plataformas de compartilhamento e a segunda, que é abordada de maneira principiológica neste documento, diz respeito ao conteúdo das informações. A atividade engloba alguns desafios, no entanto há diversos benefícios observados que podem contribuir para o encorajamento e a ampliação da adesão entre as instituições. De forma não exaustiva, é possível elencar alguns desses ganhos:

Aumento da agilidade defensiva

as ameaças são constantemente aperfeiçoadas para superarem os mecanismos de defesa das organizações e explorarem novas vulnerabilidades. O compartilhamento de informações permite maior agilidade no conhecimento dessas progressões, por parte das instituições, provendo elementos para que o tempo de resposta ao incidente possa ser menor, assim como a probabilidade de sucesso do ataque.

Conscientização do desenvolvimento das novas ameaças

com o aperfeiçoamento das técnicas e a ampliação da superfície de ataque – promovida principalmente pela expansão do trabalho remoto –, novas formas de malware têm surgido. O trabalho em conjunto com instituições semelhantes e do mesmo segmento, via compartilhamento das informações, permite à instituição acompanhar o surgimento de novas formas de ataque.

Expansão do conhecimento

informações sobre ameaças sofridas por determinada organização podem estar correlacionadas a elementos observados e compartilhados por outra instituição que sofreu ataque semelhante. Por meio da interação na comunidade de compartilhamento, é possível complementar e expandir o conhecimento a respeito das técnicas, das táticas e dos procedimentos utilizados pelos atores de ameaças, fortalecendo os indicadores compartilhados.

Otimização do uso dos recursos

a obtenção de informações de maneira mais ágil, via comunidades de compartilhamento, oferece oportunidade para a instituição alocar seus esforços de segurança cibernética nos pontos de maior vulnerabilidade, de forma mais proativa e menos reativa, o que torna o trabalho das equipes responsáveis mais efetivo e eficiente.

Redução dos custos de cibersegurança

compartilhar informações sobre incidentes em plataformas de compartilhamento também é uma forma de dividir os custos de inteligência cibernética da organização entre os demais participantes da comunidade. Por meio do trabalho conjunto, é construído conhecimento de uso coletivo, aumentando a eficiência da defesa cibernética da instituição contra ameaças e ataques.

Incidente de segurança cibernética

Um incidente de segurança cibernética não significa necessariamente que as informações já estão comprometidas; significa apenas que a informação pode estar ameaçada[1]. Dessa forma, pode-se caracterizar a ameaça cibernética como uma circunstância com potencial para explorar uma ou mais vulnerabilidades, que pode afetar de forma adversa a segurança cibernética da instituição[2].

Quando compartilhar informações

Um dos principais desafios para a ampliação da prática do compartilhamento de informações entre as instituições do mercado é o receio de possíveis consequências para sua reputação a partir de incidentes materializados, principalmente por conta de eventual divulgação dos impactos aos clientes. Contudo, o compartilhamento de informações não ocorre somente com base em incidentes materializados, mas também em toda e qualquer forma de ameaça recebida pela instituição. Caso a instituição identifique qualquer fragilidade ou possível incidente de segurança, o ato de compartilhar tempestivamente informações relativas ao que foi detectado pode auxiliar diversas outras organizações a se defenderem contra possíveis incidentes, contribuindo para a preservação da confidencialidade, integridade e disponibilidade dos dados ou dos sistemas da instituição, beneficiando a continuidade dos negócios da companhia.

1 – Disponível em – CTIR Gov (2021).

2 – Disponível em – FSB (2018).

Onde compartilhar

O compartilhamento de informações acerca das ameaças cibernéticas entre pares do mercado pode ser realizado via plataformas de compartilhamento especializadas. Esses locais podem contar com requisitos mínimos de segurança que auxiliam a formação da comunidade e a construção da confiança necessária para a sustentação da prática de compartilhamento de dados entres as instituições[3]. Como exemplos de plataformas de compartilhamento, é possível citar MISP, FS-ISAC, entre outros[4]. De forma a fortalecer os benefícios da atividade, recomenda-se que haja convergência entre as organizações participantes da comunidade na escolha da plataforma de compartilhamento de informações.

3 – Para mais orientações sobre plataformas de compartilhamento, ver Guia de Cibersegurança ANBIMA (2021).

