Obrigações de controlo de fornecedores externos

Segurança das informações e cibersegurança

para fornecedores classificados como de baixo risco cibernético e de informação

Versão 9.0, abril de 2019

Designação do controlo	Descrição do controlo	Por que é importante
1. Governação, política e normas em matéria de informação/cibersegurança	O fornecedor tem de ter implementados processos de governação de riscos de informação/cibernéticos que garantam uma compreensão do respetivo ambiente tecnológico e do estado dos controlos de segurança das informações e cibersegurança, bem como um programa de proteção para proteger o fornecedor contra ameaças cibernéticas em conformidade com a boa prática do setor (nomeadamente, NIST, SANS, ISO27001) e os requisitos do setor aplicáveis. O fornecedor deve efetuar avaliações de risco regulares relativamente à segurança das informações/cibersegurança e deve implementar estes controlos e tomar estas medidas, conforme necessário, para mitigar os riscos identificados. O fornecedor tem de respeitar as políticas e normas aprovadas pela direção sénior para gestão do risco de informação/cibernético do fornecedor. O fornecedor tem de definir funções e responsabilidades pela segurança das informações/cibersegurança.	Se este controlo não for implementado, o Barclays ou os respetivos fornecedores podem não possuir nem conseguir demonstrar uma supervisão apropriada relativamente à segurança das informações/cibersegurança. As políticas e normas documentadas são elementos cruciais da governação e gestão de risco. Definem a visão da direção relativamente aos controlos necessários para gerir o risco de informação/cibernético.
2. Processo de gestão de incidentes	Tem de ser estabelecido e gerido um processo de resposta a incidentes para tratar e reportar regularmente de forma atempada os incidentes que envolvam informações do Barclays e/ou serviços utilizados pelo Barclays. No âmbito do procedimento de resposta a incidentes, têm de ser definidos os seguintes pontos: • Incidentes de segurança e violações de dados que tenham afetado ou tido como alvo ativos do Barclays e/ou serviços a serem prestados ao Barclays têm de ser relatados ao Barclays assim que possível e têm de ser fornecidas atualizações sobre os progressos das ações corretivas. • O fornecedor tem de garantir que as ações corretivas identificadas após um incidente são corrigidas com um plano de correção (ação, responsabilidade, data de conclusão) e comunicadas ao Barclays.	Um processo de gestão e resposta a incidentes ajuda a garantir que os incidentes são rapidamente contidos e impedidos de assumir maiores proporções.
3. Segurança de ponto final	O fornecedor tem de garantir que os pontos finais utilizados para aceder à rede do Barclays, ou para processar dados do Barclays, são reforçados para proteção contra ataques.	Se este controlo não for implementado, a rede e os pontos finais do Barclays e do

	Tal inclui, entre outras coisas, limitação da área de ataque através da desativação de software/serviços/portas desnecessárias, garantindo que todas as versões aplicadas estão dentro dos períodos de suporte público, existem capacidades de proteção contra malware e de firewall do anfitrião e estão devidamente configuradas, tendo sido implementados controlos para mitigação de tentativas de exploração de vulnerabilidades.	fornecedor podem ficar vulneráveis a ciberataques.
4. Computação em nuvem	Toda a utilização de serviços de computação em nuvem (públicos/privados/comunitários/híbridos), nomeadamente SaaS/PaaS/IaaS, utilizados no âmbito da prestação de serviços ao Barclays, tem de estar adequadamente protegida. Os controlos para proteger a informação e o serviço do Barclays têm de ser proporcionais ao perfil de risco e à sensibilidade do ativo informacional para impedir fugas de dados e violações de cibersegurança.	Se este princípio não for implementado, os ativos informacionais do Barclays incorretamente protegidos podem ficar comprometidos, o que pode resultar em sanções legais e regulamentares ou em prejuízos para a reputação.
5. Proteção contra malware	Devem ser implementados controlos e ferramentas antimalware para conferir proteção adequada contra software malicioso, como vírus e outras formas de malware.	As soluções antimalware são essenciais para a proteção de ativos informacionais do Barclays contra códigos maliciosos.
6. Segurança de rede	O fornecedor tem de garantir que todos os sistemas de TI explorados por si ou pelo seu subcontratante que suporte serviços disponibilizados ao Barclays estão protegidos contra movimentações laterais de ameaças na rede do fornecedor (e de subcontratantes relevantes). O fornecedor deve considerar os seguintes mecanismos de proteção em função do serviço(s) prestado(s) ao Barclays: **Ligações externas:** Todas as ligações externas à rede devem ser documentadas, encaminhadas por uma firewall e verificadas e aprovadas antes de as ligações serem estabelecidas para prevenir violações na segurança de dados. **Acesso sem fios:** Todos os acessos sem fios à rede devem estar sujeitos a protocolos de autorização, autenticação, segregação e encriptação para impedir violações de segurança. **Deteção/prevenção de intrusões:** Devem ser adotadas ferramentas de deteção e prevenção de intrusões em todos os locais adequados na rede e os resultados devem ser monitorizados em conformidade, com o	Se este princípio não for implementado, as redes externas ou internas podem ser sabotadas por invasores a fim de obterem acesso aos serviços e dados que estas contêm.

	intuito de detetar violações de cibersegurança, incluindo Ameaças Avançadas Persistentes (AAP). **Recusa de serviço distribuído (DoSD):** Deve ser implementada uma abordagem de defesa aprofundada na rede e nos principais sistemas para uma proteção contínua contra interrupções de serviços devido a ataques cibernéticos. *Nota: O termo "rede", na aceção deste controlo, refere-se a qualquer rede não pertencente ao Barclays por que o fornecedor seja responsável, incluindo a rede do subcontratante do fornecedor.*	
7. Proteção de aplicação	O desenvolvimento de software/aplicações do fornecedor garante que todas as principais atividades de segurança foram incorporadas no processo de desenvolvimento do software para impedir interrupções de serviços, vulnerabilidades de segurança e violações de cibersegurança. O fornecedor deve garantir que se encontra implementada a separação de funções para o desenvolvimento de sistemas, incluindo garantir que os programadores de sistemas não têm acesso ao ambiente dinâmico, exceto em casos de emergência em que este acesso estivesse protegido com controlos adequados como procedimentos de acesso rápido. Estas atividades, nestas circunstâncias, devem ser registadas e sujeitas a revisão independente. O fornecedor tem de garantir que o código fonte é executado, armazenado e enviado em segurança para o Barclays.	Os controlos que protegem o desenvolvimento da aplicação ajudam a garantir que as aplicações estão protegidas no momento da implementação.
8. Simulação de ameaça/teste de penetração/avaliação de segurança de TI	O fornecedor tem de colaborar com um prestador de serviços de segurança qualificado e independente para realizar uma avaliação de segurança de TI/um teste de penetração que abranja a infraestrutura de TI e aplicações referentes ao(s) serviço(s) disponibilizados ao Barclays pelo fornecedor. Esta avaliação tem de ser realizada pelo menos anualmente para identificar vulnerabilidades que possam ser exploradas para violar a confidencialidade dos dados do Barclays através de ciberataques. O fornecedor tem de gerir um mecanismo consistente para registar, triar e dar resposta às vulnerabilidades identificadas.	Se este controlo não for implementado, os fornecedores podem não conseguir avaliar as ameaças cibernéticas com que se deparam, nem a adequação e a eficácia das respetivas defesas.

