Obrigações de controlo de fornecedores externos

Segurança das informações e cibersegurança (ICS)

Versão 10.0 Datada de outubro de 2020

Área de controlo/Título	Descrição do controlo	Por que é importante
1. Governação e normas em matéria de segurança das informações/cibersegurança	O fornecedor tem de dispor de uma estrutura de segurança devidamente estabelecida e consistente com os padrões do setor para governação em matéria de segurança das informações e cibersegurança, a fim de garantir a compreensão das suas pessoas, processos, ambiente tecnológico e estado dos controlos da segurança das informações/cibersegurança, bem como um programa de proteção para proteger o fornecedor contra ameaças cibernéticas em conformidade com a boa prática do setor (nomeadamente, NIST, ISO/IEC 27001) e os requisitos do setor aplicáveis. A estrutura de governação em matéria de segurança deve ser desenvolvida, documentada, aprovada e implementada, incluindo medidas de salvaguarda administrativas, técnicas e físicas com vista à proteção dos ativos e dos dados contra perda, uso indevido, acesso não autorizado, divulgação, alteração e destruição. O programa de segurança deve incluir, entre outras, as seguintes áreas: • Uma política, procedimentos e programa padrão no âmbito da segurança das informações e cibersegurança que eficazmente crie, implemente e meça continuamente a eficácia da implementação dos padrões e da política de segurança das informações e cibersegurança; • Um programa de segurança abrangente, com uma estrutura de liderança clara e supervisão executiva, a fim de criar uma cultura de responsabilidade e sensibilização para a segurança; • Políticas e procedimentos relativos à segurança das informações e cibersegurança aprovados e comunicados a toda a organização; • A garantia de que as políticas e procedimentos relativos à segurança das informações e cibersegurança são revistos de forma rotineira (pelo menos, uma vez por ano ou em caso de alteração material);	Se este princípio não for implementado, o Barclays ou os respetivos fornecedores podem não possuir nem conseguir demonstrar uma supervisão apropriada relativamente à segurança das informações/cibersegurança. Uma estrutura de governação da segurança define o nível de segurança para toda a organização.

	• O fornecedor deve garantir que é aplicada responsabilização individual pelas informações e sistemas, garantindo que existe uma propriedade adequada de ambientes empresariais críticos, informações e sistemas e que esta propriedade é atribuída a indivíduos competentes; • O fornecedor coordena e procede ao alinhamento de funções e responsabilidades para o pessoal, implementando, gerindo e supervisionando a eficácia da estratégia e estrutura de segurança com os parceiros internos e externos: • Devem ser realizadas análises e avaliações pelo menos uma vez por ano, a fim de garantir que a organização aborda as situações de não conformidade das obrigações das políticas, padrões, procedimentos e conformidade estabelecidas. **O fornecedor tem de garantir que notifica o Barclays (por escrito) assim que conseguir fazê-lo legalmente caso o fornecedor seja sujeito a uma fusão, aquisição ou qualquer outro processo de alteração da propriedade.**	
2. Gestão do risco em matéria de segurança das informações/cibersegurança	O fornecedor tem de estabelecer um programa de gestão do risco em matéria de segurança que eficazmente avalie, mitigue e monitorize os riscos de segurança em todo o ambiente controlado pelo fornecedor. O programa de gestão do risco deve incluir, entre outras, as seguintes áreas: • O fornecedor deve dispor de uma estrutura de gestão do risco em matéria de segurança das informações/cibersegurança aprovada pela autoridade superior (por ex., o Conselho de Administração ou uma das suas comissões). Este facto deve ser incorporado na estratégia empresarial e na estrutura de gestão do risco globais; • Em linha com a estrutura de risco, devem ser realizadas avaliações do risco formais pelo menos uma vez por ano ou em intervalos de tempo planeados ou acionadas com base em eventos, ou seja, em resposta a um incidente ou às conclusões obtidas no seguimento do mesmo (e em conjunto com quaisquer	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. Se este princípio não for implementado, pode ser indevidamente divulgada informação sensível do Barclays e/ou poderá ocorrer perda de serviços que resulte em sanções

	alterações aos sistemas de informação), a fim de determinar a probabilidade e o impacto de todos os riscos identificados utilizando métodos qualitativos e quantitativos. A probabilidade e o impacto associados ao risco inerente e residual devem ser determinados de forma independente, tendo em conta todas as categorias do risco (por ex., resultados da auditoria, análise das ameaças e vulnerabilidades e conformidade regulamentar); • Os resultados da avaliação do risco devem incluir atualizações às políticas, procedimentos, padrões e controlos de segurança por forma a garantir que ainda se mantêm relevantes e em vigor e, sempre que adequado, alinhados com as melhores práticas do setor; • Selecionar opções adequadas de tratamento do risco de segurança das informações, tendo em conta os resultados da avaliação do risco; • Formular um plano de tratamento do risco de segurança e os critérios de aceitação do risco através de indivíduos devidamente qualificados e responsáveis; • O fornecedor deve garantir que os riscos identificados são minimizados ou eliminados no ambiente através da atribuição de prioridade ao risco e da implementação de contramedidas; • Os riscos devem ser mitigados até um nível aceitável. Os níveis de aceitação com base em critérios de risco devem ser estabelecidos e documentados de acordo com calendários de resolução razoáveis e com a aprovação das partes interessadas; • As avaliações do risco associadas aos requisitos de governação dos dados devem ter em conta os seguintes elementos: o Classificação dos dados e proteção contra utilização e acesso não autorizados, perda, destruição e falsificação; o Conhecimento do local onde se encontram armazenados os dados e onde são transmitidos pelas aplicações, bases de dados, servidores e infraestrutura da rede;	legais e regulamentares ou em danos para a reputação.

	○ Conformidade com os períodos de retenção definidos e com os requisitos de eliminação no final da vida útil dos dados. • O fornecedor deve realizar, pelo menos, uma avaliação anual do risco de segurança relativamente à segurança das informações/cibersegurança, considerando uma cadência mais frequente com base nos ambientes específicos. **O fornecedor notificará o Barclays se não conseguir remediar ou reduzir quaisquer áreas materiais de risco que possam afetar o serviço prestado ao Barclays.**	
3. Utilização aprovada	O fornecedor deve produzir e divulgar requisitos de utilização aceitável para informar os colaboradores do fornecedor sobre as respetivas responsabilidades. Devem ser considerados os seguintes pontos: • Utilização da Internet; • Utilização de "software como um serviço" ("Software as a Service" [SaaS]); • Utilização de repositórios de códigos públicos; • Utilização de plug-ins baseados no browser e freeware/shareware; • Utilização de redes sociais; • Utilização do e-mail empresarial; • Utilização de mensagens instantâneas; • Utilização de equipamento de TI disponibilizado pelo fornecedor; • Utilização de equipamento de TI não disponibilizado pelo fornecedor (p. ex., "Bring Your Own Device" [traga o seu próprio dispositivo]); • Utilização de dispositivos de memória portáteis/amovíveis; • Responsabilidades aquando do tratamento de ativos informacionais do Barclays; e • 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.

4. Formação e sensibilização	O fornecedor tem de estabelecer um programa de formação de sensibilização para a segurança destinado a todos os funcionários, contratantes e utilizadores terceiros que utilizem os sistemas da organização e com mandato para tal, sempre que adequado. Todos os indivíduos com acesso a dados/informações do Barclays têm de receber formação de sensibilização para a segurança e atualizações regulares sobre os procedimentos, processos e políticas da organização relacionados com a função profissional desempenhada na mesma. Os níveis de formação e sensibilização têm de ser proporcionais às função desempenhadas e registados numa plataforma de gestão da aprendizagem adequada. O fornecedor tem de garantir que todo o pessoal sob o seu controlo recebe formação obrigatória sobre segurança das informações, incluindo as melhores práticas sobre cibersegurança e proteção dos dados do Barclays no prazo de um mês após a sua entrada na organização, tendo atualizações, pelo menos, a título anual. Os elementos abaixo deverão ser incluídos sempre que necessário: Grupos de alto risco, tais como aqueles com acesso privilegiado ao sistema ou a exercer funções empresariais sensíveis (incluindo utilizadores privilegiados, executivos sénior, pessoal da área da segurança das informações e cibersegurança e partes interessadas externas), deverão receber formação de sensibilização situacional na área da segurança das informações e cibersegurança de acordo com as suas funções e responsabilidades.	A formação e a sensibilização auxiliam todos os outros controlos no âmbito deste plano. Se este princípio não for implementado, os colaboradores relevantes não estarão conscientes dos riscos cibernéticos e de vetores de ataque, e não conseguirão detetar nem prevenir ataques.
5. Gestão de incidentes de segurança	O fornecedor tem de estabelecer uma estrutura de gestão de incidentes em matéria de cibersegurança que eficazmente valide, contenha e remova/mitigue o incidente de segurança do ambiente controlado pelo fornecedor. O fornecedor tem de garantir que existem planos escritos de resposta a incidentes que definem as funções do pessoal, bem como as fases do tratamento/gestão do incidente:	Um processo de gestão e resposta a incidentes ajuda a garantir que os incidentes são rapidamente contidos e impedidos de assumir maiores proporções.

