Supplier Control Obligation (SCO)

Requisitos de controlo de gestão

Informações, segurança física e cibernética, tecnologia, planeamento de recuperação, privacidade de dados, gestão de dados e EUDA

CG 1.0 – Governança e responsabilização

O fornecedor deve ter uma estrutura padrão do setor estabelecida e consistente para a gestão de tecnologias de informação, segurança das tecnologias da informação, segurança física, planeamento de recuperação, gestão de dados e gestão de informações pessoais (privacidade de dados/proteção de dados) (NIST, ISO/IEC 27001, COBIT, BS10012, SSAE 18, ITIL) ou uma estrutura padrão de melhores práticas do setor semelhante, para garantir que as salvaguardas ou contramedidas dos seus processos, tecnologia e ambiente físico estão comprovadas como funcionando de forma eficaz. Um programa bem estruturado de governança em toda a empresa tem de garantir que os conceitos básicos de disponibilidade, integridade e confidencialidade são apoiados por controlos adequados. Os controlos devem ser concebidos para mitigar ou reduzir os riscos de perda, perturbação ou corrupção de informações e o fornecedor deve garantir que os controlos dos requisitos do Barclays são aplicados e funcionam eficazmente para proteger o(s) serviço(s) fornecido(s) ao Barclays.

Tem de ser estabelecido um quadro de governança e tem de incluir salvaguardas administrativas, técnicas e físicas para proteger os ativos e informações/dados contra perda acidental e/ou deliberada, divulgação, alteração ou destruição, roubo, utilização inadequada ou indevida e acesso, utilização ou divulgação não autorizados.

O programa de governança e responsabilização tem de incluir, entre outras, as seguintes áreas:

- Políticas de governança – um conjunto de políticas de governança deve ser definido, aprovado pela gestão, publicado e comunicado aos funcionários do fornecedor e às partes relevantes, e mantido.
    - Políticas, procedimentos e programas padrão que eficazmente criem, implementem e meçam continuamente a eficácia da implementação das normas e da política.
    - Um programa de governança abrangente, com uma estrutura de liderança clara e supervisão executiva, a fim de criar uma cultura de responsabilização e sensibilização.
    - Uma comunicação contínua de políticas e procedimentos aprovados em toda a organização.
    - Adaptação de requisitos legais às políticas e práticas, à proteção de dados como conceito estrutural e a outros controles para garantir que as políticas e os processos são efetivamente implementados
- As políticas para todas as áreas do domínio devem ser revistas em intervalos planeados ou se ocorrerem alterações significativas para garantir a sua conformidade, adequação e eficácia contínuas.
    - Deve ser assegurado que as políticas e procedimentos/normas são regularmente revistos (pelo menos anualmente ou no momento de quaisquer alterações materiais, conforme o que ocorrer primeiro).

- Nomear um indivíduo ou indivíduos/equipa experiente e com as qualificações devidas com quem o Barclays possa estabelecer ligação para os requisitos de OCF, incluindo segurança física e de construção, informações e cibersegurança e gestão de informações pessoais (privacidade de dados/proteção de dados), planeamento de recuperação, gestão de dados e que serão responsáveis por garantir que os requisitos de controlo do Barclays ou do fornecedor são efetivamente implementados e monitorizados.
- O fornecedor deve coordenar e alinhar funções e responsabilidades para o pessoal que implementa, gere e supervisiona a eficácia dos controlos internamente e com subcontratantes/subprocessadores.

- O fornecedor deve implementar uma infraestrutura segura e uma estrutura de controlo para proteger a organização contra quaisquer ameaças (incluindo cibersegurança)
- O Fornecedor deve definir um programa de auditoria independente para examinar se os controlos do Fornecedor são implementados, mantidos e têm de ser realizados, no mínimo, anualmente.

Orientação para cliente de serviços na nuvem (fornecedor)

Uma política de segurança de informações para computação na nuvem deve ser definida como uma política específica de tópico do cliente de serviços na nuvem. A política de segurança de informações do cliente de serviços na nuvem para computação em nuvem deve ser consistente com os níveis aceitáveis de riscos de segurança de informações da organização para as suas informações e outros ativos. Ao definir a política de segurança de informações para a computação em nuvem, o cliente de serviços na nuvem deve ter em conta o seguinte:

- As informações armazenadas no ambiente de computação em nuvem podem estar sujeitas a acesso e gestão pelo prestador de serviços na nuvem.
- Os recursos podem ser mantidos no ambiente de computação em nuvem, por exemplo, programas de aplicações.
- Os processos podem ser executados num serviço na nuvem virtualizado com vários utilizadores.
- Os utilizadores do serviço na nuvem e o contexto em que utilizam o serviço na nuvem.
- Os administradores de serviços na nuvem com acesso privilegiado ao cliente de serviços na nuvem.
- As localizações geográficas da organização do fornecedor de serviços na nuvem e os países onde o fornecedor de serviços na nuvem pode armazenar os dados do cliente de serviços na nuvem (incluindo o armazenamento temporário).

A política de segurança relevante do cliente de serviços na nuvem deve identificar o fornecedor de serviços na nuvem como um tipo de fornecedor e geri-lo de acordo com a política de segurança. Isso deve ter como objetivo mitigar os riscos introduzidos pelo acesso e gestão dos dados do cliente de serviços na nuvem associados ao fornecedor de serviços na nuvem.

O cliente de serviços na nuvem deve considerar leis e regulamentos relevantes de jurisdições que regem o fornecedor de serviços na nuvem, além dos que regem o cliente de serviços na nuvem. O cliente de serviços na nuvem deve obter provas da conformidade do fornecedor de

serviços na nuvem com os regulamentos e normas relevantes necessários para a empresa do cliente de serviços na nuvem. Esses elementos de prova podem também ser os atestados/certificados produzidos por auditores externos.

O Fornecedor tem de notificar o Barclays por escrito assim que o conseguir fazer legalmente, caso o Fornecedor seja sujeito a uma fusão, aquisição ou qualquer outro processo de alteração de propriedade.

CG 2.0 - Gestão de risco

O Fornecedor tem de estabelecer um programa de gestão do risco que eficazmente avalie, mitigue e monitorize os riscos em todo o ambiente controlado pelo Fornecedor.

O programa de gestão do risco tem de incluir, entre outras, as seguintes áreas:

- O fornecedor deve ter um quadro de gestão de risco devidamente aprovado (por exemplo, informações pessoais se processar dados de IP, informações, cibernética, física, tecnologia, planeamento de dados e recuperação) e ser capaz de demonstrar a sua integração na estratégia empresarial
- Em linha com o quadro de risco, têm de ser realizadas avaliações do risco formais pelo menos uma vez por ano ou em intervalos de tempo planeados, utilizando uma abordagem baseada no risco, ou acionadas com base em eventos, ou seja, em resposta a um incidente ou às conclusões obtidas no seguimento do mesmo, em conjunto com quaisquer alterações aos sistemas de informação ou construção física ou espaço, 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).
- Estabelece e mantém critérios de risco que incluem:
  - os critérios de aceitação do risco, e
  - critérios para a realização de avaliações de risco,
- Identifica os riscos:
  - aplicar o processo de avaliação de riscos para identificar riscos associados à perda de confidencialidade, integridade e disponibilidade de informações dentro do âmbito do quadro de risco, e
  - identificar os proprietários dos riscos,
- Analisa os riscos:
  - avaliar as potenciais consequências que poderiam resultar dos riscos identificados,
  - avaliar a probabilidade realista de ocorrência dos riscos identificados, e

