



# 4º WEBINÁRIO

PARA EQUIPES DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS (ETIR) DOS ÓRGÃOS PERTENCENTES À REDE FEDERAL DE GESTÃO DE INCIDENTES CIBERNÉTICOS (REGIC)

**Data: 5 Nov 24**

**Local: On-line - Plataforma Teams**

GABINETE DE  
SEGURANÇA  
INSTITUCIONAL

GOVERNO FEDERAL  
**BRASIL**  
UNIÃO E RECONSTRUÇÃO



# PROGRAMAÇÃO



Responsável	Data	Horário	Atividade
SSIC	05 NOV 24	9:30	- Aceitar os convidados, para acesso à plataforma
		10:00	- Abertura do Evento
		10:05	- Interpretação da notificação - Entendimento da criticidade do caso e sua relação com possíveis incidentes cibernéticos críticos - Tratamento recomendado
		10:50	- Intervalo
		11:00	- Análise de casos reais - Conclusão e recomendações CTIR relacionadas
		11:25	- Comentário e questionários
		11:50	- Encerramento do Evento



# 4º WEBINÁRIO

PARA EQUIPES DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS (ETIR) DOS ÓRGÃOS PERTENCENTES À REDE FEDERAL DE GESTÃO DE INCIDENTES CIBERNÉTICOS (REGIC)

**Data: 5 Nov 24**

**Local: On-line - Plataforma Teams**

GABINETE DE  
SEGURANÇA  
INSTITUCIONAL

GOVERNO FEDERAL  
**BRASIL**  
UNIÃO E RECONSTRUÇÃO



# TEMA:



## O Processo de Notificação de Vazamento de Credenciais no Âmbito da Rede Federal de Gestão de Incidentes Cibernéticos - ReGIC

- Interpretação da notificação;
- Entendimento da criticidade do caso e sua relação com possíveis incidentes cibernéticos críticos;
- Tratamento recomendado do incidente;

## Intervalo

- Análise de Casos reais;
- Conclusão e recomendações CTIR relacionadas;





# WHOAMI



## **Formação**

- Análise e Desenvolvimento de Sistemas da Informação - UNESA
- Pós Graduação Gestão de Riscos e Cibersegurança - CENES

## **Na área do Tratamento e Resposta a Incidentes**

- Curso Fundamentals of Incident Handling - CERT Br
- Curso Advanced Topics in Incident Handling – CERT Br

## **Software Livre**

- Usuário e entusiasta

- **Interpretação da notificação;**
- Entendimento da criticidade do caso e sua relação com possíveis incidentes cibernéticos críticos;
- Tratamento recomendado do incidente;

Intervalo

- Análise de Casos reais;
- Conclusão e recomendações CTIR relacionadas;

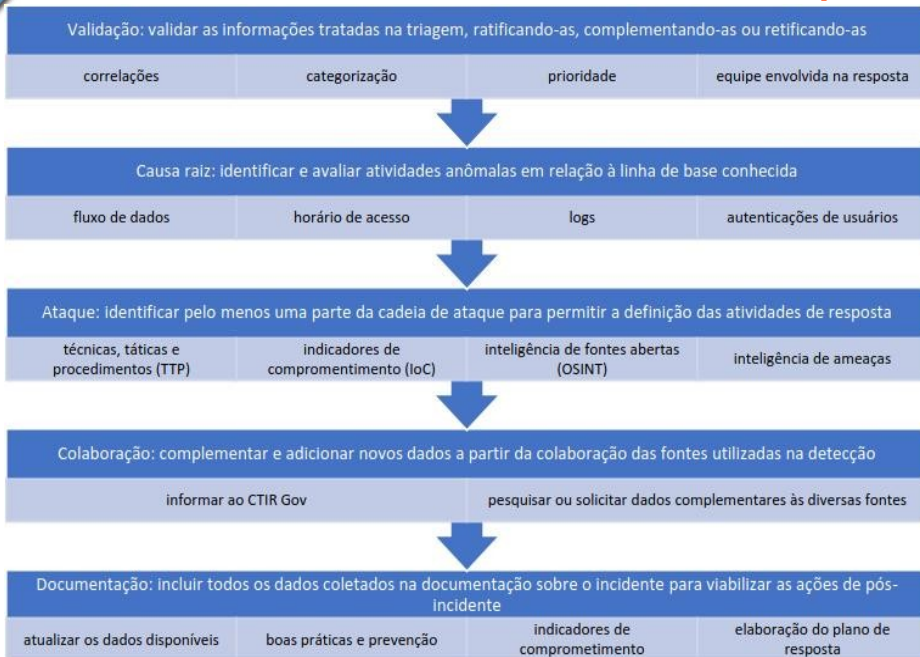


# Interpretar notificação

**Importância de reportar um incidente :**  
**Os ataques estão cada vez mais precisos e inteligentes;**  
**Focado na celeridade da resposta para Contenção e Erradicação.**

**PLANGIC - Plano de Gestão de Incidente Cibernético preconiza :**

## TRATAMENTO DE INCIDENTES CIBERNÉTICOS



Na atividade da Colaboração (Figura), Pág. 09, é obrigatória a comunicação ao CTIR Gov apenas dos incidentes que:

- possam implicar em perda de vidas;
- afetem a disponibilidade, integridade, confiabilidade e autenticidade de ativos de informação de:
  - infraestruturas críticas – energia, água, transporte, finanças, comunicações, defesa e biossegurança; e
  - serviços governamentais digitais;
- implique em vazamento de:
  - dados pessoais; e
  - informação classificada ou sensível; e
- possam potencial de exploração danosa em larga escala.





# Comunicação de Incidentes de Rede



[https://www.gov.br/ctir/pt-br/canais\\_atendimento/comunicacao-de-incidentes-de-rede/comunicacao-de-ocorrencia-de-incidentes-de-redes](https://www.gov.br/ctir/pt-br/canais_atendimento/comunicacao-de-incidentes-de-rede/comunicacao-de-ocorrencia-de-incidentes-de-redes)

## Reportar para onde ?

**Instruções básicas de como notificações de incidentes cibernéticos devem ser enviados ao CTIR Gov.**



CTIR Gov, atende por meio do e-mail: **[ctir@ctir.gov.br](mailto:ctir@ctir.gov.br)**

INOC-DBA BR: 266031\*800 (<https://inoc.nic.br/>)

Para comunicação através de um canal seguro, por favor utilize a seguinte chave PGP:  
PGP - CTIR Gov