	• Validação do incidente - estabelecer um processo de validação de incidentes que faça uso de diversas fontes de dados e seja integrado em toda a empresa, de forma a validar eficazmente um incidente de segurança; • Classificação do incidente - estabelecer um processo de classificação de incidentes que classifique de forma eficaz e rápida um incidente validado em todos os tipos de eventos, permitindo a execução rápida de atividades de resposta ao incidente; • Contenção do incidente - utilizar pessoas, processos e capacidades tecnológicas para rápida e eficazmente conter um incidente de segurança no ambiente; • Remoção/mitigação da ameaça - aproveitar pessoas, processos e capacidades tecnológicas para rápida e eficazmente remover/mitigar uma ameaça de segurança e/ou os seus componentes do ambiente. O fornecedor procurará estabelecer que as atividades de resposta sejam melhoradas sempre que possível, incorporando as conclusões retiradas de atividades de deteção/resposta atuais e anteriores. O fornecedor deve 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. • Os testes têm de incluir a validação da capacidade para informar o Barclays, demonstrando a capacidade para contactar pessoas relevantes; • Comunicação - o fornecedor tem de nomear um ponto de contacto para quaisquer incidentes de segurança que fará a ligação com o Barclays na eventualidade de um incidente. O fornecedor deverá comunicar ao Barclays os detalhes de contacto do(s) indivíduo(s) e todas as alterações aos mesmos, incluindo quaisquer contactos e números de telefone disponíveis fora do horário de expediente.	

	Os detalhes devem incluir: nome, responsabilidades dentro da organização, cargo, endereço de e-mail e/ou número de telefone O fornecedor informará o Barclays, dentro de um prazo razoável após tomar conhecimento de qualquer incidente que afete o serviço prestado ao Barclays ou informações/dados do Barclays e, em qualquer situação, nunca mais de **2 (duas) horas** depois da hora em que o incidente é detetado pelo fornecedor. Na eventualidade de existir uma suspeita ou uma violação efetiva de dados, o prestador de serviços informará o Barclays de tais incidentes, em linha com os requisitos no âmbito da proteção de dados do país afetado. O fornecedor entregará ao Barclays um relatório relativo a qualquer incidente que afete o serviço prestado ao Barclays ou informações/dados do Barclays. O relatório deverá incluir os seguintes detalhes: • data e hora; • local; • tipo de incidente; • impacto; • estado; • mitigação ou ação tomada. Estes incidentes devem ser reportados ao Gestor de Fornecedores do Barclays e ao Centro de Operações Conjuntas ("Joint Operations Centre") do Barclays através do endereço de e-mail **"Chief Security Office" (Gabinete do Diretor de Segurança, CSO) do Barclays, "Joint Operations Centre" (Centro de Operações Conjuntas, JOC) - gcsojoc@barclays.com.**	
6. Classificação e proteção de informações	O fornecedor tem de possuir uma estrutura/plano estabelecido e adequado para a classificação e tratamento de informações (alinhado com as boas práticas do setor e/ou os requisitos do Barclays) que abranja os seguintes componentes:	Os controlos adequados devem ser operados eficazmente de modo a garantir que a informação sensível

	• Atribuição do esquema de rótulos de informação correto; • Tratamento das informações de forma segura, em linha com o seu nível de classificação atribuído; • Garantir que todo o pessoal tem conhecimento dos requisitos de rotulagem e tratamento do fornecedor/Barclays e da forma como aplicar corretamente a classificação das informações. O fornecedor tem de consultar o esquema de rotulagem de informações e os requisitos de tratamento do Barclays (Anexo B, Tabelas B1 e B2) ou um esquema alternativo para garantir que o fornecedor protege e defende as informações do Barclays retidas ou processadas. Este requisito é aplicável a todos os ativos de informações retidos ou processados em nome do Barclays.	do Barclays se restringe àqueles que a ela devem ter acesso (confidencialidade), que se encontra protegida de alterações não autorizadas (integridade) e que pode ser recuperada e apresentada quando solicitado (disponibilidade). A não implementação destes requisitos poderá fazer com que a informação sensível do Barclays fique vulnerável a modificação, divulgação, acesso, danos, perda ou destruição não autorizados, o que poderá resultar em sanções legais e regulamentares, prejuízos para a reputação ou perda/perturbação dos negócios.
7. Gestão de ativos (hardware e software)	O fornecedor tem de garantir um programa de gestão de ativos eficaz, estabelecido para todo o ciclo de vida dos ativos. A gestão de ativos deve governar o ciclo de vida dos mesmos, desde a aquisição até à retirada, conferindo visibilidade e segurança a todas as classes de ativos no ambiente. O fornecedor tem de manter um inventário completo e rigoroso de todos os ativos críticos para o negócio situados em todos os pontos e/ou locais geográficos nos quais presta serviços ao Barclays e incluindo qualquer equipamento do Barclays presente nas instalações do fornecedor, de subcontratantes do prestador de serviços ou fornecido pelo Barclays, garantindo que existe pelo menos um teste anual para validar a atualidade, integralidade e rigor do inventário de ativos.	É essencial um inventário de ativos informacionais completo e rigoroso para garantir controlos adequados. Se este princípio 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,

	O processo de gestão de ativos deve cobrir as seguintes áreas: • Os ativos e infraestruturas de informações são protegidos com base na sua classificação, caráter crítico e valor empresarial; • Manter um inventário rigoroso e atualizado de todos os ativos tecnológicos com o potencial de armazenar ou processar informações. Este inventário deve incluir todos os ativos, ligados ou não à rede da organização (específico do serviço Barclays); • **Os fornecedores com uma configuração de Nível 1, Nível 2 e Nível 3 têm de manter inventários de ativos atualizados, completos e rigorosos (incluindo computadores de secretária, computadores portáteis, equipamento de rede, tokens RSA ou quaisquer ativos fornecidos pelo Barclays);** • Garantir que ativos não autorizados são removidos da rede, colocados em quarentena ou o inventário é atualizado de forma atempada; • Manter uma lista atualizada de todo o software autorizado necessário para a prestação do serviço do Barclays; • Garantir que apenas as aplicações de software ou sistemas operativos atualmente suportados e a receber atualizações do prestador de serviços são adicionados ao inventário de software autorizado da organização. O software não suportado deve ser classificado como "não suportado" no sistema de inventário. O fornecedor deve garantir a implementação de procedimentos eficazes e eficientes para a mitigação de tecnologias não suportadas e o fim de vida, retirada e destruição de ativos e dados para eliminar o risco de comprometimento dos dados.	perda de dados, prejuízos para a reputação e censura regulamentar.
8. Destruição/eliminação /desativação de	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 e, que garanta que os dados do Barclays não são recuperáveis.	A destruição segura de ativos informacionais ajuda a garantir que os ativos informacionais do Barclays não são recuperáveis para serem

informações físicas e lógicas	O fornecedor deve estabelecer políticas e procedimentos com processos empresariais e medidas técnicas de apoio implementados para a eliminação segura e remoção completa dos dados do Barclays dos meios de armazenamento, garantindo que os dados não são recuperáveis através de quaisquer meios forenses informáticos.	utilizados no âmbito de violações ou perdas de dados ou de atividades maliciosas.
9. Segurança de limites e da 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 tem de detetar/prevenir/corrigir o fluxo de informações transferido através das redes com diferentes níveis de confiança, com um foco nos dados que possam danificar a segurança. Os mecanismos de integridade da rede devem cobrir as seguintes áreas: • Manutenção de um inventário atualizado de todos os limites de rede da organização (através de uma arquitetura/diagrama de rede); • O design e implementação da rede têm de ser revistos, pelo menos, uma vez por ano ou, se ocorrer um requisito motivado por um evento que provoque alterações; • As ligações externas à rede do fornecedor devem ser documentadas, encaminhadas por uma firewall e verificadas e aprovadas antes de as ligações serem estabelecidas para prevenir violações da segurança; • As redes do fornecedor são protegidas através da aplicação de princípios "defesa em profundidade" (por ex., segmentação da rede, firewalls, controlos de acesso físicos ao equipamento de rede, etc.); • O fornecedor deve dispor de tecnologias de prevenção da intrusão na rede para detetar e prevenir a entrada de tráfego malicioso na rede; • A utilização de fortes capacidades de firewall na rede para providenciar uma camada de defesa de perímetro contra ataques maliciosos à rede;	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.

