Supplier Control Obligation (SCO)

Segurança das informações e cibersegurança (ICS)

Versão final 14.0 Outubro de 2024

Área de controlo/Título	Descrição do controlo	Por que é importante
1. Utilização aprovada	O fornecedor deve garantir que as informações e outros ativos associados estão devidamente protegidos, e são devidamente utilizados e tratados. Devem ser identificadas, documentadas e implementadas regras para a utilização aceitável e procedimentos para o tratamento de informações e outros ativos associados. Os funcionários do fornecedor, incluindo contratados, subcontratantes, subprocessadores das suas responsabilidades, que usem ou tenham acesso às informações da organização e outros ativos associados, devem ser informados sobre os requisitos de segurança de informações para proteger e lidar com as informações da organização e outros ativos associados. Devem ser responsáveis pela respetiva utilização de quaisquer instalações de processamento de informações. A organização deve estabelecer uma política específica de tópico sobre o uso aceitável de informações e outros ativos associados e comunicá-la a qualquer pessoa que use ou trate informações e outros ativos associados. O fornecedor tem de adotar as medidas adequadas para garantir a conformidade com os requisitos de utilização aceitável. Podem 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 (por ex., "Bring Your Own Device" [traga o seu próprio dispositivo]). • Utilização de dispositivos de memória portáteis/amovíveis. • Responsabilidades aquando do tratamento, gravação e armazenamento de ativos informacionais do Barclays. • Saída de canais de fuga de dados; e • Risco e consequências de utilização indevida dos pontos acima e/ou quaisquer resultados ilegais, danosos ou ofensivos decorrentes dessa utilização indevida.	Um requisito de utilização aceitável contribui para um ambiente de controlo que protege os ativos informacionais.
2. Segurança de limites e da rede	O fornecedor tem de garantir que todos os sistemas e aplicações operados pelo fornecedor e/ou subcontratantes/subprocessadores que suportem os serviços Barclays estão protegidos contra ameaças de rede de entrada e saída. Devem ser implementados controlos	Se este princípio não for implementado, as redes externas ou internas podem

	para garantir a segurança das informações nas redes e a proteção dos serviços ligados contra acesso não autorizado. O fornecedor deve identificar, proteger, detetar e responder a quaisquer alertas e violações de segurança. Os controlos de segurança da rede garantem a proteção das informações nas redes e respetivos mecanismos de processamento de informações de suporte, devendo incluir, entre outras, as seguintes áreas: • Manutenção de um inventário atualizado de todos os limites de rede da organização (através de uma arquitetura/diagrama de rede), devendo ser revisto pelo menos anualmente. • As ligações externas à rede do fornecedor devem ser documentadas, verificadas e aprovadas antes de as ligações serem estabelecidas para prevenir violações da segurança. • As redes do fornecedor devem ser protegidas através da aplicação de princípios "defesa em profundidade" (por ex., segmentação da rede, firewalls, etc.). • O fornecedor deve ter tecnologias de prevenção de intrusão na rede para detetar e evitar tráfego malicioso para todo o tráfego de entrada/saída e atualizar bases de dados de assinatura de acordo com as melhores práticas do setor e aplicar atualizações do fornecedor da solução de forma atempada. • O Fornecedor tem de garantir que a conectividade privada entre as nuvens privadas virtuais (VPC) e as redes de terceiros no local é encriptada e que o tráfego não é exposto à Internet pública. • Todo o tráfego da rede deve passar por um proxy configurado para filtrar ligações não autorizadas. • A separação lógica entre as portas/interfaces de gestão de dispositivos e o tráfego/LAN do utilizador; controlos de autenticação adequados. • Proteção das comunicações entre dispositivos e estações/consola de gestão. • Garantia de que o registo e a monitorização incluem a deteção e alerta de atividades suspeitas (utilizando comportamentos e indicadores de acionadores de compromisso), como através de uma SIEM (ferramenta de gestão de segurança de informações e eventos). • Ligação em rede entre gabinetes/fornecedor do serviço de nuvem/centros de dados tem de ser encriptada através de um protocolo de segurança. Os ativos informacionais/dados do Barclays em trânsito dentro da rede alargada (WAN) do fornecedor têm de ser encriptados. • O fornecedor deve rever as regras da firewall (firewall externa e interna) e deve revê-las pelo menos anualmente. • O fornecedor deve garantir que o acesso à rede interna é monitorizado através de controlos de acesso à rede adequados. • Todos os acessos sem fios à rede devem estar sujeitos a protocolos de autorização, autenticação, segmentação e encriptação forte para impedir violações de segurança. • O fornecedor tem de possuir uma rede separada (logicamente) para serviço(s) do Barclays.	ser sabotadas por invasores a fim de obterem acesso aos serviços e dados que estas contêm.

