Obrigações de controlo de fornecedores externos

Segurança das informações e cibersegurança

para fornecedores classificados como de alto risco cibernético e de informação

Versão 9.0, abril de 2019

Área de controlo/Título	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/cibersegurança, bem como um programa de proteção para proteger o fornecedor contra ameaças às informações/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, em qualquer caso, não menos do que uma vez a cada 12 meses) e deve implementar estes controlos e tomar estas medidas, conforme necessário, para mitigar os riscos identificados. Se for identificado um risco substancial que possa afetar adversamente a reputação ou o serviço fornecido ao Barclays, o fornecedor deve informar o Barclays. O fornecedor tem de respeitar as políticas e normas aprovadas pela direção sénior para gestão do risco de informação/cibernético do fornecedor e de as rever pelo menos anualmente.	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. Utilização aprovada	O fornecedor tem de produzir e divulgar requisitos de utilização aceitável para informar os colaboradores do fornecedor sobre as respetivas responsabilidades. Devem ser considerados os seguintes pontos: a) Utilização da Internet; b) Utilização de redes sociais; c) Utilização do e-mail empresarial; b) Utilização de mensagens instantâneas; e) Utilização de equipamento de TI disponibilizado pelo fornecedor; f) Utilização de equipamento de TI não disponibilizado pelo fornecedor (p. ex., "Bring Your Own Device" [traga o seu próprio dispositivo]); g) Utilização de dispositivos de memória portáteis/amovíveis; h) Responsabilidades aquando do tratamento de ativos informacionais do Barclays; e I) Saída de canais de fuga de dados O fornecedor tem de adotar as medidas adequadas para garantir a conformidade com os requisitos de utilização aceitável.	Um requisito de utilização aceitável contribui para um ambiente de controlo que protege os ativos informacionais.
3. Funções e responsabilidades	O fornecedor tem de definir e comunicar funções e responsabilidades pela segurança das informações/cibersegurança. Estas têm de ser revistas periodicamente (e, em qualquer caso, não menos do que uma vez a cada 12 meses) e após qualquer alteração substancial ao modelo de operação ou de negócios do fornecedor. As principais funções têm de incluir um executivo sénior, responsável pela segurança das informações/cibersegurança.	Uma clara definição das funções e responsabilidades auxilia a implementação do plano de obrigações de controlo de fornecedor externo.

4. Cumprimento de requisitos legislativos e estatutários locais	O fornecedor tem de garantir que os requisitos legislativos e estatutários relacionados com a segurança das informações aplicáveis à jurisdição onde opera são cumpridos e que tal conformidade é adequadamente documentada. Nota: As equipas locais poderão especificar requisitos adicionais associados à legislação e à regulamentação bancárias locais aplicáveis aos fornecedores em que se apoia o Barclays Suíça e o Barclays Mónaco.	O não cumprimento dos requisitos legislativos e estatutários locais pode ter graves repercussões para o fornecedor e para o Barclays, incluindo penalidades e, em casos extremos, a perda da licença bancária do Barclays.
5. Formação e sensibilização	O fornecedor tem de oferecer ações de formação e de sensibilização a todos os colaboradores relevantes. A formação e a sensibilização devem ser adequadas às suas funções e responsabilidades e têm de ser suficientes para os colaboradores conseguirem compreender e identificar prováveis ataques e proceder ao relato de preocupações. No mínimo, a formação tem de incluir segurança online (no trabalho, em casa e em viagem), riscos de engenharia social e medidas de combate práticas. O fornecedor tem de garantir que, num período de tempo razoável, todos os colaboradores (novos/transferidos) realizam formação para garantir que compreendem as respetivas funções e responsabilidades em matéria de segurança das informações. Deve ser dada formação avançada em consciencialização de segurança das informações/cibersegurança aos administradores do sistema pelo menos anualmente no sentido de lhes fornecer informações sobre os cenários/ameaças específicos das suas funções, como identificar ameaças às informações/cibernéticas, como proteger contra as mesmas e como proceder ao relato de preocupações.	A formação e a sensibilização auxiliam todos os outros controlos no âmbito deste plano. Se este controlo não for implementado, os colaboradores relevantes não estarão conscientes dos riscos cibernéticos e de vetores de ataque, e não conseguirão detetar nem prevenir ataques.