	• Todo o tráfego da rede para ou da internet passa por um proxy de camada de aplicação autenticada que foi configurado para filtrar ligações não autorizadas; • Os dispositivos de rede são reforçados em segurança de forma a prevenir um ataque malicioso; • A separação lógica entre as portas/interfaces de gestão de dispositivos e o tráfego do utilizador; controlos de autenticação adequados; • Todas as regras de configuração que permitem o fluxo de tráfego nos dispositivos de rede devem ser documentadas num sistema de gestão de configuração com uma razão empresarial específica para cada regra; • Recusa de comunicação através de portas TCP ou UDP ou tráfego de aplicação não autorizados para garantir que apenas os protocolos autorizados poderão cruzar o limite da rede para dentro ou fora da rede, em cada um dos limites de rede da organização; • Realização de análises regulares de forma de cada limite de rede confiável, a fim de detetar ligações não autorizadas que estejam acessíveis por todo o limite; • Proteção das comunicações entre dispositivos e estações/consola de gestão; • Configuração de sistemas de monitorização para registar os pacotes de rede que passam o limite em cada um dos limites de rede da organização; • Ligação em rede entre gabinetes/fornecedor do serviço de nuvem/centros de dados tem de ser encriptada através de um protocolo de segurança. Os dados Barclays em trânsito dentro da rede alargada (WAN) do fornecedor têm de ser encriptados; • O fornecedor tem de rever as regras da firewall (externa e interna) anualmente; • Todos os acessos sem fios à rede devem estar sujeitos a protocolos de autorização, autenticação, segmentação e encriptação para impedir violações de segurança; • 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;	

	• O acesso por login remoto à rede do fornecedor tem de utilizar uma autenticação multifator. O fornecedor tem de garantir que todos os servidores utilizados para a prestação do serviço ao Barclays não são implantados em redes não confiáveis (redes fora do seu perímetro de segurança, que estejam fora do seu controlo administrativo, por ex., com acesso à internet) sem os devidos controlos de segurança. O fornecedor que acolha informações do Barclays (incluindo um subcontratante) num centro de dados ou nuvem tem de possuir uma certificação ISO/IEC 27001 e/ou SOC 1 ou 2 válida para a gestão de segurança (ou certificação/certificações que demonstrem controlos equivalentes, suportada(s) por um relatório de um auditor independente). Redes T2 e T3: • As redes T2 têm de estar logicamente segregadas da rede corporativa do fornecedor através de uma firewall e todo o tráfego de entrada e saída deve ser restringido e monitorizado; • A configuração do encaminhamento deve garantir apenas ligações à rede do Barclays e não deve encaminhar para quaisquer outras redes do fornecedor; • O router Edge do fornecedor que liga os gateways da extranet do Barclays tem de ser configurado de forma segura, com um conceito que limite os controlos das portas, protocolos e serviços; o Garantir a ativação de registos e monitorização. *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.*	
10. Deteção de recusa de serviço	O fornecedor tem de manter uma capacidade para detetar e proteger contra ataques de Denial of Service (DoS) e Denial of Service Distribuído (DDoS).	Se este princípio não for implementado, o Barclays e os respetivos fornecedores podem não

	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 a disponibilidade.	conseguir impedir que um ataque de recusa de serviço atinja o seu objetivo.
11. Acesso remoto	O acesso remoto à rede do Barclays através da aplicação Citrix Barclays e/ou aos dados Barclays que residem/armazenados no interior do ambiente gerido pelo fornecedor não é fornecido por predefinição nem faz a ligação a partir de locais não aprovados/fora de gabinetes/a partir de casa e qualquer acesso remoto tem de ser aprovado e autorizado pelo Barclays (gabinete do Diretor de segurança - equipa ECAM). O fornecedor tem de garantir o estabelecimento dos seguintes componentes para o acesso remoto: • O acesso por login remoto à rede do fornecedor tem de ser encriptado durante os dados em trânsito e utilizar uma autenticação multifator; • O acesso à rede Barclays tem de ser realizado através de uma aplicação Citrix Barclays, com um token RSA (hard e soft) fornecido pelo Barclays; • O fornecedor deverá manter um inventário de todos os tokens RSA (hard e soft) fornecidos pelo Barclays e um processo de gestão que inclua a revisão e monitorização da distribuição, utilização e retorno dos tokens (hard token); • O fornecedor tem de manter registos dos indivíduos a quem foi pedido para trabalhar remotamente e a justificação para tal pedido; • **O fornecedor deve realizar uma reconciliação de todos os utilizadores remotos trimestralmente e fornecer um certificado ao Barclays (gabinete do Diretor de segurança - equipa ECAM);** • O Barclays procederá à desativação das credenciais de autenticação mediante notificação de que o acesso já não é necessário (por ex., cessação do contrato do funcionário, reatribuição do projeto, etc.) num prazo de **24 (vinte e quatro) horas;**	Os controlos de acesso remoto ajudam a garantir que dispositivos inseguros e não autorizados não estão remotamente ligados ao ambiente Barclays.

<table>
<tr>
<td></td>
<td>

O Barclays desativará prontamente as credenciais de autenticação sempre que estas não tenham sido utilizadas durante um período de tempo (tal período de não utilização não deve exceder um mês);
O fornecedor tem de garantir que o ponto final utilizado para ligar remotamente os sistemas de informação Barclays está configurado de forma segura (por ex., nível de patch, estado do antimalware, etc.);
Os serviços que dispõem de acesso de impressão remoto através da aplicação Citrix Barclays têm de ser autorizados pelo Barclays (gabinete do Diretor de segurança - equipa ECAM). O fornecedor tem de manter registos e realizar uma reconciliação trimestral;
Os dispositivos pessoais/"bring your own device" (BYOD) não podem dispor de acesso ao ambiente Barclays nem aos dados Barclays que residam/armazenados no ambiente gerido pelo fornecedor (incluindo pessoal do fornecedor, consultores, funcionários de contingência, prestadores de serviços e parceiros de serviços geridos).

Nota: o acesso remoto à rede Barclays e os dados Barclays não é permitido exceto se especificamente aprovado e autorizado pelo Barclays.
</td>
<td></td>
</tr>
<tr>
<td>12. Gestão de registos de segurança</td>
<td>
O fornecedor tem de garantir que existe uma estrutura estabelecida de apoio de auditoria e gestão de registos que confirme que os principais sistemas de TI (incluindo aplicações, equipamento de rede, dispositivos de segurança e servidores) estão definidos nos principais eventos de registo, sendo que os registos têm de ser centralizados, protegidos de forma adequada e retidos pelo fornecedor durante um período mínimo de 12 meses.
<table>
<tr><th>Categoria</th><th>Sistemas/serviço de baixo impacto</th><th>Sistemas/serviço de médio impacto</th><th>Sistemas/serviço de alto impacto</th></tr>
</table>
</td>
<td>Se este controlo não for implementado, os fornecedores não poderão detetar nem responder à utilização inadequada ou maliciosa dos seus serviços ou dados num período de tempo razoável.</td>
</tr>
</table>

Retenção dos registos	3 meses	6 meses	12 meses

O processo de gestão de registos deve cobrir as seguintes áreas:

- O fornecedor deve estabelecer políticas e procedimentos para a gestão dos registos;
- O fornecedor deve criar e manter uma infraestrutura de gestão de registos;
- O fornecedor deve definir as funções e responsabilidades de indivíduos e equipas que se espere estejam envolvidos na gestão dos registos;
- Recolha, gestão e análise dos registos de eventos de auditoria que possam ajudar a detetar, compreender ou recuperar de um ataque;
- Ativação do registo de sistema de forma a incluir informações detalhadas como a origem de um evento, data, utilizador, carimbo de data/hora, endereços de origem, endereços de destino e outros elementos úteis;
- Exemplo de registo de eventos:
    - IDS/IPS, router, firewall, proxy Web, software de acesso remoto (VPN), servidores de autenticação, aplicações, registos de bases de dados;
    - Logins bem-sucedidos, tentativas de login falhadas (por exemplo, ID ou palavra-passe de utilizador incorretos), criação, modificação e eliminação de contas de utilizador;
    - Registos de alteração de configuração.
- Os serviços Barclays relacionados com as aplicações empresariais e com os sistemas de infraestruturas técnicas nos quais os registos têm de ser ativados, incluindo aqueles que foram terceirizados ou que se encontram "na nuvem";
- A análise de registos de evento relacionados com a segurança (incluindo normalização, agregação e correlação);
- Sincronização dos carimbos de data/hora nos registos de evento a uma fonte comum e de confiança;

	• Proteção de registos de evento relacionados com a segurança (por ex., através de encriptação, controlo de acesso e cópia de segurança); • Tomada das medidas necessárias para remediar quaisquer problemas identificados e responder a incidentes de cibersegurança de forma rápida e eficaz; • Implementação de ferramentas de gestão da segurança de informações e eventos (SIEM) ou ferramentas analíticas dos registos para uma correlação e análise dos registos; • Implementação de ferramentas conforme adequado para executar a agregação e correlação central, em tempo real, de atividades anómalas, alertas da rede e do sistema e informações sobre eventos e ameaças cibernéticas a partir de múltiplas fontes (internas e externas), para melhor detetar e prevenir ciberataques multifacetados. 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.	
13. Defesas contra malware	O fornecedor tem de estabelecer políticas e procedimentos e implementar processos de apoio ao negócio e medidas técnicas a fim de prevenir a execução de malware em dispositivos de ponto final do utilizador detidos ou geridos pela organização (ou seja, estações de trabalho emitidas, computadores portáteis e dispositivos móveis) e componentes de rede e sistemas da infraestrutura de TI. O fornecedor tem de garantir a aplicação ininterrupta de proteção contra malware em todos os ativos de TI relevantes no intuito de impedir a perturbação do serviço ou violações de segurança. A proteção contra malware deve possuir ou incluir os seguintes elementos:	As soluções antimalware são essenciais para a proteção de ativos informacionais do Barclays contra códigos maliciosos.