KeyID: 221BFF78 e Fingerprint: 2BBE CB49 EC3A D4FE 5C4D 9FF9 BD0F 2FF0 221B FF78



### Sobre o INOC-DBA

O INOC-DBA é uma rede voIP exclusiva para os Sistemas Autônomos, as redes que formam a Internet: fornece uma *hotline*, uma forma rápida e simples de comunicação entre seus NOCs (Centros de Operação de Redes) e CSIRTs (Equipes de Tratamento de Incidentes de Segurança). No INOC as ligações são feitas usando o ASN, que é o número que identifica cada rede no BGP, na tabela de roteamento global da Internet... **LEIA MAIS**



[https://www.gov.br/ctir/pt-br/canais\\_atendimento/padrees-para-notificacao-de-incidentes-de-seguranca-ao-ctir-gov](https://www.gov.br/ctir/pt-br/canais_atendimento/padrees-para-notificacao-de-incidentes-de-seguranca-ao-ctir-gov)

## Estabelecer uniformidade e padrão nas notificações.

### Padrões para Notificação de Incidentes Cibernéticos ao CTIR Gov :

#### Objetivo

Definir padrões e esclarecer os procedimentos relacionados ao processo de notificação de incidentes cibernéticos pela Administração Pública Federal (APF) ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov).

#### Referências

1. Norma Complementar nº 05 /IN01/DSIC/GSIPR, de 14/Ago/09, que disciplina a criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) nos órgãos e entidades da APF.
2. Norma Complementar nº 08 /IN01/DSIC/GSIPR, de 19/Ago/10, que disciplina o gerenciamento de incidentes de segurança em redes de computadores realizado pelas ETIR dos órgãos e entidades da APF.



#### Sobre o INOC-DBA

O INOC-DBA é uma rede VoIP exclusiva para os Sistemas Autônomos, as redes que formam a Internet: fornece uma *hotline*, uma forma rápida e simples de comunicação entre seus NOCs (Centros de Operação de Redes) e CSIRTs (Equipes de Tratamento de Incidentes de Segurança). No INOC as ligações são feitas usando o ASN, que é o número que identifica cada rede no BGP, na tabela de roteamento global da Internet... **LEIA MAIS**



[https://www.gov.br/ctir/pt-br/canais\\_atendimento/padrees-para-notificacao-de-incidentes-de-seguranca-ao-ctir-gov](https://www.gov.br/ctir/pt-br/canais_atendimento/padrees-para-notificacao-de-incidentes-de-seguranca-ao-ctir-gov)



CTIR Gov Em Números

Alertas e  
Recomendações

Celeridade e Efetividade nas  
ações.

## Finalidades da notificação :

Conforme estabelecem o item 10.6 da NC nº 05 e o item 6 da NC nº 08, as equipes de tratamento e resposta a incidentes em redes computacionais dos órgãos e entidades da APF deverão comunicar de imediato a ocorrência de todos os incidentes de segurança ocorridos na sua área de atuação ao CTIR GOV, a fim de permitir a geração de estatísticas e soluções integradas para a Administração Pública Federal, de acordo com os padrões e procedimentos definidos neste documento.

## Comunicação :

A comunicação entre órgãos e instituições da APF e o CTIR Gov deve ocorrer por meio das ETIR ou por pessoas com essa atribuição, de forma centralizada, preferencialmente por meio de e-mail institucional relacionado a incidentes de segurança, como sugestão: [etir@orgao.gov.br](mailto:etir@orgao.gov.br).

O ponto único de contato para as notificações de incidentes cibernéticos ao CTIR Gov é o endereço eletrônico: [ctir@ctir.gov.br](mailto:ctir@ctir.gov.br). Questões gerenciais ou relacionadas à Coordenação-Geral de Tratamento de Incidentes de Rede (CGTIR) serão tratadas por meio do correio eletrônico: [contato@ctir.gov.br](mailto:contato@ctir.gov.br).



### Sobre o INOC-DBA

O INOC-DBA é uma rede voIP exclusiva para os Sistemas Autônomos, as redes que formam a Internet: fornece uma *hotline*, uma forma rápida e simples de comunicação entre seus NOCs (Centros de Operação de Redes) e CSIRTs (Equipes de Tratamento de Incidentes de Segurança). No INOC as ligações são feitas usando o ASN, que é o número que identifica cada rede no BGP, na tabela de roteamento global da Internet... [LEIA MAIS](#)





# Procedimento para comunicação



## Traffic Light Protocol (TLP)

▶ O CTIR Gov adere ao padrão Traffic Light Protocol (TLP) 2.0, conforme definido pelo Forum of Incident Response and Security Teams (FIRST). **Para o envio de notificações, recomenda-se utilizar o TLP apropriado no assunto e no corpo do e-mail.** De maneira apropriada serão tratadas as notificações de acordo com as marcações

**CLEAR**, **GREEN**, **AMBER**, **AMBER+STRICT** ou **RED**.

# Traffic Light Protocol (TLP)

- a. **TLP:RED** = Somente para os olhos e ouvidos dos indivíduos destinatários, não é permitido compartilhamento nenhum. Fontes podem usar TLP:RED quando não é possível atuar sobre a informação sem colocar em risco significativo a privacidade, reputação ou operações das organizações envolvidas. Destinatários não podem compartilhar informações TLP:RED com mais ninguém. No contexto de uma reunião, por exemplo, informações TLP:RED são limitadas àqueles presentes na reunião.
- b. **TLP:AMBER** = Divulgação limitada, destinatários só podem disseminar para aqueles que necessitam saber (*need-to-know basis*) dentro de sua própria organização e com seus clientes. Note que o **TLP:AMBER+STRICT** restringe o compartilhamento apenas para a própria organização. Fontes podem usar o TLP:AMBER quando é necessário apoio para agir de maneira efetiva sobre a informação, mas ainda assim há riscos para a privacidade, reputação ou operações das organizações envolvidas. Destinatários podem compartilhar TLP:AMBER com membros de sua própria organização e com seus clientes, mas somente com aqueles que necessitam saber da informação (*need-to-know basis*) para proteger sua organização e seus clientes e evitar danos continuados. Nota: se a fonte quiser restringir o compartilhamento **somente** para a organização ela deve especificar TLP:AMBER+STRICT.
- c. **TLP:GREEN** = Divulgação limitada, destinatários podem divulgar dentro de sua comunidade. Fontes podem usar TLP:GREEN quando a informação é útil para a conscientização dentro de sua comunidade mais ampla. Destinatários podem compartilhar informações TLP:GREEN com seus pares e organizações parceiras dentro de sua comunidade, mas não por meio de canais publicamente acessíveis. Informações TLP:GREEN não podem ser compartilhadas fora de uma comunidade. Nota: quando a "comunidade" não estiver definida, assume-se que é a comunidade de segurança/defesa cibernética.
- d. **TLP:CLEAR** = Destinatários podem disseminar para o mundo, não há limites na divulgação. Fontes podem usar TLP:CLEAR quando há um risco mínimo ou não há previsão de risco de mau uso da informação, de acordo com regras e procedimentos aplicáveis para divulgação pública. Desde que respeitadas as regras padrão de direitos autorais, as informações TLP:CLEAR podem ser compartilhadas sem restrições.