4 – A menção às ferramentas especificadas ocorre meramente com caráter exemplificativo e não representa uma avaliação prévia da Associação. É de responsabilidade de cada instituição realizar avaliação própria para utilização de qualquer ferramenta de compartilhamento de informação de incidentes cibernéticos.

Recomendações de Governança e Gestão[5]

Comprometimento de lideranças

Como forma de reforçar o engajamento da organização no compartilhamento de informações de incidentes cibernéticos e conscientizar os diversos níveis organizacionais em relação às responsabilidades e aos esforços da instituição acerca do tema, recomenda-se o comprometimento da alta gestão por meio de comunicação interna na disseminação dos benefícios decorrentes da prática do compartilhamento de informações.

---

5 – Para mais tópicos relacionados a governança e gestão de incidente, ver: Cyber-threat intelligence information sharing guide (GOV.UK, 2021) e Guide to Cyber Threat Information Sharing (NIST, 2016).

Metas e objetivos

É recomendado que a instituição estabeleça metas e objetivos que representem os resultados esperados com o andamento do compartilhamento de informações. Tais intenções devem auxiliar a organização nos processos de definição do escopo das atividades de compartilhamento de informações de incidentes cibernéticos.

Definição de escopo

Orienta-se que a instituição defina as etapas que precedem a atividade de compartilhamento, de forma a assegurar que as fontes de informações e as capacidades necessárias para sustentar a prática de compartilhamento estejam disponíveis na organização. Os processos podem envolver, de maneira não exaustiva:

- Listar tipos de informações a serem compartilhadas;
- Estabelecer padronização das informações compartilhadas;
- Definir método de designação de manipulação das informações (classificação de risco);
- Preservação de origem dos dados;
- Descrição das condições e circunstâncias do compartilhamento.

Inventário das fontes internas de informação

De forma a auxiliar a atividade de compartilhamento, para que a instituição consiga reunir dados acerca das ameaças cibernéticas de forma eficiente e contribuir de maneira ativa dentro da comunidade de compartilhamento de informações, é recomendado que a instituição elabore um inventário de fontes internas de informações.

Treinamentos e orientações

A prática de compartilhamento de informações sobre incidentes cibernéticos é mais eficaz quando a instituição conta com profissionais com conhecimento a respeito das ameaças e suas decorrências, e orientados para colaborar, direta e/ou indiretamente, com a segurança cibernética e a resiliência operacional da organização. Além de orientações recorrentes de conscientização a respeito do tema, recomenda-se que a instituição busque fornecer treinamentos periódicos que envolvam toda a hierarquia da instituição[6].

Designação de manipulação de informações

Informações acerca de ameaças cibernéticas frequentemente envolvem dados sensíveis para as organizações, o que pode significar um desafio importante na ampliação da prática de compartilhamento. É recomendado que a instituição leve em consideração a privacidade e a reputação das partes interessadas e/ou forneça orientações claras quanto à sensibilidade dos dados. Cabe aos receptores observarem as atribuições dadas pela fonte, assim como a maneira de disseminação e armazenamento expressa nessas orientações. Como exemplo de metodologia, é possível citar o Traffic Light Protocol (TLP), um conjunto de designações utilizado para garantir que as informações sensíveis sejam compartilhadas com o público apropriado[7].

6 – Para mais recomendações acerca de treinamentos, ver Guia de Cibersegurança ANBIMA (2021).
7 – Ver ANEXO II

Preservação da origem das informações

Para garantir a proteção dos proprietários das informações e assegurar que, ao consumi-las, as instituições receptoras estarão em acordo com a regulação de proteção de dados, é recomendado que as organizações preservem a origem das informações, através do rastreamento do provedor, e de como os dados foram coletados, transformados ou processados. Com intuito de permitir o compartilhamento tempestivo das informações, cumprindo obrigações de proteção, recomenda-se a formulação de procedimentos de rastreamento de origem, descrevendo papéis e responsabilidades das partes interessadas.

Produção e publicação de indicadores

Organizações que se propõem a produzir e publicar indicadores, ao invés de apenas consumi-los, podem se beneficiar substancialmente dessa prática. Entre os benefícios obtidos, pode-se citar:

- Ganho de expertise no enfrentamento às ameaças;
- Auxílio a outras organizações de maneira mais efetiva na resposta a incidentes;
- Aquisição e/ou ampliação da confiança dos demais membros da comunidade.

Além dos ganhos para a instituição, a produção e a publicação de indicadores são importantes para construir e sustentar o fluxo de informação dentro da comunidade.