	• Software antimalware gerido de forma central para monitorizar e defender continuamente cada uma das estações de trabalho e servidores da organização; • Garantia de que o software antimalware da organização atualiza regularmente o seu motor de análise e a base de dados de assinaturas; • Envio de todos os eventos de deteção de malware para ferramentas de administração antimalware empresariais e servidores de registo de eventos para análise e emissão de alertas; • O fornecedor deve implementar controlos adequados para proteger contra malware móvel e ataques em todos os dispositivos móveis que se ligue às redes do Barclays ou do fornecedor e acedam aos dados Barclays. NB. "Antimalware" deve incluir a deteção de, entre outros, códigos móveis não autorizados, vírus, spyware, software "keylogger", "botnets", "worms", "trojans", etc.	
14. Normas de configuração segura	O fornecedor tem de estabelecer uma estrutura para garantir que todos os sistemas/equipamento de rede configuráveis são configurados de forma segura, de acordo com as normas do setor (por ex., NIST, SANS, CIS). O processo padrão de configuração deve cobrir as seguintes áreas: • Estabelecimento de políticas, procedimentos e ferramentas para as normas de configuração de segurança para todos os dispositivos da rede e sistemas operativos; • Realização de verificações regulares (anuais) de reforço a fim de garantir que qualquer não conformidade com as normas de segurança de referência é prontamente retificada. Verificações e monitorização adequadas são aplicadas de forma a garantir a manutenção da integridade das construções/dispositivos; • Os sistemas e dispositivos de rede são configurados de forma a funcionar de acordo com princípios de segurança (por ex., o conceito de limitar os controlos de portas, protocolos e serviços e inexistência de software não autorizado).	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.

	Garantir que a gestão da configuração governa normas de configuração seguras em todas as classes de ativos e deteta, alerta e responde eficazmente a alterações ou desvios da configuração.	
15. Segurança de ponto final	O fornecedor tem de garantir que os pontos finais utilizados para aceder à rede do Barclays, ou para aceder/processar dados do Barclays, são reforçados para proteção contra ataques. A construção de segurança de pontos finais tem de possuir: • Encriptação de discos; • Desativação de todo o software/serviços/portas desnecessários; • Desativação do acesso por direitos de administração para os utilizadores locais; • O pessoal do fornecedor não poderá alterar as definições básicas, como o Pacote de serviço predefinido, a partição do sistema e serviços predefinidos, etc.; • A porta USB tem de ser desativada de forma a proibir a cópia de dados Barclays para meios externos; • Atualização com as assinaturas de antivírus e "patches" de segurança mais recentes; • Prevenção de perda de dados limitada a impossibilidade de "cortar-copiar-colar" e captura de ecrã de dados Barclays; • Por predefinição, o acesso à impressora tem de estar desativado; • O fornecedor deve restringir a capacidade de aceder a websites de redes sociais, serviços de "webmail" e websites com a capacidade de armazenar informações na internet, como o Google Drive, Dropbox, iCloud; • A partilha/transferência de dados Barclays deve ser desativada utilizando ferramentas/software de mensagens instantâneas; • Capacidade e processos para detetar software não autorizado identificado como malicioso e prevenir a instalação de software não autorizado.	Se este controlo não for implementado, a rede e os pontos finais do Barclays e do fornecedor podem ficar vulneráveis a ciberataques.

	NB. Os meios amovíveis/dispositivos portáteis devem ser desativados por predefinição e apenas ativados por motivos empresariais legítimos. O fornecedor deve manter imagens ou modelos seguros para todos os sistemas na empresa com base nas normas de configuração aprovadas pela organização. Qualquer implementação de sistema novo ou sistema existente que fique comprometido deve ser duplicado (impresso) utilizando uma dessas imagens ou modelos. Dispositivos móveis utilizados para os serviços Barclays: 1. O fornecedor tem de garantir que implementa capacidades de gestão de dispositivos móveis (MDM) a fim de controlar e gerir, de forma segura, os dispositivos móveis ao longo do ciclo de vida e que tenham acesso e/ou contenham informação classificada do Barclays, reduzindo o risco de comprometimento dos dados; 2. O fornecedor tem de garantir a implementação de capacidades de bloqueio e eliminação remotos de dispositivos móveis com vista à proteção das informações na eventualidade de um dispositivo ser perdido, furtado ou comprometido; 3. Encriptação de dados de dispositivos móveis (dados Barclays); 4. Todos os serviços baseados na nuvem não devem ser permitidos (por predefinição) nos dispositivos móveis disponibilizados pelo fornecedor.	

16. Prevenção de fuga de dados	O fornecedor tem de estabelecer uma estrutura para garantir a aplicação de proteção contra a fuga inadequada de dados, assegurando que a proteção inclui os seguintes canais de fuga de dados (entre outros):
	
	• Transferência não autorizada de informações para fora da rede interna/da rede do fornecedor;
	  ○ E-mail
	  ○ Internet/gateway Web (incluindo armazenamento online e "webmail")
		Devem ser operados eficazmente controlos adequados de modo a garantir que a informação do Barclays se restringe àqueles que a ela devem ter acesso (confidencialidade), que se encontra protegida de alterações não

	• 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.	autorizadas (integridade) e que pode ser recuperada e apresentada quando solicitado (disponibilidade). A não implementação destes requisitos poderá fazer com que a informação sensível do Barclays fique vulnerável a modificação, divulgação, acesso, danos, perda ou destruição não autorizados, o que poderá resultar em sanções legais e regulamentares, prejuízos para a reputação ou perda/perturbação dos negócios.
17. Proteção de dados	O fornecedor tem de garantir que os dados Barclays mantidos sob custódia/na rede do fornecedor dispõem de proteção de dados alcançada através de uma combinação de técnicas de encriptação, proteção de integridade e prevenção de perda de dados. É importante tomar os devidos cuidados para limitar o acesso aos dados Barclays. Os controlos de proteção de dados devem cobrir as seguintes áreas: 1. Devem ser estabelecidas políticas e procedimentos e implementados processos empresariais de suporte e medidas técnicas, de forma a inventariar, documentar e manter fluxos de dados relativamente aos dados mantidos (de forma permanente ou temporária) nas aplicações (físicas e virtuais) de distribuição geográfica do serviço e nos componentes da rede de infraestrutura e sistema e/ou partilhados com terceiros; 2. Manutenção de um inventário de todas as informações sensíveis (dados Barclays) armazenados, processados ou transmitidos pelo fornecedor; 3. Estabelecimento de normas de classificação de dados a fim de garantir a classificação e proteção devida das informações sensíveis (dados Barclays); 4. Garantia de que todos os dados na organização são marcados com base na norma de classificação de dados; 5. Política de utilização de dados - acesso a dados; 6. Proteção de dados inativos; a. Encriptação dos dados inativos a fim de prevenir a exploração de informações sensíveis através de acessos não autorizados.	

	7. Monitorização da atividade da base de dados; a. Monitorizar o acesso e a atividade da base de dados para identificar atividades maliciosas de forma rápida e eficaz. 8. Proteção de dados em uso; a. Garantia de que a visualização e utilização de informações sensíveis são controladas através de capacidades de gestão do acesso a fim de proteger contra a exploração de informações sensíveis; b. Utilização de mascaramento de dados e tecnologias de ocultação para proteger eficazmente os dados sensíveis em uso contra uma divulgação inadvertida e/ou exploração maliciosa. 9. Proteção de dados em trânsito; a. Utilização de capacidades de encriptação fortes para garantir a proteção dos dados em trânsito; b. A encriptação dos dados em trânsito é, normalmente, efetuada através de encriptação de transporte ou payload (mensagem ou campo seletivo). Os mecanismos de encriptação de transporte incluem, entre outros: • "Transport Layer Security" (TLS) • Túnel seguro (IPsec) • "Secure Shell" (SSH) c. Os protocolos de segurança no transporte têm de ser configurados de forma a prevenir a negociação de algoritmos mais fracos e/ou extensões de chaves mais curtas, quando ambos os pontos finais suportam a opção mais forte.	

	10. Cópia de segurança de dados; a. Adoção de disposições para garantir que a informação é devidamente salvaguardada e recuperável em conformidade com os requisitos acordados com o Barclays; b. Garantia de que as cópias de segurança são devidamente protegidas através de segurança física ou encriptação durante o seu armazenamento, bem como quando são movidas pela rede. Esta condição inclui as cópias de segurança remotas e os serviços na nuvem; c. Garantia de que todos os dados Barclays são submetidos a uma cópia de segurança de forma automática e de forma regular.	
18. Segurança de software de aplicação	O fornecedor tem de desenvolver aplicações 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 apoiar o serviço prestado ao Barclays, o fornecedor tem de estabelecer uma estrutura de desenvolvimento segura a fim de prevenir violações da segurança e de identificar e resolver vulnerabilidades no código durante o processo de desenvolvimento. A segurança de software de aplicação deve cobrir as seguintes áreas:	Os controlos que protegem o desenvolvimento da aplicação ajudam a garantir que as aplicações estão protegidas no momento da implementação.