- determinar os níveis de risco
- Avalia os riscos:
  - comparar os resultados da análise de risco com os critérios de risco estabelecidos, e
  - dar prioridade aos riscos analisados para o tratamento de riscos
- Tratamento de riscos:
  - selecionar opções adequadas de tratamento de riscos, tendo em conta os resultados da avaliação do risco,
  - determinar todos os controlos necessários para implementar as opções de tratamento de risco escolhidas,
  - produzir uma declaração de aplicabilidade que contenha os controlos e justificação necessários para as inclusões, quer sejam ou não implementadas, e
  - 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. O fornecedor deve monitorizar continuamente as contramedidas para que sejam eficazes.
- O fornecedor tem de realizar, no mínimo, uma avaliação anual dos riscos em relação a informações, cibersegurança, segurança física, gestão de informações pessoais (privacidade de dados/proteção de dados) e planeamento de recuperação. Com base em ambientes específicos com ameaças atuais e emergentes, o fornecedor deve considerar uma cadência mais frequente.
  - Avaliar, pelo menos anualmente, os locais críticos para o funcionamento de processos/serviços fornecidos ao Barclays (incluindo centros de dados)
- A organização deve reter informações documentadas sobre o processo de avaliação de riscos de segurança de informações.
- As avaliações de risco associadas aos requisitos de governança de dados (incluindo informações pessoais se processar dados de IP) devem considerar o seguinte:
  - Classificação dos dados e proteção contra utilização e acesso não autorizados, perda, destruição e falsificação.
  - Conhecimento do local onde se encontram armazenados os dados e onde são transmitidos pelas aplicações, bases de dados, servidores e infraestrutura da rede.
  - Conformidade com os períodos de retenção definidos e com os requisitos de eliminação no final da vida útil dos dados.
- O fornecedor, enquanto atua como responsável pelo tratamento ou subcontratante, tem de avaliar o possível risco de privacidade ao tratar volumes sensíveis ou elevados de dados do Barclays para garantir que quaisquer alterações no seu processamento/tratamento de dados do Barclays não originam um risco de privacidade
- O Fornecedor tem de desenvolver e implementar a estrutura de governança organizacional para permitir uma compreensão contínua das prioridades de gestão de riscos da organização informadas pelo risco de privacidade

CG 3.0 – Funções e responsabilidades

O fornecedor é responsável por garantir que todos os seus funcionários, incluindo, entre outros, contratantes, subcontratantes e subprocessadores envolvidos na prestação de serviços ao Barclays, têm conhecimento e cumprem os requisitos de controlo do Barclays. O Fornecedor tem de garantir que uma equipa adequada de especialistas e/ou indivíduos com competências proporcionais e adequadas, funções e responsabilidades definidas para apoiar e/ou gerir os requisitos de controlo do Barclays está disponível para operar eficazmente no que respeita à proteção do(s) serviço(s) do Barclays.

O fornecedor tem de definir e comunicar funções e responsabilidades para apoiar eficazmente os requisitos de controlo do Barclays. Estas funções e responsabilidades têm de ser revistas periodicamente (e, em qualquer caso, não menos do que uma vez a cada 12 meses) e após qualquer alteração substancial ao modelo de operação ou de negócios do fornecedor.

É da responsabilidade do fornecedor garantir que os seus funcionários, contratantes, subcontratantes/subprocessadores estão familiarizados e em conformidade com os requisitos de controlo desta norma e das políticas e norma associadas. O fornecedor deve nomear um ponto de contacto para estabelecer ligação com o Barclays para qualquer encaminhamento para níveis hierárquicos superiores resultante da não conformidade com os requisitos de controlo. Os requisitos contratuais específicos devem ser transmitidos por escrito aos subcontratantes/subprocessadores do fornecedor.

Orientação para cliente de serviços na nuvem (fornecedor)

O cliente de serviços na nuvem deve concordar com o fornecedor de serviços na nuvem uma atribuição adequada de funções e responsabilidades de segurança da informação e confirmar que pode cumprir as suas funções e responsabilidades atribuídas. As funções e responsabilidades de ambas as partes devem ser indicadas num acordo. O cliente de serviços na nuvem deve identificar e gerir a sua relação com a assistência ao cliente e a função de assistência do fornecedor de serviços na nuvem.

O cliente de serviços na nuvem deve definir ou alargar as suas políticas e procedimentos existentes de acordo com a sua utilização de serviços na nuvem e informar os respetivos utilizadores de serviços na nuvem das suas funções e responsabilidades no que respeita à utilização do serviço na nuvem.

CG 4.0 - Formação e sensibilização

O Fornecedor tem de executar continuamente um programa de formação de sensibilização para todos os funcionários do Fornecedor, incluindo contratantes, contratações a curto prazo e consultores. Todos os funcionários do Fornecedor que trabalhem para os serviços do Barclays e/ou tenham acesso a dados/informações do Barclays ou a outros ativos físicos têm de receber formação adequada e atualizações regulares de sensibilização sobre as políticas, processos e procedimentos da organização relacionados com a sua função profissional desempenhada na mesma. Os níveis de formação e sensibilização devem preparar os funcionários do fornecedor para desempenharem as

suas funções de forma segura e garantir que os funcionários do fornecedor compreendem as suas responsabilidades ao aceder ou tratar quaisquer dados do Barclays, incluindo quaisquer dados pessoais. Os registos do programa a ser executado têm de ser realizados numa plataforma de gestão de aprendizagem adequada ou através de um processo manual.

O fornecedor tem de garantir que todos os funcionários do fornecedor realizam formação obrigatória e de sensibilização, incluindo cibersegurança, segurança física, planeamento de recuperação, gestão de informações pessoais (proteção de dados/privacidade de dados), gestão de dados, gestão de serviços de TI, EUDA e proteção de dados Barclays no prazo de um mês após a adesão à organização e/ou após a adesão ao(s) serviço(s) Barclays. Além de atualizar anualmente a formação, o Fornecedor tem de certificar-se de que os funcionários do Fornecedor compreendem as suas responsabilidades e estão cientes dos riscos associados aos dados do Barclays, às leis e regulamentos aplicáveis, bem como a outros fatores que possam afetar o desempenho ou representar um risco para o banco. Toda a formação administrada deve ser registada e mantida por todos os funcionários do fornecedor que trabalhem no(s) serviço(s) Barclays e apresentada para inspeção pelo Barclays, quando solicitado.

O Fornecedor tem de garantir que o seu programa de formação de sensibilização inclui os seguintes tópicos de Cibersegurança – engenharia social e ameaça interna; recomenda-se que o Fornecedor realize testes de simulação de ataques de engenharia social utilizando técnicas como testes de simulação de Phishing para todos os funcionários a nível empresarial com monitorização contínua com vista a garantir que a ameaça desses riscos é claramente compreendida e para mitigar as questões identificadas.

Grupos de alto risco, como aqueles com acesso a sistema(s) privilegiado(s), acesso a espaço crítico ou de alto risco ou em funções de negócios confidenciais (incluindo utilizadores privilegiados como programadores e assistentes, executivos sénior, pessoal de segurança da informação e partes interessadas externas), devem receber formação de sensibilização situacional de segurança da informação e segurança física de acordo com as suas funções e responsabilidades.