Recomendações de compartilhamento

Indicadores de comprometimento (IoC)

Indicadores de comprometimento, conhecidos a partir do acrônimo em inglês "IoC"[8], são evidências que indicam, com alta probabilidade, um acesso não autorizado a um sistema operacional ou elemento de rede[9]. Quando identificados, podem auxiliar a instituição a mapear ameaças em seu

8 – IoC é acrônimo do termo em inglês *Indicator of Compromise*

9 – Definição trazida pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Governo (CTIR Gov, 2021). Disponível em: CTIR GOV.

ambiente e, portanto, é também um tipo de informação útil a ser compartilhada entre pares de mercado, para que, da mesma forma, outras entidades possam se defender contra agentes maliciosos. De forma não exaustiva, podemos listar os seguintes exemplos de IoC:

- Endereços de IP
- Uniform Resource Locator (URL)
- Arquivo executável suspeito
- Título de e-mail suspeito
- Remetente de e-mail suspeito
- Hash

Atributos mínimos a serem compartilhados

A padronização de informações é apontada como boa prática para a ampliação e o fortalecimento das atividades de compartilhamento[10]. Com propósito de auxiliar as instituições na adesão e estimular a participação ativa das organizações dentro dos canais de compartilhamento de informações entre os pares do mercado, este tópico propõe um modelo, por meio de exemplos não exaustivos, para comportar um conjunto de atributos mínimos a serem compartilhados de acordo com o tipo/classificação do incidente cibernético. Além de promover a estruturação e aumentar a agilidade no compartilhamento, o uso de um formato comum abre possibilidade de implementos para configuração automática de ferramentas de segurança e redução da necessidade de assistência humana.

10 – NIST (2016)

Representação de atributos mínimos de compartilhamento:

Phishing

Definição	Atributos mínimos
Links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais .	• Data da ocorrência • Data e hora da identificação • Status da análise • Segmento da entidade • Atributos (ex.: URL, remetente

Ransomware

Definição	Atributos mínimos
Software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido .	• Data da ocorrência • Data e hora da identificação • Status da análise • Segmento da entidade • Atributos (ex.: IP; remetente)

DDoS

Definição	Atributos mínimos
Ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição .	• Data da ocorrência • Data e hora da identificação • Status da análise • Segmento da entidade • Atributos (ex.: URL)

Fonte: Elaboração própria

Atributos adicionais

Iniciada a investigação do incidente, novas informações acerca da ameaça reportada podem ser reveladas. Dessa forma, sugere-se uma segunda etapa no compartilhamento de informações, com inclusão de novos elementos que permitam maior nível de detalhamento a respeito do ataque. O objetivo dessa etapa é enriquecer os indicadores inicialmente informados e manter o reporte atualizado, fortalecendo o conhecimento a respeito da ameaça. Entre os elementos complementares, de forma não exaustiva, pode-se citar:

- Breve resumo/descrição;
- Plataformas afetadas (sistemas operacionais, aplicações, hardware);
- Impacto estimado;
- Opções de mitigação (inclui correções permanentes/temporárias);
- Referências para mais informações;
- Observações gerais.

Glossário

A uniformização dos termos relacionados a incidentes cibernéticos é parte fundamental para que o compartilhamento, o recebimento e a compreensão dos dados por parte das instituições participantes da comunidade ocorram de maneira tempestiva, intensificando a eficiência da segurança cibernética. Dessa forma, este tópico se propõe a reunir alguns dos principais termos do universo de segurança cibernética com as respectivas definições.

Glossário de termos relacionados a incidentes cibernéticos

Termo	Definição
Alerta de ETIR	Informação descritiva de um incidente cibernético, de forma reativa, para notificação de usuários. (GSI, 2021)
Ambiente cibernético	Inclui usuários, redes, dispositivos, software, processos de informação armazenada ou em trânsito, serviços e sistemas que possam ser conectados direta ou indiretamente a redes e computadores. (GSI, 2021)
Análise de vulnerabilidades	Verificação e exame técnico de vulnerabilidades, para determinar onde estão localizadas e como foram exploradas. (GSI, 2021)
Artefato malicioso	Qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas ou rede de computadores. (GSI, 2021)
Assinatura do ataque	Padrão característico ou distintivo que pode ser pesquisado ou usado para corresponder a ataques previamente identificados. (NICCS, 2022)
Backdoor	Qualquer mecanismo inserido no sistema, intencional ou acidentalmente, com o objetivo de permitir o acesso não documentado ao sistema ou aos seus dados. (GSI, 2021)
Botnet	Rede formada por diversos computadores zumbis (infectados com bots). Permite potencializar as ações danosas executadas pelos bots e ser usada em ataques de negação de serviço, esquemas de fraude, envio de spam, entre outros. (GSI, 2021)