	• Devem ser implementadas e adotadas normas de codificação segura de acordo com as Boas Práticas do setor a fim de prevenir vulnerabilidades de segurança e interrupções de serviço, defendendo, simultaneamente, contra possíveis vulnerabilidades bem conhecidas; • Estabelecimento de práticas de codificação seguras e adequadas à linguagem de programação; • Todo o desenvolvimento tem de ser executado num ambiente que não envolva produção; • Manutenção de ambientes separados para os sistemas de produção e não produção; Os programadores não devem ter acesso não monitorizado a ambientes de produção; • Segregação de deveres para os ambientes de produção e não produção; • os sistemas são desenvolvidos em linha com as melhores práticas de desenvolvimento (por ex., OWASP); • O código deve ser armazenado de forma segura e submetido a processos de garantia de qualidade; • O código deve ser devidamente protegido contra modificação não autorizada assim que os testes sejam aprovados e entregues à produção; • Utilização apenas de componentes de terceiros atualizados e de confiança para o software desenvolvido pelo fornecedor; • Aplicação de ferramentas de análise estática e dinâmica para garantir a adesão a práticas de codificação seguras; • O fornecedor tem de garantir que os dados dinâmicos (incluindo dados pessoais) não serão utilizados em ambientes de não produção; • As aplicações e interfaces de programação (API) deverão ser concebidas, desenvolvidas, implementadas e testadas de acordo com as principais normas do setor (por ex., OWASP para aplicações Web). O fornecedor deve proteger as aplicações Web mediante a implementação de firewalls para aplicações Web (WAF) que analisem todo o tráfego que flua na aplicação em	

	questão e identifique ataques comuns às aplicações Web. Para as aplicações não baseadas na Web, devem ser implementadas firewalls de aplicações específicas se estiverem disponíveis tais ferramentas para o tipo de aplicação em questão. Se o tráfego for encriptado, o dispositivo deverá manter-se por detrás da encriptação ou conseguir desencriptar o tráfego antes da análise. Se nenhuma destas opções for adequada, deve ser implementada uma firewall de aplicação Web baseada no anfitrião.	

19. 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. Os processos de gestão de acesso devem ser definidos de acordo com as boas práticas do setor, devendo incluir o seguinte: • O fornecedor deve garantir que os processos de gestão de acesso devem ser documentados e aplicados a todos os sistema de TI (que armazenam e processam os Ativos de Informação do Barclays) e quando implementados, devem fornecer controlos adequados para: novos colaboradores/transferências/colaboradores que cessam funções/acessos remotos.	Controlos LAM apropriados ajudam a garantir que os ativos informacionais são protegidos contra utilização indevida. Devem ser eficazmente operados controlos adequados, de modo a garantir que a informação do Barclays se restringe àqueles que a ela devem ter acesso (confidencialidade), que se encontra protegida de alterações não autorizadas (integridade) e que pode ser recuperada e apresentada quando solicitado (disponibilidade). A não implementação destes requisitos poderá fazer com que a informação sensível do Barclays fique vulnerável a modificação, divulgação, acesso, danos, perda ou destruição não autorizados, o que poderá resultar em sanções legais e regulamentares, prejuízos para a reputação ou perda/perturbação dos negócios.

	• Devem ser implementados controlos para autorização, de modo a assegurar que o processo de concessão, modificação e revogação do acesso inclui um nível de autorização correspondente aos privilégios que estão a ser concedidos. • Devem ser implementados controlos para garantir que os processos de gestão de acesso incluem mecanismos adequados para a verificação de identidade. • Cada conta tem de ser associada a um indivíduo, que deve ser responsável por qualquer atividade realizada com acesso à mesma. • Retificação de acesso - devem ser implementados controlos a fim de garantir que as permissões de acesso são revistas pelo menos a cada 12 meses, de modo a assegurar que correspondem ao seu objetivo. • Todas as permissões de acesso privilegiado devem ser revistas a, pelo menos, cada seis (6) meses e devem ser implementados controlos adequados para requisitos de acesso privilegiado. • Controlo dos colaboradores transferidos – acesso alterado no prazo de 24 horas 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. • Acesso remoto - os controlos de acesso remoto só podem ser permitidos através de mecanismos acordados pelo Barclays (gabinete do Diretor de segurança - equipa ECAM) e o acesso remoto tem de utilizar autenticação multifator. • Autenticação - comprimento e complexidade de palavras-passe adequada, frequência das alterações das palavras-passe, autenticação multifator, gestão segura das credenciais de palavra-passe ou outros controlos têm de ser seguidos de acordo com as melhores práticas do setor. • Contas inativas - não utilizadas por um período igual ou superior a 60 dias consecutivos devem ser suspensas/desativadas. •	

	• As palavras-passe para contas interativas devem ser alteradas pelo menos a cada 90 dias e devem ser diferentes das 12 (doze) palavras-passe anteriores. • As contas privilegiadas devem ser alteradas após cada utilização e, no mínimo, a cada 90 dias. • As contas interativas devem ser desativadas após um máximo de 5 (cinco) tentativas de acesso consecutivas falhadas.	
20. Gestão de vulnerabilidade	O fornecedor tem de estabelecer políticas e procedimentos e implementar processos de apoio e medidas técnicas para a deteção atempada de vulnerabilidades dentro das aplicações detidas ou geridas pela organização, da rede da infraestrutura e dos componentes do sistema, a fim de garantir a eficiência dos controlos de segurança implementados. A gestão de vulnerabilidades deve cobrir as seguintes áreas: • Estabelecimento de políticas e procedimentos e implementação de processos de apoio e medidas técnicas para a deteção atempada de vulnerabilidades dentro das aplicações detidas ou geridas pela organização, da rede da infraestrutura e dos componentes do sistema, a fim de garantir a eficiência dos controlos de segurança implementados; • Cargos e responsabilidades definidos; • Ferramentas e infraestrutura adequadas para análise de vulnerabilidades; • Realização de análises de vulnerabilidades de forma rotineira, de forma a identificar eficazmente vulnerabilidades conhecidas e desconhecidas em todas as classes de ativos no ambiente; • Utilização de um processo de classificação do risco para dar prioridade à resolução das vulnerabilidades detetadas; • Estabelecimento de um processo de validação de resolução de vulnerabilidades que verifique rápida e eficazmente a resolução de vulnerabilidades em todas as classes de ativos no ambiente;	Se este controlo não for implementado, os atacantes podem explorar as vulnerabilidades dos sistemas para realizarem ciberataques contra o Barclays e os respetivos fornecedores.

	• Garantia de que as vulnerabilidades são tratadas de forma eficaz através de atividades de resolução robustas e gestão de "patches" para reduzir o risco de exploração de vulnerabilidades; • Comparação regular dos resultados das análises consecutivas das vulnerabilidades a fim de verificar quais destas foram resolvidas de forma atempada. Todos os problemas de segurança e vulnerabilidades passíveis de afetar substancialmente a infraestrutura de alojamento/aplicações Web do Barclays disponibilizadas pelo fornecedor e cujos riscos o fornecedor tenha decidido assumir têm de ser comunicados ao Barclays de imediato e acordados com o Barclays por escrito (gabinete do Diretor de segurança - equipa ECAM).	
21. Gestão de patch	O fornecedor tem de estabelecer políticas e procedimentos e implementar processos de apoio ao negócio e medidas técnicas a fim de implementar "patches" de segurança em dispositivos de ponto final do utilizador geridos (por ex., estações de trabalho emitidas, computadores portáteis e dispositivos móveis) e componentes de rede e sistemas da infraestrutura de TI. O fornecedor tem de garantir que são atempadamente aplicados os "patches" de segurança mais recentes aos sistemas/ativos/redes/aplicações, assegurando que: • O fornecedor deve testar todos os "patches" nos sistemas que representem de forma rigorosa a configuração dos sistemas de produção alvo antes da implementação nos sistemas de produção e garantir a verificação do funcionamento correto do serviço de "patch" antes de qualquer atividade do patch. Se o sistema não puder receber "patches", será necessário implementar contramedidas adequadas; • Todas as alterações essenciais de TI anteriores à implementação devem ser registadas, testadas e aprovadas através de um processo de gestão de alterações	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.