	O Fornecedor tem de garantir que todos os servidores e aplicações utilizados para a prestação do serviço ao Barclays não são implementados em redes não fidedignas (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 subcontratantes e subprocessadores) num centro de dados ou nuvem tem de possuir uma certificação de melhores práticas do setor para a gestão de segurança de rede. 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/terminação de última milha 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 Garantia de que o registo e a monitorização incluem a deteção e alerta de atividades suspeitas (utilizando comportamentos e indicadores de acionadores de compromisso), como através de uma SIEM (ferramenta de gestão de segurança de informações e eventos). **O fornecedor terceiro tem de garantir que quaisquer sistemas e aplicações que forneçam serviços que o Barclays considere serem, e comuniquem ao Fornecedor como sendo, de alto risco têm de ser segmentados em rede. A partição de uma aplicação empresarial e dos seus componentes principais de infraestruturas subjacentes (excluindo infraestruturas críticas partilhadas e generalizadas) no seu próprio segmento de rede, utilizando tecnologias de segurança aprovadas do Barclays (firewalls ou outras tecnologias equivalentes) para cumprir os princípios que se seguem.** i. É necessário adotar uma abordagem de segmentação para limitar a exposição ao risco, inibir o movimento lateral na rede e reduzir o risco de transmissão na rede. As aplicações devem ser implementadas em segmentos autónomos para ajudar a limitar o risco na medida do possível. Exemplo: zona de pagamentos mais rápida. Todas as infraestruturas e dados relacionados com aplicações empresariais têm de ser implementados numa zona de aplicação segura e autónoma, sempre que possível, e separados da rede interna do Barclays utilizando uma tecnologia de aplicação aprovada pelo CSO (por ex., firewalls de rede, solução de segmentação aprovada). Nota – alguns cenários podem requerer a divisão de componentes, como a aplicação e a base de dados em várias zonas, por ex., quando são utilizadas plataformas partilhadas. Cada aplicação deve ser avaliada individualmente, com a abordagem mais adequada definida e acordada com um consultor de segurança do CSO. ii. Os serviços devem ser segregados física ou logicamente. A estrutura de rede subjacente (por ex., cablagem/comutadores) pode ser partilhada com outras aplicações e serviços, ou seja, os segmentos podem ser logicamente definidos sem	

	o requisito de aplicar a segmentação através da separação física da restante rede Barclays. iii. As zonas de aplicação devem restringir os fluxos de tráfego de e para outras zonas (incluindo a rede interna CIPE), com base naquelas necessárias para o serviço funcionar e em quaisquer ferramentas de gestão, monitorização e segurança aprovadas. As configurações devem estipular portas, protocolos e endereços IP específicos para caminhos de comunicação permitidos, todas as outras comunicações devem ser restringidas por padrão. As regras que contêm intervalos devem ser evitadas e aprovadas apenas por exceção para garantir que apenas os requisitos mínimos de conectividade estão ativados. iv. Os recipientes devem ser devidamente segregados com controlos lógicos fortes que impeçam o movimento lateral interrecipiente, impondo assim o isolamento. O comprometimento de um recipiente não deve resultar no comprometimento de outros recipientes que estejam a funcionar no mesmo host/cluster. v. Todas as implementações de segmentação devem oferecer um recurso centralizado de gestão de políticas com funcionalidade (ou integração) para verificar e relatar a conformidade com as políticas (consulte o documento de Conformidade de firewall) e fornecer um registo auditável de alterações. vi. Devem ser realizadas inspeções/controlos com estado sempre que possível/exequível. vii. As capacidades de segmentação devem funcionar de forma "à prova de falhas", ou seja, se a capacidade falhar, os conjuntos de regras aprovados para bloquear/permitir o tráfego devem permanecer aplicados. viii. Qualquer tráfego entre sistemas de produção e não produção nas zonas de aplicação só deve ser permitido por exceção e deve ser registado. **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 controlos de segurança de rede adequados para salvaguardar o serviço Barclays - • O cliente de serviços na nuvem (CSC) deve definir os seus requisitos para segregar redes de forma a obter isolamento de inquilinos no ambiente partilhado de um serviço na nuvem e verificar se o prestador de serviços na nuvem cumpre esses requisitos. • A política de controlo de acesso do cliente de serviços na nuvem para a utilização de serviços de rede deve especificar requisitos para o acesso do utilizador a cada serviço na nuvem separado utilizado. *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.*	
3. 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 o respetivo fornecedor podem não conseguir impedir