6. 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. • Tem de ser estabelecido um processo de resposta a incidentes para tratar e reportar de forma regular e atempada as intrusões que envolvam informações do Barclays e/ou serviços utilizados pelo Barclays. • As violações que, tanto quanto se saiba, não afetaram o sistema do Barclays e as ações corretivas/atualizações das mesmas têm de ser relatadas Barclays para fins informativos. • O fornecedor tem de garantir que as equipas e processos de resposta a incidentes são testados, pelo menos anualmente, para garantir que o fornecedor consegue dar resposta a incidentes de cibersegurança identificados. Os testes têm de incluir a validação da capacidade para informar o Barclays, comprovando a capacidade para contactar pessoas relevantes. • Tem de ser definido e aplicado um processo para identificar e gerir a mitigação das vulnerabilidades após um incidente de segurança sem comprometer investigações ou atividades de resposta. • O fornecedor tem de dispor de processos e procedimentos para realizar uma análise da causa originária de eventos internos (do fornecedor) e externos. • 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 o Barclays.	Um processo de gestão e resposta a incidentes ajuda a garantir que os incidentes são rapidamente contidos e impedidos de assumir maiores proporções.

7. Melhoria contínua	O fornecedor tem de aprender continuamente com os eventos e aplicar as ilações daí retiradas para melhorar as defesas de risco cibernético.	Se este controlo não for implementado, os fornecedores não poderão utilizar as ilações de eventos anteriores para melhorar e reforçar o respetivo ambiente de controlo.
8. Propriedade dos ativos informacionais	O fornecedor tem de ter um contacto designado para estabelecer a ligação com o responsável pelos ativos informacionais do Barclays.	A propriedade dos ativos informacionais é fundamental para a sua proteção adequada.
9. 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 B2A2), 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.
10. Gestão de ativos	O fornecedor tem de manter um inventário rigoroso de todos os ativos de TI pertinentes utilizados para disponibilizar serviços ao Barclays e de o rever pelo menos anualmente para confirmar que está atualizado, completo e rigoroso.	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.
11. Segurança em trânsito	Os ativos informacionais do Barclays (exceto se considerados "não restritos" ou equivalentes) têm de ser protegidos em trânsito de forma proporcional ao risco associado.	Em trânsito, os controlos protegem as informações do Barclays contra interceção e divulgação.

12. Destruição/eliminação/ desativação de informações físicas e lógicas	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 são recuperáveis.	A destruição segura de ativos informacionais ajuda a garantir que os ativos informacionais do Barclays não são recuperáveis para serem utilizados no âmbito de violações ou perdas de dados ou de atividades maliciosas.
13. 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: • através da separação lógica entre as portas/interfaces de gestão de dispositivos e o tráfego do utilizador; • controlos de autenticação adequados; e • a ativação de todos os controlos de mitigação de explorações disponíveis no sistema operativo e nos agentes e aplicações instalados. O fornecedor tem de definir e aplicar capacidades para detetar dispositivos não autorizados, software identificado como malicioso e software de alto risco não autorizado na sua rede. O fornecedor tem de posicionar sensores de rede para detetar ameaças em todos os pontos de entrada e saída do perímetro de rede. *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.*	Se este controlo não for implementado, as redes externas e internas podem ficar comprometidas pela ação de atacantes.