	aprovado e consistente para prevenir qualquer perturbação nos serviços ou violações de segurança; • O fornecedor tem de garantir que os "patches" são refletidos nos ambientes de produção e de DR.	
22. 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, incluindo o ponto de recuperação de desastres e as aplicações Web referentes ao(s) serviço(s) disponibilizado(s) 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. O teste deve ser efetuado de acordo com as Boas Práticas do setor. Relativamente aos serviços prestados pelo fornecedor relacionados com a infraestrutura de alojamento/aplicação em nome do 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. • Todos e quaisquer riscos assumidos têm de ser comunicados e acordados com o Barclays (gabinete do Diretor de segurança - equipa ECAM).	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. A informação Barclays pode ser divulgada e/ou poderá ocorrer perda de serviços que resulte em sanções legais e regulamentares ou em danos para a reputação.
23. Criptografia	• Lógica da criptografia - o fornecedor tem de documentar a lógica subjacente à utilização de tecnologia criptográfica e alisar modo a garantir que continuam a ser adequada para a finalidade; • Procedimentos do ciclo de vida da criptografia - o fornecedor tem de possuir e manter um conjunto de procedimentos de gestão do ciclo de vida da criptografia	Se este controlo não for implementado, poderão não existir controlos técnicos e físicos, originando atrasos e perturbações de serviço ou violações de cibersegurança.

	que detalhem os processos "ponto a ponto" para a gestão de chaves, desde a geração ao carregamento, distribuição e destruição; • Aprovação manual de operações - o fornecedor tem de garantir que todos os eventos geridos por humanos para chaves e certificados digitais (incluindo o registo e geração de novas chaves e certificados) são aprovados no nível adequado, sendo retido um registo da aprovação; • Certificados digitais - o fornecedor tem de garantir que todos os certificados são adquiridos a um conjunto de Autoridades de certificação (CA) que prestam serviços de revogação e políticas de gestão de certificados; tem ainda de garantir que os certificados autoassinados são utilizados apenas nas situações em que é tecnicamente impossível suportar uma solução baseada na CA e tem de dispor de controlos manuais em vigor para garantir a integridade, autenticidade das chaves, alcançando-se a revogação e renovação atempada; • Geração de chaves e "criptoperiod" - o fornecedor tem de garantir que todas as chaves são geradas aleatoriamente pelo hardware certificado ou por um Gerador de números pseudoaleatórios criptograficamente seguro (CSPRNG) no software; o O fornecedor tem de garantir que todas as chaves são, depois, submetidas a um período de vida ("criptoperiod") definido e limitado, sendo substituídas ou desativadas após este período. Este requisito também deve estar em linha com os requisitos do National Institute of Standards and Technology (NIST) e outros requisitos do setor aplicáveis. • Proteção do armazenamento de chaves - o fornecedor tem de garantir que as chaves criptográficas secretas/privadas existem apenas nas seguintes formas: o No limite criptográfico de um dispositivo/módulo certificado por hardware; o Na forma criptográfica sob outra chave estabelecida ou derivada de palavra-passe; o Nas partes de componentes divididos, dividir entre grupos de depositários distintos;	

	○ Limpeza da memória do anfitrião referente ao período da operação criptográfica, exceto se exigido para proteção de HSM. • O fornecedor tem de garantir que as chaves são geradas e mantidas dentro do limite da memória dos HSM para chaves de alto risco. Isso inclui: ○ Chaves de serviços regulados nos quais os HSM são mandatados; ○ Certificados que representam o Barclays nas CA públicas; ○ Certificados de raiz, de emissão, OCSP e RA (autoridade de registo) utilizados para emissão de certificados que protejam os serviços Barclays; ○ Chaves que protejam repositórios de chaves agregados e armazenados, credenciais de autenticação ou dados PII. • Cópia de segurança e armazenamento de chaves - o fornecedor mantém uma cópia de segurança de todas as chaves a fim de prevenir a interrupção do serviço se as chaves forem corrompidas ou necessitarem de ser restauradas. O acesso às cópias de segurança é restrito a locais protegidos sob conhecimento dividido e controlo dual. As cópias de segurança de chaves têm de ter, pelo menos, uma proteção criptográfica nas mesmas, bem como nas chaves em uso; • Inventário - o fornecedor mantém um inventário completo e atualizado da utilização criptográfica nos serviços por este prestados ao Barclays, que detalhe todas as chaves criptográficas, certificados digitais, software criptográfico e hardware criptográfico geridos pelo fornecedor a fim de prevenir danos em caso de acidente. É evidenciado pela assinatura do inventário revista, pelo menos, a cada trimestre e fornecida ao Barclays. Os inventários têm de incluir, sempre que relevante: ○ Equipa de suporte de TI; ○ Ativos associados; ○ Algoritmos, comprimento das chaves, ambiente, hierarquia das chaves, autoridade certificadora, impressão digital, proteção de armazenamento de chaves e finalidade técnica e operacional.	

	• Finalidade funcional e operacional - as chaves têm de ter uma única finalidade funcional e operacional e não podem ser partilhadas entre múltiplos serviços ou fora do âmbito dos serviços Barclays; • Pistas de auditoria - o fornecedor deve realizar e reter evidências de uma análise aos registos auditável a cada trimestre, pelo menos, para todos os eventos de gestão do ciclo de vida de chaves e certificados, que demonstre uma cadeia completa da custódia de todas as chaves, incluindo a geração, distribuição, carregamento e destruição, a fim de detetar qualquer utilização não autorizada; • Hardware - o fornecedor armazena os dispositivos de hardware em zonas seguras e mantém pistas de auditoria ao longo do ciclo de vida das chaves, por forma a garantir que a cadeia de custódia dos dispositivos criptográficos não é comprometida. Estas pistas são revistas trimestralmente; o O fornecedor tem de garantir que o hardware criptográfico é certificado, no mínimo, com um Nível 2 FIPS140-2 e que alcança o Nível 3 na Gestão de segurança física e de chaves criptográficas ou PCI HSM. O fornecedor pode escolher permitir cartões inteligentes com base em chips ou tokens eletrónicos certificados pelo FIPS como hardware aceitável para o armazenamento de chaves que representem e sejam detidas por pessoas singulares ou clientes (mantidas fora do local). • Comprometimento de chaves - o fornecedor mantém e monitoriza um plano de comprometimento de chaves por forma a garantir a geração de chaves de substituição, independentemente da chave comprometida, a fim de impedir que a chave comprometida forneça informações relativas à sua substituição. Se ocorrer um incidente que envolva um comprometimento, o Barclays deve ser notificado através do endereço de e-mail **"Chief Security Office" (Gabinete do Diretor de Segurança, CSO) do Barclays, "Joint Operations Centre" (Centro de Operações Conjuntas, JOC) - gcsojoc@barclays.com.** • Grau de segurança de algoritmos e chaves - o fornecedor assegura que os algoritmos e o comprimento das chaves utilizadas estão em conformidade com os	

	requisitos do National Institute of Standards and Technology (NIST) e outras normas do setor aplicáveis; o Algoritmos fortes e um comprimento das chaves adequado minimizam o risco de perda ou comprometimento de dados sensíveis por parte de "hackers" com capacidades de processamento sofisticadas; o A intensidade da encriptação implementada tem de ser conforme à apetência pelo risco, visto que pode ter um impacto operacional ou no desempenho.	
24. Computação em nuvem	O fornecedor tem de possuir uma certificação ISO/IEC 27017 ou 27001 ou SOC 1 ou 2 estabelecida e de apoio a processos empresariais, bem como medidas técnicas implementadas para garantir que qualquer utilização da tecnologia na nuvem é sujeita a controlos de segurança adequados devidamente implementados. os dados Barclays armazenados na nuvem como parte do serviço prestado ao Barclays têm de ser aprovados pelo mesmo (gabinete do Diretor de segurança - equipa ECAM). Os controlos na nuvem devem abranger os seguintes modelos de implementação (IaaS/PaaS/SaaS): • Gestão de identidade e acesso/controlo de acesso; • Conectividade da rede; • Proteção de dados (em trânsito/inativos/armazenados); • Registo e monitorização de segurança; • Encriptação e gestão de chaves; • Segurança da aplicação e interface; • Segurança da infraestrutura e virtualização; • Segregação de serviços.	Se este controlo não for implementado, os dados do Barclays incorretamente protegidos podem ficar comprometidos, o que pode resultar em sanções legais e regulamentares ou em danos para a reputação.