	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 DDoS/DoS adequada para assegurar a disponibilidade. Se o fornecedor estiver a alojar **sistemas e aplicações que forneçam serviços** e detenham dados do Barclays ou sustentem um serviço de categorias 0 ou 1 de resiliência, este deve ter proteção DoS adequada para garantir a disponibilidade.	que um ataque de recusa de serviço atinja o seu objetivo.
4. Trabalho remoto (Acesso remoto)	O fornecedor deve garantir a segurança das informações enquanto os funcionários trabalham remotamente. Devem ser implementadas medidas de segurança para proteger as informações acedidas e processadas fora das instalações da organização enquanto trabalham remotamente. O fornecedor deve fornecer instruções aos colaboradores relativamente ao trabalho a partir de casa. **Acesso remoto à rede Barclays** O acesso remoto à rede Barclays através da aplicação Barclays Citrix não é fornecido por predefinição. Para aceder à Rede Barclays a partir de locais não aprovados/fora do escritório/a partir de casa, e qualquer acesso remoto, têm de ser obtidas aprovação e autorização prévias do Barclays (gabinete do Diretor de segurança – Equipa TPSecM [externalcyberassurance@barclayscorp.com]). O fornecedor tem de garantir o estabelecimento dos seguintes controlos para o acesso remoto: • O acesso à rede Barclays exige um token RSA (soft) e uma versão suportada da aplicação Citrix Workspace; o Barclays fornecerá detalhes • O fornecedor deve manter um registo atualizado e correto dos seus funcionários aprovados para trabalhar remotamente/em regime misto com justificação empresarial para cada funcionário aprovado, incluindo subcontratantes/subprocessadores. • **O Fornecedor tem de realizar a reconciliação de todos os funcionários com acesso remoto trimestralmente, fornecendo os seus resultados ao Barclays (gabinete do Diretor de segurança – Equipa TPSecM [externalcyberassurance@barclayscorp.com]).** • 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 a contar da data de saída/último dia no escritório (LDIO)** • 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 se ligar remotamente aos 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 remota através da aplicação Citrix Barclays têm de ser aprovados e autorizados pelo Barclays (gabinete do Diretor	Os controlos de Acesso remoto ajudam a garantir que dispositivos inseguros e não autorizados não estão remotamente ligados ao ambiente Barclays.

	de segurança – Equipa TPSecM – externalcyberassurance@barclayscorp.com). O fornecedor tem de manter registos e realizar uma reconciliação trimestral. • Os dispositivos pessoais/"bring your own device" (BYOD) (limitados a computador portátil/computador de secretária) 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, contratantes e parceiros de serviços geridos, subcontratantes/subprocessadores). Nota: o acesso remoto à rede Barclays e os dados Barclays não é permitido exceto se especificamente aprovado e autorizado pelo Barclays. Acesso remoto ao ambiente/rede do fornecedor Acesso remoto ao ambiente gerido pelo fornecedor para prestação de serviços que inclui dados da Barclays residentes/armazenados e/ou processados no ambiente/rede do fornecedor. O Fornecedor tem de garantir o estabelecimento dos seguintes controlos para a rede corporativa do Fornecedor para acesso remoto. • O acesso por login remoto à rede do fornecedor tem de ser fortemente encriptado durante os dados em trânsito e com a utilização de uma autenticação multifator. • O fornecedor pode utilizar o ambiente de trabalho virtual para acesso remoto • O fornecedor tem de manter registos de indivíduos que tenham estado a trabalhar remotamente/em regime misto. • O fornecedor deve realizar a reconciliação de todos os utilizadores remotos de acordo com os prazos do fornecedor • O fornecedor procederá à desativação das credenciais de autenticação que já não necessitem de acesso (por ex., cessação do contrato do funcionário, reatribuição do projeto, etc.) num prazo de 24 (vinte e quatro) horas a contar da data de saída/último dia no escritório (LDIO) • Os dispositivos pessoais/"bring your own device" (BYOD) (imitados a computador portátil/computador de secretária) não podem dispor de acesso aos dados Barclays que residam/armazenados no ambiente gerido pelo fornecedor (incluindo pessoal do fornecedor, consultores, funcionários de contingência, contratantes e parceiros de serviços geridos). Os funcionários devem receber as regras do fornecedor relativas ao trabalho a partir de casa, incluindo o que fazer e o que não fazer. As capacidades de trabalho remoto (incluindo a partir de casa) são proibidas durante o decurso normal de negócios, quando terceiros sejam contratualmente obrigados a prestar serviços a partir do espaço dedicado do Banco ou das instalações do fornecedor ou quando são aplicáveis requisitos regulamentares. No entanto, são permitidas disposições em planos de continuidade de negócios de terceiros em caso de resposta a recuperação de	