Todo o pessoal de segurança física (quer seja empregado pelo fornecedor, um proprietário ou um fornecedor externo) tem de ser admitido ou contratado através de um prestador de serviços acreditado e licenciado de acordo com a legislação local e, quando exigido pela jurisdição, ter uma licença pessoal para assumir deveres de segurança. O pessoal de segurança física deve receber formação de segurança proporcional às suas funções e responsabilidades. Toda a formação administrada deve ser documentada e deve ser mantido um registo de formação para todo o pessoal de segurança e apresentado para inspeção pelo Barclays, quando solicitado

O Fornecedor tem de garantir que o seu pessoal externo com acesso a dados que contenham quaisquer informações pessoais tem conhecimento dos riscos de privacidade e cumpre as suas obrigações e responsabilidades de acordo com as políticas, processos, procedimentos, acordos e valores de privacidade da organização relacionados. Toda a formação administrada deve ser documentada e deve ser mantido um registo de formação para todo o pessoal e apresentado para inspeção pelo Barclays, quando solicitado.

O fornecedor deve formar os funcionários para que desempenhem as suas funções de gestão de dados (gestão de elementos de dados críticos ou aplicações geridas por terceiros) de forma eficaz.

O proprietário da EUDA do fornecedor tem de identificar os funcionários do fornecedor com responsabilidades EUDA e garantir que realizam a formação de sensibilização adequada à sua função pelo menos uma vez por ano, e manter provas que demonstrem a conformidade com o controlo.

Orientação para cliente de serviços na nuvem (fornecedor)

O cliente de serviços na nuvem deve adicionar os seguintes itens a programas de sensibilização e formação para gestores comerciais de serviços na nuvem, administradores de serviços na nuvem, integradores de serviços na nuvem e utilizadores de serviços na nuvem, incluindo funcionários e contratantes relevantes:

- Normas e procedimentos para a utilização de serviços na nuvem.
- Riscos de segurança da informação relacionados com os serviços na nuvem e a forma como esses riscos são geridos.
- Riscos do ambiente do sistema e da rede com a utilização de serviços na nuvem.
- Considerações legais e regulamentares aplicáveis.

Os programas de sensibilização e formação sobre segurança de informações relativos a serviços na nuvem devem ser fornecidos à gestão e aos gestores de supervisão, incluindo os de unidades de negócios. Estes esforços apoiam uma coordenação eficaz das atividades de segurança de informações.

CG 5.0 - Gestão de incidentes

O fornecedor tem de ter uma estrutura de gestão de incidentes estabelecida que permita gerir, conter e remover/atenuar eficazmente um incidente e a sua causa subjacente do ambiente do fornecedor.

O fornecedor tem de dispor de um procedimento de gestão de incidentes e crises que inclua o processo de encaminhamento de incidentes/crises para o Barclays. O fornecedor tem de garantir que as equipas e processos de resposta a incidentes/crises são testados, pelo menos anualmente, para demonstrar que o fornecedor consegue dar resposta a quaisquer incidentes de forma efetiva e eficiente. O Fornecedor também tem de testar a sua capacidade de notificar, dentro de um prazo definido, os contactos relacionados com um incidente e demonstrar a mesma ao Barclays quando solicitado.

O Fornecedor tem de ter um plano de resposta a Incidentes bem documentado que defina as funções dos funcionários do Fornecedor, bem como as fases do tratamento/gestão do incidente:

- Responsabilidades e procedimentos – devem ser estabelecidas responsabilidades e procedimentos de gestão para garantir uma resposta rápida, eficaz e ordenada a incidentes.
- Comunicar eventos de incidentes – os eventos de incidentes devem ser comunicados através de canais de gestão adequados o mais rapidamente possível e o mecanismo de comunicação tem de ser o mais fácil e acessível a todos os funcionários e contratantes do Fornecedor.
- Avaliação de eventos de incidentes – os eventos de incidentes têm de ser avaliados para determinar a criticalidade, classificação e resposta necessárias.
    - Classificação de incidentes – estabelecer uma escala de classificação de incidentes e decidir se o evento deve ser classificado como incidente. A classificação e a atribuição de prioridades relativamente a incidentes podem ajudar a identificar o impacto e a extensão de um incidente.
- Resposta a incidentes – os incidentes devem ser respondidos de acordo com os procedimentos documentados de gestão de incidentes do fornecedor.
    - Contenção do incidente – utilizar pessoas, processos e capacidades tecnológicas para rápida e eficazmente conter um incidente no ambiente.
    - Remoção/mitigação da ameaça – alavancar pessoas, processos e capacidades tecnológicas para rápida e eficazmente remover/mitigar uma ameaça de segurança e/ou os seus componentes do ambiente.
- Aprendizagem de incidentes – o conhecimento obtido através da análise e resolução de incidentes deve ser utilizado para reduzir a probabilidade ou o impacto de futuros incidentes.
- Recolha de provas – o Fornecedor deve definir e aplicar procedimentos para a identificação, recolha, aquisição e conservação de informações que possam servir de prova.

Após o Incidente – na sequência de uma perturbação do(s) serviço(s) do Barclays, tem de ser apresentado ao Barclays um **Relatório pós-incidente** no prazo máximo de quatro **semanas de calendário** a contar do restabelecimento dos níveis normais de funcionamento do serviço. Requisito mínimo de Relatório pós-incidente:

- Eventos em torno da situação.
- Modo de gestão do Incidente/da Crise.
- Análise da causa originária.
- Se está classificado como "Evento de risco" pelo Fornecedor ou pelo Barclays (ou seja, se é considerado suficientemente significativo para ser notificado/encaminhado para as partes interessadas relevantes em conformidade com as políticas aplicáveis do conhecimento do Fornecedor).
- Se representa um "risco de conduta" (por ex., se o fornecedor está a lidar diretamente com clientes do Barclays).

- Qualquer compensação do cliente do Barclays que seja do conhecimento do fornecedor;
- Melhoria contínua para prevenir novas ocorrências; e
- O fornecedor deve procurar estabelecer que as atividades de resposta sejam melhoradas sempre que possível, incorporando as conclusões retiradas de atividades de deteção/resposta atuais e anteriores.

Para comunicação – o fornecedor tem de nomear um ponto de contacto que fará a ligação com o Barclays na eventualidade de um incidente/crise. O fornecedor tem de comunicar ao Barclays os dados 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 dados devem incluir: - nome, responsabilidades dentro da organização, cargo, endereço de e-mail e número de telefone

Se, em qualquer altura, o Fornecedor confirmar que qualquer incidente afeta os Serviços do Barclays, os Sistemas do Barclays ou os Dados do Barclays, o Fornecedor deverá notificar imediatamente o Barclays.

Quando o fornecedor tomar conhecimento de um incidente cibernético, incluindo através de notificação de uma entidade Barclays, o fornecedor deverá imediatamente, mas em caso algum posterior ao exigido pela legislação aplicável ou, se tal não for exigido, no prazo de 48 horas após a primeira informação sobre o incidente cibernético, notificar o Barclays enviando um e-mail para gcsojoc@barclays.com, e fornecer todas as informações relevantes, incluindo, se possível (a) as categorias e o número aproximado de registos de dados Barclays afetados e, se aplicável, as categorias e o número aproximado de titulares de dados afetados; (b) o impacto e as consequências prováveis do incidente cibernético para o Barclays e, se aplicável, os titulares de dados afetados; e (c) as ações corretivas e atenuantes tomadas ou a serem tomadas pelo fornecedor.

