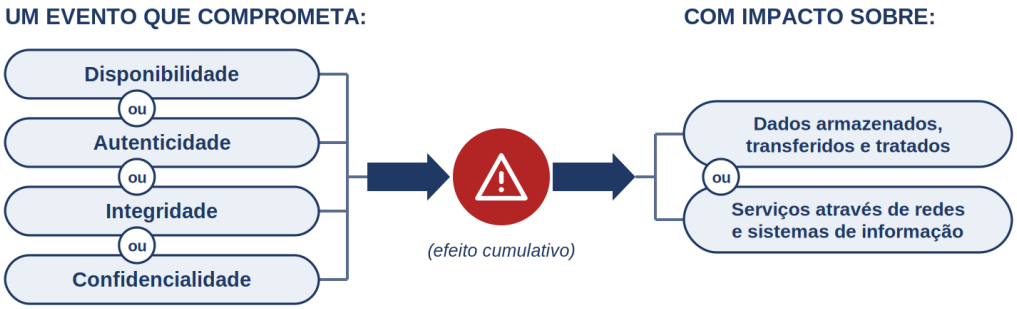
GESTÃO E REPORTE DE INCIDENTES

Decreto-Lei n.º 125/2025, de 4/12 (Regime Jurídico da Cibersegurança) e Regulamento n.º 756/2026, de 22/6

A comunicação atempada e eficaz dos incidentes é um dos pilares do **Regime Jurídico da Cibersegurança (RJC)**, aprovado pelo Decreto-Lei n.º 125/2025, que transpõe a Diretiva (UE) 2022/2555 (**NIS2**) e revoga o regime anterior (Lei n.º 46/2018 e DL n.º 65/2021). A presente informação orienta os responsáveis de segurança das entidades do Governo Regional da Madeira.

O QUE É UM INCIDENTE?

Evento com um efeito adverso real na segurança das redes e dos sistemas de informação.



COMO SE GERE UM INCIDENTE, EM SEIS PASSOS

Da preparação às lições aprendidas — o ciclo de resposta a incidentes, num esquema de muito alto nível.

1	2	3	4	5	6
Preparação	**Deteção e Análise**	**Contenção**	**Erradicação**	**Recuperação**	**Lições Aprendidas**
Políticas, equipa e ferramentas de deteção já definidas e testadas.	Confirmar o incidente e avaliar a sua gravidade e âmbito.	Isolar sistemas afetados para travar a propagação.	Remover a ameaça e corrigir a vulnerabilidade explorada.	Repor sistemas e dados em segurança, com monitorização reforçada.	Relatório pós-incidente (PIR): causas, eficácia e melhorias a aplicar.

Sequência: Preparação → Deteção e Análise → Contenção → Erradicação → Recuperação → Lições Aprendidas.

QUEM ESTÁ ABRANGIDO?

O RJC aplica-se a **entidades essenciais**, **importantes** e **"públicas relevantes"** — categoria em que se integra, em regra, a administração pública direta, indireta e setor empresarial da Região Autónoma da Madeira (RAM):

Grupo A — 250 ou mais trabalhadores;

Grupo B — entre 75 e 249 trabalhadores.

NOTA

- Em caso de dúvida sobre a **classificação da sua entidade**, contactar o CNCS (Centro Nacional de Cibersegurança), através da plataforma MyCiber.
- Caso o RJC não se aplique à sua entidade (< 75 trabalhadores), poderá notificar de forma **voluntária** um incidente de cibersegurança.

ACONTECEU UM INCIDENTE, E AGORA? A QUEM DEVO REPORTAR?

DENTRO DO GRM

- **Causa disrupção ou risco de perdas financeiras/reputacionais?** Envolver o GCPD — gcpd.ciber@madeira.gov.pt / 291 145 177.
- **Envolve dados pessoais?** Comunicar ao interlocutor RGPD da sua entidade.

ENTIDADES EXTERNAS (Empresas e outras entidades)

- O incidente que teve conhecimento é **significativo**? Reportar ao CNCS através da plataforma eletrónica **MyCiber**
- Poderá solicitar apoio / orientação ao **CCC-Madeira** (https://ccc-madeira.pt/) através dos canais disponíveis para o efeito.

