

# INCIDENTE

---

## de Segurança

---



# DA INFORMAÇÃO





## O que é um Incidente de Segurança da Informação?

Um Incidente de Segurança da Informação é qualquer violação de segurança, seja acidental ou intencional, que possa resultar na destruição, perda, alteração, divulgação ou acesso não autorizado aos dados tratados pelo IgesDF. Isso pode ocorrer tanto por meios físicos quanto digitais, representando uma quebra nas políticas de segurança do Instituto.

Dessa forma, os dados sob nossa responsabilidade ficam em risco, seja por erro humano ou por um ataque malicioso. Esses incidentes podem comprometer a integridade, a confidencialidade e a disponibilidade das informações, afetando a segurança dos nossos processos e a confiança dos nossos pacientes.

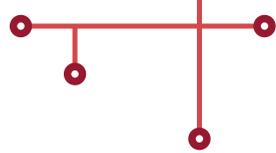
Na área da saúde, isso pode comprometer informações críticas de pacientes, prontuários e processos médicos.

## Vamos pensar conosco?

Se um dado sigiloso, como uma informação médica de um paciente, cair nas mãos erradas, isso pode prejudicar a segurança do paciente e a reputação do IgesDF.

## Quais são os principais tipos de incidentes?

- Acesso não autorizado;
  - Compartilhamento não autorizado de credenciais de acesso;
  - Uso indevido de recursos tecnológicos;
  - Violação das políticas de segurança e privacidade;
  - Manejo inadequado de dados pessoais e institucionais;
  - Processamento inadequado ou ilegal de dados;
  - Acesso não autorizado a dados pessoais;
  - Violação de dados pessoais;
- 



## **E como esses incidentes podem afetar a Segurança a Informação nos tratamentos no dia a dia?**

### **Exemplo 1: Acesso não autorizado a prontuários médicos**

Um funcionário sem permissão acessa os dados médicos de um paciente sem necessidade e reporta para terceiros não autorizados as informações. Isso é um incidente sério que deve ser reportado!

### **Exemplo 2: Perda de dispositivos**

Um notebook do Instituto contendo informações de pacientes foi esquecido em um lugar público. Essa perda pode resultar em exposição de dados confidenciais do IgesDF e deve ser reportado.

### **Exemplo 3: E-mails sem verificação do remetente**

Um funcionário recebe um e-mail que parece ser de algum diretor do Instituto solicitando o envio de dados de pacientes. O colaborador não verifica se o e-mail é institucional (@igesdf.org.br) e envia informações para terceiros externos que não são autorizados a receber esse dado. Esse incidente também deve ser reportado.

### **Exemplo 4: E-mails maliciosos (phishing)**

Um colaborador do IgesDF, recebeu um e-mail falso se passando pelo iFood com uma oferta de desconto. Ao abrir o e-mail, é instalado um vírus que captura informações da rede interna. Assim que ele inseriu suas credenciais corporativas, elas foram utilizadas por criminosos para acessar informações confidenciais de pacientes e relatórios internos. Não devemos utilizar o e-mail institucional para listas externas as atividades desenvolvidas.

### **Exemplo 5: Uso inadequado de senhas**

Um profissional de saúde compartilha sua senha com outro colega para "facilitar o trabalho". Isso coloca os dados dos pacientes em risco e é um comportamento perigoso.

### **Exemplo 6: Documentos impressos esquecidos\*\***

Um colaborador esquece documentos impressos com dados de pacientes na própria impressora ou em algum lugar dentro da unidade. Qualquer pessoa que passar por lá pode acessar essas informações.

## Por que é TÃO IMPORTANTE reportar um Incidente de Segurança?

Reportar um incidente de segurança **IMEDIATAMENTE** é crucial para evitar ou minimizar danos. Quando algo errado acontece, precisamos atuar rápido para proteger nossos pacientes e nossa equipe!

- **Evita a exposição de dados sensíveis:** Quanto mais rápido agirmos, menores as chances de que informações sejam utilizadas indevidamente.
- **Protege a reputação do IgesDF:** Pacientes confiam que suas informações estão seguras conosco. Agir rápido garante que mantemos essa confiança.
- **Cumprimento da LGPD:** A Lei Geral de Proteção de Dados exige que protejamos os dados pessoais dos pacientes. Reportar incidentes nos ajuda a cumprir essa lei.