**Dentre os diversos tipos de incidentes cibernéticos possíveis de serem notificados, destacam-se:**

- ✓ Abuso de sítios (desfiguração/defacement, injeção de links/código - spamdexing, erros de código, cross-site scripting, abuso de fórum ou livros de visita, etc.);
- ✓ Inclusão remota de arquivos (remote file inclusion - RFI) em servidores web;
- ✓ Uso abusivo de servidores de e-mail;
- ✓ Hospedagem ou redirecionamento de artefatos ou código malicioso;
- ✓ Ataques de negação de serviço (DoS, DDoS, DRDoS);
- ✓ Uso ou acesso não autorizado a sistemas ou dados;
- ✓ Varredura de portas (Port Scan);
- ✓ Comprometimento de computadores ou redes;
- ✓ Desrespeito à Política de Segurança da Informação/Cibernética ou uso inadequado dos recursos de Tecnologia da Informação (TI);
- ✓ Ataques de engenharia social (Phishing);



Dentre os diversos tipos de incidentes cibernéticos possíveis de serem notificados, destacam-se:

- ✓ Cópia e distribuição não autorizada de material protegido por direitos autorais;
- ✓ Uso abusivo ou indevido de redes sociais para difamação, calúnia, ameaças ou fraudes;
- ✓ Ataques contra sistemas de autenticação (Brute Force Attack);
- ✓ **Indisponibilidade de ativos por criptografia (Ransomware Attack);**
- ✓ Exploração de vulnerabilidades;
- ✓ **Vazamentos de dados (Data Leak);** e
- ✓ Outros incidentes cibernéticos.



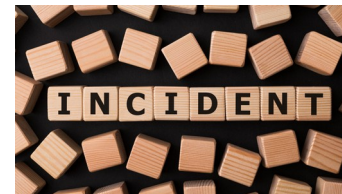


# Padrão de Notificação de Incidentes



## Construção básica da notificação :

DESTINATÁRIO: [ctir@ctir.gov.br](mailto:ctir@ctir.gov.br).



ASSUNTO: Deve-se fazer constar no assunto da notificação: "[TLP:MARCAÇÃO]", "ÓRGÃO/ENTIDADE" e o "TIPO DE INCIDENTE".

CORPO DO E-MAIL: Deve-se repetir o TLP e após, descrever sucintamente o incidente ocorrido, informando, quando cabível, informações, tais como: situação atual do incidente; IP ou lista de IPs envolvidos; organizações/entidades envolvidas; pessoas ou serviços de rede envolvidos; registros de sistemas (logs) com o respectivo timezone; cronologia dos acontecimentos; ações adotadas; outros detalhes técnicos e incidentes correlacionados.

ANEXO(S): Deverão ser anexadas as informações que facilitem a análise e a resposta ao incidente, tais como: logs de servidores e/ou serviços, cabeçalho de e-mails (headers), código(s) malicioso(s), captura de tela(s) (print screen), entre outros.

Em necessidade de comunicação por meio seguro, a mensagem deve ser criptografada com a chave pública (PGP) do CTIR Gov, disponibilizada em

[PGP - CTIR Gov](#)

Impressão digital (Fingerprint): 9798 2E5B 6EC7 B6ED B98E 60F4 9409 D6F7 6438 EEFF





# Exemplo fictício de Notificação



From: etir@orgao.gov.br

To: ctir@ctir.gov.br

Subject: [TLP:AMBER] ORGAO.GOV.BR - Phishing

[TLP:AMBER]

Prezados,

1. Foram identificadas tentativas de ataques de Phishing contra colaboradores deste órgão nas últimas 24h.
2. Nossos sistemas identificaram XX diferentes casos, oriundos da mesma fonte. Todos os casos foram bloqueados por nossa ferramenta de segurança e não houve danos.
3. Remetemos em anexo os headers completos da amostra, para a tomada das providências cabíveis. Informamos que todos os horários estão em UTC-3.

Att,

ETIR Órgão.

[TLP:AMBER]



# Exemplo real de Notificação



## ETIR Setorial notificando o CTIR Gov :

Ter Mar 12 14:27:36 2024 [Redacted]

Prezado,

Agradecemos o compartilhamento da informação.

Atenciosamente,

Equipe CTIR Gov.

Ter Mar 12 10:15:18 2024 **root - Tiquete criado**

Assunto: Possível vazamento de dados

Prezados,

Recebemos a seguinte informação de nosso provedor de serviço de [Redacted]

"Identificado no BreachForums o ator "sombraman1919" disponibilizando no um suposto banco de dados do [Redacted], contendo 1.048.576 linhas. Na amostra disponibilizada é possível identificar nome completo, CPF, data de nascimento, endereço, entre outros dados."

Obs.: O [Redacted] não possui o arquivo contendo as informações para compartilhar, pois recebeu apenas o extrato relativo aos dados de seus usuários.

[Redacted]

ETIR- [Redacted]



# Exemplo notificação parceira



**Sanitização.**

[TLP:AMBER] Leak

Exibir Histórico Básicos Pessoas Datas Vínculos Jumbo Lembretes Ações

### Metadados do ticket

#### Sumário

Identificador: [REDACTED]  
Estado: novo  
Prioridade: [REDACTED]  
Fila: Leak

#### Lembretes

Novo lembrete:  
Assunto: [REDACTED]  
Proprietário: [REDACTED]  
Vencimento: [REDACTED]