14. Defesa do perímetro	O fornecedor tem de manter um inventário de ligações de rede externas, anfitriões acessíveis pela Internet e transferências de dados utilizadas para transmitir dados do Barclays novamente para o Barclays ou quaisquer terceiros (incluindo, entre outros, quaisquer subcontratantes do fornecedor). Tem de ser implementado no perímetro um design de rede de várias zonas e separado, com base na exposição ao risco e nas necessidades da unidade de negócio. Só podem ser colocados no perímetro dispositivos que exijam ou facilitem o acesso a/de redes externas.	Uma proteção adequada para o perímetro ajuda a garantir que a rede e os ativos informacionais do Barclays são adequadamente protegidos.
15. Acesso de rede e acesso remoto	O fornecedor tem de garantir que o acesso à rede interna é monitorizado e apenas dispositivos autorizados passam pelos controlos de acesso à rede adequados. 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.). O acesso remoto a ambientes do Barclays não é fornecido por predefinição para assistência na localização do fornecedor/fora do horário de expediente/fora do horário de funcionamento. Qualquer acesso remoto deve ser aprovado pelas equipas do Barclays relevantes (incluindo o diretor de segurança).	Os controlos de acesso à rede ajudam a garantir que os dispositivos inseguros não estão ligados à rede do fornecedor, evitando novas vulnerabilidades.
16. Deteção de recusa de serviço	O fornecedor tem de implementar e manter capacidades para detetar ataques de recusa de serviço (DoS). O fornecedor tem de garantir que canais externos ou com ligação à Internet que suportem serviços disponibilizados ao Barclays são obrigados a ter uma proteção DoS adequada para assegurar os critérios de disponibilidade acordados com o Barclays.	Se este controlo não for implementado, o Barclays e os respetivos fornecedores podem não conseguir impedir que um ataque de recusa de serviço atinja o seu objetivo.

17. Monitorização/registo	O fornecedor tem de garantir a implementação de uma capacidade de monitorização da infraestrutura de TI, 24 horas por dia, 7 dias por semana, para identificação de potenciais eventos de cibersegurança. O fornecedor tem de reunir e correlacionar dados dos eventos a partir de fontes e sensores do sistema aplicáveis e analisados para identificação e compreensão de ataques/incidentes. Aquando da identificação de quaisquer incidentes e/ou violações substanciais de controlos de segurança, o fornecedor deve garantir que é seguido o processo de gestão de incidentes (secção 6 supra). Todos os principais sistemas, incluindo aplicações essenciais, têm de ser configurados pelo fornecedor para registar eventos-chave e a hora do sistema tem de ser sincronizada pelo fornecedor em todos os sistemas utilizando o protocolo de horário de rede (Network Time Protocol – NTP). Os registos têm de ser centralizados, protegidos de forma adequada e mantidos pelo fornecedor durante um mínimo de 12 meses. Os eventos-chave registados têm de incluir aqueles com potencial de impacto na confidencialidade, integridade e disponibilidade do serviço para o Barclays e que podem ajudar na identificação ou investigação de incidentes substanciais e/ou violações de direitos de acesso que ocorrem relativamente a sistemas do fornecedor.	Se este controlo não for implementado, os fornecedores não conseguirão detetar nem responder a violações de cibersegurança nem recuperar e aprender com eventos cibernéticos que ocorreram na respetiva rede através da análise de registos relevantes.
18. Segregação de ativos informacionais	O fornecedor tem de guardar ativos informacionais do Barclays numa rede separada (de forma lógica ou física) de outros clientes.	Uma rede separada ajuda a garantir que os ativos informacionais do Barclays são adequadamente protegidos contra a divulgação não autorizada.

