MATRIZ DE SOLUÇÕES Q.SAFE IT

		Q.SAFE IT Seg. Periférica	Q.SAFE IT Seg. Endpoint	Q.SAFE IT Recuperação de Dados	Q.SAFE IT Formação em Cibersegurança	Q.SAFE IT Gestão de Direitos de Informação	Q.SAFE IT Monitorização
Capítulo IV, Artigo 20, Governance							
20.2	Os Estados-Membros asseguram que os membros dos órgãos de administração das entidades essenciais e importantes são obrigadas a seguir formação, devendo incentivar entidades essenciais e importantes a oferecerem formação semelhante à dos seus trabalhadores numa base regular, a fim de adquirirem conhecimentos suficientes e competências que lhes permitam identificar riscos e avaliar a gestão dos riscos de cibersegurança; práticas e seu impacto nos serviços prestados pela entidade.	-	-	-	●	-	-
Capítulo IV, Artigo 21, Cybersecurity risk-management measures							
21.2 21.2a)	Os Estados Membros devem assegurar que as entidades essenciais e importantes adotem medidas técnicas, operacionais e organizacionais adequadas e proporcionias para gerir os riscos que ameças a segurança dos sistemas de rede e de informação	●	●	●	-	-	●
21.2b)	Plano para tratamento de incidentes	●	●	-	-	●	●
21.2c)	Um plano para gerenciar operações de negócios durante e após um incidente de segurança. Isso significa que os backups devem estar atualizados. Deve igualmente existir um plano para garantir o acesso aos sistemas informáticos e às suas funções operacionais durante e após um incidente de segurança.	-	●	●	-	-	●
21.2d)	Segurança da cadeia de abastecimento, incluindo aspetos de segurança respeitantes às relações entre cada entidade e os respetivos fornecedores ou prestadores de serviços diretos.	●	●	-	-	●	●
21.2e)	Segurança na aquisição, desenvolvimento e manutenção dos sistemas de rede e informação, incluindo lidar e relatar vulnerabilidades;	-	●	-	-	-	●
21.2f)	Políticas e procedimentos para avaliar a eficácia das medidas de gestão dos riscos de cibersegurança;	-	●	-	-	●	●
21.2g)	Práticas básicas de ciber-higiene e formação em cibersegurança;	-	-	-	●	-	-
21.2h)	Políticas e procedimentos relativos à utilização de criptografia e, se for caso disso, de encriptação;	●	●	-	-	●	-
21.2i)	Procedimentos de segurança dos recursos humanos da empresa, garantir políticas de controlo do acesso (dados sensíveis ou importantes) e gestão de ativos. A empresa também deve ter uma visão geral de todos os ativos relevantes e garantir que eles sejam adequadamente utilizados e manuseados.	●	●	●	-	●	●

MATRIZ DE SOLUÇÕES Q.SAFE IT		Q.SAFE IT Seg. Periférica	Q.SAFE IT Seg. Endpoint	Q.SAFE IT Recuperação de Dados	Q.SAFE IT Formação em Cibersegurança	Q.SAFE IT Gestão de Direitos de Informação	Q.SAFE IT Monitorização
Capítulo IV, Artigo 23, Reporting Obligations							
23.4 d)	Os Estados-Membros devem assegurar que, para efeitos de notificação ao CSIRT ou, se aplicável, à autoridade competente: a) sem demora injustificada e, em qualquer caso, no prazo de 24 horas após tomar conhecimento do incidente significativo, um aviso antecipado, que, quando aplicável, deve indicar se o incidente é suspeito de ser causado por atos ilícitos ou maliciosos ou pode ter um impacto transfronteiriço; b) sem demora injustificada e, em qualquer caso, no prazo de 72 horas após tomar conhecimento do incidente significativo, uma notificação de incidente, que, quando aplicável, deve atualizar as informações referidas no ponto (a) e indicar uma avaliação inicial do incidente significativo, incluindo a sua gravidade e impacto, bem como, quando disponível, os indicadores de comprometimento; c) a pedido de um CSIRT ou, se aplicável, da autoridade competente, um relatório intermédio sobre as atualizações relevantes; d) um relatório final, o mais tardar um mês após a apresentação da notificação de incidente referida no ponto (b), incluindo o seguinte: (i) uma descrição detalhada do incidente, incluindo a sua gravidade e impacto; (ii) o tipo de ameaça ou causa raiz que provavelmente desencadeou o incidente;	•	•	•	-	-	•

POWERED BY: QUANTINFOR CONSULTORIA INFORMÁTICA