<table>
<tr><td></td><td>desastres/crise/pandemia de acordo com o Barclays e quaisquer requisitos de segurança exigidos para o trabalho remoto no âmbito do acordo contratual.</td><td></td></tr>
<tr><td>5. Gestão de registos de segurança</td><td>O fornecedor tem de ter uma estrutura de gestão de registos e de apoio de auditoria bem estabelecida. A estrutura deve incluir os principais sistemas de TI, incluindo aplicações, equipamentos de rede, dispositivos de segurança e servidores definidos para registar eventos principais. Para registar eventos, gerar provas, garantir a integridade das informações de registo, os registos devem ser invioláveis, impedir o acesso não autorizado, identificar eventos de segurança de informações que possam levar a um incidente de segurança de informações e apoiar investigações. O fornecedor deve garantir que os registos são centralizados, devidamente protegidos contra adulteração e/ou eliminação e mantidos pelo fornecedor por um período mínimo de 12 meses ou conforme requisito regulamentar, o que for mais extenso.

<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><tr><td>Retenção dos registos</td><td>3 meses</td><td>6 meses</td><td>12 meses</td></tr></table>
A estrutura de gestão de registos de segurança deve cobrir as seguintes áreas:
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 monitorizar, detetar, compreender e/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.
Os exemplos de registo de eventos podem incluir:
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 as melhores práticas do setor adequadas têm de estar ativadas, incluindo aqueles que foram terceirizados ou que se encontram "na nuvem".
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, MFA, controlo de acesso e cópia de segurança).</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>

	• 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. • A análise do registo deve abranger a análise e interpretação de eventos de segurança de informações, para ajudar a identificar atividades incomuns ou comportamentos anómalos, que podem representar indicadores de comprometimento. • Os eventos-chave registados têm de incluir aqueles com potencial de impacto na confidencialidade, integridade e disponibilidade dos serviços para o Barclays e que podem ajudar na identificação ou investigação de incidentes e/ou violações de direitos de acesso que ocorrem relativamente a sistemas do fornecedor. • Testagem periodicamente de que a estrutura continua a cumprir os requisitos acima. 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 controlos de Gestão de registos de segurança adequados para salvaguardar o serviço Barclays - • O cliente de serviços na nuvem deve definir e documentar os seus requisitos para o registo de eventos e verificar se o serviço na nuvem cumpre esses requisitos. • Se uma operação privilegiada for delegada ao cliente de serviços na nuvem, a operação e o desempenho dessas operações devem ser registados. O cliente de serviços na nuvem deve determinar se as capacidades de registo fornecidas pelo fornecedor de serviços na nuvem são adequadas ou se o cliente de serviços na nuvem deve implementar capacidades de registo adicionais. • O cliente de serviços na nuvem deve solicitar informações sobre a sincronização do relógio utilizada para os sistemas do fornecedor de serviços na nuvem. • O cliente de serviços na nuvem deve solicitar informações ao fornecedor de serviços na nuvem sobre as capacidades de monitorização de serviços disponíveis para cada serviço na nuvem.	
6. Defesas contra malware	Em linha com as melhores práticas do setor, o fornecedor deve ter políticas e procedimentos estabelecidos, bem como processos de apoio ao negócio e medidas técnicas implementados para prevenir a execução de malware em todo o ambiente 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 incluir, entre outros, 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 o ambiente de TI da organização. • Garantia de que o software antimalware da organização atualiza o seu mecanismo de verificação. • Atualizar regularmente 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 e ataques a dispositivos móveis utilizados para serviços Barclays. • O gateway de e-mail analisa todas as comunicações de e-mail recebidas, enviadas e internas, incluindo anexos e URLs quanto a sinais de conteúdo malicioso ou nocivo. Nota: "antimalware" deve incluir a deteção de, entre outros, códigos móveis não autorizados, vírus, spyware, software "keylogger", "botnets", "worms", "trojans", etc.	
8. Segurança de ponto final	O fornecedor deve adotar uma abordagem unificada de gestão de pontos finais para garantir que os seus pontos finais utilizados para aceder à rede do Barclays, ou para aceder aos e/ou processar ativos informacionais/dados Barclays, são reforçados para proteção contra ataques. Têm de ser implementadas as melhores práticas do setor e a segurança de ponto final tem de incluir, entre outros: • Encriptação total do disco rígido. • Desativação de todo o software/serviços/portas desnecessários. • Desativação do acesso por direitos de administração para os utilizadores locais. • Funcionários do fornecedor não poderão alterar as definições básicas, como o Pacote de serviço predefinido, a partição do sistema e serviços predefinidos, antivírus, etc. • Desativação da porta USB para não permitir copiar Informações/dados Barclays para suportes externos • Atualização com as assinaturas de antivírus e patches de segurança mais recentes. • Desativação do serviço de spooler de impressão • Ferramenta de prevenção de dados para proteger contra a violação de dados do Barclays • O fornecedor deve garantir que bloqueia a transferência de dados não autorizada de dados Barclays para websites de redes sociais, serviços de webmail e websites com capacidade para armazenar informações como, entre outros, o Google Drive, Dropbox, iCloud. • Desativação da partilha/transferência de dados Barclays em ferramentas/software de mensagens instantâneas. • Deteção, interrupção e correção da presença e/ou utilização de software não autorizado, incluindo software malicioso.	Se este controlo não for implementado, a rede e os pontos finais do Barclays e do fornecedor podem ficar vulneráveis a ciberataques.