9. Ativos e tecnologias de proteção de segurança	Têm de ser aplicadas tecnologias apropriadas para fazer face a ameaças cibernéticas atuais e emergentes mediante a manutenção de base de controlos consistente para impedir ataques, execução, exploração e exfiltração. Os sistemas anfitriões e os dispositivos de rede que fizerem parte dos sistemas do fornecedor têm de ser configurados para funcionarem em conformidade com a boa prática do setor (p. ex., NIST, SANS, ISO27001). Os ativos ou sistemas para o seu armazenamento ou processamento devem estar protegidos contra adulteração física, perdas, danos ou apreensões, bem como contra configurações ou alterações inadequadas. A destruição ou eliminação de ativos informacionais do Barclays armazenados em formato físico ou eletrónico tem de ser realizada de uma forma segura, adequada ao risco associado, que garanta que não é recuperável. Os sistemas têm de ser configurados de forma segura, de modo a prevenir violações desnecessárias. Deve estar implementada a monitorização, auditoria e registo de sistemas para detetar atividade maliciosa ou inadequada.	Se este controlo não for implementado, os ativos do Barclays ou os ativos utilizados pelos fornecedores para prestar serviços ao Barclays podem ficar comprometidos, o que pode resultar em perdas financeiras, perda de dados, prejuízos para a reputação e censura regulamentar.
10. Gestão de Acesso Lógico (Logic Access Management, ou LAM)	O acesso às informações tem de ser restrito e de ter em devida consideração os princípios da necessidade de tomar conhecimento, do privilégio mínimo e da separação de funções. Cabe ao responsável pelo ativo informacional decidir quem necessita de que tipo de acesso. • O princípio da necessidade de tomar conhecimento estabelece que as pessoas só devem ter acesso às informações de que necessitem para desempenhar as funções autorizadas. Por exemplo, se um colaborador lida exclusivamente com clientes estabelecidos no Reino Unido, não "necessita de tomar conhecimento" de informações referentes a clientes estabelecidos nos EUA. • O princípio do privilégio mínimo estabelece que as pessoas devem ter apenas o nível mínimo de privilégio necessário para desempenhar as funções autorizadas. Por exemplo, se um colaborador necessita de consultar o endereço do cliente, mas não de o modificar, o "mínimo privilégio" exigido é o acesso para leitura, que lhe deverá ser atribuído ao invés do acesso para leitura/escrita. • O princípio da separação de funções estabelece que pelo menos dois indivíduos são responsáveis por partes distintas de qualquer tarefa, a fim de evitar erros e fraudes. Por exemplo, o colaborador que solicita a criação de uma conta não deve ser o mesmo que aprova o pedido.	Controlos LAM apropriados ajudam a garantir que os ativos informacionais são protegidos contra utilização indevida.

	Estes princípios devem ser aplicados em função do risco, tendo em conta o nível de confidencialidade da informação. Cada conta tem de ser associada a um indivíduo, que deve ser responsável por qualquer atividade realizada com acesso à mesma. Tal não exclui a utilização de contas partilhadas. Porém, continua a ser necessário que um indivíduo seja responsável por cada conta partilhada. Devem ser definidos processos de gestão de acesso, de acordo com a boa prática do setor, que incluam, no mínimo, o seguinte: • um processo de autorização sólido, implementado antes da criação/alteração/eliminação de contas; • um processo de revisão do acesso do utilizador regular; • controlo dos colaboradores transferidos – Acesso alterado/eliminado no prazo de 5 dias úteis a contar da data de transferência; • controlo dos colaboradores que cessam funções – Todo o acesso lógico utilizado para prestar serviços ao Barclays eliminado no prazo de 24 horas a contar da data de cessação de funções e todos os outros acessos secundários eliminados no prazo de 7 dias; e • contas inativas não utilizadas por um período igual ou superior a 60 dias consecutivos têm de ser suspensas. • As palavras-passe para contas interativas têm de ser alteradas pelo menos a cada 90 dias e têm de ser diferentes das doze (12) palavras-passe anteriores. • As contas privilegiadas têm de ser alteradas após cada utilização e, no mínimo, a cada 90 dias. • As contas interativas têm de ser desativadas após um máximo de cinco (5) tentativas de acesso consecutivas falhadas. Nos casos em que é permitido o acesso remoto a ativos informacionais do Barclays armazenados num ambiente gerido pelo fornecedor, têm de existir dois fatores de autenticação e autorização do ponto final, levando em consideração a identidade do utilizador, o tipo de dispositivo e a postura de segurança do dispositivo (p. ex., nível de patch, situação do antimalware, dispositivo móvel com acesso ou não ao sistema operativo, etc.).	
11. Prevenção de fuga de dados	O risco de fuga de dados de informações relacionadas com o(s) serviço(s) prestado(s) pelo fornecedor à saída do Barclays através da rede ou de um meio físico tem de ser avaliado e mitigado. Devem ser considerados os seguintes canais de fuga de dados:	Controlos apropriados de prevenção de fuga de dados são um elemento fundamental da proteção de dados, ajudando a garantir que as informações do Barclays não se perdem.