19. Proteção contra códigos maliciosos/malware	Quando suportados a nível do sistema operativo, os sistemas de TI, os serviços de TI e os dispositivos de TI têm de dispor sempre de soluções antimalware no intuito de impedir a perturbação do serviço ou violações de segurança. O fornecedor tem de: • Estabelecer e manter proteção atualizada contra códigos maliciosos/malware, em conformidade com a boa prática do setor (p. ex., NIST, ISO27001); e • Garantir proteção contra a transferência de códigos maliciosos para sistemas do Barclays, clientes do Barclays e outros terceiros, em conformidade com os métodos padrões do setor (p. ex., NIST, ISO27001).	As soluções antimalware são essenciais para a proteção de ativos informacionais do Barclays contra códigos maliciosos.
20. Normas de compilação seguras e conciliação das alterações de segurança	O fornecedor tem de definir e implementar normas de compilação para todo o software "out of the box" configurável utilizado em grande escala (p. ex., sistemas operativos, bases de dados) e firmware de infraestrutura habitualmente utilizada (p. ex., SAN ou dispositivos de rede). As não conformidades com a norma de compilação têm de ser corrigidas. As alterações de segurança (p. ex., mudanças de configuração de proteção, modificação de privilégios de conta) têm de criar sempre um registo que seja guardado num ambiente inviolável. Tem de ser realizada uma reconciliação entre as modificações aplicadas e as modificações autorizadas. 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 controlos de normas de compilação ajudam a proteger ativos informacionais contra acesso não autorizado. A conformidade com as normas de compilação e os controlos que assegurem que as modificações são autorizadas ajudam a garantir a proteção dos ativos informacionais do Barclays.
21. 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.	Se este controlo não for implementado, os ativos informacionais do Barclays podem não ser suficientemente protegidos contra ciberataques.

22. 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. 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.	Se este controlo não for implementado, a rede e os pontos finais do Barclays e do fornecedor podem ficar vulneráveis a ciberataques.
23. Deteção de software e dispositivos não autorizados	O fornecedor tem de garantir que dispõe de capacidade e processos para detetar dispositivos não autorizados, software identificado como malicioso e software de alto risco não autorizado.	Se este controlo não for implementado, os fornecedores podem não conseguir detetar, remover ou desativar dispositivos ou software maliciosos não autorizados, expondo assim os ativos do Barclays a ciberataques.
24. 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: • 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); • Transferência não autorizada de informações para meios portáteis; • Troca insegura de informações com terceiros (subcontratantes); • Impressão ou reprodução inadequada de informações; • Erros e omissões na classificação e rotulagem de ativos; e • Fuga de informação não autorizada através do Sistema de Nomes de Domínio (DNS)	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.

25. Armazenamento e processamento seguros	Têm de existir controlos para proteger ativos informacionais (relacionados com o(s) serviço(s) prestado(s) pelo fornecedor ao Barclays) sempre que forem armazenados ou processados (tal aplica-se a informações armazenadas como parte de métodos estruturados e não estruturados).	Geralmente, os ativos informacionais são guardados em conjunto e, como tal, representam uma concentração de risco, devendo ser protegidos.
26. Cópia de segurança e recuperação	Têm de ser adotadas disposições para garantir que a informação é devidamente salvaguardada e recuperável em conformidade com os requisitos acordados com o responsável pelos ativos informacionais do Barclays, devendo a segurança dos ativos informacionais ser preservada ao longo do processo. A frequência e o método de cópia de segurança têm de ser acordados com o responsável pelo ativo informacional. Os ativos informacionais que foram objeto de cópia de segurança têm de ter controlos definidos para garantir que o acesso só é concedido quando necessário.	As cópias de segurança guardam ativos informacionais e, como tal, têm de ser sujeitas aos mesmos controlos.

27. 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. 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. Têm de 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;	Controlos LAM apropriados ajudam a garantir que os ativos informacionais são protegidos contra utilização indevida.

	• um processo de revisão do acesso do utilizador regular, pelo menos anualmente, para confirmar o acesso do utilizador; • 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.	
28. Métodos de acesso	As atividades realizadas com recurso a uma conta têm de ser rastreáveis até a um indivíduo. Têm de ser aplicadas medidas técnicas e processuais para impor o nível adequado de acesso aos ativos informacionais. Os controlos de segurança referentes a contas (p. ex. procedimentos de autenticação forte ou acesso rápido) têm de ser proporcionais ao risco de comprometimento ou uso abusivo das contas. O método de acesso tem de ser definido de acordo com a boa prática do setor e incluir, no mínimo, o seguinte: • 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. O acesso remoto a serviços Barclays tem de ser autorizado através de mecanismos acordados pelas equipas do Barclays relevantes e utilizar autenticação multifator.	Os controlos de gestão de acesso ajudam a garantir que apenas utilizadores aprovados podem aceder a ativos informacionais.