Exibir Histórico Básicos Pessoas Datas Vínculos Jumbo Lembretes Ações

### Histórico

Seg Out 28 17:45:13 2024 root - Ticket criado  
Assunto: [TLP:AMBER] Leak

- gov.br,11\*\*\*\*\*94,Plaintext
- gov.br,xv\*\*\*\*\*48,Plaintext
- gov.br,81\*\*\*\*\*66,Plaintext
- gov.br,14\*\*\*\*\*15,Plaintext
- gov.br,dg\*\*\*\*\*20,Plaintext
- gov.br,co\*\*\*\*\*23,Plaintext
- gov.br,20\*\*\*\*\*26,Plaintext
- gov.br,ki\*\*\*\*\*41,Plaintext
- gov.br,do\*\*\*\*\*21,Plaintext
- gov.br,al\*\*\*\*\*20,Plaintext
- gov.br,he\*\*\*\*\*11,Plaintext
- gov.br,12\*\*\*\*\*18,Plaintext
- gov.br,sc\*\*\*\*\*10,Plaintext
- gov.br,Ej\*\*\*\*\*3#,Plaintext
- gov.br,SS\*\*\*\*\*es,Plaintext
- gov.br,ed\*\*\*\*\*05,Plaintext
- gov.br,Ag\*\*\*\*\*0@,Plaintext
- gov.br,7m\*\*\*\*\*oz,Plaintext
- gov.br,10\*\*\*\*\*03,Plaintext
- gov.br,an\*\*\*\*\*os,Plaintext
- gov.br,12\*\*\*\*\*ro,Plaintext
- gov.br,n\*\*\*\*\*3\*,Plaintext
- gov.br,Kl\*\*\*\*\*20,Plaintext
- gov.br,Kj\*\*\*\*\*40,Plaintext
- gov.br,RO\*\*\*\*\*JO,Plaintext
- gov.br,Er\*\*\*\*\*49,Plaintext
- gov.br,ta\*\*\*\*\*23,Plaintext
- gov.br,00\*\*\*\*\*sp,Plaintext
- gov.br,am\*\*\*\*\*00,Plaintext



# O porquê da sanitização.



## 1. NIST Special Publication 800-63B (Digital Identity Guidelines):

- Sanitização das credenciais: O NIST recomenda não enviar credenciais em texto claro. Se houver necessidade de incluir qualquer credencial vazada, ela deve ser adequadamente sanitizada (como por exemplo, omitir partes críticas das credenciais ou substituir senhas por hashes).
- **Notificação segura:** As notificações devem ser feitas por meio de canais seguros, preferencialmente criptografados, como S/MIME ou PGP, para garantir que as credenciais não sejam interceptadas por terceiros mal-intencionados durante a comunicação.

**NIST**  
**National Institute of  
Standards and Technology**

## 2. OWASP (Open Web Application Security Project):

O OWASP recomenda não incluir a senha ou qualquer credencial em formato plaintext em qualquer notificação de incidente. Senhas ou informações sensíveis nunca devem ser expostas diretamente em e-mails, notificações ou sistemas públicos sem antes serem criptografadas ou parcialmente ocultadas.

Também sugere o uso de hashes em vez de senhas reais, permitindo que o usuário altere suas credenciais diretamente sem qualquer exposição.



# OWASP

Open Web Application  
Security Project

## 3. GDPR (Artigo 34) e LGPD (Artigos 48 e 49):

Ambas as leis recomendam que, em caso de violação de dados, os responsáveis notifiquem os titulares e autoridades competentes sem expor mais dados do que o necessário. Isso implica que as credenciais vazadas não devem ser enviadas em sua totalidade (especialmente senhas em texto claro).

O GDPR é explícito ao dizer que qualquer comunicação de incidente deve garantir que os dados pessoais envolvidos não estejam acessíveis a outros durante a comunicação.





# O porquê da sanitização.



## 4. NCSC (UK National Cyber Security Centre):

O NCSC oferece diretrizes que recomendam que, em caso de vazamento de credenciais, as organizações devem notificar os usuários sem expor as credenciais diretamente. Eles sugerem enviar um alerta sobre a necessidade de troca de senha e fornecer orientações sobre como realizar essa troca de maneira segura, em vez de incluir qualquer parte da senha no e-mail.



National Cyber  
Security Centre

- Interpretação da notificação;
- Entendimento da criticidade do caso e sua relação com possíveis incidentes cibernéticos críticos;
- Tratamento recomendado do incidente;

Intervalo

- Análise de Casos reais;
- Conclusão e recomendações CTIR relacionadas;





- Toda a preocupação com **transmissão segura, sanitização** e o **melhor contato**, surgem com as estatísticas noticiadas.
- A relação entre uma notificação e posterior comprometimento.
- Há uma estreita correlação entre um vazamento e um ataque bem sucedido.



### Vazamento de dados dispara 340% no Brasil - ConvergenciaDigital

O Brasil teve 5 milhões de contas de usuários online vazadas no terceiro trimestre de 2024, um aumen

[convergenciadigital.com.br](https://convergenciadigital.com.br)

<https://convergenciadigital.com.br/seguranca/vazamentos-de-dados-dispara-340-no-brasil/>

14:50



### Brasil foi o 5º país mais atingido por ransomwares no 3Q 2024

Brasil foi o 5º país mais atingido por ransomwares no 3Q 2024, revela ISH Tecnologia Ao todo, foram 829 incidentes em todo o mundo no período; país foi o

[minutodaseguranca.blog.br](https://minutodaseguranca.blog.br)

<https://minutodaseguranca.blog.br/brasil-foi-o-5-pais-mais-atingido-por-ransomwares-no-3q-2024/>

07:42



### Brasil enfrenta quase 2 milhões de ataques de malware por dia - Security Leaders

O Panorama de Ameaças da Kaspersky de 2024 revela que a empresa bloqueou mais de 725 milhões de ataques de malware no Brasil entre junho de 23 e julho de

[securityleaders.com.br](https://securityleaders.com.br)

<https://securityleaders.com.br/brasil-enfrenta-quase-2-milhoes-de-ataques-de-malware-por-dia/>

11:47



### Brasil é o 4º país com mais ameaças cibernéticas na América Latina

Brasil é o 4º país com mais ameaças cibernéticas na América Latina, com 7,76% das detecções no 1º semestre de 2024

[minutodaseguranca.blog.br](https://minutodaseguranca.blog.br)

<https://minutodaseguranca.blog.br/brasil-e-o-4o-pais-com-mais-ameacas-ciberneticas-na-america-latina/>

07:48



### Ransomware cai 26% no Brasil, mas país segue como maior vítima na América Latina - Security Leaders

O Panorama de Ameaças da Kaspersky de 2024 revela que a empresa bloqueou mais de 487 mil ataques de ransomware de junho de 2023 a julho de 2024 no Brasil