	• Transferência não autorizada de informações para fora da rede interna/da rede do fornecedor; • Perda ou roubo de ativos informacionais do Barclays em meios eletrónicos portáteis (incluindo informações eletrónicas contidas em computadores portáteis, dispositivos móveis e meios portáteis); • Troca insegura de informações com terceiros; e • Impressão ou reprodução inadequada de informações.	
12. Esquema de classificação de informações	***Sempre que adequado****, o fornecedor tem de aplicar o esquema de classificação de informações e os requisitos de tratamento do Barclays (Anexo B, Tabelas B1 e B2), ou um esquema alternativo acordado com o Barclays, a todos os ativos informacionais retidos ou processados em nome do Barclays. * "***sempre que adequado***" *refere-se ao benefício de classificar comparado com o custo associado. Por exemplo, não seria adequado classificar um documento se, ao fazê-lo, ocorresse a violação dos requisitos regulamentares antiadulteração.*	É essencial um inventário de ativos informacionais completo e rigoroso para garantir controlos adequados.
13. Direito de inspeção	O fornecedor deve permitir ao Barclays, mediante notificação por escrito do Barclays pelo menos dez dias úteis antes, realizar uma análise de segurança a qualquer local ou tecnologia utilizada pelo fornecedor ou respetivos subcontratantes para desenvolver, testar, melhorar, manter ou operar os sistemas do fornecedor utilizados nos serviços para assim rever a conformidade do fornecedor com as respetivas obrigações. O fornecedor deve também permitir que o Barclays realize imediatamente uma inspeção após um incidente de segurança. Qualquer não conformidade dos controlos identificada pelo Barclays durante uma inspeção deve ser avaliada pelo Barclays e o Barclays deve especificar um plano calendarizado de resolução. O fornecedor deve então implementar qualquer resolução necessária dentro desse plano calendarizado. O fornecedor deve disponibilizar todo o apoio razoavelmente solicitado pelo Barclays relativamente a qualquer inspeção.	Se tal não for acordado, os fornecedores não conseguirão garantir totalmente a conformidade com estas obrigações de segurança.

Anexo A: Glossário

Definição	
Ameaças Avançadas Persistentes (AAP)	Uma ameaça avançada persistente (AAP) é um ataque silencioso a uma rede informática, em que uma pessoa ou grupo obtém acesso não autorizado a uma rede e fica por detetar por um período prolongado.
Ativo informacional	Qualquer informação que tenha valor, à luz dos respetivos requisitos de confidencialidade, integridade e disponibilidade. Qualquer elemento de informação ou grupo de informações que tem valor para a organização. Geralmente congregados a um alto nível (do processo empresarial).
Autenticação multifator	Autenticação que utiliza duas ou mais técnicas de autenticação distintas. Um exemplo é a utilização de um token de segurança, em que o sucesso da autenticação depende de algo que o utilizador possui (ou seja, o token de segurança) e de algo de que é conhecedor (ou seja, o código PIN do token de segurança).
Código malicioso	Software escrito com o intuito de contornar a política de segurança de um sistema, dispositivo ou aplicação de TI. São exemplos de código malicioso os vírus, cavalos de troia e worms de computador.
Conta	Um conjunto de credenciais (por exemplo, uma ID de utilizador e palavra-passe) através do qual é gerido o acesso a um sistema de TI utilizando controlos de acesso lógico.
Conta partilhada	Uma conta atribuída a mais do que um colaborador, consultor, contratante ou colaborador de agência que tenha acesso autorizado, numa situação em que contas individuais não são uma opção adequada devido à natureza do sistema avaliado.
Conta privilegiada	Uma conta que proporciona um elevado nível de controlo de um sistema de TI específico. Estas contas são geralmente utilizadas para efeitos de manutenção do sistema, administração de segurança ou realização de modificações de configuração num sistema de TI. Os exemplos incluem "Administrador", "raiz", contas Unix com uid=0, contas de suporte, contas de administração de segurança, contas de administração do sistema e contas de administradores locais.
Destruição/eliminação	O ato de sobregravar, apagar ou destruir fisicamente informações de tal forma que não é possível recuperá-las.
Privilégio mínimo	O nível mínimo de acesso/permissões que permite que um utilizador ou conta desempenhe as respetivas funções.
Recusa de serviço (Ataque)	Uma tentativa de tornar um recurso informático indisponível para os utilizadores a que se destina.
Sistema	No contexto do presente documento, um sistema consiste em pessoas, procedimentos, equipamento de TI e software. Os elementos desta entidade composta são utilizados em conjunto no ambiente operacional ou de suporte pretendido para realizar determinada tarefa ou atingir um objetivo específico, suporte, ou requisito de missão.
Utilizador	Uma conta designada para um colaborador de um fornecedor, consultor, contratante ou colaborador de agência que tenha acesso autorizado a um sistema sem privilégios elevados.

Anexo B: Esquema de classificação de informações do Barclays

Tabela B1: Esquema de classificação de informações do Barclays

Etiqueta	Definição	Exemplos
Secreto	As informações têm de ser classificadas como secretas se a sua divulgação não autorizada puder ter um impacto negativo no Barclays, avaliado, segundo o quadro de gestão de risco da empresa (ERMF), como "crítico" (financeiro ou não financeiro). O acesso a estas informações está limitado a um público específico e a sua distribuição não pode exceder este círculo sem a autorização do seu autor. O público pode incluir destinatários externos mediante a autorização expressa do responsável pela informação.	• Informação sobre potenciais fusões ou aquisições. • Informação de planeamento estratégico – empresarial e organizacional. • Certas informações de configuração de segurança. • Certos resultados e relatórios de auditoria. • Atas do Comité Executivo. • Dados de autenticação ou de identificação e verificação (ID&V) – clientes/consumidores e colegas. • Grandes volumes de informações de titulares de cartões. • Previsões de lucros ou resultados financeiros anuais (antes da divulgação pública). • Quaisquer elementos abrangidos por um acordo formal de não divulgação (NDA).
Restrito – Interno	As informações têm de ser classificadas como restritas-internas se os destinatários previstos forem apenas colaboradores autenticados do Barclays e prestadores de serviços geridos (MSP) do Barclays com contrato vigente e se estiverem limitadas a um público específico. A divulgação não autorizada teria um impacto negativo no Barclays, avaliado segundo o ERMF, como "importante" ou "limitado" (financeiro ou não financeiro). As informações não se destinam a distribuição geral, mas podem ser encaminhadas ou partilhadas pelos destinatários de acordo com o princípio da necessidade de tomar conhecimento.	• Estratégias e orçamentos. • Avaliações de desempenho. • Remuneração dos colaboradores e dados pessoais. • Avaliações de vulnerabilidade. • Resultados e relatórios de auditorias.
Restrito – Externo	As informações têm de ser classificadas como restritas-externas se os destinatários previstos forem colaboradores autenticados do Barclays e MSP do Barclays com contrato vigente e se estiverem limitadas a um	• Planos de novos produtos. • Contratos com clientes. • Contratos legais.