29. Proteção de aplicação	As aplicações têm de ser desenvolvidas com recurso a práticas de codificação seguras e em ambientes seguros. Nos casos em que o fornecedor desenvolver aplicações para utilização pelo Barclays, ou que sejam utilizadas para suportar o serviço ao Barclays, têm de existir processos e controlos para identificação e resolução de vulnerabilidades no código durante o processo de desenvolvimento. Os binários de aplicações têm de ser protegidos contra alterações não autorizadas enquanto implementados ou enquanto estiverem nas bibliotecas de origem. 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.	Os controlos que protegem o desenvolvimento da aplicação ajudam a garantir que as aplicações estão protegidas no momento da implementação.

30. Gestão de vulnerabilidade	O fornecedor tem de gerir um mecanismo consistente para registar, triar e dar resposta às vulnerabilidades identificadas. O fornecedor tem de estabelecer capacidades para identificar e classificar vulnerabilidades em sistemas de TI e software em função do risco em todas as plataformas utilizadas pela organização. O fornecedor tem de garantir que a gestão de vulnerabilidades opera rotineiramente (BAU) nas respetivas operações, incluindo processos para detetar e avaliar o risco das vulnerabilidades, eliminar ou resolver vulnerabilidades em todos os sistemas e evitar a introdução de novas vulnerabilidades durante os processos de mudança e implementação de novos sistemas. Todos os problemas de segurança e vulnerabilidades passíveis de afetar substancialmente os sistemas do Barclays ou os serviços prestados pelo fornecedor ao Barclays cujos riscos o fornecedor tenha decidido assumir têm de ser comunicados ao Barclays de imediato e acordados com o Barclays por escrito. O fornecedor tem de instalar patches de segurança de TI e atualizações de vulnerabilidade de segurança mediante um processo interno (do fornecedor) aprovado de modo atempado para se impedirem eventuais violações de segurança. Os sistemas do fornecedor que, por algum motivo, não possam ser atualizados, têm de dispor de medidas para proteção do sistema vulnerável.	Se este controlo não for implementado, os atacantes podem explorar as vulnerabilidades dos sistemas para realizarem ciberataques contra o Barclays e os respetivos fornecedores.

31. 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/simulação de ameaça 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. Todas as vulnerabilidades devem ser priorizadas e acompanhadas até à sua resolução. Todos e quaisquer riscos assumidos têm de ser comunicados e acordados com o Barclays. O fornecedor tem de informar o Barclays do âmbito da avaliação de segurança e acordar com o Barclays o mesmo, em particular no que se refere à data/horas de início e fim, para impedir a perturbação de atividades-chave do Barclays.	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.

32. Gestão de alterações e patch	Os dados do Barclays e os sistemas para o seu armazenamento ou processamento devem estar protegidos contra alterações inadequadas que possam comprometer a sua disponibilidade ou integridade. O fornecedor deve desenvolver e implementar uma estratégia de gestão de patch que seja suportada por controlos de gestão e por procedimentos de gestão de patch e documentação operacional. Logo que fiquem disponíveis, os patches de segurança de TI e as atualizações de vulnerabilidades de segurança devem ser instalados através de um processo aprovado de forma atempada, a fim de prevenir violações de segurança. Os sistemas de fornecedores que, por alguma razão, não possam ser atualizados, devem ter medidas de segurança instaladas para proteger o sistema vulnerável. Todas as modificações têm de ser realizadas em conformidade com o processo de gestão da mudança aprovado do fornecedor. As aplicações de fonte aberta devem ser verificadas relativamente a vulnerabilidades restantes. O fornecedor deve garantir que são implementadas soluções de emergência quando disponíveis e aprovadas, exceto se tal introduzir riscos empresariais mais elevados. Os sistemas do fornecedor que, por alguma razão, não possam ser atualizados, devem ter medidas de segurança instaladas para proteger integralmente o sistema vulnerável. Todas as modificações têm de ser realizadas em conformidade com o processo de gestão da mudança do fornecedor.	Se este controlo não for implementado, os serviços podem tornar-se vulneráveis a problemas de segurança, o que pode comprometer os dados do consumidor, provocar perda de serviços ou permitir outras atividades maliciosas.
33. Criptografia	O fornecedor tem de rever e avaliar a tecnologia e os algoritmos criptográficos que utiliza de modo a garantir que continuam a ser adequados para a finalidade. A intensidade da encriptação implementada tem de ser conforme à apetência pelo risco, visto que pode ter um impacto operacional ou no desempenho. As implementações criptográficas devem cumprir os requisitos e algoritmos definidos.	A atualização e a adequação da proteção de encriptação e dos algoritmos garantem a proteção ininterrupta dos ativos informacionais do Barclays.