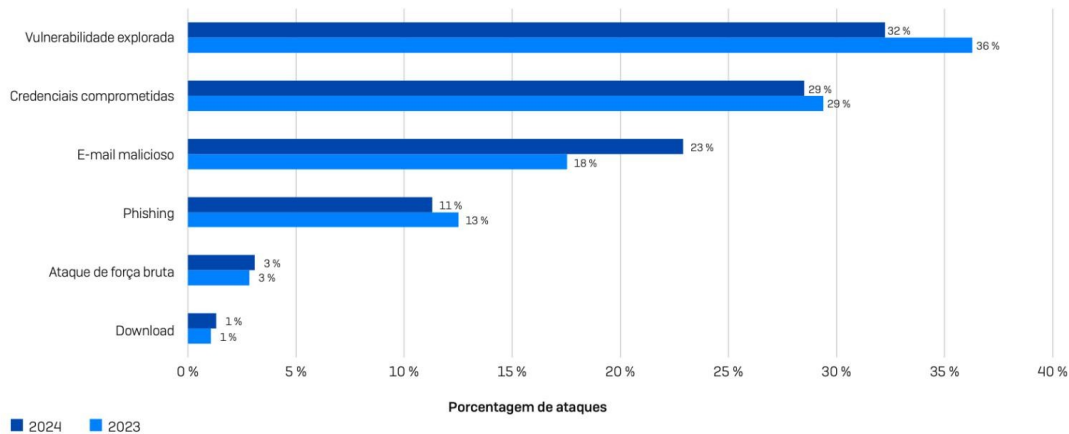
[securityleaders.com.br](https://securityleaders.com.br)

<https://securityleaders.com.br/ransomware-cai-26-no-brasil-mas-pais-segue-como-maior-vitima-na-america-latina/>

11:45

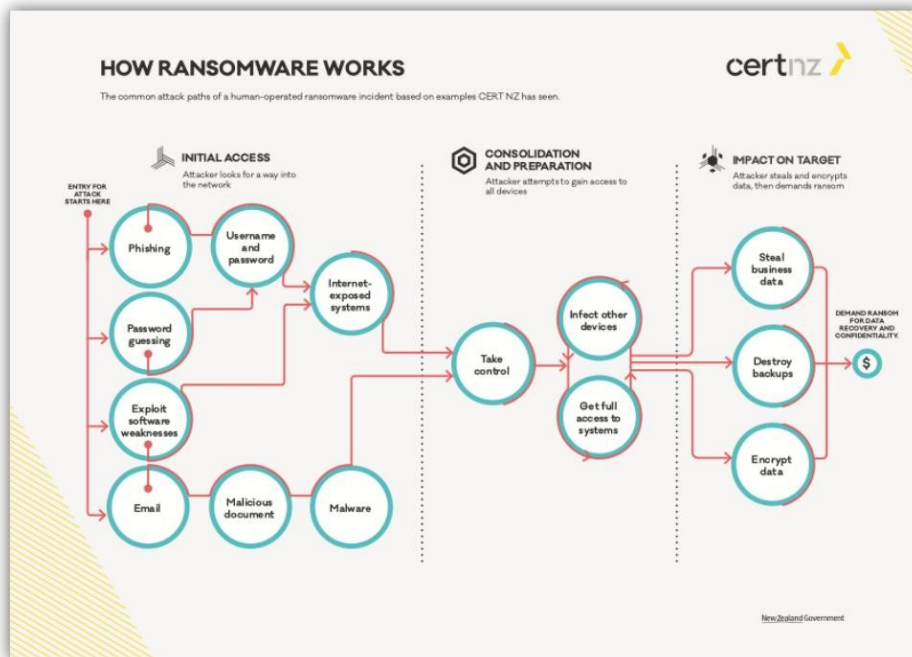
TLP: CLEAR

## Causas primárias dos ataques de *ransomware*



Você sabe a causa primária do ataque de ransomware que a sua organização enfrentou no último ano? Sim. n=2.974 organizações atingidas por ransomware.

Fonte: <https://www.sophos.com/pt-br/content/state-of-ransomware>



Fonte: <https://www.cert.govt.nz/assets/ransomware/cert-lifecycle-of-a-ransomware-incident-business-version.pdf>



- Interpretação da notificação;
- Entendimento da criticidade do caso e sua relação com possíveis incidentes cibernéticos críticos;

**- Tratamento recomendado do incidente;**

Intervalo

- Análise de Casos reais;
- Conclusão e recomendações CTIR relacionadas;



# Tratamento recomendado dado ao incidente



Recebeu uma notificação versando sobre eventos de credenciais vazadas? O que fazer ?



Conjunto de Boas práticas / Framework / Caderno de Instruções / Instrução Normativa / Metodologia / Governança e Gestão de TI / etc...

## Órgãos da Administração Pública Federal :

Programa de Privacidade e Segurança da Informação - PPSI

## Convidados e parceiros que não se enquadram na Administração Pública Federal :

ISO 27035-1

ISO 27035-2

COBIT ... ITIL...

# Tratamento recomendado dado ao incidente



Recebeu uma notificação versando sobre eventos de credenciais vazadas? **O que fazer ? Como fazer ?** Focar na celeridade do tratamento.

## - **Orgãos da Administração Pública Federal :**

### **PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)**

[https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia\\_framework\\_psi.pdf](https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf)

#### 3.5 Controle 5: Gestão de Contas

Usar processos e ferramentas para atribuir e gerenciar autorização de credenciais para contas de usuário, contas de administrador, contas de serviço para ativos e softwares institucionais.

##### Por que implementar?

É mais fácil para um agente de ameaça (externo ou interno) obter acesso não autorizado a ativos ou dados da organização usando credenciais de usuário válidas do que "hackeando" o ambiente. Existem várias formas de obter acesso a contas de usuário; como por exemplo:

- senhas fracas;
- contas ainda válidas depois que um colaborador deixa de trabalhar na organização;
- contas de teste;
- contas compartilhadas;
- contas de serviço incorporadas em aplicações para scripts;
- um usuário com a mesma senha que ele usa para uma conta *on-line* que foi comprometida (em um *dump* de senha pública);
- engenharia social em um usuário para fornecer sua senha;
- malware para capturar senhas ou tokens na memória ou na rede.

Contas administrativas ou com privilégio alto são alvos preferenciais porque permitem que atacantes adicionem novas contas ou façam alterações em ativos que podem torná-los mais vulneráveis a ataques. As contas de serviço também são críticas, pois geralmente são compartilhadas entre as equipes, internas e externas à organização e as vezes desconhecidas, apenas para serem reveladas em auditorias de gestão de contas padrão.

Além disso, as INs GSI/PR nº 2 de 5 de fevereiro de 2013 e NCs nº 01/IN02/NSC/GSIPR e seus anexos (Anexo A e Anexo B), preveem ações a serem observadas e implementadas neste controle.

#### 3.5.1 Aplicabilidade e Implicações de privacidade

O gerenciamento de contas é aplicável a todos os aplicativos, dispositivos e serviços. Todos os usuários precisarão de uma conta para acessar aplicativos, dispositivos e provedores de serviços internos ou externos.