	público específico ou terceiros autorizados pelo responsável pela informação. A divulgação não autorizada teria um impacto negativo no Barclays, avaliado segundo o ERMF, como "importante" ou "limitado" (financeiro ou não financeiro). As informações não se destinam a distribuição geral, mas podem ser encaminhadas ou partilhadas pelos destinatários de acordo com o princípio da necessidade de tomar conhecimento.	• Pequenas quantidades de informação/informações individuais de clientes/consumidores destinadas a serem enviadas externamente. • Comunicações de clientes/consumidores. • Nova emissão de materiais de oferta (p. ex. brochuras, prospetos de oferta). • Documentos finais de investigação. • Informações não públicas relevantes (MNPI) externas ao Barclays. • Todos os relatórios de investigação. • Alguns materiais de marketing. • Comentários de mercado.
Não restrito	Informações destinadas a distribuição geral ou cuja distribuição não teria impacto na organização.	• Materiais de marketing. • Publicações. • Anúncios públicos. • Anúncios de emprego. • Informações sem impacto no Barclays.

Tabela B2: Esquema de classificação de informações do Barclays – requisitos de tratamento

*** Informações de configuração de segurança do sistema, resultados de auditoria e registos pessoais podem ser classificados como restritos-internos ou secretos, dependendo do impacto da divulgação não autorizada no negócio.

Etapa do ciclo de vida	Restrito – Interno	Restrito – Externo	Secreto
Criação e introdução	• Os ativos têm de ser atribuídos a um responsável pela informação.	• Os ativos têm de ser atribuídos a um responsável pela informação.	• Os ativos têm de ser atribuídos a um responsável pela informação.
Armazenamento	• Os ativos (físicos ou eletrónicos) não podem ser armazenados em áreas públicas (incluindo áreas públicas nas instalações dos fornecedores, onde os visitantes podem ter um acesso sem supervisão).	• Os ativos (físicos ou eletrónicos) não podem ser guardados onde indivíduos não autorizados os podem ver ou obter acesso aos mesmos.	• Os ativos (físicos ou eletrónicos) não podem ser guardados onde indivíduos não autorizados os podem ver ou obter acesso aos mesmos.

	• As informações não podem ser deixadas em áreas públicas nas instalações onde os visitantes podem ter acesso sem supervisão.	• Os ativos guardados em formato eletrónico têm de ser protegidos através de encriptação ou controlos de compensação adequados caso exista um risco significativo de que pessoas não autorizadas consigam obter acesso aos mesmos.	• Os ativos guardados em formato eletrónico têm de ser protegidos através de encriptação ou controlos de compensação adequados caso exista um risco significativo de que pessoas não autorizadas consigam obter acesso aos mesmos. • Todas as chaves privadas que sejam utilizadas para proteger dados do Barclays, a respetiva identidade e/ou reputação têm de ser protegidas por módulos de proteção de hardware (HSM) certificados FIPS 140-2 Nível 3 ou superior.
Acesso e utilização	• Os ativos (físicos ou eletrónicos) não podem ser deixados em áreas públicas fora das instalações. • Os ativos (físicos ou eletrónicos) não podem ser deixados em áreas públicas nas instalações onde os visitantes possam ter acesso sem supervisão. • Se necessário, os ativos eletrónicos têm de ser protegidos por controlos de gestão de acesso lógico adequados.	• Os ativos (físicos ou eletrónicos) não podem ser utilizados nem deixados sem vigilância onde indivíduos não autorizados os podem ver ou obter acesso aos mesmos. Os ativos podem ser utilizados se existirem controlos adequados (p. ex., telas de privacidade). • Os ativos impressos têm de ser retirados imediatamente da impressora. Se tal não for possível, tem de utilizar-se ferramentas de impressão segura. • Os ativos eletrónicos têm de ser protegidos por controlos de gestão de acesso lógico adequados.	• Os ativos (físicos ou eletrónicos) não podem ser utilizados nem deixados sem vigilância onde indivíduos não autorizados os podem ver ou obter acesso aos mesmos. Os ativos podem ser utilizados se existirem controlos adequados (p. ex., telas de privacidade). • Os ativos impressos têm de ser impressos com recurso a ferramentas de impressão segura. • Os ativos eletrónicos têm de ser protegidos por controlos de gestão de acesso lógico adequados.
Partilha	• Os ativos em papel têm de integrar uma etiqueta de informação visível. A etiqueta tem de encontrar-se pelo menos na página do título. • Os ativos eletrónicos têm de integrar uma etiqueta de informação bem visível. • Os ativos só podem ser distribuídos utilizando sistemas, métodos ou fornecedores aprovados pela organização.	• Os ativos em papel têm de ter uma etiqueta de informação visível. A etiqueta tem de encontrar-se pelo menos na página do título. • Os envelopes que contenham ativos em papel têm de incluir uma etiqueta de informação visível na parte da frente. • Os ativos eletrónicos têm de integrar uma etiqueta de informação bem visível. As cópias eletrónicas de documentos com várias páginas têm de integrar uma etiqueta de informação visível em todas as páginas.	• Os ativos em papel têm de incluir uma etiqueta de informação visível em todas as páginas. • Os envelopes que contêm ativos em papel têm de incluir uma etiqueta de informação na parte da frente e de ser selados através de um sistema que não permita a violação. Antes da distribuição, têm de ser colocados no interior de um segundo envelope sem etiquetas.