34. Computação em nuvem	Toda a utilização de serviços de computação em nuvem (públicos/privados/comunitários/híbridos), nomeadamente SaaS/PaaS/IaaS, no âmbito de serviços prestados ao Barclays acordados tem de ser revista e aprovada pelas equipas do Barclays relevantes (incluindo o diretor de segurança); e 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.
35. 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.
36. Espaço Dedicado do Banco	Para serviços fornecidos que requeiram Espaço Dedicado do Banco (EDB) formal, devem ser implementados EDB específicos físicos e requisitos técnicos. (Se o EDB constituir um requisito do serviço, os requisitos de controlo constantes do Anexo C serão aplicáveis.)	Se este controlo não for implementado, poderão não existir controlos técnicos e físicos, originando atrasos e perturbações de serviço ou violações de cibersegurança.

Anexo A: Glossário

Definições	
Ativo informacional	Qualquer informação que tenha valor, à luz dos respetivos requisitos de confidencialidade, integridade e disponibilidade. Ou Qualquer elemento de informação ou grupo de informações que tem valor para a organização.
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.
Cópia de segurança, salvaguarda	A cópia de segurança ou o processo de salvaguarda refere-se à realização de cópias dos dados que possam ser utilizadas para restaurar o ficheiro original na sequência de um evento de perda de dados.
Criptografia	A aplicação de teoria matemática para desenvolver técnicas e algoritmos que podem ser aplicados a dados para garantir o cumprimento de objetivos como a confidencialidade, a integridade dos dados e/ou a autenticação.
Destruição/eliminação	O ato de sobregravar, apagar ou destruir fisicamente informações de tal forma que não é possível recuperá-las.
Encriptação	A transformação de uma mensagem (dados, voz ou vídeo) numa forma sem sentido que não pode ser compreendida por leitores não autorizados. Trata-se de uma transformação de um formato de texto simples num formato de texto cifrado.
Espaço Dedicado do Banco	Por Espaço Dedicado do Banco (EDB) entendem-se quaisquer instalações na posse ou sob o controlo de um membro do grupo fornecedor ou subcontratante que sejam exclusivamente dedicadas ao Barclays ou a partir das quais os serviços sejam prestados ou entregues.
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.
Responsável pelo ativo informacional	A pessoa que, na organização, é responsável por classificar um ativo e garantir que este é tratado corretamente.

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.	• Estratégias e orçamentos. • Avaliações de desempenho. • Remuneração dos colaboradores e dados pessoais. • Avaliações de vulnerabilidade. • Resultados e relatórios de auditorias.

	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.	
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 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). • As informações não podem ser deixadas em áreas públicas nas instalações onde os visitantes podem ter 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 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 (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 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 (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.

		• 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 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.	• 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.

Anexo C: Espaço Dedicado do Banco (EDB) – requisitos de controlo (Nota: confirmar com o representante de recursos, caso seja necessário)

Área de controlo	Designação do controlo	Descrição do controlo
Espaço Dedicado do Banco	Separação física	A área física ocupada deve ser dedicada ao Barclays e não partilhada com outras empresas/prestadores de serviços.