	• O tempo limite do ecrã de bloqueio é ultrapassado, limita a conexão TCP IP apenas à rede corporativa, agente de segurança Advanced EPS para detetar comportamentos suspeitos Nota: 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 numa empresa com base nas normas de configuração aprovadas pela organização. Qualquer implementação de sistema novo ou sistema existente que ficou comprometido deve ser configurada utilizando imagens ou modelos aprovados. Nos casos em que é atribuído acesso de pontos finais (computador portátil/computador de secretária) à rede Barclays através de aplicações Citrix Barclays pela Internet, o fornecedor deverá instalar a ferramenta de análise de ponto final (EPA) disponibilizada pelo Barclays para validar a segurança do ponto final e a conformidade do sistema operativo, sendo que apenas os dispositivos que passem nas verificações da análise de ponto final obterão acesso remoto à rede Barclays através da aplicação Citrix Barclays. Caso o Fornecedor não consiga instalar ou utilizar a ferramenta EPA, tem de abordar o tema junto do seu Gestor de relações Barclays/equipa de suporte de TI/equipa TPSecM Barclays. Dispositivos móveis utilizados para os serviços Barclays - • O fornecedor tem de garantir que implementa capacidades de gestão unificada de pontos finais (UEM) ou gestão de dispositivos móveis (MDM) a fim de controlar e gerir de forma segura os dispositivos móveis ao longo do ciclo de vida que tenham acesso e/ou contenham informação classificada do Barclays, reduzindo o risco de comprometimento dos dados. • O fornecedor deve garantir a existência e a utilização 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 • Encriptação de dados Barclays armazenados e/ou processados nos dados do dispositivo móvel • O fornecedor tem de garantir que os dispositivos móveis não estão enraizados e que a política de autenticação forte está ativada	

9. Prevenção de fuga de dados	O fornecedor deve utilizar uma estrutura eficaz aprovada pela gestão para proteger os dados Barclays de fugas/transferência de dados não autorizada e incluir, entre outros, canais de fuga de dados: -
	
	• Transferência não autorizada de informações para fora da rede interna/da rede do fornecedor
	  ○ E-mail
	  ○ Internet/gateway Web (incluindo armazenamento online e webmail)
	  ○ DNS
	• Perda ou roubo de ativos informacionais do Barclays em meios eletrónicos portáteis (incluindo informações eletrónicas contidas em computadores portáteis, dispositivos móveis e meios portáteis).
		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 autorizadas (integridade) e que pode ser recuperada e apresentada