	• Os ativos só podem ser distribuídos a pessoas empregadas pela empresa, ou ao abrigo de uma obrigação contratual adequada para com a empresa, ou no âmbito de uma necessidade comercial inequivocamente reconhecida, por exemplo, negociação contratual.	• Os ativos só podem ser distribuídos utilizando sistemas, métodos ou fornecedores aprovados pela organização. • Os ativos só podem ser distribuídos a pessoas empregadas pela empresa, ou ao abrigo de uma obrigação contratual adequada para com a empresa, ou no âmbito de uma necessidade comercial inequivocamente reconhecida, por exemplo, negociação contratual. • Os ativos só podem ser distribuídos a pessoas com uma necessidade comercial de os receberem. • Um ativo não pode ser enviado por fax a menos que o remetente tenha confirmado que os destinatários estão preparados para o receber. • Os ativos eletrónicos têm de ser encriptados com recurso a um mecanismo de proteção criptográfico aprovado, sempre que estiverem a ser distribuídos fora da rede interna.	• Os ativos eletrónicos têm de integrar uma etiqueta de informação bem visível. As cópias eletrónicas de documentos com várias páginas têm de integrar uma etiqueta de informação visível em todas as páginas. • Os ativos só podem ser distribuídos utilizando sistemas, métodos ou fornecedores aprovados pela organização. • Os ativos só podem ser distribuídos a pessoas empregadas pela empresa, ou ao abrigo de uma obrigação contratual adequada para com a empresa, ou no âmbito de uma necessidade comercial inequivocamente reconhecida, por exemplo, negociação contratual. • Os ativos só podem ser distribuídos a pessoas especificamente autorizadas a recebê-los pelo responsável pela informação. • Os ativos não podem ser enviados por fax. • Os ativos eletrónicos têm de ser encriptados com recurso a um mecanismo de proteção criptográfico aprovado, sempre que estiverem a ser distribuídos fora da rede interna. • Tem de ser mantida uma cadeia de custódia para ativos eletrónicos.
Arquivo e eliminação	• Os ativos em papel têm de ser eliminados com recurso a um serviço de eliminação confidencial. • As cópias de ativos eletrónicos também têm de ser eliminadas dos "cestos de reciclagem" do sistema ou dispositivos semelhantes em tempo útil.	• Os ativos em papel têm de ser eliminados com recurso a um serviço de eliminação confidencial. • As cópias de ativos eletrónicos também têm de ser eliminadas dos "cestos de reciclagem" do sistema ou dispositivos semelhantes em tempo útil.	• Os ativos em papel têm de ser eliminados com recurso a um serviço de eliminação confidencial. • As cópias de ativos eletrónicos também têm de ser eliminadas dos "cestos de reciclagem" do sistema ou dispositivos semelhantes em tempo útil. • Os suportes onde ativos eletrónicos secretos tiverem sido guardados têm de ser devidamente limpos antes ou durante a eliminação.

Segredo bancário

Controlos adicionais apenas para as jurisdições com segredo bancário (Suíça/Mónaco)

Área de controlo/Título	Descrição do controlo	Por que é importante
1. Funções e responsabilidades	O fornecedor tem de definir e comunicar funções e responsabilidades pelo tratamento de dados de identificação do cliente (a seguir designados por "DIC"). O fornecedor tem de rever os documentos que destacam as funções e responsabilidades referentes aos DIC após qualquer modificação substancial no modelo de operação (ou negócio) do fornecedor ou, pelo menos, anualmente e de os distribuir com a jurisdição com segredo bancário adequada. As principais funções têm de incluir um executivo sénior, responsável pela proteção e supervisão de todas as atividades relacionadas com DIC (para consultar a definição de DIC, ver Anexo A).	Uma clara definição das funções e responsabilidades auxilia a implementação do plano de obrigações de controlo de fornecedor externo.
2. Relato de violação de DIC	Têm de existir controlos e processos documentados por forma a garantir que quaisquer violações com impacto nos DIC são relatadas e geridas. Qualquer violação dos requisitos de tratamento (conforme definidos na tabela C2) tem de receber resposta por parte do fornecedor e de ser comunicada imediatamente à jurisdição com segredo bancário correspondente (no prazo máximo de 24 horas). Tem de ser estabelecido um processo de resposta a incidentes para tratar e reportar de forma regular e atempada eventos que envolvam DIC. O fornecedor tem de garantir que as ações corretivas identificadas após um incidente são corrigidas com um plano de correção (ação, responsabilidade, data de conclusão) e partilhadas e acordadas com a jurisdição com segredo bancário correspondente.	Um processo de resposta a incidentes ajuda a garantir que os incidentes são rapidamente contidos e impedidos de assumir maiores proporções. As violações que afetem os DIC podem resultar num forte prejuízo para a reputação do Barclays e conduzir à aplicação de penalidades e à perda da licença bancária na Suíça ou no Mónaco.

3. Formação e sensibilização	Os colaboradores do fornecedor que tenham acesso a DIC e/ou que os tratem têm de realizar uma formação* que introduza os requisitos de segredo bancário de DIC após qualquer alteração à regulamentação ou pelo menos anualmente. O fornecedor tem de garantir que todos os novos colaboradores do fornecedor (que tenham acesso a DIC e/ou que os tratem) realizam, num período de tempo razoável (cerca de 3 meses), formação que garanta que compreendem as respetivas responsabilidades em matéria de DIC. O fornecedor tem de manter um registo dos colaboradores que realizaram a formação. * as jurisdições com segredo bancário deverão fornecer orientações sobre o conteúdo esperado da formação.	A formação e a sensibilização auxiliam todos os outros controlos no âmbito deste plano.
4. Esquema de classificação de informações	***Sempre que adequado****, o fornecedor tem de aplicar o esquema de classificação de informações do Barclays (Anexo C, Tabela C1), ou um esquema alternativo acordado com a jurisdição com segredo bancário, a todos os ativos informacionais retidos ou processados em nome da jurisdição com segredo bancário. Os requisitos de tratamento dos DIC estão previstos na Tabela C2 do Anexo C. * "***sempre que adequado***" *refere-se ao benefício de classificar comparado com o custo associado. Por exemplo, não seria adequado classificar um documento se, ao fazê-lo, ocorresse a violação dos requisitos regulamentares antiadulteração.*	É essencial um inventário de ativos informacionais completo e rigoroso para garantir controlos adequados.
5. Computação em nuvem/armazenamento externo	Todo o recurso à computação em nuvem e/ou ao armazenamento externo de DIC (em servidores que se encontrem fora da jurisdição com segredo bancário ou das infraestruturas do fornecedor) no âmbito dos serviços prestados a essa jurisdição tem de ser aprovado pelas correspondentes equipas locais pertinentes (incluindo o diretor de segurança, o departamento jurídico e de conformidade); e os controlos têm de ser aplicados de acordo com a jurisdição com segredo bancário em causa para assegurar a proteção contra a inadequação da informação dos DIC, tendo em conta o perfil de elevado risco que apresentam.	Se este princípio não for implementado, os dados de identificação do cliente (DIC) incorretamente protegidos podem ficar comprometidos, o que pode resultar em sanções legais e regulamentares ou em prejuízos para a reputação.

** Dados de identificação do cliente são dados especiais devido à legislação em matéria de segredo bancário vigente na Suíça e no Mónaco. Como tal, os controlos aqui enumerados complementam os controlos enumerados anteriormente.