Espaço Dedicado do Banco	Controlo de acesso físico	Os controlos automáticos seguros devem estar em funcionamento para o acesso a EDB, incluindo: 1) Para pessoal autorizado; i) Crachá com fotografia de identificação sempre visível ii) Leitores de cartões implementados nas proximidades iii) Mecanismo antirretorno ativado 2) Controlos para visitantes/prestadores de serviços i) Livro de registos com assinatura ii) Crachá de utilização limitada sempre visível
Espaço Dedicado do Banco	Controlo de acesso físico	Devem ser configurados alarmes que serão reportados através de um sistema de acesso centralizado com controlo de acesso auditável.
Espaço Dedicado do Banco	Controlo de acesso físico e limpeza	Monitoriza os controlos garantindo que o acesso adequado é concedido ao EDB e a outras áreas críticas. Apenas devem ter permissão para estar no EDB pessoal de limpeza e pessoal de apoio autorizados, como eletricistas, manutenção de AC, limpeza, etc.
Espaço Dedicado do Banco	Acesso remoto - Identificação e verificação	Todos os utilizadores individuais devem apenas efetuar a sua autenticação na rede do Barclays a partir do EDB utilizando o token de autenticação multifator fornecido pelo Barclays.
Espaço Dedicado do Banco	Acesso remoto - Tokens de software	A instalação de qualquer software do RSA e tokens de software deve ser efetuada por pessoal autorizado nos computadores aprovados do EDB.
Espaço Dedicado do Banco	Acesso remoto - Assistência fora de expediente	O acesso remoto ao ambiente EDB não é fornecido por predefinição para assistência fora do horário de expediente/fora do horário de funcionamento. Qualquer acesso remoto deve ser aprovado pelas equipas do Barclays relevantes (incluindo o diretor de segurança).
Espaço Dedicado do Banco	E-mail e Internet	A conectividade da rede deve ser configurada de forma segura, de modo a restringir e-mails e atividade na Internet na rede EDB.
Espaço Dedicado do Banco	Desenvolvimento de software, ambiente de teste e desenvolvimento	O fornecedor tem de garantir que o desenvolvimento de software para programas detidos pelo Barclays é realizado unicamente no Espaço Dedicado do Banco (EDB).
Espaço Dedicado do Banco	Controlos de rede - Transmissão	Toda a informação deve ser transmitida de forma segura entre o ambiente EDB e o Barclays e a gestão de dispositivos de rede deve ser efetuada utilizando protocolos seguros.

Espaço Dedicado do Banco	Controlos de rede - Encaminhamento	A configuração do encaminhamento deve garantir apenas ligações à rede do Barclays e não deve encaminhar para quaisquer outras redes.
Espaço Dedicado do Banco	Controlos de rede - Sem fios	As redes sem fios não devem ser utilizadas no segmento da rede do Barclays relativo aos serviços de provisão.

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 B2) 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 D, Tabela D1), 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 D2 do Anexo D. * "***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 D: 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