No caso de qualquer roubo efetivo, suspeito ou alegado, utilização ou divulgação não autorizada de quaisquer dados pessoais protegidos devido a uma falha das salvaguardas de segurança do fornecedor (ou de qualquer pessoal do fornecedor) ou acesso não autorizado a dados pessoais protegidos do, ou através do, fornecedor (ou de qualquer pessoal do fornecedor), ou perda, danos ou destruição de dados pessoais protegidos na posse ou controlo do fornecedor ou de qualquer pessoal do fornecedor, ou outro processamento não autorizado de quaisquer dados pessoais protegidos, o fornecedor deverá notificar o Barclays assim que possível, e, em qualquer caso, no prazo de 24 horas após tomar conhecimento do evento relevante, enviando um e-mail para gcsojoc@barclays.com, e prestar total cooperação e assistência ao Barclays relativamente a esse evento, incluindo o fornecimento de todas as informações relevantes, tais como dados, hora, localização, tipo de incidente, impacto, estado e medidas de mitigação tomadas.

Se for utilizado um subcontratante/subprocessador para prestar o serviço, em que este irá deter ou processar dados/informações ou ativos do Barclays, o fornecedor tem de obter o acordo do Barclays. O fornecedor tem de ter uma relação contratual com os subcontratantes/subprocessadores e tem de garantir que os subcontratantes/subprocessadores possuem acreditação de um quadro padrão de melhores práticas do setor semelhante que opere eficazmente para proteger os dados/informações do Barclays que processam e/ou detêm. Em caso de incidente com o subcontratante/subprocessador, é necessário garantir que a notificação de incidente acima indicada é seguida.

Orientação para cliente de serviços na nuvem (fornecedor)

O cliente de serviços na nuvem deve verificar a atribuição de responsabilidades para a gestão de incidentes e garantir que cumpre os requisitos do cliente de serviços na nuvem. O cliente de serviços na nuvem deve solicitar informações ao fornecedor de serviços na nuvem sobre os mecanismos para:
– o cliente de serviços na nuvem comunicar um incidente/evento que tenha detetado ao fornecedor de serviços na nuvem.
– o cliente de serviços na nuvem receber relatórios sobre um incidente/evento detetado pelo fornecedor de serviços na nuvem.
– o cliente de serviços na nuvem acompanhar o estado de um evento de segurança de informações comunicado.

CG 6.0 – Gestão de ativos de TI (hardware e software)

O Fornecedor tem de possuir e operar um programa de gestão de ativos eficaz ao longo do ciclo de vida dos ativos. A gestão de ativos deve governar o ciclo de vida dos mesmos, desde a aquisição até à retirada e/ou eliminação segura, conferindo visibilidade e segurança a todas as classes de ativos no ambiente.

O fornecedor tem de manter um inventário completo, rigoroso e atualizado de todos os ativos críticos para o negócio situados em todos os pontos e/ou locais geográficos no âmbito dos serviços ao Barclays, incluindo qualquer equipamento do Barclays presente nas instalações do fornecedor, de subcontratantes/subprocessadores, fornecido pelo Barclays, garantindo que existe pelo menos um teste anual para validar a atualidade, integralidade e rigor do inventário de ativos e demonstrando os resultados ao Barclays quando tal for solicitado.

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

- Inventário dos ativos - os ativos associados a informações e instalações de processamento de informações devem ser identificados e deve ser mantido um inventário desses ativos.
    - O fornecedor tem de manter um inventário rigoroso e atualizado de todos os ativos de hardware de TI com o potencial de armazenar ou processar informações.
    - O fornecedor tem de ter um inventário de ativos informacionais preciso e atualizado para o equipamento Barclays alojado no fornecedor e/ou ativos de TI do Barclays fornecidos ao fornecedor.
    - O Fornecedor com uma configuração de Nível 1, Nível 2 e Nível 3 tem 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).
    - O Fornecedor tem de realizar uma reconciliação de todos os ativos do Barclays (Hardware e Software) anualmente e informar o Barclays (gabinete do Diretor de segurança – Equipa TPSecM) dos seus resultados.
    - Manter um inventário atualizado de todos os produtos de software implementados e autorizados necessários para a prestação de serviços Barclays e cumprir os termos e condições das respetivas licenças.

    - O inventário de ativos do cliente de serviços na nuvem tem de incluir informações e recursos associados armazenados no ambiente de computação em nuvem. Os registos do inventário têm de indicar onde os ativos são mantidos, por ex., a identificação do serviço na nuvem.
- Utilização aceitável de ativos – as regras para a utilização aceitável de informações e de ativos associados a informações e instalações de processamento de informações devem ser identificadas, documentadas e implementadas.
    - Assegurar que os ativos não autorizados são removidos da rede.
    - 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 eliminação segura de ativos e dados para eliminar o risco
    - Identificar software e hardware não suportados no sistema de inventário.
- Devolução de ativos – todos os funcionários do Fornecedor e subcontratantes/subprocessadores (no âmbito dos serviços ao Barclays) devem devolver todos os ativos do Barclays na sua posse após a cessação do respetivo emprego, contrato ou acordo.
    - Os ativos Barclays "perdidos ou roubados" devem ser devidamente investigados e comunicados ao Barclays de acordo com o controlo de gestão de incidentes.
    - No caso de ativos do fornecedor "perdidos ou roubados" conterem informações do Barclays, tal deve ser comunicado ao Barclays de acordo com o controlo de gestão de incidentes.

O fornecedor tem de informar imediatamente o Barclays sobre modificações conhecidas na sua capacidade para prestar assistência, direta ou indiretamente, a ativos de TI utilizados na prestação de serviços ao Barclays, incluindo sempre que os produtos tenham vulnerabilidades de segurança, devendo também garantir uma atualização atempada ou a retirada de operação desses ativos de TI.

Transporte de ativos Barclays - o fornecedor irá garantir que todos os ativos e dados Barclays são transportados de forma segura, com controlos proporcionais à classificação e ao valor dos ativos e dos bens transportados (numa perspetiva que abranja os danos financeiros e danos para a reputação), incluindo o impacto do ambiente de ameaça nos quais são transportados.

Gestão de assistência (fornecedor)

O fornecedor tem de informar imediatamente o Barclays sobre modificações conhecidas na sua capacidade para prestar assistência, direta ou indiretamente, a ativos de TI utilizados na prestação de serviços ao Barclays, incluindo sempre que os produtos tenham vulnerabilidades de segurança, devendo também garantir uma atualização atempada ou a retirada de operação desses ativos de TI.

O fornecedor deve garantir que quaisquer potenciais alterações nos acordos de assistência de terceiros principais são identificadas e comunicadas ao Barclays para os ativos afetados, de forma a garantir que as informações do produto são mantidas atualizadas.

Orientação para cliente de serviços na nuvem (fornecedor)

O inventário de ativos do cliente de serviços na nuvem deve ter em conta as informações e os recursos associados armazenados no ambiente de computação em nuvem. Os registos do inventário devem indicar onde os ativos são mantidos, por ex., a identificação do serviço na nuvem.

A instalação de software licenciado comercialmente num serviço na nuvem pode causar uma violação dos termos de licença do software. O cliente de serviços na nuvem deve ter um procedimento para identificar requisitos de licenciamento específicos da nuvem antes de permitir que qualquer software licenciado seja instalado num serviço na nuvem. Deve ser dada especial atenção aos casos em que o serviço na nuvem é elástico e escalável e o software pode ser executado em mais sistemas ou núcleos de processador do que o permitido pelos termos da licença.