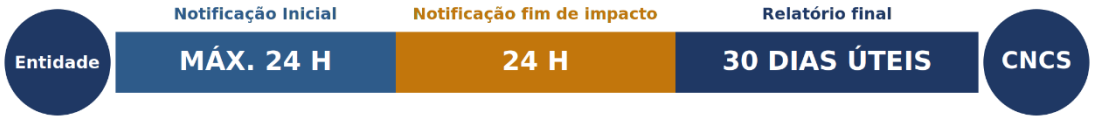
O incidente é considerado significativo quando:

1. Tiver causado, ou for suscetível de causar, graves perturbações operacionais dos serviços ou perdas financeiras à entidade em causa; OU
2. Tiver afetado, ou for suscetível de afetar, outras pessoas singulares ou coletivas, causando danos materiais ou imateriais consideráveis.

Ponderar ainda: n.º de utilizadores afetados, duração, gravidade da perturbação e dimensão do impacto económico/social (art. 40.º/3 RJC).

O INCIDENTE É SIGNIFICATIVO E DEVO REPORTAR AO CNCS. E AGORA?

TEMPESTIVIDADE



Em concreto:

- **Notificação Inicial** (24h) — descrição do incidente (causa/efeitos) e estimativa de impacto; indicação de eventual ato ilícito.
- **Notificação de fim de impacto** (24h após o fim do impacto) — atualização, avaliação de impacto e medidas de mitigação adotadas.
- **Relatório Final** (30 dias úteis) — descrição pormenorizada, medidas adotadas e situação residual de impacto.

NOTA: Quando necessário, deve ser enviada uma **atualização aos 72h** da notificação inicial (art. 42.º/3 RJC). Se o incidente persistir, o CNCS pode pedir **relatórios intercalares semanais** até ao relatório final (art. 44.º/3 RJC).

CONTACTOS CNCS

Via principal — Plataforma eletrónica MyCiber do CNCS: notificações submetidas na área reservada da entidade (registo e qualificação prévios obrigatórios).

Vias excecionais — apenas se a plataforma estiver indisponível ou a entidade sem capacidade operacional temporária:

- cert@cert.pt (cifrável via chave PGP do CERT.PT)
- (+351) 210 497 399
- Plataforma / Formulário: MYCIBER (https://myciber.gov.pt/)
- Permanente 24/7: (+351) 910 599 284

PRÉ-REQUISITOS PARA NOTIFICAR (expecto se notificação voluntária)

- Autoidentificação e qualificação da entidade junto do CNCS (art. 8.º RJC).
- Designação e comunicação do Responsável de Cibersegurança (art. 31.º RJC).
- Designação e comunicação do Ponto de Contacto Permanente (art. 32.º RJC).

COMUNICAÇÕES ADICIONAIS

- **Destinatários dos serviços:** informar, sem demora injustificada, sobre incidentes com impacto significativo suscetíveis de os afetar (art. 48.º RJC).
- **Divulgação pública:** o CNCS pode tornar público o incidente, quando do interesse público (art. 51.º RJC).
- **Impacto na UE:** o CNCS informa os Estados-Membros afetados e a ENISA (art. 50.º RJC).
- **Suspeita de crime:** reportar sem demora à PGR/DIAP Madeira (291 213 400), PJ/UNC3T (unc3t@pj.pt ou formulário de Queixa Eletrónica), e, quando aplicável, ao GNS-Gabinete Nacional de Segurança (informação classificada).

E se envolver dados pessoais?

Corre em paralelo à notificação ao CNCS, sempre que o incidente envolva dados pessoais ou afete diretamente terceiros.

Destinatário	Prazo	Quando se aplica
CNPD	**Até 72 h**	Se houver dados pessoais comprometidos (RGPD, art. 33.º) e resultar num risco para os direitos e liberdades das pessoas singulares
Titulares dos dados	**Sem demora injustificada**	Quando a violação for suscetível de implicar um risco elevado para os seus direitos (RGPD, art. 34.º).

CONSEQUÊNCIAS DO INCUMPRIMENTO

O incumprimento do dever de notificação é contraordenação **MUITO GRAVE** (art. 61.º RJC): coimas até **4 000 000 €** (entidade, Grupo A) ou **350 000 €** (Grupo B), e até **16 000 €** para a pessoa singular responsável.

A mera notificação não gera, por si só, responsabilidade acrescida — em caso de dúvida, a orientação é reportar.