Termo	Definição
DIC	Dados de identificação do cliente.
SIC	Segurança das informações e cibersegurança.
Colaborador do fornecedor	Qualquer pessoa diretamente afetada ao fornecedor como agente do quadro ou qualquer pessoa que preste serviços ao fornecedor por um período de tempo limitado (designadamente, como consultor).
Ativo	Qualquer elemento de informação ou grupo de informações que tem valor para a organização.
Sistema	No contexto do presente documento, um sistema consiste em pessoas, procedimentos, equipamento de TI e software. Os elementos desta entidade composta são utilizados em conjunto no ambiente operacional ou de suporte pretendido para realizar determinada tarefa ou atingir um objetivo específico, suporte, ou requisito de missão.
Utilizador	Uma conta designada para um colaborador de um fornecedor, consultor, contratante ou colaborador de agência que tenha acesso autorizado a um sistema detido pelo Barclays sem privilégios elevados.

Anexo B: DEFINIÇÃO DE DADOS DE IDENTIFICAÇÃO DO CLIENTE

Os **DIC diretos (DICD)** podem ser definidos como identificadores únicos (detidos pelo cliente) que permitem, pela sua natureza e por si só, identificar um cliente sem acesso a dados das aplicações bancárias do Barclays. Têm de ser inequívocos, não podem estar sujeitos a interpretações e podem incluir informações como o nome próprio, o apelido, o nome da empresa, a assinatura, a ID da rede social, etc. Os DIC diretos referem-se a dados do cliente não detidos ou criados pelo banco.

Os **DIC indiretos (DICI)** dividem-se em 3 níveis

- Os **DICI L1** podem ser definidos como identificadores únicos (detidos pelo banco) que permitem identificar inequivocamente um cliente caso seja concedido acesso a aplicações bancárias ou outras **aplicações de terceiros**. O identificador tem de ser inequívoco, não pode estar sujeito a interpretações e pode incluir identificadores como o número de conta, o código IBAN, o número de cartão de crédito, etc.

- Os **DICI L2** podem ser definidos como informação (detida pelo cliente) que, em combinação com outra, permite inferir a identidade de um cliente. Embora esta informação não possa, por si só, ser utilizada para identificar um cliente, pode ser utilizada juntamente com outra informação para esse efeito. Os DICI L2 têm de ser protegidos e geridos com o mesmo rigor que os DICD.

- Os **DICI L3** podem ser definidos como identificadores únicos mas anonimizados (detidos pelo banco) que permitem identificar um cliente se for concedido acesso a aplicações bancárias. Distinguem-se dos DICI L1 pelo facto de a sua informação estar classificada como "restrita-externa" e não como "segredo bancário", o que significa que não estão sujeitos aos mesmos controlos.

Consulte a figura 1, a árvore de decisão de DIC, para uma visão geral do método de classificação.

Os DIC diretos e indiretos L1 não podem ser partilhados com nenhuma pessoa que se encontre fora do banco e estão sempre sujeitos ao princípio da necessidade de tomar conhecimento. Os DICI L2 podem ser partilhados em função da necessidade de tomar conhecimento, mas não podem ser partilhados juntamente com qualquer outro elemento de DIC. Com a partilha de múltiplos elementos de DIC, há a possibilidade de criar uma "combinação tóxica" potencialmente capaz de revelar a identidade de um cliente. Por combinação tóxica, entende-se uma combinação que associe, pelo menos, dois DICI L2. Os DICI L3 podem ser partilhados, uma vez que não estão classificados como informação de nível segredo bancário, exceto se o uso recorrente do mesmo identificador puder resultar na recolha de dados DICI L2 suficientes para revelar a identidade do cliente.

Classificação da informação	Segredo bancário			Restrita – Interna
Classificação	**DIC diretos (DICD)**	**DIC indiretos (DICI)**		
		Indiretos (L1)	**Potencialmente Indiretos (L2)**	**Identificadores impessoais (L3)**
Tipo de informação	Nome do cliente	Número da partição/ID da partição	Nome próprio	ID de processamento interno
	Nome da empresa	Número de MACC (conta monetária num ID de partição Avaloq)	Data de nascimento	Identificador estático único
	Extrato de conta	Morada	Nacionalidade	Identificador dinâmico
	Assinatura	IBAN	Título	ID externo da partição

	ID da rede social	Dados de início de sessão de banco eletrónico	Situação familiar	
	Número de passaporte	Número de cofre-forte	Código postal	
	Número de telefone	Número de cartão de crédito	Situação patrimonial	
	Endereço de e-mail		Apelido	
	Cargo ou título PEP		Última visita de cliente	
	Nome artístico		Língua	
	Endereço IP		Género	
	Número de fax		Validade do CC	
			Pessoa a contactar	
			Naturalidade	
			Data de abertura de conta	
			Posição longa/valor de transação	

Exemplo: Se enviar um e-mail ou partilhar documentos com pessoas externas (incluindo terceiros na Suíça/no Mónaco) ou colegas internos de outra filial/subsidiária estabelecida na Suíça/no Mónaco ou noutros países (p. ex. UK)

1. Nome do cliente

   (DICD) = Violação do segredo bancário

2. ID da partição

   (DICI L1) = Violação do segredo bancário

3. Situação patrimonial + Nacionalidade

   (DICI L2) + (DICI L2) = Violação do segredo bancário

Anexo C: Esquema de classificação de informações do Barclays

Tabela C1: Esquema de classificação de informações do Barclays

** A classificação de segredo bancário é específica a jurisdições com segredo bancário.

Etiqueta	Definição	Exemplos
Segredo bancário	Informação relacionada com quaisquer dados suíços de identificação do cliente, diretos ou indiretos (DIC). A classificação de "segredo bancário" aplica-se a informação relacionada com quaisquer dados de identificação do cliente, diretos ou indiretos. Por conseguinte, o acesso por todos os colaboradores, mesmo quando localizados na jurisdição responsável, não é adequado. Só as pessoas que necessitam de tomar conhecimento para cumprirem as respetivas funções oficiais ou responsabilidades contratuais precisam de aceder a estas informações. A divulgação, o acesso ou a partilha interna e externa não autorizados da entidade titular dessa informação pode ter um impacto grave, resultar em processos penais e ter consequências civis e administrativas, nomeadamente penalidades e a perda da licença bancária, se tiver sido divulgada a pessoal não autorizado interna e externamente.	• Nome do cliente • Morada do cliente • Assinatura • Endereço IP do cliente (mais exemplos no Anexo B)