CG 7.0 – Eliminação/destruição segura de ativos físicos e remanência de dados de informação eletrónica

A destruição ou eliminação segura de ativos informacionais Barclays, incluindo imagens utilizadas para o serviço, armazenadas em forma física e/ou eletrónica, tem de ser realizada de acordo com um método seguro adequado e verificando se os dados Barclays não são recuperáveis.

O Fornecedor tem de estabelecer procedimentos com processos empresariais de apoio e medidas técnicas para eliminar de forma segura utilizando métodos de saneamento adequados, incluindo, entre outros, a eliminação, purga e destruição para remoção/eliminação segura e recuperação de dados do Barclays de todos os suportes de armazenamento, tornando os dados do Barclays irrecuperáveis por meios forenses informáticos conhecidos.

Os dados Barclays armazenados em meios têm de ser eliminados de forma a tornar os dados irrecuperáveis, utilizando técnicas de eliminação de dados adequadas, como limpeza segura, purga, apagamento de dados ou destruição de ativos ou um método baseado em software para reescrever os dados ou utilização da estrutura padrão do setor para eliminação de dados (NIST). Todos os equipamentos (ativos informacionais) têm de ser eliminados no final da respetiva vida útil e/ou vida de funcionamento (avariados, desativados devido a um serviço retirado ou já não necessários, utilizados num ensaio ou prova de conceito; podem ser utilizados serviços de eliminação de dados para equipamentos a serem reutilizados, etc.).

Os requisitos de eliminação aplicam-se aos subcontratantes/subprocessadores do fornecedor que são utilizados para prestar o serviço ao Barclays.

A eliminação de informação impressa tem de ser realizada através de trituração em trituradora de corte transversal (inclui informação de cartão de pagamento), cumprindo no mínimo a norma P4 DIN66399, ou pode ser incinerada em conformidade com a norma BS EN15713:2009.

Para o Barclays, tem de ser mantida a evidência de eliminação de dados, disponibilizando registo, evidência e rastreio de auditoria, tendo de incluir:

- Prova de destruição e/ou eliminação (incluindo data e método utilizado)
- Registos de auditoria do sistema para eliminação.
- Certificados de eliminação de dados.
- Identificação de quem realizou a eliminação (incluindo quaisquer parceiros de eliminação, terceiros ou contratantes)
- Deve ser gerado um relatório de destruição e verificação para confirmar o sucesso ou falha de qualquer processo de destruição/eliminação. (ou seja, um processo de reescrita deve fornecer um relatório detalhando quaisquer setores que não puderam ser apagados).

Durante o término do serviço ao Barclays, o fornecedor tem de assegurar que os dados Barclays são destruídos de modo seguro após notificação e autorização do Barclays.

Orientação para cliente de serviços na nuvem (fornecedor)

O cliente de serviços na nuvem deve solicitar a confirmação de que o fornecedor de serviços na nuvem possui as políticas e os procedimentos para a eliminação segura ou reutilização de recursos. O cliente de serviços na nuvem deve solicitar uma descrição documentada da cessação do processo de serviço que abrange a devolução e remoção dos recursos do cliente de serviços na nuvem, seguida da eliminação de todas as cópias desses recursos dos sistemas do fornecedor de serviços na nuvem. A descrição deve listar todos os ativos e documentar o agendamento para a cessação do serviço, o que deve ocorrer de forma atempada.

CG 8.0 – Classificação das informações e tratamento de dados

O fornecedor tem de possuir uma estrutura/plano estabelecido e adequado para a classificação de informações e tratamento de dados (alinhado com as boas práticas do setor e/ou os requisitos do Barclays) que abranja os seguintes componentes:

- Classificação das informações - as informações devem ser classificadas quanto ao seu caráter crítico e sensibilidade à divulgação ou modificação não autorizada.
- Rotulagem das informações - deve ser desenvolvido e implementado um conjunto adequado de procedimentos de rotulagem de informações, de acordo com o esquema de classificação de informações adotado pelo fornecedor.
- Tratamento de ativos - os procedimentos de tratamento de ativos devem ser desenvolvidos e implementados de acordo com o esquema de classificação de informações adotado pelo fornecedor.

O fornecedor deve ainda 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 classificação de informações e os requisitos de tratamento do Barclays (Anexo A, Tabela A1 e A2), ou um esquema alternativo para garantir que o fornecedor protege e defende as informações do Barclays retidas e/ou processadas.

Este requisito é aplicável a todos os ativos informacionais do Barclays retidos ou processados em nome do Barclays, incluindo subcontratantes/subprocessadores.

Orientação para cliente de serviços na nuvem (fornecedor)

O cliente de serviços na nuvem deve classificar as informações e os recursos associados mantidos no ambiente de computação na nuvem de acordo com os procedimentos adotados pelo cliente de serviços na nuvem para classificação. Quando aplicável, é possível adotar a funcionalidade fornecida pelo fornecedor de serviços na nuvem que suporta a classificação.

CG 9.0 Cópia de segurança de informações/dados

O fornecedor tem de ter um processo de cópia de segurança de dados estabelecido para garantir a realização de uma cópia de segurança da infraestrutura regular e precisa, de forma a evitar a perda de dados. É efetuada uma cópia de segurança das informações armazenadas num formato eletrónico para manter as mesmas em segurança em caso de falha do sistema, catástrofes ou incidentes. Os planos de cópia de segurança devem ser desenvolvidos, testados e implementados para satisfazer a política específica do tópico sobre cópias de segurança.

No plano de cópia de segurança devem ser levados em consideração os seguintes elementos:

- Determinação dos requisitos de cópia de segurança – os requisitos para a cópia de segurança de dados são claramente definidos, registados e acordados com a empresa
- Produção de registos precisos e completos das cópias de segurança e procedimentos de restauro documentados.
- Frequência de cópia de segurança (por exemplo, cópia de segurança total ou diferencial)
- Armazenamento seguro de cópias de segurança
    - armazenar as cópias de segurança num local remoto seguro e protegido, a uma distância suficiente para não serem afetadas por qualquer dano causado por uma catástrofe no local principal.
- Teste regular dos suportes de cópia de segurança para garantir que podem ser utilizados em caso de emergência, quando necessário. Teste da capacidade de restaurar dados de cópia de segurança num sistema de teste, não substituindo o suporte de armazenamento original no caso de o processo de cópia de segurança ou restauro falhar e provocar danos ou perdas irreparáveis nos dados.
- Atenção para garantir que é detetada uma perda de dados inadvertida antes da realização da cópia de segurança.
- Confirmação se a cópia de segurança é adequado para o efeito

Garantia de que as cópias de segurança são devidamente protegidas através de segurança física e/ou encriptação durante o seu armazenamento, bem como quando são movidas pela rede/localizações. Esta condição inclui as cópias de segurança remotas e os serviços na nuvem.

Garantir que todos os dados do Barclays são regularmente salvaguardados de acordo com o requisito de serviço.

Quando o fornecedor de serviços na nuvem fornecer capacidade de cópia de segurança como parte do serviço na nuvem, o cliente de serviços na nuvem deve solicitar as especificações da capacidade de cópia de segurança do fornecedor de serviços na nuvem. O cliente de serviços na nuvem também deve verificar se cumpre os seus requisitos de cópia de segurança. O cliente de serviços na nuvem é responsável pela implementação das capacidades de cópia de segurança quando o fornecedor de serviços na nuvem não as fornecer.