Glossário de termos relacionados a incidentes cibernéticos

Termo	Definição
Emissão de alertas e advertências	Serviço que consiste em divulgar alertas ou advertências imediatas, como uma reação diante de um incidente de segurança em redes de computadores, com o objetivo de advertir a comunidade ou dar orientações sobre como a comunidade deve agir diante do problema. (GSI, 2021)
Espalhamento (hashing)	Tabela de espalhamento (hashing) que associa uma chave a um endereço. Esse endereço é usado como base para armazenamento e recuperação de registros, sendo bastante similar à indexação, pois associa a chave ao endereço relativo a um registro. No espalhamento, os endereços parecem aleatórios, não existindo conexão óbvia entre a chave e o endereço. (GSI, 2021)
Exploração de dia zero	Ataque digital que faz uso das "Vulnerabilidades de Dia Zero" para instalar software malicioso em um aparelho. É considerada uma ameaça grave, pois é impossível reconhecê-la, uma vez que a falha não é conhecida. Ela pode ser mitigada e algumas vezes evitada por meio de ferramentas de segurança que monitorem o comportamento do tráfego e o acesso aos equipamentos para identificar atividades suspeitas ou maliciosas. (GSI, 2021)
Infraestrutura crítica	Instalações, serviços, bens e sistemas, virtuais ou físicos que, se forem incapacitados, destruídos ou tiverem desempenho extremamente degradado, provocarão sério impacto social, econômico, político, internacional ou à segurança. (GSI, 2021)

Glossário de termos relacionados a incidentes cibernéticos

Termo	Definição
Jailbreak	Processo que modifica o sistema operacional original de um dispositivo, permitindo que ele execute aplicativos não autorizados pelo fabricante. Um aparelho com um software do tipo jailbreak é capaz de instalar aplicativos anteriormente indisponíveis nos sites oficiais do fabricante, por meio de instaladores não oficiais, assim como aplicações adquiridas de forma ilegal. O uso de técnicas jailbreak não é recomendado pelos fabricantes, já que permitem a execução de aplicativos não certificados, que podem inclusive conter malware embutidos. (GSI, 2021)
Matriz RACI	Também conhecida como tabela RACI, trata-se de uma ferramenta visual, que define com clareza as atribuições, papéis e responsabilidades de cada colaborador nas atividades de um processo. A sigla RACI representa responsible (responsável), accountable (aprovador), consulted (consultado) e informed (informado). (GSI, 2021)
Prevenção de perda de dados (DLP)	Prática de detectar e prevenir vazamentos de dados, extração de dados e/ou destruição de dados sensíveis de uma organização. O termo DLP refere-se tanto a ações contra a perda de dados (evento no qual os dados são definitivamente perdidos pela organização), quanto a ações contra vazamentos de dados (transferência indevida de dados para fora da fronteira da organização). (GSI, 2021)
Rootkit	Conjunto de programas e técnicas que permitem esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido. É importante ressaltar que o nome rootkit não indica que as ferramentas que o compõem são usadas para obter acesso privilegiado em um computador (root ou administrator), mas sim para manter o acesso privilegiado em um computador previamente comprometido. (GSI, 2021)

Glossário de termos relacionados a incidentes cibernéticos

Termo	Definição
Táticas, Técnicas e Procedimentos (TTPs)	O comportamento do agente malicioso. Uma tática é o nível geral de descrição desse comportamento, enquanto as técnicas dão uma descrição detalhada do comportamento no contexto de uma tática, e os procedimentos fornecem uma descrição de nível ainda mais detalhada em contexto de uma técnica. (NIST, 2016)
Teste de penetração (Pentest)	Também chamado de teste de intrusão, é fundamental para a análise de vulnerabilidades e consiste em testar todos os sistemas em busca de, além das já verificadas na fase anterior, vulnerabilidades conhecidas e disponibilizadas por especialistas ou pelas instituições detentoras dos softwares que estão sendo utilizados pela instituição. (GSI, 2021)
Worm	Programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o worm não embute cópias de si mesmo em outros programas ou arquivos, e não necessita ser explicitamente executado para se propagar. Sua propagação se dá por meio da exploração de vulnerabilidades existentes ou de falhas na configuração de programas instalados em computadores. (GSI, 2021)
Zumbi	Nome dado a um computador infectado por bot, pois pode ser controlado remotamente, sem o conhecimento do seu proprietário. (GSI, 2021)