	• Transferência não autorizada de informações para dispositivos portáteis através de ligação (por exemplo, série, USB) e sem fios (por exemplo, Bluetooth, Wi-Fi). • Troca insegura de informações com terceiros (subcontratantes, subprocessadores). • Impressão ou reprodução inadequada de informações. As medidas de prevenção de fugas de dados devem ser aplicadas a sistemas, redes e quaisquer outros dispositivos que processem, armazenem ou transmitam dados/informações do Barclays.	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
10. Segurança de dados	O fornecedor tem de proteger os dados Barclays detidos e/ou processados pelo mesmo através de uma combinação de técnicas de encriptação, proteção da integridade e prevenção de perdas de dados. O acesso aos dados Barclays tem de ser restringido apenas aos seus funcionários autorizados e protegido contra contaminação, ataques de agregação, ataques de inferência, ameaças de armazenamento, incluindo, entre outras, ameaças de ambientes de computação em nuvem. Os controlos de segurança de dados devem incluir, entre outras, as seguintes áreas: 1. O fornecedor é obrigado a cumprir sempre quaisquer leis de proteção de dados aplicáveis. 2. Estabelecimento de políticas, processos e procedimentos, apoiando processos empresariais e medidas técnicas. Documentação e manutenção de fluxos de dados mantidos na localização geográfica do serviço (física e virtual). Deve abranger detalhes relacionados com aplicações e componentes do sistemas parte do fluxo de dados. 3. Manutenção de diagrama de fluxo de dados Barclays mantidos em localizações geográficas (incluindo físicas e virtuais) em aplicações e componentes do sistema. 4. Manutenção de um inventário de todas as informações Barclays sensíveis/confidenciais armazenadas, processadas ou transmitidas pelo fornecedor. 5. Garantia de que todos os dados Barclays são classificados e marcados com base na norma de classificação e proteção de informações aprovada pela gestão. 6. Proteção de dados inativos. a. Encriptação forte de dados inativos para evitar a exposição de ativos informacionais Barclays 7. Monitorização da atividade da base de dados. a. Monitorizar e registar o acesso e a atividade da base de dados para identificar atividades maliciosas de forma rápida e eficaz. 8. Proteção de dados em utilização. a. Garantia de controlos da capacidade de gestão do acesso ao processamento de informações sensíveis, 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 utilização 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 forte 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: 10. "Transport Layer Security" (TLS) (conforme as melhores práticas do setor relativas a criptografia moderna, incluindo utilização/rejeição de protocolos e cifras) 11. Todos os dados armazenados no ambiente de produção e não produção devem ser protegidos com encriptação (consultar controlo 16 Criptografia)	
11. Segurança de software de aplicação	O fornecedor tem de desenvolver aplicações com recurso a práticas de codificação seguras e em ambientes seguros. Quando o fornecedor desenvolver aplicações para utilização pelo Barclays, ou que sejam utilizadas para apoiar o serviço prestado ao Barclays, o fornecedor deve estabelecer uma estrutura de desenvolvimento segura de software para integrar a segurança no ciclo de vida do desenvolvimento de software. O fornecedor deve testar e corrigir vulnerabilidades no software antes de o entregar ao Barclays. A segurança de software de aplicação deve incluir, entre outras, as seguintes áreas:	Os controlos que protegem o desenvolvimento da aplicação ajudam a garantir que as aplicações estão protegidas no momento da implementação.

	• Estabelecimento e adoção de normas de codificação segura aprovadas pela gestão e alinhadas com as melhores práticas do setor para evitar vulnerabilidades e interrupções de serviço. • 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 do setor relativas ao desenvolvimento seguro (por ex., OWASP). • O código deve ser armazenado de forma segura e submetido a processos de garantia de qualidade. • Não deve copiar informações sensíveis para os ambientes de desenvolvimento e teste do sistema, a menos que sejam fornecidos controlos equivalentes para os sistemas de desenvolvimento e teste. • 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 informações pessoais) não são utilizados em ambientes de não produção. • As aplicações e interfaces de programação (API) deverão ser concebidas, desenvolvidas, implementadas e testadas de acordo com as melhores práticas do setor (por ex., OWASP para aplicações Web). • Utilização proibida de repositórios de códigos públicos 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 e atuais 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. 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 exequível, deve ser implementada uma firewall de aplicação Web baseada no anfitrião. O fornecedor tem de garantir que todas as soluções de aplicação que utilizam a Internet baseadas em "software como um serviço" ("Software as a Service" [SaaS]) utilizadas para o Barclays Service têm de ter controlo de acesso suplementar (controlo de autenticação), para além de um controlo de autenticação tradicional (nome de utilizador/palavra-passe). O fornecedor deve incluir, entre outras, as seguintes áreas: • Autenticação multifatores (por exemplo, token, SMS) • SSO (Início de sessão único) • Controlo de acesso baseado em endereço IP	