O fornecedor tem de garantir que todos os sistemas e serviços de TI utilizados na prestação de serviços ao Barclays dispõem de processos de restauro e de cópia de segurança adequados que funcionem de acordo com as necessidades do Barclays e cuja eficácia seja comprovada periodicamente.

O fornecedor tem de garantir que todos os suportes de cópia de segurança associados à prestação de serviços ao Barclays, juntamente com as condições de tratamento e armazenamento desses suportes, permanecem seguros e fiáveis em todas as circunstâncias

CG 10.0 - Gestão de configuração

O fornecedor deve definir e implementar processos e ferramentas para aplicar as configurações definidas (incluindo configurações de segurança) para hardware, software, serviços (incluindo serviços na nuvem) e redes, para sistemas recém-instalados, bem como para sistemas operacionais ao longo da sua vida útil.

Gerir configurações – o fornecedor deve ter um conjunto de configurações aprovadas e testadas para hardware, software e redes. Estes devem ser registados e deve ser mantido um registo de todas as alterações de configuração. Estes registos devem ser armazenados em segurança. Isto pode ser alcançado de várias formas, como bases de dados de configuração ou modelos de configuração.

Configurações de monitorização – as configurações devem ser monitorizadas com um conjunto abrangente de ferramentas de gestão do sistema (por exemplo, utilitários de manutenção, assistência remota, ferramentas de gestão empresarial, software de cópia de segurança e restauro) e devem ser revistas regularmente para verificar as definições de configuração, avaliar os pontos fortes da palavra-passe, bem como atividades realizadas. As configurações reais podem ser comparadas com os modelos de destino definidos. Quaisquer desvios devem ser resolvidos, quer pela aplicação automática da configuração-alvo definida, quer pela análise manual do desvio, seguida de ações corretivas.

Registo e manutenção de itens de configuração - o fornecedor tem de manter registos individuais completos e rigorosos para todos os itens de configuração abrangidos e utilizados na prestação de serviços ao Barclays (incluindo a responsabilidade e as dependências/mapeamentos a montante/jusante). O fornecedor tem de dispor de controlos para garantir a manutenção contínua da precisão e integralidade dos dados.

Isolamento do ambiente de produção - o fornecedor tem de garantir que os serviços de produção disponibilizados ao Barclays não dependem de componentes não envolvidos na produção, de modo a evitar uma prestação de serviços insegura ou não fiável.

Configuração segura - o fornecedor tem de estabelecer uma estrutura para garantir que todos os sistemas e/ou equipamento de rede configuráveis são configurados de forma segura, de acordo com as melhores práticas do setor (por ex., NIST, SANS, CIS).

- Estabelecimento de políticas, procedimentos/medidas organizacionais e ferramentas para permitir a implementação de normas de configuração segundo as melhores práticas do setor para todos os dispositivos da rede e sistemas operativos, aplicações e servidores.
- Realização de verificações regulares (anualmente, no mínimo) 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 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, inexistência de software não autorizado, remoção e desativação de contas de utilizador desnecessárias, alteração de palavras-passe predefinidas, remoção de software desnecessário, etc.).
- Realizar auditorias periódicas de configuração pelo menos anualmente para garantir que o ambiente de produção real não tem nenhuma configuração não autorizada.
- 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.

Orientação para cliente de serviços na nuvem (fornecedor) utilizado para fornecer serviços ao Barclays

O cliente de serviços na nuvem (CSC) tem de garantir que são implementados os controlos de configuração segura adequados para salvaguardar o serviço Barclays -

- Ao configurar máquinas virtuais, os clientes de serviços na nuvem devem garantir que são reforçados aspetos adequados (por ex., apenas as portas, protocolos e serviços estritamente necessários) e que estão implementadas medidas técnicas adequadas (por ex., antimalware, registo de eventos) para cada máquina virtual utilizada.

CG 11.0 Requisitos de segurança para inteligência artificial (IA)

O Fornecedor tem de consultar o Barclays (gabinete do Diretor de segurança – Equipa TPSecM – externalcyberassurance@barclayscorp.com) se estiver a utilizar ferramentas de IA para qualquer parte do ciclo de vida dos serviços e/ou a processar dados do Barclays.

O Fornecedor tem de, sempre que utilizar IA para qualquer parte do ciclo de vida dos serviços e/ou processar dados do Barclays, operar um sistema de Gestão de IA. Esse sistema de Gestão deve, no mínimo, documentar processo/procedimentos sobre os seguintes pontos:

- Governança de IA – o Fornecedor deve definir e estabelecer um quadro de governança para a utilização de ferramentas de IA (incluindo ferramentas de IA de Terceiros). Este quadro de governança deve garantir que as ferramentas de IA são concebidas/implementadas ou integradas nos processos existentes de forma a proteger contra a perda de dados, danos no sistema, interrupções do serviço e consequências regulamentares. Um programa bem estruturado de governança tem de garantir que os conceitos básicos de disponibilidade, integridade e confidencialidade são apoiados por controlos adequados. Os controlos têm de ser concebidos para mitigar ou reduzir os riscos de perda, perturbação ou corrupção de informações através do Sistema de IA, e o Fornecedor tem de garantir que os controlos de segurança são aplicados e estão a funcionar corretamente para proteção dos dados e serviços do Barclays aquando de interações com tal Sistema de IA.

- Segurança de IA – o Fornecedor tem de definir e estabelecer um quadro de segurança de IA que deve incluir, entre outras, as seguintes áreas:
  - Políticas relacionadas com IA – o Fornecedor deve documentar uma política de IA que especifique os requisitos para a utilização ou desenvolvimento seguro e responsável dos sistemas de IA
  - Organização interna – o Fornecedor deve garantir a responsabilização dentro da organização por manter a sua abordagem responsável pela implementação, utilização e gestão de sistemas de IA.
  - Recursos para sistemas de IA – o Fornecedor deve garantir que a organização contabiliza os recursos (incluindo componentes e ativos do sistema de IA) do sistema de IA para compreender e abordar totalmente os riscos e impactos.
  - Dados para sistemas de IA – o Fornecedor tem de garantir que a organização compreende o papel e os impactos dos dados (incluindo Dados do Barclays) em sistemas de IA na aplicação e desenvolvimento, fornecimento ou utilização de sistemas de IA ao longo dos seus ciclos de vida.
  - Informações para as partes interessadas em sistemas de IA – o Fornecedor deve garantir que quaisquer partes interessadas relevantes (incluindo o Barclays) têm as informações necessárias para compreender e avaliar os riscos do Sistema de IA e os seus impactos (positivos e negativos).
  - Relações com terceiros e clientes – o Fornecedor deve garantir que a organização compreende as suas responsabilidades e continua a ser responsável relativamente ao Sistema de IA e que os riscos são devidamente distribuídos quando estão envolvidos terceiros em qualquer fase do ciclo de vida do sistema de IA.

EUDA – quando os serviços do Fornecedor ou a capacidade ou funcionalidade do produto do Fornecedor fornecidos ao Barclays utilizarem EUDA e a IA for implementada ou utilizada para suportar estes EUDA, o Fornecedor tem de informar o Barclays e garantir que a utilização de IA não entra em conflito com os requisitos de OCF do EUDA do Barclays.

Nota: o requisito de controlo de segurança acima indicado não se aplica apenas à inteligência artificial (IA), mas também à aprendizagem automática (ML), uma vez que a inteligência artificial e a aprendizagem automática estão intimamente relacionadas e ligadas. O Fornecedor tem de implementar todos os requisitos de controlo indicados acima para a utilização de ferramentas de ML para qualquer parte do ciclo de vida dos serviços e/ou para processar dados do Barclays.