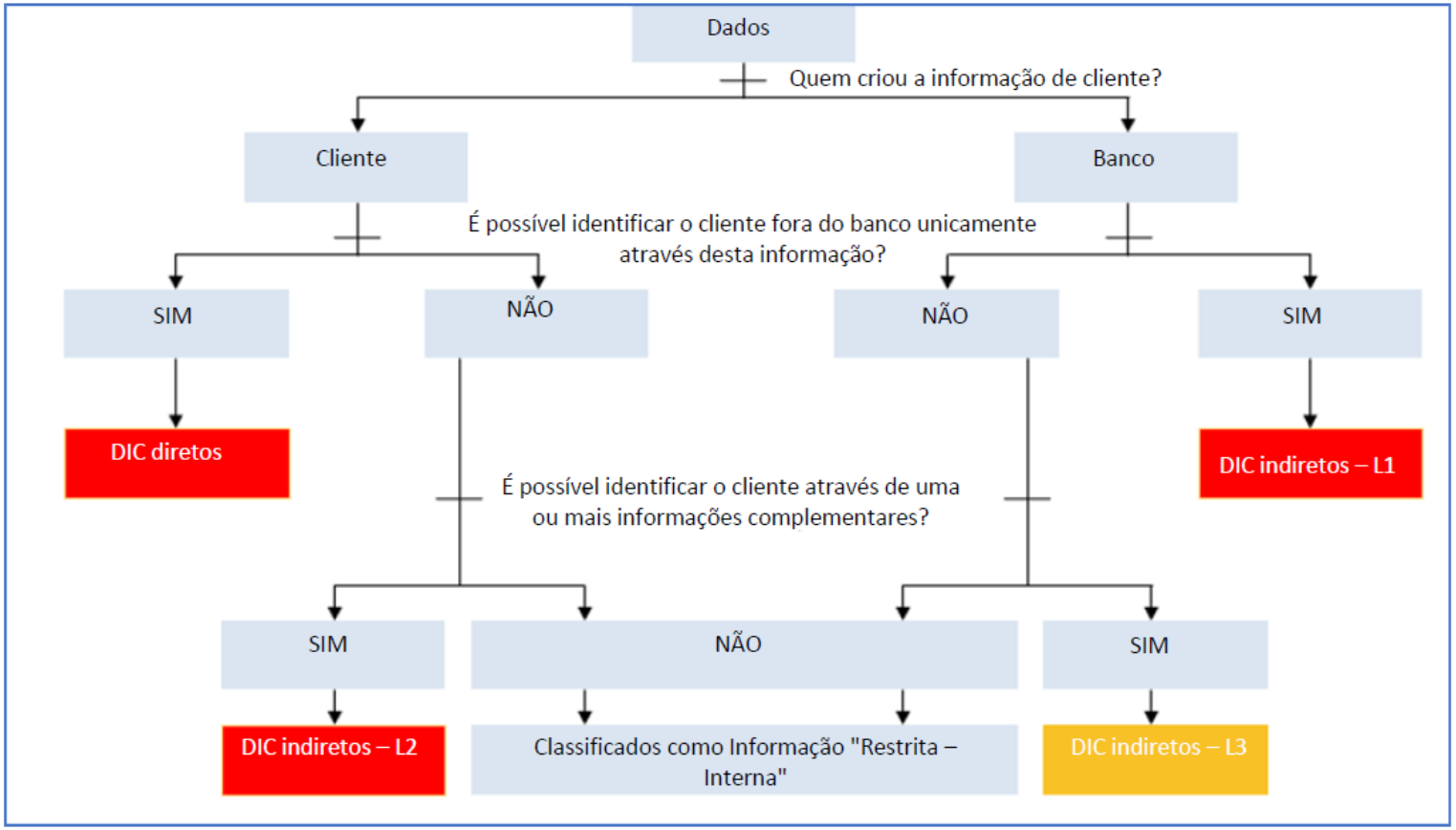
   (DICD) = Violação do segredo bancário

2. ID da partição

   (DICI L1) = Violação do segredo bancário

3. Situação patrimonial + Nacionalidade

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


Dados
Quem criou a informação de cliente?
Cliente
Banco
É possível identificar o cliente fora do banco unicamente através desta informação?
SIM
NÃO
NÃO
SIM
DIC diretos
DIC indiretos – L1
É possível identificar o cliente através de uma ou mais informações complementares?
SIM
NÃO
SIM
DIC indiretos – L2
Classificados como Informação "Restrita – Interna"
DIC indiretos – L3

Anexo E: Esquema de classificação de informações do Barclays

Tabela E1: 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 D)

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).	• Informação sobre potenciais fusões ou aquisições. • Informação de planeamento estratégico – empresarial e organizacional.

	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.	• 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 (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 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).	• 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.

	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.	• 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 E2: 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 (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 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 em papel têm de incluir 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 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 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.