	O controlo de acesso suplementar tem de ser fornecido para funcionários do fornecedor/subcontratados/subprocessadores/funcionários do Barclays/clientes e/ou clientes do Barclays.	
12. Gestão de acesso lógico (Logic Access Management, ou LAM)	O acesso a ativos informacionais (incluindo software, hardware e dados) só pode ser concedido com base na necessidade de conhecimento, seguindo o princípio de privilégio mínimo. O proprietário do sistema de TI/ativo informacional é responsável por fornecer uma lista de todas as contas que têm acesso ao sistema/ativo informacional, bem como definir o modelo de segurança de acesso lógico, incluindo aceder a perfis e regras de segregação de deveres (SOD). As aplicações Web alojadas pelo fornecedor são abrangidas pela integração de gestão de acesso lógico (LAM) do Barclays e têm de ser implementados controlos LAM do Barclays para estas aplicações. • A base **necessidade de tomar conhecimento** significa que os funcionários só devem ter acesso às informações de que necessitem para desempenhar as funções autorizadas. Por exemplo, se um funcionário lida exclusivamente com clientes estabelecidos no Reino Unido, não "necessita de tomar conhecimento" de informações referentes a clientes estabelecidos nos EUA. • O princípio de **Privilégio Mínimo** significa que os funcionários devem ter apenas o nível mínimo de acesso necessário para desempenhar as suas funções autorizadas. Por exemplo, se um funcionário 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. • A **segregação de deveres (SoD)** é uma abordagem para estruturar tarefas de forma a que uma tarefa não possa ser concluída por um único indivíduo, com o objetivo principal de mitigar o risco de fraude. Por exemplo, o funcionário que solicita a criação de uma conta não deve ser o mesmo que aprova o pedido. Os processos de gestão de acesso têm de ser definidos, documentados e aplicados de acordo com as melhores práticas da indústria, em que, de acordo com a Política de informação e cibersegurança do Grupo Barclays e com a Norma de gestão de identidade e acesso (IAM), se exige o seguinte: • **Integração LAM do Barclays:** O fornecedor tem de garantir que os processos de gestão de acesso estão a tirar partido do conjunto de ferramentas central IAM do Barclays para facilitar os controlos LAM. As listas de controlo de acesso (ACLs) do sistema de TI	Controlos LAM apropriados ajudam a garantir que os ativos informacionais são protegidos contra utilização indevida. Os controlos de gestão de acesso ajudam a garantir que apenas utilizadores aprovados podem aceder a ativos informacionais.

	devem ser enviadas à equipa do IAM no âmbito do processo de integração do sistema de TI no conjunto de ferramentas IAM. Para assegurar o funcionamento mais eficaz dos controlos LAM a jusante, o Fornecedor tem de garantir que a frequência de alimentação é uma alimentação automatizada diária. Nos sistemas que suportam o acesso principal dos utilizadores, por exemplo, Domínio/Acesso remoto, Troca, a ACL tem de ser diária. • Controlos de quem entra: todo o acesso deve ser adequado e aprovado antes do fornecimento. • Controlos de quem muda: todo o acesso deve ser revisto antes do dia da transferência para confirmar o acesso que deve ser retido, revogado e ativado. O acesso confirmado para revogação tem de ser removido antes do dia de transferência. • Controlos de quem sai: todo o acesso utilizado para aceder aos recursos de informações do Barclays e/ou prestar serviços ao Barclays tem de ser removido na data de fim do contrato do funcionário com o Fornecedor. • Titularidade da conta: uma conta exclusiva tem de ser associada a um funcionário, que deve ser responsável por qualquer atividade realizada com acesso à mesma. Os detalhes da conta e as palavras-passe não podem ser partilhados com qualquer outro funcionário. • Contas inativas: contas que não são utilizadas por um período igual ou superior a 60 dias consecutivos devem ser suspensas/desativadas (sendo mantidos os respetivos registos). • Recertificação de acesso: todo o acesso deve ser revisto, a cada 12 meses (para acesso não privilegiado) e a cada 6 meses (para acesso privilegiado), para garantir que o acesso permanece adequado. • Verificação de identidade (ID&V): têm de ser implementados controlos para garantir que os processos de gestão de acesso incluem mecanismos para a verificação de identidade. • Autenticação: todas as contas devem ser autenticadas antes que o acesso lógico seja concedido. As aplicações e os mecanismos de autenticação não devem exibir palavras-passe ou PIN. O comprimento e a complexidade adequados da palavra-passe, o histórico de palavras-passe, a frequência de alterações da palavra-passe, a autenticação multifatores e a gestão segura de credenciais têm de estar implementados. • Proteção de credenciais não pessoais: as credenciais não pessoais (ou seja, palavras-passe e segredos) têm de ser introduzidas numa ferramenta de gestão de credenciais adequada (por exemplo, CyberArk). Quando tal não for possível, as credenciais têm de ser protegidas para que nenhum ser humano consiga utilizá-las. Quando for necessária	