Definição de IA/ML: IA significa um sistema baseado em máquinas concebido para funcionar com um nível de autonomia e capaz, de gerar, para um determinado conjunto de objetivos, resultados como previsões, recomendações ou decisões que influenciam ambientes físicos ou virtuais. ML é um subconjunto da IA que se refere à capacidade de uma máquina melhorar o seu próprio desempenho a partir da experiência obtida através de iterações e sem ser explicitamente programada com regras.

Um método/uma aplicação/uma ferramenta que se enquadre na definição acima é considerada IA/ML se demonstrar caraterísticas de IA/ML[1] o utilizar um algoritmo de IA/ML listado[2].

1. Um método/uma aplicação/uma ferramenta tem caraterísticas de IA/ML se contiver parâmetros treinados em dados e a adequação desses parâmetros não pode ser avaliada individualmente por um especialista na matéria. Isso pode dever-se ao elevado número de parâmetros, à complexidade do cálculo ou à frequência com que são atualizados. Para fins desta definição, "parâmetros" significa variáveis numéricas no algoritmo que podem ser variadas para afetar o respetivo resultado; "adequação" significa que o resultado do modelo é adequado para o propósito, dado a seu uso; e "especialista na matéria" significa o proprietário do modelo ou o programador do modelo (se agir como delegado para o desenvolvimento do modelo).

2. Os algoritmos de IA/ML incluem Bagging (random forest, etc.), Boosting (GBM, XGBoost, etc.), Clustering (K-means, DBSCAN, etc.), Deep learning/rede neural, Aprendizagem baseada em instâncias (KNN, etc.), Regressão regularizada (por exemplo, Lasso, Ridge), Reforço da aprendizagem, Máquina de vetores de suporte.

Direito de inspeção

O fornecedor tem de permitir ao Barclays, mediante notificação por escrito do Barclays pelo menos dez (10) dias úteis antes, realizar uma análise de segurança a qualquer local ou tecnologia utilizada pelo fornecedor ou respetivos subcontratantes/subprocessadores 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 perante o Barclays. O fornecedor também tem de permitir que o Barclays realize uma inspeção no mínimo anual e/ou imediatamente após um incidente de segurança.

Qualquer não conformidade dos controlos identificada pelo Barclays durante uma inspeção tem de ser avaliada em termos de risco pelo Barclays e o Barclays tem de especificar um prazo de resolução. O fornecedor tem, então, de implementar qualquer resolução necessária dentro desse prazo.

O fornecedor tem de disponibilizar todo o apoio razoavelmente solicitado pelo Barclays relativamente a qualquer inspeção e documentação enviada durante a inspeção. A documentação tem de ser preenchida e devolvida ao Barclays prontamente. O fornecedor também tem de apoiar o Barclays com a entidade avaliadora, juntamente com provas solicitadas durante qualquer análise de garantia. Cada Parte suportará os seus próprios custos relativamente a qualquer revisão/auditoria/avaliação.

Anexo A: Esquema de classificação de informações do Barclays e requisitos de tratamento de dados

Tabela A1: 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 estiverem limitadas a um público específico. A divulgação não autorizada teria um impacto negativo no Barclays, avaliado segundo o ERMF, como "importante" ou "limitado" (financeiro ou não financeiro). As informações não se destinam a distribuição geral, mas podem ser encaminhadas ou partilhadas pelos destinatários de acordo com o princípio da necessidade de tomar conhecimento.	• Estratégias e orçamentos • Avaliações de desempenho • Remuneração dos colaboradores e dados pessoais • Avaliações de vulnerabilidade
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	• Planos de novos produtos • Contratos com clientes • Contratos legais

	o ERMF, como "importante" ou "limitado" (financeiro ou não financeiro). As informações não se destinam a distribuição geral, mas podem ser encaminhadas ou partilhadas pelos destinatários de acordo com o princípio da necessidade de tomar conhecimento.	• Pequenas quantidades de informação/informações individuais de clientes/consumidores destinadas a serem enviadas externamente • Comunicações de clientes/consumidores. • Nova emissão de materiais de oferta (p. ex. brochuras, prospetos de oferta) • Documentos finais de investigação • Informações não públicas relevantes (MNPI) externas ao Barclays • Todos os relatórios de investigação • Alguns materiais de marketing • Comentários de mercado • 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 A2: Esquema de classificação de informações do Barclays – requisitos de tratamento de dados

*** 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 (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.		• 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.
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., ecrãs 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., ecrãs 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 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 em papel têm de integrar uma etiqueta de informação visível. A etiqueta tem de encontrar-se pelo menos na página do título. • Os ativos eletrónicos têm de integrar uma etiqueta de informação bem visível. • Os ativos só podem ser distribuídos utilizando sistemas, métodos ou fornecedores aprovados pela organização.	• Os ativos em papel têm de ter uma etiqueta de informação visível. A etiqueta tem de encontrar-se pelo menos na página do título. • Os envelopes que contenham ativos em papel têm de incluir uma etiqueta de informação visível na parte da frente • Os ativos eletrónicos têm de integrar uma etiqueta de informação bem visível. As cópias eletrónicas de documentos com várias páginas têm de integrar uma etiqueta de informação visível em todas as páginas.

	• Os ativos eletrónicos têm de integrar uma etiqueta de informação bem visível. As cópias eletrónicas de documentos com várias páginas têm de integrar uma etiqueta de informação visível em todas as páginas. • Os ativos só podem ser distribuídos utilizando sistemas, métodos ou fornecedores aprovados pela organização. • Os ativos só podem ser distribuídos a pessoas empregadas pela empresa, ou ao abrigo de uma obrigação contratual adequada para com a empresa, ou no âmbito de uma necessidade comercial inequivocamente reconhecida, por exemplo, negociação contratual. • Os ativos só podem ser distribuídos a pessoas especificamente autorizadas a recebê-los pelo responsável pela informação. • Os ativos não podem ser enviados por fax. • Os ativos eletrónicos têm de ser encriptados com recurso a um mecanismo de proteção criptográfico aprovado, sempre que estiverem a ser distribuídos fora da rede interna. • Tem de ser mantida uma cadeia de custódia para ativos eletrónicos.	• Os ativos só podem ser distribuídos a pessoas empregadas pela empresa, ou ao abrigo de uma obrigação contratual adequada para com a empresa, ou no âmbito de uma necessidade comercial inequivocamente reconhecida, por exemplo, negociação contratual.	• Os ativos só podem ser distribuídos utilizando sistemas, métodos ou fornecedores aprovados pela organização. • Os ativos só podem ser distribuídos a pessoas empregadas pela empresa, ou ao abrigo de uma obrigação contratual adequada para com a empresa, ou no âmbito de uma necessidade comercial inequivocamente reconhecida, por exemplo, negociação contratual. • Os ativos só podem ser distribuídos a pessoas com uma necessidade comercial de os receberem. • Os ativos não podem ser enviados por fax a menos que o remetente tenha confirmado que os destinatários estão preparados para os 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.