<b>2. CONTROLE DE ESTRUTURAÇÃO BÁSICA DE GESTÃO EM PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO</b>	<b>35</b>
<b>3. CONTROLES DE CIBERSEGURANÇA</b>	<b>36</b>
<b>3.1 Controle 1: Inventário e Controle de Ativos Institucionais</b>	<b>36</b>
3.1.1 Aplicabilidade e Implicações de Privacidade	37
<b>3.2 Controle 2: Inventário e Controle de Ativos de Software</b>	<b>37</b>
3.2.1 Aplicabilidade e Implicações de Privacidade	38
<b>3.3 Controle 3: Proteção de Dados</b>	<b>39</b>
3.3.1 Aplicabilidade e Implicações de Privacidade	40
<b>3.4 Controle 4: Configuração Segura de Ativos Institucionais e Software</b>	<b>40</b>
3.4.1 Aplicabilidade e Implicações de Privacidade	41
<b>3.5 Controle 5: Gestão de Contas</b>	<b>42</b>
3.5.1 Aplicabilidade e Implicações de privacidade	42
<b>3.6 Controle 6: Gestão do Controle de Acesso</b>	<b>43</b>
3.6.1 Aplicabilidade e Implicações de Privacidade	44
<b>3.7 Controle 7: Gestão Contínua de Vulnerabilidades</b>	<b>44</b>
3.7.1 Aplicabilidade e Implicações de Privacidade	45
<b>3.8 Controle 8: Gestão de Registros de Auditoria</b>	<b>46</b>
3.8.1 Aplicabilidade e Implementações de Privacidade	46

# Tratamento recomendado dado ao incidente



Recebeu uma notificação versando sobre eventos de credenciais vazadas? **O que fazer ? Como fazer ?** Focar na celeridade do tratamento.

- **Convidados e parceiros não enquadrados na Administração Pública Federal : ABNT NBR ISO/IEC 27035-1:2023**

## Normas e Princípios Essenciais

Um dos pilares dessa prática é a ABNT NBR ISO/IEC 27035-1:2023 – Gestão de Incidentes de Segurança da Informação, Parte 1: Princípios e Processo. Esta norma serve como base para uma abordagem estruturada na preparação, detecção, resposta e aprendizado com incidentes de segurança. Como resultado, ela oferece diretrizes genéricas, aplicáveis a organizações de todos os tamanhos e setores.

## Principais Aspectos da Norma

A ABNT NBR ISO/IEC 27035-1:2023 abrange conceitos fundamentais, como a importância da prontidão para incidentes, métodos de detecção precoce, processos de resposta eficazes e a necessidade de análise pós-incidente para melhorias contínuas. Todavia, convém compartilhar que ela destaca a aplicabilidade desses princípios a todas as organizações, independentemente de seu perfil ou porte.

## Aplicação Prática

Com o exposto, a implementação dessa norma pode capacitar as organizações a fortalecerem suas defesas cibernéticas, minimizando os impactos de incidentes de segurança. Ao seguir as diretrizes da ISO/IEC 27035-1, as empresas podem desenvolver planos de resposta personalizados, identificar vulnerabilidades e melhorar a resiliência cibernética.





# Tratamento recomendado dado ao incidente



Recebeu uma notificação versando sobre eventos de credenciais vazadas? **O que fazer ? Como fazer ?** Focar na celeridade do tratamento.

- **Convidados e parceiros não enquadrados na Administração Pública Federal : ABNT NBR ISO/IEC 27035-2:2023**

A ABNT NBR ISO/IEC 27035-2:2023 é uma norma que fornece diretrizes para o planejamento e preparação da resposta a incidentes de segurança da informação.

- **Estabelecer uma política robusta de gestão de incidentes de segurança da informação**, com o total comprometimento da Alta Direção. Essa política servirá como base sólida para todas as suas ações.
- **Manter as políticas de segurança da informação atualizadas**, tanto no âmbito da organização quanto nos sistemas, serviços e redes. Isso garante que você esteja sempre um passo à frente das ameaças.
- **Criar um plano de gestão de incidentes de segurança da informação detalhado**, definindo as etapas a serem seguidas em caso de um incidente, desde a detecção até a recuperação.
- **Formar uma Equipe de Gestão de Incidentes qualificada e treinada**, pronta para agir com rapidez e eficiência na contenção e resolução de incidentes.
- **Estabelecer relacionamentos e conexões com stakeholders internos e externos**, assegurando a comunicação eficaz e o apoio necessário durante um incidente.
- **Obter o suporte técnico e outros recursos essenciais**, incluindo apoio organizacional e operacional, para garantir uma resposta eficaz.
- **Implementar instruções e treinamentos de conscientização sobre gestão de incidentes de segurança da informação**, educando os colaboradores e *stakeholders* sobre seus papéis e responsabilidades em caso de um incidente.



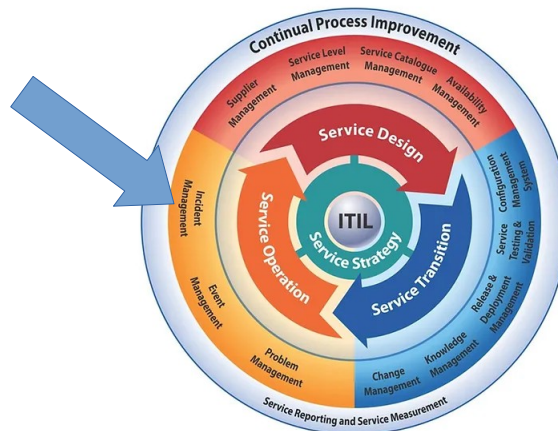
**NBR 27035-2:2023**

Gestão de incidentes de segurança da informação  
Parte 2. Diretrizes para planejar e preparar a  
resposta a incidentes

# Tratamento recomendado dado ao incidente



Recebeu uma notificação versando sobre eventos de credenciais vazadas? **O que fazer ? Como fazer ?** Focar na celeridade do tratamento.



Apenas ilustrativo e sugestivo....Não taxativo.

## De forma mais prática :

1. De acordo com informações recebidas de organização parceira, identificamos que uma ou mais contas pessoais relacionadas a domínio sob vossa responsabilidade podem ter sido comprometidas, conforme log relacionado no item 7 ao final desta notificação.
- 2. Os e-mail constantes do log correspondem a contas que podem ter sido comprometidas devido a infecções por malware, acesso indevido a bases de dados, ataques de phishing ou outras atividades maliciosas. Importante: o campo "Senha" é sanitizado na origem, não apresentando todos os caracteres. Portanto, não foi possível confirmar a validade das credenciais, nem foram realizados testes de acesso.
- 3. Cabe ressaltar que, embora possam ocorrer falsos positivos nos dados enviados, a maioria das credenciais encaminhadas por notificações desta natureza têm sido confirmadas como válidas. Solicitamos, portanto, a devida atenção ao assunto e a verificação das informações fornecidas, bem como o feedback a respeito das ações tomadas por parte da organização.