Acrônimos relacionados à segurança cibernética

Acrônimo	Significado
AP	Access Point – Ponto de Acesso
AS	Autonomous System – Sistema Autônomo
CBT	Computer Based Training - Treinamento Baseado em Computador
CERT	Computer Emergency Response Team – Centro de Estudos, Resposta e Tratamento de Incidentes
CIRT	Critical Information Infrastructure Protection – Proteção de Infraestrutura Crítica de Informação
CIRT	Computer Incident Response Team – Grupo de Resposta a Incidentes
CSIRT	Computer Security Incident Response Team – Grupo de Resposta a Incidentes de Segurança
DDoS	Distributed Denial of Service – Ataque Distribuído de Negação de Serviço
DoS	Denial of Service – Negação de Serviço
HIDS	Host-based Intrusion Detection System – Sistema de Detecção de Intruso Hospedado
IAP	Independent Application Provider – Provedor de Aplicação Independente
ICMP	Internet Control Message Protocol – Protocolo de Internet de Controle de Mensagem
ICT	Information and Communications Technology – Tecnologia de Comunicação e Informação

Acrônimos relacionados à segurança cibernética

Acrônimo	Significado
IDS	Intrusion Detection System – Sistema de Detecção de Intrusão
IP	Internet Protocol – Protocolo de Internet
IPO	Information Providing Organization – Organização Provendo Informação
IPS	Intrusion Prevention System – Sistema de Prevenção de Intrusão
IRO	Information Receiving Organization – Organização Recebendo Informação
ISP	Internet Service Provider – Provedor de Serviços de Internet
ISV	Independent Software Vendor – Vendedor de Software Independente
IT	Information Technology – Tecnologia da Informação
NDA	Non-Disclosure Agreement – Acordo de Não Divulgação
SDLC	Software Development Life-Cycle – Ciclo de Vida de Desenvolvimento de Software
SSID	Service Set IDentifier – Identificador do Conjunto de Serviço
TCP	Transmission Control Protocol – Protocolo de Controle de Transmissão
UDP	User Datagram Protocol – Protocolo de Datagrama de Usuário
URI	Uniform Resource Identifier – Identificador Uniforme de Recurso
URL	Uniform Resource Locator – Localizador Uniforme de Recurso

Apêndice

ANEXO I: Fontes internas de informação

Etapas sugeridas para a identificação de fontes internas de informação de ameaças

Identifique sensores, ferramentas e repositórios que produzam informações sobre ameaças e confirmem que os dados são produzidos a uma dada frequência e precisão para apoiar tomadas de decisão.

Identifique informações de ameaças que são coletadas e analisadas como parte de uma estratégia contínua de monitoramento da organização.

Localize informações sobre ameaças que são coletadas e armazenadas, mas não necessariamente analisadas ou revisadas continuamente. Se uma organização encontra informações úteis sobre ameaças que estão sendo subutilizadas, métodos de integração dessas informações em suas práticas de segurança cibernética e gerenciamento de riscos devem ser explorados.

Identifique informações de ameaças que sejam adequadas para compartilhamento com terceiros e que possam ajudá-los a responder de forma mais eficaz às ameaças.

ANEXO II: Designações de compartilhamento

Designações do Traffic Light Protocol (TLP), versão 1.0

Cor	Quando usar	Como pode ser compartilhado
TLP:RED Não deve ser divulgado, restrito somente aos participantes	As fontes podem usar o TLP:RED quando as outras partes não puderem agir de forma efetiva sobre a informação e qualquer mau uso da informação possa causar impactos na privacidade, na reputação ou nas operações de uma das partes.	Destinatários não podem compartilhar informações TLP:RED com ninguém além dos presentes na troca de informações, reunião ou conversa específica na qual a informação foi originalmente divulgada. No contexto de uma reunião, por exemplo, informações TLP:RED são limitadas aos presentes na reunião. Na maioria das vezes, o TLP:RED deve (should) ser usado para trocar informações pessoalmente ou de forma oral.
TLP:AMBER Divulgação limitada, restrita às organizações dos participantes	As fontes podem usar TLP:AMBER quando é necessário apoio para agir de maneira efetiva sobre a informação, mas ainda assim há riscos para a privacidade, a reputação ou as operações, se esta for divulgada fora das organizações envolvidas.	Destinatários só podem compartilhar informações TLP:AMBER com membros de suas próprias organizações e com clientes que necessitam saber dessa informação para se proteger ou evitar danos futuros. As fontes são livres para especificar limites adicionais para o compartilhamento: esses limites devem obrigatoriamente (must) ser respeitados.