Anexo B: Definições

Informações confidenciais do Barclays significa quaisquer informações obtidas pelo Responsável do Fornecedor, pelo Fornecedor ou por qualquer Pessoal do Fornecedor (ou a que qualquer um deles tenha acesso) relacionadas com estes termos gerais e/ou qualquer contrato relacionado com (i) quaisquer atividades empresariais, produtos e/ou desenvolvimentos passados, presentes ou futuros de qualquer Entidade Barclays e/ou (ii) funcionários, clientes, contrapartes, terceiros/fornecedores e/ou contratantes de qualquer entidade Barclays (que não Entidades do Fornecedor), incluindo toda a propriedade intelectual detida por qualquer Entidade Barclays (incluindo em conformidade com qualquer Contrato) ou qualquer Fornecedor externo/contratante, Dados pessoais protegidos, estes Termos gerais, cada Módulo e cada Contrato, e registos mantidos no âmbito de qualquer Contrato e quaisquer informações relacionadas com os planos, preços, metodologias, processos, dados financeiros, Direitos de propriedade intelectual, investigação, sistemas, programas e/ou tecnologias da informação da entidade ou pessoa aplicável;

Dados Barclays significa todos os dados, informações, texto, desenhos e outros materiais incorporados em qualquer suporte, incluindo todos os suportes eletrónicos, óticos, magnéticos ou tangíveis que (i) são acessíveis pelo fornecedor em ligação com qualquer contrato, (ii) são fornecidos ao fornecedor por qualquer entidade Barclays, ou (iii) que o fornecedor gera, recolhe, processa, armazena ou transmite em ligação com qualquer contrato, excluindo os materiais do fornecedor.

Sistemas Barclays significa os sistemas eletrónicos de informação que incluem um ou mais hardware, equipamento, software, periféricos e redes de comunicações detidas, controladas, operadas e/ou utilizadas por qualquer entidade Barclays.

Incidente cibernético significa qualquer evento, quer este tenha sido confirmado como tendo realmente ocorrido ou se o fornecedor ou o Barclays tiverem motivos razoáveis para acreditar que ocorreu (com base numa ameaça credível, informações ou outro), que tenha resultado ou tenha tido o potencial para resultar em risco para (i) a confidencialidade, integridade ou disponibilidade total dos dados Barclays, ou (ii) para a confidencialidade, integridade ou disponibilidade total e funcionamento normal de um sistema do fornecedor ou de um sistema Barclays.

Incidentes de tecnologia - Uma interrupção não programada de um serviço de TI ou uma redução na qualidade de um serviço de TI, incluindo, sem limitação, a falha de um item de configuração que ainda não tenha afetado um serviço. **Incidente grave** – Um Incidente que represente um risco/impacto significativo para o Barclays e que possa resultar em consequências graves, incluindo perda grave de produtividade, danos na reputação/regulamentares e impacto nos principais processos empresariais, controlos ou sistemas.

Avaliação do impacto da proteção de dados significa uma avaliação do impacto das operações de tratamento previstas na proteção de dados pessoais, conforme exigido pela legislação de proteção de dados.

Legislação de proteção de dados significa, na medida aplicável ao desempenho de quaisquer obrigações dos fornecedores ao abrigo de qualquer contrato: (i) a diretiva da UE relativa à privacidade e às comunicações eletrónicas 2002/58/CE (conforme periodicamente modificada ou substituída), (ii) o regulamento geral de proteção de dados da UE 2016/679 (o **RGPD**), as decisões e orientações da Comissão Europeia e toda a legislação nacional de implementação, (iii) o RGPD do Reino Unido, (iv) disposições da lei Gramm – Leach – Bliley relativas a informações pessoais não públicas, (v) a lei sobre a portabilidade e responsabilidade de seguros de saúde de 1996, e (vi) todas as outras leis, regulamentos e orientações regulamentares aplicáveis relativos à proteção de dados e privacidade em (a) qualquer jurisdição na qual a entidade Barclays relevante esteja localizada, as obrigações dos fornecedores sejam executadas, o titular dos dados relevante esteja localizado ou quaisquer dados pessoais protegidos estejam a ser processados, armazenados ou utilizados e (b) qualquer jurisdição na qual o fornecedor desempenhe qualquer uma das suas obrigações ao abrigo de qualquer contrato;

Obrigações de controlo da privacidade de dados significa qualquer programa de privacidade de dados que faça parte do Anexo 7 (Obrigações de controlo de fornecedores externos).

Titular dos dados tem o significado que lhe é atribuído pela legislação de proteção de dados. Sempre que tal termo não seja definido pela legislação de proteção de dados, deve significar uma pessoa singular identificada ou uma pessoa singular identificável que possa ser identificada, direta ou indiretamente, nomeadamente por referência a um identificador, como seja um nome, um número de identificação, dados de localização, um identificador online
ou um ou mais fatores específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.

Boas práticas do setor significa, em relação a qualquer tarefa e a quaisquer circunstâncias, o exercício do mais elevado grau de competência, diligência, prudência e previsão que seriam razoavelmente esperados de uma pessoa altamente qualificada e experiente que exerça o mesmo tipo de tarefa sob circunstâncias idênticas ou semelhantes.

Dados pessoais tem o significado que lhe é atribuído na legislação de proteção de dados. Quando esse termo não for definido pela legislação de proteção de dados, significa qualquer informação relacionada com, ou que direta ou indiretamente identifique, um titular dos dados.

Violação de dados pessoais tem o significado que lhe é atribuído na legislação de proteção de dados. Quando esse termo não for definido pela Legislação de proteção de dados, significa qualquer violação de segurança que resulte na destruição acidental ou ilegal, perda, alteração, divulgação não autorizada de, ou acesso a, Dados pessoais transmitidos, armazenados ou de outra forma Processados.

Tratamento tem o significado que lhe é atribuído na legislação de proteção de dados. Quando esse termo não for definido pela legislação de proteção de dados, significa qualquer operação ou conjunto de operações que seja realizada com base em dados pessoais, quer seja ou não por meios automáticos, tais como (sem limitação) recolha, registo, organização, armazenamento, adaptação ou alteração, recuperação, consulta, utilização, divulgação por

transmissão, disseminação ou disponibilização, alinhamento ou combinação, bloqueio, eliminação ou destruição, sendo que **Tratar** e **Tratado** devem ter os significados correspondentes;

Subcontratante significa qualquer terceiro que, periodicamente, forneça bens e/ou serviços relacionados com: (a) o fornecimento de produtos, serviços e/ou materiais a entregar; e/ou (b) o tratamento ou outra utilização de quaisquer dados pessoais protegidos, conforme permitido por um contrato.

Pessoal do fornecedor/de terceiros significa todas e quaisquer pessoas e/ou entidades que executem qualquer parte dos serviços ou forneçam qualquer produto ao abrigo de qualquer contrato, incluindo funcionários, subcontratantes e/ou agentes do fornecedor ou de qualquer um dos seus subcontratantes.

Sistemas do fornecedor/de terceiros significa quaisquer sistemas eletrónicos de informação (que podem incluir um ou mais hardware, equipamento, software, periféricos e redes de comunicações) que (ou parte dos quais) sejam: (i) utilizados para fornecer quaisquer produtos ou serviços a qualquer afiliada do Barclays em ligação com um contrato, ou (ii) que sejam mantidos, administrados, monitorizados ou estejam sob o controlo do fornecedor ou de um subcontratante em ligação com um contrato.

Sistema significa quaisquer sistemas eletrónicos de informação (que podem incluir um ou mais hardware, equipamento, software, periféricos e redes de comunicações) que (ou parte dos quais) sejam utilizados para fornecer quaisquer bens ou Serviços a qualquer Afiliada do Barclays em ligação com um Contrato.