Etiqueta	Definição	Exemplos
Secreto	As informações têm de ser classificadas como secretas se a sua divulgação não autorizada puder ter um impacto negativo no Barclays, avaliado, segundo o quadro de gestão de risco da empresa (ERMF), como "crítico" (financeiro ou não financeiro). O acesso a estas informações está limitado a um público específico e a sua distribuição não pode exceder este círculo sem a autorização do seu autor. O público pode incluir destinatários externos mediante a autorização expressa do responsável pela informação.	• Informação sobre potenciais fusões ou aquisições. • Informação de planeamento estratégico – empresarial e organizacional. • Certas informações de configuração de segurança das informações. • Certos resultados e relatórios de auditoria. • Atas do Comité Executivo. • Dados de autenticação ou de identificação e verificação (ID&V) – clientes/consumidores e colegas. • Grandes volumes de informações de titulares de cartões. • Previsões de lucros ou resultados financeiros anuais (antes da divulgação pública). • Quaisquer elementos abrangidos por um acordo formal de não divulgação (NDA).
Restrito – Interno	As informações têm de ser classificadas como restritas-internas se os destinatários previstos forem apenas colaboradores autenticados do Barclays e prestadores de serviços geridos	• Estratégias e orçamentos. • Avaliações de desempenho. • Remuneração dos colaboradores e dados pessoais. • Avaliações de vulnerabilidade.

	(MSP) do Barclays com contrato vigente e se estiverem limitadas a um público específico. A divulgação não autorizada teria um impacto negativo no Barclays, avaliado segundo o ERMF, como "importante" ou "limitado" (financeiro ou não financeiro). As informações não se destinam a distribuição geral, mas podem ser encaminhadas ou partilhadas pelos destinatários de acordo com o princípio da necessidade de tomar conhecimento.	• Resultados e relatórios de auditorias.
Restrito – Externo	As informações têm de ser classificadas como restritas-externas se os destinatários previstos forem colaboradores autenticados do Barclays e MSP do Barclays com contrato vigente e se estiverem limitadas a um público específico ou terceiros autorizados pelo responsável pela informação. A divulgação não autorizada teria um impacto negativo no Barclays, avaliado segundo o ERMF, como "importante" ou "limitado" (financeiro ou não financeiro). As informações não se destinam a distribuição geral, mas podem ser encaminhadas ou partilhadas pelos destinatários de acordo com o princípio da necessidade de tomar conhecimento.	• Planos de novos produtos. • Contratos com clientes. • Contratos legais. • Pequenas quantidades de informação/informações individuais de clientes/consumidores destinadas a serem enviadas externamente. • Comunicações de clientes/consumidores. • Nova emissão de materiais de oferta (p. ex. brochuras, prospetos de oferta). • Documentos finais de investigação. • Informações não públicas relevantes (MNPI) externas ao Barclays. • Todos os relatórios de investigação. • Alguns materiais de marketing. • Comentários de mercado.
Não restrito	Informações destinadas a distribuição geral ou cuja distribuição não teria impacto na organização.	• Materiais de marketing. • Publicações. • Anúncios públicos. • Anúncios de emprego. • Informações sem impacto no Barclays.

Tabela C2: Esquema de classificação de informações – requisitos de tratamento

** Requisitos específicos de tratamento dos DIC para garantir a sua confidencialidade em conformidade com os requisitos regulamentares

Etapa do ciclo de vida	Requisitos de segredo bancário
Criação e classificação	De acordo com a classificação "restrito-externo" e: • Os ativos têm de ser atribuídos a um responsável por DIC.
Armazenamento	De acordo com a classificação "restrito-externo" e: • Os ativos só podem ser armazenados em suportes amovíveis pelo período explicitamente exigido por uma necessidade comercial específica, pelos reguladores ou auditores externos. • Grandes volumes de ativos informacionais que sejam objeto de segredo bancário não podem ser armazenados em dispositivos/suportes portáteis. Para mais informações, contacte a equipa local de segurança das informações e cibersegurança (a seguir designada por "SIC"). • Os ativos (físicos ou eletrónicos) não podem ser guardados onde indivíduos não autorizados os podem ver ou obter acesso aos mesmos, de acordo com o princípio da necessidade de tomar conhecimento ou de ter acesso. • Para a guarda dos ativos (físicos ou eletrónicos) têm de ser seguidas práticas de segurança no local de trabalho, tais como a política da secretária limpa e o bloqueio do computador. • Os suportes amovíveis de ativos informacionais só podem ser utilizados para efeitos de armazenamento pelo período explicitamente exigido e têm de ser trancados quando não estão a ser utilizados. • As transferências ad hoc de dados para dispositivos/suportes portáteis estão sujeitas à aprovação do responsável pelos dados, do departamento de conformidade e da SIC.

Acesso e utilização	De acordo com a classificação "restrito-externo" e: • Os ativos não podem ser eliminados/consultados fora do local (instalações do Barclays) sem a autorização formal do responsável pelos DIC (ou do seu representante). • Os ativos não podem ser eliminados/consultados fora da jurisdição de registo do cliente sem a autorização formal do responsável pelos DIC (ou do seu representante) e do cliente (renúncia/procuração). • Aquando da recolha de ativos físicos fora do local, têm de ser seguidas práticas seguras de teletrabalho, que garantam que não é possível espiar por cima do ombro.
	• Certifique-se de que pessoas não autorizadas não podem observar ou aceder a ativos eletrónicos que contenham DIC através da utilização do acesso restrito a aplicações empresariais.
Partilha	De acordo com a classificação "restrito-externo" e: • Os ativos só podem ser distribuídos de acordo com o "princípio da necessidade de tomar conhecimento" E entre o pessoal e os sistemas de informação da jurisdição com segredo bancário de que são provenientes. • A transferência de ativos numa base ad hoc com recurso a suportes amovíveis está sujeita à aprovação do responsável pelos ativos informacionais e da SIC. • As comunicações eletrónicas têm de ser encriptadas quando em trânsito. • Os ativos (em papel) enviados por e-mail têm de ser enviados com recurso a um serviço que exija um aviso de receção. • Os ativos só podem ser distribuídos de acordo com o "princípio da necessidade de tomar conhecimento".
Arquivo e eliminação	De acordo com a classificação "restrito-externo"

*** Informações de configuração de segurança do sistema, resultados de auditoria e registos pessoais podem ser classificados como restritos-internos ou secretos, dependendo do impacto da divulgação não autorizada no negócio