25. Espaço Dedicado do Banco (BDS)	Para serviços fornecidos que requeiram Espaço Dedicado do Banco (BDS) formal, devem ser implementados BDS específicos físicos e requisitos técnicos. (Se o BDS constituir um requisito do serviço, os requisitos de controlo serão aplicáveis.) Os diferentes tipos de BDS são: Nível 1 (primeira classe) - toda a infraestrutura de TI gerida é pelo **Barclays** através da disponibilização de uma LAN, WAN e ambiente de trabalho geridos pelo **Barclays** a um local do fornecedor com um espaço dedicado ao Barclays. Nível 2 (classe executiva) - toda a infraestrutura de TI gerida é pelo **fornecedor** ligando a gateways do **Barclays** - LAN, WAN e ambiente de trabalho são detidos e geridos pelo fornecedor. Nível 3 (classe económica) - toda a infraestrutura de TI gerida é pelo **fornecedor** ligando a gateways do **Barclays** - LAN, WAN e dispositivos de ambiente de trabalho são detidos e geridos pelo fornecedor.	Se este controlo não for implementado, poderão não existir controlos técnicos e físicos, originando atrasos e perturbações de serviço ou violações de cibersegurança.
25.1 BDS - Separação física	A área física ocupada deve ser dedicada ao Barclays e não partilhada com outras empresas/prestadores de serviços. Deve ser lógica e fisicamente segregada.	
25.2 BDS - Controlo de acesso físico	• O fornecedor tem de dispor de um processo de acesso físico que abranja métodos de acesso e autorização ao BDS sempre que os serviços sejam prestados; • A entrada e saída de zonas do BDS têm de ser limitadas e monitorizadas por mecanismos de controlo de acesso físico a fim de garantir que apenas o pessoal autorizado dispõe de acesso; • Um cartão de acesso eletrónico autorizado, para aceder às zonas do BDS; • O fornecedor tem de conduzir verificações trimestrais para garantir que apenas os indivíduos autorizados têm acesso ao BDS. As exceções são exaustivamente investigadas até à sua resolução; • Os direitos de acesso são eliminados num prazo de 24 horas para todos os colaboradores que cessem funções e que sejam transferidos; • Utilizar salvaguardas para patrulhar, de forma rotineira, o interior do BDS por forma a identificar eficazmente os acessos não autorizados ou atividade potencialmente maliciosa;	

	• Os controlos automáticos seguros devem estar em funcionamento para o acesso ao BDS, incluindo: Se para pessoal autorizado: o Crachá com fotografia de identificação sempre visível; o Leitores de cartões implementados nas proximidades; o Mecanismo antirretorno ativado; • O fornecedor tem de dispor de processos e procedimentos para o controlo e monitorização de pessoas externas, incluindo terceiros com acesso físico às zonas do BDS para efeitos de manutenção e limpeza.
25.3 BDS - Videovigilância	• Implementar sistemas de videovigilância para as zonas do BDS a fim de detetar, de forma eficaz, qualquer acesso não autorizado ou atividade maliciosa e auxiliar nas investigações; • Todos os pontos de entrada e saída da zona BDS devem contar com videovigilância; • As câmaras de segurança são posicionadas adequadamente e providenciam imagens claras e identificáveis em todos os momentos, a fim de captar qualquer atividade maliciosa e auxiliar nas investigações. O fornecedor tem de armazenar as gravações do CCTV durante 30 dias e todas as gravações e gravadores do CCTV têm de estar situados em locais seguros para prevenir a sua modificação, eliminação ou a visualização "casual" de quaisquer ecrãs de CCTV associados; o acesso às gravações tem de ser controlado e limitado às pessoas autorizadas.
25.4 BDS - Acesso à rede Barclays e aos tokens de autenticação do Barclays	• Todos os utilizadores individuais devem apenas efetuar a sua autenticação na rede do Barclays a partir do BDS utilizando o token de autenticação multifator fornecido pelo Barclays; • O fornecedor tem de manter registos dos indivíduos que receberam tokens de autenticação do Barclays e trimestralmente o fornecedor tem de elaborar uma reconciliação; • O Barclays procederá à desativação das credenciais de autenticação mediante notificação de que o acesso já não é necessário (por ex., cessação do contrato do funcionário, reatribuição do projeto, etc.) num prazo de 24 (vinte e quatro) horas; • O Barclays desativará prontamente as credenciais de autenticação sempre que estas não tenham sido utilizadas durante um período de tempo (tal período de não utilização não deve exceder um mês); • Os serviços que dispõem de acesso de impressão remoto através da aplicação Citrix Barclays têm de ser autorizados pelo Barclays (gabinete do Diretor de segurança - equipa ECAM). O fornecedor tem de manter registos e realizar uma reconciliação trimestral.

	Consultar a Secção 11 - Segurança do acesso remoto
25.5 BDS - Assistência fora de expediente	O acesso remoto ao ambiente BDS não é fornecido por predefinição para assistência fora do horário de expediente/fora do horário de funcionamento/trabalho a partir de cada. Qualquer acesso remoto deve ser aprovado pelas equipas do Barclays relevantes (incluindo o gabinete do Diretor de segurança - equipa ECAM).
25.6 BDS - Segurança da rede	• Manutenção de um inventário atualizado de todos os limites de rede da organização (através de uma arquitetura/diagrama de rede); • O design e implementação da rede tem de ser revista, pelo menos, uma vez por ano; • A rede do BDS tem de estar logicamente segregada da rede corporativa do fornecedor através de uma firewall e todo o tráfego de entrada e saída deve ser restringido e monitorizado; • A configuração do encaminhamento deve garantir apenas ligações à rede do Barclays e não deve encaminhar para quaisquer outras redes do fornecedor; • O router Edge do fornecedor que liga os gateways da extranet do Barclays tem de ser configurado de forma segura, com um conceito que limite os controlos das portas, protocolos e serviços; o Garantir a ativação de registos e monitorização. • A rede do BDS tem de ser monitorizada e apenas dispositivos autorizados passam pelos controlos de acesso à rede adequados. Consultar a Secção 9 - Segurança de limites e da rede
25.7 BDS - Rede sem fios	As redes sem fios têm de ser desativadas no segmento da rede do Barclays relativo à provisão dos serviços Barclays.
25.8 BDS - Segurança de pontos finais	Devem ser configuradas construções de computadores seguras segundo as melhores práticas do setor centro da rede do BDS. A construção da segurança dos dispositivos de ponto final do BDS tem de possuir: • Encriptação de discos; • O arranque a partir de outros dispositivos ativos deve ser desativado; • Desativação de todo o software/serviços/portas desnecessários; • Desativação do acesso por direitos de administração para os utilizadores locais;

	• O pessoal do fornecedor não poderá alterar as definições básicas, como o Pacote de serviço predefinido e serviços predefinidos, etc.; • A porta USB tem de ser desativada de forma a proibir a cópia de dados Barclays para meios externos; • Atualização com as assinaturas de antivírus e "patches" de segurança mais recentes; • Prevenção de perda de dados limitada a impossibilidade de "cortar-copiar-colar" e a ferramenta de captura de ecrã ou impressão da captura de dados Barclays; • Por predefinição, o acesso à impressora tem de estar desativado; • A partilha/transferência de dados Barclays deve ser desativada utilizando ferramentas/software de mensagens instantâneas; • Capacidade e processos para detetar software não autorizado identificado como malicioso e prevenir a instalação de software não autorizado. Consultar a Secção 15 - Controlo da segurança de pontos finais

25.9 BDS - 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 do BDS;
	• O fornecedor deve restringir a capacidade de aceder a websites de redes sociais, serviços de "webmail" e websites com a capacidade de armazenar informações na internet, como o Google Drive, Dropbox, iCloud;
	• A transferência não autorizada de dados Barclays para fora da rede do BDS tem de ser protegida contra fugas de dados:
	  • E-mail
	  • Internet/gateway Web (incluindo armazenamento online e "webmail")
	• Implementação de filtros de URL com base na rede que limitem a capacidade de um sistema se ligar apenas a websites internos ou na internet relacionados com a organização do fornecedor;
	• Bloqueio de todos os anexos e/ou carregamento da funcionalidade para websites;
	• Garantia de que são permitidos apenas browsers e clientes de e-mail totalmente suportados.

25.10 BDS - Opção "Bring your own device"/dispositivo pessoal	**Os dispositivos pessoais/opção "bring your own device" não podem ter acesso ao ambiente Barclays e/ou aos dados Barclays**

Direito de inspeção	O fornecedor tem de permitir ao Barclays, mediante notificação por escrito do Barclays pelo menos 10 (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 também tem de permitir que o Barclays realize uma inspeção no mínimo anual ou imediatamente após um incidente de segurança. Qualquer não conformidade dos controlos identificada pelo Barclays durante uma inspeção tem de ser avaliada pelo Barclays e o Barclays deve especificar um prazo de resolução. O fornecedor deve, então, implementar qualquer resolução necessária dentro desse prazo. O fornecedor tem de disponibilizar todo o apoio razoavelmente solicitado pelo Barclays relativamente a qualquer inspeção e a documentação enviada durante a inspeção deve ser preenchida e devolvida ao Barclays.	Se tal não for acordado, os fornecedores não conseguirão garantir totalmente a conformidade com estas obrigações de segurança.

Anexo A: Glossário

Definições	
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.

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.
Espaço Dedicado do Banco	Por Espaço Dedicado do Banco (BDS) 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.
BYOD	"Bring your own devices"
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.
Dados	Registo de factos, conceitos ou instruções num meio de armazenamento para comunicação, recuperação e processamento por um meio automático e apresentação sob a forma de informações compreensíveis pelos humanos.
Recusa de serviço (Ataque)	Uma tentativa de tornar um recurso informático indisponível para os utilizadores a que se destina.
Destruição/eliminação	O ato de sobregravar, apagar ou destruir fisicamente informações de tal forma que não é possível recuperá-las.
ECAM	Equipa de "External Cyber Assurance and Monitoring" (Garantia e monitorização cibernética externa) que avalia a postura do fornecedor em termos de segurança.
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.
HSM	"Hardware Security Module" (módulo de segurança de hardware). Dispositivo dedicado que providencia a geração, armazenamento e utilização de uma chave criptográfica segura, incluindo a aceleração dos processos criptográficos.
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.
Responsável pelo ativo informacional	A pessoa que, na organização, é responsável por classificar um ativo e garantir que este é tratado corretamente.
Privilégio mínimo	O nível mínimo de acesso/permissões que permite que um utilizador ou conta desempenhe as respetivas funções.