## Como reportar um incidente?

Caso você perceba um incidente de segurança, **NÃO ESPERE!** Entre em contato imediatamente pelo canal especializado em lidar com situações como essas, na aba "LGPD" do nosso "GLPI - antigo ATENDE TI"

Ao relatar um incidente, forneça o máximo de detalhes possível, como:

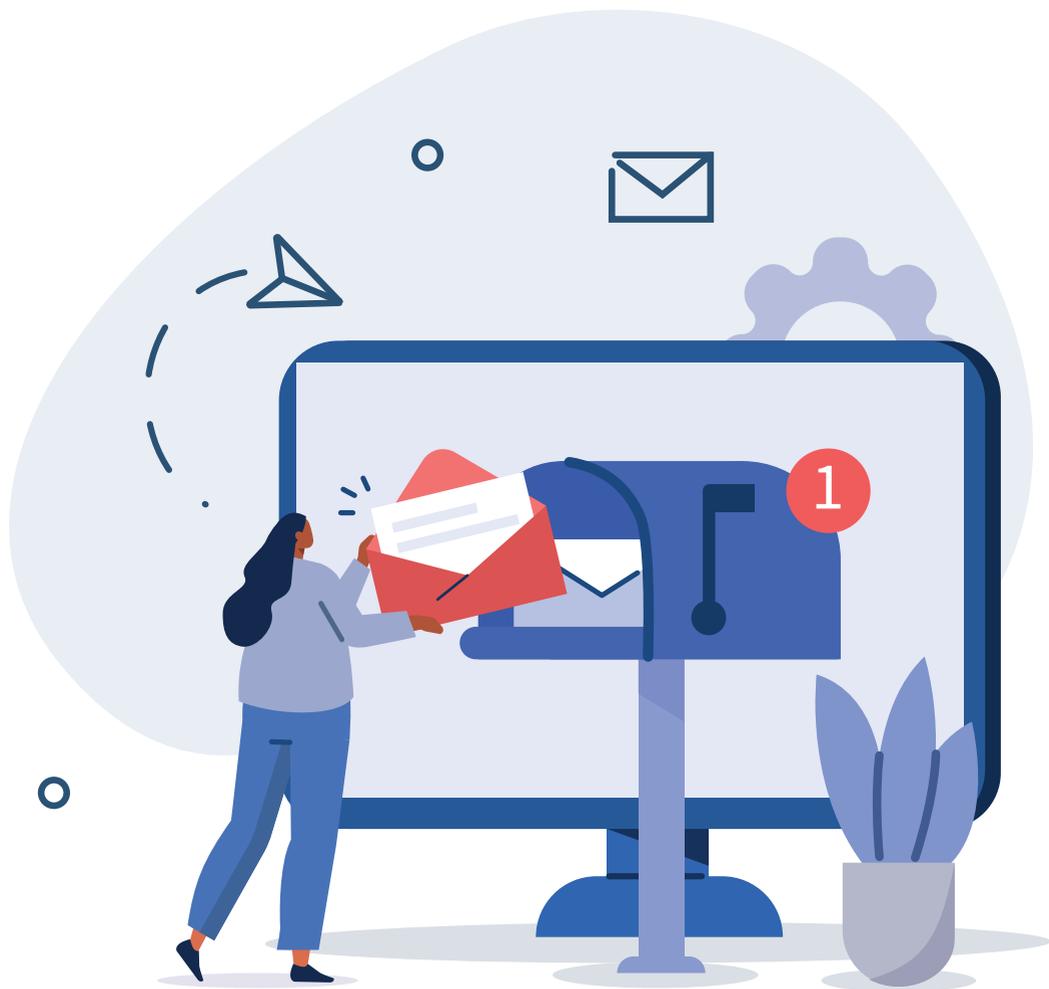
- O que aconteceu;
- Quem foi envolvido;
- Quando e onde ocorreu;
- Quais informações ou sistemas podem estar comprometidos.



## Lembre-se: Segurança é Responsabilidade de Todos!

Aqui, no IgesDF todos nós temos o papel de proteger informações. Não importa o seu cargo ou departamento, você faz parte da nossa segurança!

Se tiver dúvidas ou precisar de mais informações, não hesite em entrar em contato com a Coordenação de Governança em Proteção de Dados através do nosso e-mail: ***dpo@igesdf.org.br***.





# IGESDF

INSTITUTO DE GESTÃO ESTRATÉGICA  
DE SAÚDE DO DISTRITO FEDERAL

**Contéudo:**

Governança em Proteção de Dados