Etapa do ciclo de vida	Restrito – Interno	Restrito – Externo	Secreto
Criação e introdução	• Os ativos têm de ser atribuídos a um responsável pela informação.	• Os ativos têm de ser atribuídos a um responsável pela informação.	• Os ativos têm de ser atribuídos a um responsável pela informação.
Armazenamento	• Os ativos (físicos ou eletrónicos) não podem ser armazenados em áreas públicas (incluindo áreas públicas nas instalações dos fornecedores, onde os visitantes podem ter um acesso sem supervisão).	• Os ativos (físicos ou eletrónicos) não podem ser guardados onde indivíduos não autorizados os podem ver ou obter acesso aos mesmos. • Os ativos guardados em formato eletrónico têm de ser protegidos	• Os ativos (físicos ou eletrónicos) não podem ser guardados onde indivíduos não autorizados os podem ver ou obter acesso aos mesmos. • Os ativos guardados em formato eletrónico têm de ser protegidos

	• As informações não podem ser deixadas em áreas públicas nas instalações onde os visitantes podem ter acesso sem supervisão.	através de encriptação ou controlos de compensação adequados caso exista um risco significativo de que pessoas não autorizadas consigam obter acesso aos mesmos.	através de encriptação ou controlos de compensação adequados caso exista um risco significativo de que pessoas não autorizadas consigam obter acesso aos mesmos. • Todas as chaves privadas que sejam utilizadas para proteger dados do Barclays, a respetiva identidade e/ou reputação têm de ser protegidas por módulos de proteção de hardware (HSM) certificados FIPS 140-2 Nível 3 ou superior.
Acesso e utilização	• Os ativos (físicos ou eletrónicos) não podem ser deixados em áreas públicas fora das instalações. • Os ativos (físicos ou eletrónicos) não podem ser deixados em áreas públicas nas instalações onde os visitantes possam ter acesso sem supervisão. • Se necessário, os ativos eletrónicos têm de ser protegidos por controlos de gestão de acesso lógico adequados.	• Os ativos (físicos ou eletrónicos) não podem ser utilizados nem deixados sem vigilância onde indivíduos não autorizados os podem ver ou obter acesso aos mesmos. Os ativos podem ser utilizados se existirem controlos adequados (p. ex., telas de privacidade). • Os ativos impressos têm de ser retirados imediatamente da impressora. Se tal não for possível, tem de utilizar-se ferramentas de impressão segura. • Os ativos eletrónicos têm de ser protegidos por controlos de gestão de acesso lógico adequados.	• Os ativos (físicos ou eletrónicos) não podem ser utilizados nem deixados sem vigilância onde indivíduos não autorizados os podem ver ou obter acesso aos mesmos. Os ativos podem ser utilizados se existirem controlos adequados (p. ex., telas de privacidade). • Os ativos impressos têm de ser impressos com recurso a ferramentas de impressão segura. • Os ativos eletrónicos têm de ser protegidos por controlos de gestão de acesso lógico adequados.

Partilha	• Os ativos em papel têm de integrar uma etiqueta de informação visível. A etiqueta tem de encontrar-se pelo menos na página do título. • Os ativos eletrónicos têm de integrar uma etiqueta de informação bem visível. • Os ativos só podem ser distribuídos utilizando sistemas, métodos ou fornecedores aprovados pela organização. • Os ativos só podem ser distribuídos a pessoas empregadas pela empresa, ou ao abrigo de uma obrigação contratual adequada para com a empresa, ou no âmbito de uma necessidade comercial inequivocamente reconhecida, por exemplo, negociação contratual.	• Os ativos em papel têm de ter uma etiqueta de informação visível. A etiqueta tem de encontrar-se pelo menos na página do título. • Os envelopes que contenham ativos em papel têm de incluir uma etiqueta de informação visível na parte da frente. • Os ativos eletrónicos têm de integrar uma etiqueta de informação bem visível. As cópias eletrónicas de documentos com várias páginas têm de integrar uma etiqueta de informação visível em todas as páginas. • Os ativos só podem ser distribuídos utilizando sistemas, métodos ou fornecedores aprovados pela organização. • Os ativos só podem ser distribuídos a pessoas empregadas pela empresa, ou ao abrigo de uma obrigação contratual adequada para com a empresa, ou no âmbito de uma necessidade comercial inequivocamente reconhecida, por exemplo, negociação contratual. • Os ativos só podem ser distribuídos a pessoas com uma necessidade comercial de os receberem. • Um ativo não pode ser enviado por fax a menos que o remetente tenha confirmado que os destinatários estão preparados para o receber. • Os ativos eletrónicos têm de ser encriptados com recurso a um mecanismo de proteção criptográfico aprovado, sempre que estiverem a ser distribuídos fora da rede interna.	• Os ativos em papel têm de incluir uma etiqueta de informação visível em todas as páginas. • Os envelopes que contêm ativos em papel têm de incluir uma etiqueta de informação na parte da frente e de ser selados através de um sistema que não permita a violação. Antes da distribuição, têm de ser colocados no interior de um segundo envelope sem etiquetas. • Os ativos eletrónicos têm de integrar uma etiqueta de informação bem visível. As cópias eletrónicas de documentos com várias páginas têm de integrar uma etiqueta de informação visível em todas as páginas. • Os ativos só podem ser distribuídos utilizando sistemas, métodos ou fornecedores aprovados pela organização. • Os ativos só podem ser distribuídos a pessoas empregadas pela empresa, ou ao abrigo de uma obrigação contratual adequada para com a empresa, ou no âmbito de uma necessidade comercial inequivocamente reconhecida, por exemplo, negociação contratual. • Os ativos só podem ser distribuídos a pessoas especificamente autorizadas a recebê-los pelo responsável pela informação. • Os ativos não podem ser enviados por fax. • Os ativos eletrónicos têm de ser encriptados com recurso a um mecanismo de proteção criptográfico aprovado, sempre que estiverem a ser distribuídos fora da rede interna. • Tem de ser mantida uma cadeia de custódia para ativos eletrónicos.

Arquivo e eliminação	• Os ativos em papel têm de ser eliminados com recurso a um serviço de eliminação confidencial. • As cópias de ativos eletrónicos também têm de ser eliminadas dos "cestos de reciclagem" do sistema ou dispositivos semelhantes em tempo útil.	• Os ativos em papel têm de ser eliminados com recurso a um serviço de eliminação confidencial. • As cópias de ativos eletrónicos também têm de ser eliminadas dos "cestos de reciclagem" do sistema ou dispositivos semelhantes em tempo útil.	• Os ativos em papel têm de ser eliminados com recurso a um serviço de eliminação confidencial. • As cópias de ativos eletrónicos também têm de ser eliminadas dos "cestos de reciclagem" do sistema ou dispositivos semelhantes em tempo útil. • Os suportes onde ativos eletrónicos secretos tiverem sido guardados têm de ser devidamente limpos antes ou durante a eliminação.