Dispositivo de rede/equipamento de rede	Qualquer dispositivo de TI ligado a uma rede que é utilizada para gerir, apoiar ou controlar uma rede. Isso pode incluir, entre outros, routers, comutadores, firewalls, balanceadores de carga.
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, trojans e worms de computador.
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).
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.
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.
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.
Deve	Esta definição significa que as implicações serão entendidas e cuidadosamente avaliadas antes de se escolher uma opção diferente.
Incidente de segurança	Os incidentes de segurança são definidos como aqueles eventos que violam uma política de segurança explícita ou implícita. • Tentativas (falhadas ou bem-sucedidas) de obter acesso não autorizado a um sistema ou seus dados; • Interrupção indesejada ou ataques "denial of service"; • Utilização não autorizada de um sistema para o processamento ou armazenamento de dados;

	• Alterações às características do hardware, firmware ou software do sistema sem o conhecimento, instruções ou consentimento do proprietário; • Vulnerabilidade de uma aplicação, que resulta no acesso não autorizado a dados.

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 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)
Restrita – Interna	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	• Estratégias e orçamentos • Avaliações de desempenho • Remuneração dos colaboradores e dados pessoais • Avaliações de vulnerabilidade

	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.	
Restrito - Externo	As informações têm de ser classificadas como **restritas - internas** 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 • Resultados e relatórios de auditorias

Não restrito	As informações têm de ser classificadas como "Não restritas" se 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	Secreto	Restrito – Interno	Restrito – Externo
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 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 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.

	• 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 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 (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.
Partilha	• Os ativos em papel têm de incluir uma etiqueta de informação visível em todas as páginas.	• 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 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 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 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 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.

	• 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.		• 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.
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 suportes onde ativos eletrónicos secretos tiverem sido guardados têm de ser devidamente limpos antes ou durante a 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.

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 "CID"). O fornecedor tem de rever os documentos que destacam as funções e responsabilidades referentes aos CID 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 CID (para consultar a definição de CID, ver Anexo A). O número de pessoas com acesso a CID tem de ser mantido no mínimo, com base no princípio da necessidade de conhecer os dados.	Uma clara definição das funções e responsabilidades auxilia a implementação do plano de obrigações de controlo de fornecedor externo.

2. Relato de violação de CID	Têm de existir controlos e processos documentados por forma a garantir que quaisquer violações com impacto nos CID 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 entidade Barclays correspondente, com o 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 CID. 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. No caso de o fornecedor externo oferecer serviços de consultoria e um funcionário desse fornecedor ter despoletado incidentes de prevenção de perda de dados, o Banco notificará o incidente ao fornecedor e, sempre que aplicável, o banco tem o direito de solicitar a substituição do funcionário.	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 CID 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 CID e/ou que os tratem têm de realizar uma formação* que introduza os requisitos de segredo bancário de CID 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 CID 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 CID. 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 E, Tabela E1) 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 CID estão previstos na Tabela E2 do Anexo E. * "***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 CID (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 da informação dos CID, tendo em conta o perfil de elevado risco que apresentam.	Se este princípio não for implementado, os dados de identificação do cliente (CID) incorretamente protegidos podem ficar comprometidos, o que pode resultar em sanções legais e regulamentares ou em prejuízos para a reputação.

Anexo C: Glossário

** 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
CID	Dados de identificação do cliente.
CIS	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 **CID diretos (DCID)** 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 CID diretos referem-se a dados do cliente não detidos ou criados pelo banco.

Os **CID indiretos (ICID)** dividem-se em 3 níveis:

- Os **ICID 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 **ICID 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 ICID L2 têm de ser protegidos e geridos com o mesmo rigor que os DCID.

- Os **ICID 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 ICID 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.

Consultar a Figura 1, a árvore de decisão de CID, para uma visão geral do método de classificação.

Os CID 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 ICID L2 podem ser partilhados em função da necessidade de tomar conhecimento, mas não podem ser partilhados juntamente com qualquer outro elemento de CID. Com a partilha de múltiplos elementos de CID, 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 ICID L2. Os ICID 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 ICID L2 suficientes para revelar a identidade do cliente.

Classificação da informação	Segredo bancário	Restrita – Interna

Classificação	CID diretos (DCID)	CID indiretos (ICID)		
		Indiretos (L1)	**Potencialmente Indiretos (L2)**	**Identificadores impessoais (L3)**
Tipo de informação	Nome do cliente	Número da partição/ID da partição	Naturalidade	Qualquer identificador estritamente interno do alojamento/aplicação de processamento de CID
	Nome da empresa	Número de MACC (conta monetária num ID de partição Avaloq)	Data de nascimento	Identificador dinâmico
	Extrato de conta	ID SDS	Nacionalidade	ID da função da parte CRM
	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	Mensagem SWIFT	Posição longa/valor de transação	
	Cargo ou título PEP	ID interna do parceiro de negócios	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	

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. Reino Unido).

1. Nome do cliente

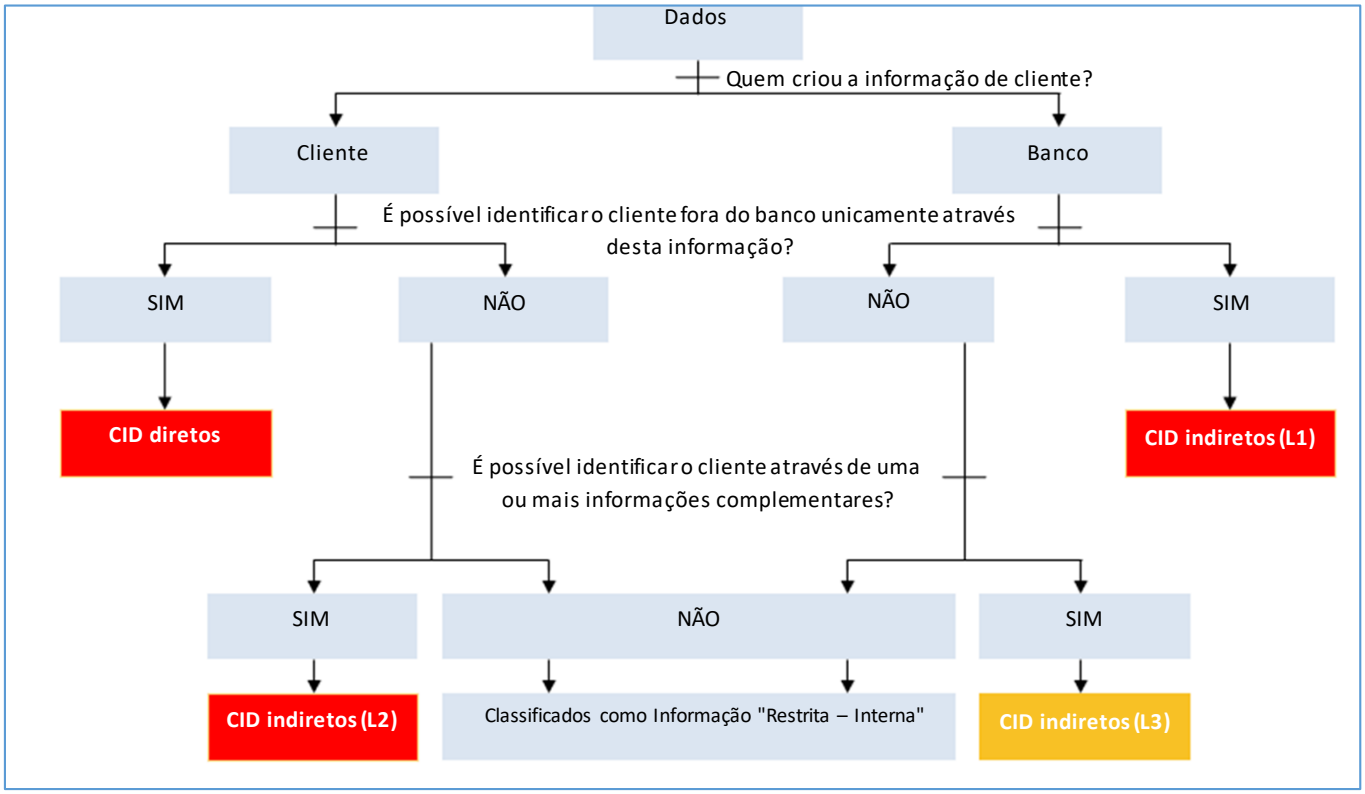
   (DCID) = Violação do segredo bancário

2. ID da partição

   (ICID L1) = Violação do segredo bancário

3. Situação patrimonial + Nacionalidade

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



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 (CID). 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). 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 (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	• 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.

	destinatários de acordo com o princípio da necessidade de tomar conhecimento.	
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 CID 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 CID.

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 "CIS"). • 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 CIS.
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 CID (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 CID (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 CID 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 CIS. • 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). • 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 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 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 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 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.