Designações do Traffic Light Protocol (TLP), versão 1.0

Cor	Quando usar	Como pode ser compartilhado
TLP:GREEN Divulgação limitada, restrito à comunidade	As fontes podem usar TLP:GREEN quando a informação é útil para a conscientização de todas as organizações participantes, bem como para seus pares no setor ou na comunidade.	Destinatários podem compartilhar informações TLP:GREEN com seus pares dentro do seu setor ou da sua comunidade, mas não por meio de canais publicamente acessíveis. Informações nessa categoria podem ser circuladas amplamente dentro de uma comunidade em particular. Informações TLP:GREEN não podem ser divulgadas fora de uma comunidade.
TLP:WHITE Divulgação não é limitada	As fontes podem usar TLP:WHITE quando o risco de mau uso da informação é mínimo ou não há previsão de risco de mau uso, de acordo com regras e procedimentos aplicáveis para divulgação pública.	Informação TLP:WHITE pode ser distribuída sem restrições, desde que respeitadas as regras padrão de direitos autorais.

Referências

Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (ANBIMA), Guia de Cibersegurança ANBIMA, 3ª ed., 2021. Disponível em: https://www.anbima.com.br/data/files/34/B3/04/8F/D96F971013C70F976B2BA2A8/Guia%20de%20Ciberseguranca%20ANBIMA.pdf

---

Centro de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos do Governo – CTIR Gov, Glossário de Segurança da Informação, nov. 2021. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/dsi/glossario-de-seguranca-da-informacao-1

Centro de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos do Governo – CTIR Gov, Indicadores de Comprometimento, nov. 2021. Disponível em: https://www.gov.br/ctir/pt-br/assuntos/noticias/2021/indicadores-de-comprometimento

---

Cyber Security Competence for Research and Innovation (CONCORDIA), *Threat Intelligence Sharing*: What kind of intelligence to share?. Disponível em: https://www.concordia-h2020.eu/blog-post/threat-intelligence-sharing/

Financial Stability Board (FSB), *Cyber Lexicon*, nov. 2018. Disponível em: https://www.fsb.org/wp-content/uploads/P121118-1.pdf

FIRST, *Traffic Light Protocol (TLP)*, 2016. Disponível em: https://www.first.org/tlp/docs/tlp-v1-pt-br.pdf

GOV.UK, *Cyber-threat intelligence information sharing guide*, mar. 2021. Disponível em: https://www.gov.uk/government/publications/cyber-threat-intelligence-information-sharing/cyber-threat-intelligence-information-sharing-guide#executive-summary

Johns Hopkins Applied Physics Laboratory, *Deploying Indicators of Compromise (IOCs)* for Network Defense. Fev. 2021. Disponível em: https://www.cisa.gov/sites/default/files/publications/Operational%20Value%20of%20IOCs_508c.pdf

National Iniciative for Cybersecurity Careers and Studies (NICCS), *Cybersecurity Glossary*, mar. 2022. Disponível em: https://niccs.cisa.gov/about-niccs/cybersecurity-glossary

National Institute of Standards and Technology (NIST), Guide to Cyber Threat Information Sharing, 2016. Disponível em: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-150.pdf

SANS Institute, *Glossary of Security Terms*. Disponível em: https://www.sans.org/security-resources/glossary-of-terms/

Expediente

Orientações para **Compartilhamento de Informações de Incidentes Cibernéticos**

Rio de Janeiro

Praia de Botafogo, 501 – 704, Bloco II, Botafogo,
Rio de Janeiro, RJ – CEP: 22250-042 | Tel.: (21) 2104-9300

São Paulo

Av. das Nações Unidas, 8501, 21° andar, Pinheiros,
São Paulo, SP – CEP: 05425-070 | Tel.: (11) 3471 4200

ANBIMA

www.anbima.com.br