# Tratamento recomendado dado ao incidente



4. Recomendamos a análise do caso e a tomada das medidas cabíveis com a urgência que o caso requer. Caso confirme a validade das credenciais, as ações recomendadas para o caso são:

- Bloqueio imediato das contas relacionadas a esta notificação e exigência de troca de senha para a reativação;
- Utilização de 2FA (duplo fator de autenticação) em todos os sistemas sempre que possível;
- Especial atenção a utilização das credenciais em acessos remotos (VPN) e outros sistemas acessíveis via internet;
- Criar ou reforçar campanhas de conscientização de usuários sobre como identificar e reportar e-mails de phishing e como se proteger de ataques de engenharia social; e
- Monitorar continuamente dispositivos conectados à rede corporativa, com especial atenção a atividades anômalas relacionadas a processos de login.

5. Solicitamos que nos informem sobre a validade ou não das credenciais. Esta informação é importante para que possamos melhorar o processo de notificações desta natureza, geração de estatísticas, confiabilidade da fonte, alertas e recomendações.

6. Caso este problema não seja de sua responsabilidade, solicitamos que a mensagem seja encaminhada aos responsáveis por tal tarefa. (Celeridade)



# hora do Intervalo



- Interpretação da notificação;
- Entendimento da criticidade do caso e sua relação com possíveis incidentes cibernéticos críticos;
- Tratamento recomendado do incidente;

## Intervalo

- **Análise de Casos reais;**
- Conclusão e recomendações CTIR relacionadas;





# Casos reais...



**406975 – 1 . Notificação criada pelo CTIR devido a report de fonte parceira versando sobre credenciais vazadas de Órgãos da nossa constituency.**

**Obs . Orgão demorou em tomar providencias. (2 meses)**

Encontrados 3 tíquetes

Editar Busca Avançado **Apresentar Resultados** Atualização em Massa Gráfico Fontes de Notícias ▾

# ▲ ▾ Assunto ▾  
Requisitante ▾

Estado ▾ Fila ▾ Proprietário ▾ Prioridade ▾  
Criado ▾ Última atualização ▾ Atualizado em ▾ Tempo Restante ▾

406975 [TLP:AMBER] Possível comprometimento de credenciais

Leak

9 meses atrás

411456 [TLP:AMBER] - PHISHING - Notificação de phishing

411470 Possível comprometimento de conta

Recarregar esta página a cada 2 minutos. ▾

Alterar

Exibir Histórico Básicos Pessoas Datas Vínculos Jumbo More ▾

jo .gov.br,  
jo .gov.br,  
jc .gov.br,  
jo .gov.br,  
jo .gov.br,  
jo .gov.br,  
jo .gov.br,  
js .gov.br,  
ju .gov.br,  
ju .gov.br,  
j .gov.br,  
j .gov.br,  
ju .gov.br,  
ju .gov.br,  
julie .gov.br,  
.gov.br,  
.gov.br,  
.gov.br,  
juridicc .gov.br,



# 2 meses depois...



## 411456 – 1. Outro Órgão da nossa constituency notifica o CTIR sobre Phishing oriundo da credencial reportada há 2 meses.

Encontrados 3 tickets

# Assunto

Requisitante

406975 [TLP:AMBER] Possível comprometimento de conta

411456 [TLP:AMBER] Possível comprometimento de conta

etir

411470 Possível comprometimento de conta

SMTP\_Abuse

7 meses atrás

Recarregar esta página a cada 2 minutos.

Alterar

Seg Mar 18 14:20:30 2024

[TLP:AMBER]

Prezados,  
o [redacted] recebeu vários e-mails, provenientes do domínio [redacted].gov.br". Como a situação indica comprometimento de conta do referido domínio, estamos realizando esta notificação e tomamos as providências para bloquear as mensagens indesejadas originárias do remetente comprometido. Incluímos em cópia o responsável pelo domínio de acordo com o Registro BR. Em anexo, segue exemplo das mensagens recebidas, extraído de nossa ferramenta antispam.

Obrigado,  
Equipe ETIR

[TLP:AMBER]

ssa Gráfico Fontes de Notícias

tário Prioridade

ado em Tempo Restante

Exibir Histórico Básicos Pessoas Datas Vinculos More

Verment o:

Salvar

Campos Personalizados

NoteType: (sem valor)

NoteContent: X-LCID

Received: from [redacted] by srv-antispam-[redacted].gov.br with Xeams SMTP; Sat, 16 Mar 2024 14:15:42 -0300 (BRT)

X-SM-EnvelopeFrom: julia [redacted].gov.br

X-SMRecipient: [redacted].gov.br

Datas

Criado: Seg Mar 18 12:00:15 2024

Inicia: Não definido

Iniciado: Seg Mar 18 14:45:21 2024





# 2 meses depois...



## 411470 – 1 . CTIR notifica o Órgão sobre Phishing oriundo da credencial reportada há 2 meses.

Seg Mar 18 14:45:22 2024 root - Tiquete criado

Assunto: Possível comprometimento de conta

[TLP:AMBER]

Prezados,

1. Recebemos notificação sobre Phishing em nossa comunidade. Identificamos o possível comprometimento/abuso de serviço SMTP na máquina [redacted].44;julia.[redacted].gov.br].
2. Solicitamos que sejam verificados os dados, uma vez que um ou mais computadores de sua rede ou contas de e-mail podem estar comprometidos.
- 2.1 Solicitamos também, caso seja confirmado o incidente, que mantenham-nos informados sobre as providências tomadas.
3. Caso este tipo de problema não seja de sua responsabilidade, solicitamos que esta mensagem seja encaminhada aos responsáveis por tal tarefa.
4. Solicitamos que referências futuras a esta notificação preservem o "Assunto" desta mensagem.

Colocamo-nos à disposição para auxiliá-los no que for necessário.

Atenciosamente,

Equipe CTIR Gov <ctir@gov.br>  
<https://www.gov.br/ctir>  
INOC-DBA (VOIP): 266031+800

O Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR Gov, subordinado ao Departamento de Segurança da Informação e Cibernética - DSIC, do Gabinete de Segurança Institucional da Presidência da República, tem como finalidade atender aos incidentes de segurança de redes computacionais do governo (domínios gov.br, jus.br, leg.br, mil.br, mp.br, def.br e tc.br).

O CTIR Gov adere ao padrão Traffic Light Protocol (TLP), conforme definido pelo Forum of Incident Response and Security Teams (FIRST): <https://www.gov.br/ctir/pt-br/assuntos/tlp>

[TLP:AMBER]

Encontrado

# Ass

Rec

406975 [TL

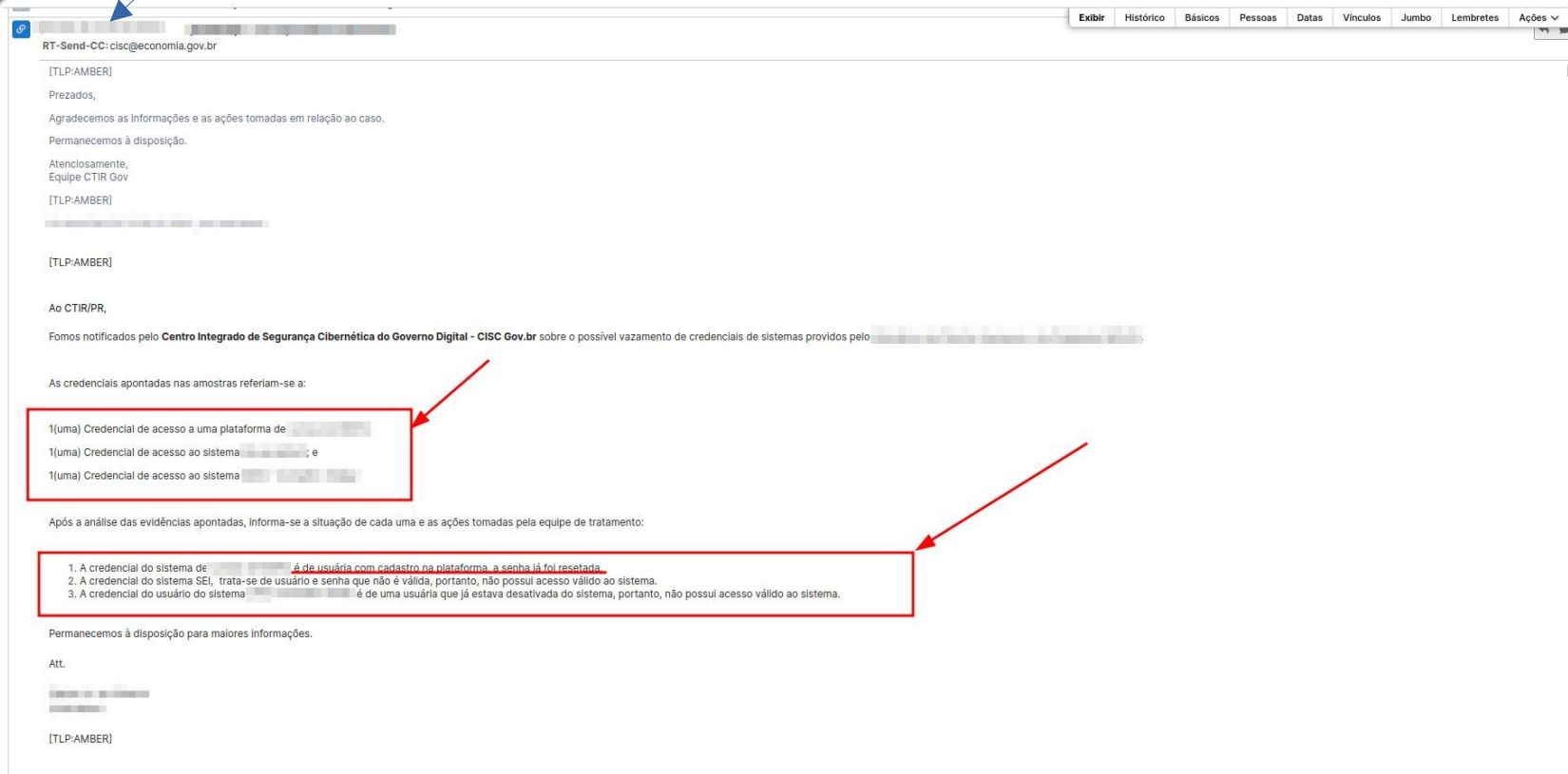
411456 [TL

ctir

411470 Pos

Recarregar est

404752 – 1 . Órgão da nossa constituency é notificado pelo CISC, versando sobre vazamento de credenciais, e o mesmo órgão nos reportou.



RT-Send-CC: cisc@economia.gov.br

[TLP:AMBER]

Prezados,

Agradecemos as informações e as ações tomadas em relação ao caso.  
Permanecemos à disposição.

Atenciosamente,  
Equipe CTIR Gov

[TLP:AMBER]

[TLP:AMBER]

Ao CTIR/PR,

Fomos notificados pelo **Centro Integrado de Segurança Cibernética do Governo Digital - CISC Gov.br** sobre o possível vazamento de credenciais de sistemas providos pelo [REDACTED]

As credenciais apontadas nas amostras referiam-se a:

1(uma) Credencial de acesso a uma plataforma de [REDACTED]  
1(uma) Credencial de acesso ao sistema [REDACTED]; e  
1(uma) Credencial de acesso ao sistema [REDACTED]

Após a análise das evidências apontadas, informa-se a situação de cada uma e as ações tomadas pela equipe de tratamento:

1. A credencial do sistema de [REDACTED] de usuário com cadastro na plataforma, a senha já foi resetada.
2. A credencial do sistema SEI, trata-se de usuário e senha que não é válida, portanto, não possui acesso válido ao sistema.
3. A credencial do usuário do sistema [REDACTED] é de uma usuária que já estava desativada do sistema, portanto, não possui acesso válido ao sistema.

Permanecemos à disposição para maiores informações.

Att.

[REDACTED]

[TLP:AMBER]

- Interpretação da notificação;
- Entendimento da criticidade do caso e sua relação com possíveis incidentes cibernéticos críticos;
- Tratamento recomendado do incidente;

## Intervalo

- Análise de Casos reais;
- **Conclusão e recomendações CTIR relacionadas;**





# Conclusão e Recomendações



- 1. ReGIC foi criada para prover um trabalho colaborativo entre órgãos da APF e Órgãos convidados (Expansão da ReGIC);**
- 2. Notificar o CTIR Gov - como CSIRT Nacional - ajuda-nos a gerar estatísticas , alertas e recomendações que serão difundidas dentro da rede;**
- 3. Estamos implantando o MISP - pretensão de disponibilizar para a ReGIC;**
- 4. Por sermos um CSIRT de Coordenação Nacional e ligados à PR, temos a prerrogativa de coordenar soluções de incidentes cibernéticos de nossa abrangência, também possuímos contatos com órgãos governamentais de outros países, assim como, participamos de fóruns internacionais sobre o assunto ;**
- 5. Notificar o CTIR através da ETIR do Órgão, ajudará muito em razão de estarmos tratando via canal técnico efetivo, resultando em ações efetivas e visibilidade para a alta gestão;**