	a utilização humana da conta, o acesso tem de ser temporário e limitado e as credenciais têm de ser repostas posteriormente. • Gestão de credenciais: as palavras-passe das contas pessoais têm de ser alteradas, no mínimo, a cada 90 dias. As palavras-passe para contas privilegiadas e interativas têm de ser alteradas a cada 120 dias ou após cada utilização humana, de modo a que nenhum ser humano tenha conhecimento da palavra-passe ou, se a palavra-passe tiver 30 caracteres ou mais, a cada 365 dias ou após cada utilização humana, para que nenhum ser humano tenha conhecimento da palavra-passe. As palavras-passe para contas interativas têm de ser diferentes das 12 palavras-passe anteriores. • Acesso com limite de tempo: o acesso privilegiado pessoal à infraestrutura de produção e recuperação de desastres utilizada pelo pessoal do Barclays ou pelo pessoal não permanente do Barclays tem de ter limitação temporal, com as aprovações adequadas em vigor. • Monitorização da atividade privilegiada: deve ser realizada uma monitorização da atividade privilegiada. 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 controlos de gestão de acesso lógico adequados para salvaguardar o serviço Barclays - • O cliente de serviços na nuvem deve utilizar técnicas de autenticação suficientes (por ex., autenticação multifator) para autenticar os administradores de serviços na nuvem do cliente de serviços na nuvem para as capacidades administrativas de um serviço na nuvem de acordo com os riscos identificados. • O cliente de serviços na nuvem deve garantir que o acesso às informações no serviço na nuvem pode ser restringido de acordo com a sua política de controlo de acesso e que essas restrições são aplicadas. Isto inclui restringir o acesso a serviços na nuvem, funções de serviços na nuvem e dados de clientes de serviços na nuvem mantidos no serviço. • Quando a utilização de programas utilitários for permitida, o cliente de serviços na nuvem deve identificar os programas utilitários a serem utilizados no seu ambiente de computação em nuvem e garantir que não interferem com os controlos do serviço na nuvem.	
13. Gestão de vulnerabilidades	O Fornecedor tem de executar um programa de gestão de vulnerabilidades eficaz através de políticas e procedimentos estabelecidos, processos de apoio/medidas organizacionais e técnicas para a monitorização eficaz, deteção atempada e correção de vulnerabilidades	Se este controlo não for implementado, os atacantes podem explorar as

<table>
<tr>
<td></td>
<td>dentro das aplicações detidas ou geridas pelo Fornecedor, ou aplicação/Código desenvolvido, rede da infraestrutura e dos componentes do sistema, a fim de garantir a eficiência dos controlos de segurança implementados.

A gestão de vulnerabilidades deve abranger, entre outras, as seguintes áreas:

• Funções e responsabilidades definidas para monitorização, comunicação, encaminhamento e correção.
• Ferramentas e infraestrutura adequadas para análise de vulnerabilidades.
• O fornecedor de serviços irá realizar análises de vulnerabilidades de forma rotineira utilizando assinaturas de vulnerabilidade atualizadas (com a regularidade prevista pelas melhores práticas do setor), 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.
• 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 (correção a ocorrer de modo oportuno e de acordo com as melhores práticas do setor ou com o programa de gestão de patches).
• 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.
• Comparação regular dos resultados das análises consecutivas das vulnerabilidades a fim de verificar quais destas foram resolvidas de forma atempada.

Para serviços do fornecedor relacionados com infraestruturas de alojamento/aplicações em nome do Barclays (incluindo terceiros de alto risco comunicados)

• O fornecedor tem de notificar imediatamente o Barclays caso sejam identificadas quaisquer vulnerabilidades críticas/altas.
• O fornecedor tem de corrigir as vulnerabilidades em linha com a tabela abaixo ou em acordo com o Barclays (gabinete do Diretor de segurança – Equipa TPSecM).
<table>
<tr><th>Prioridade</th><th>Classificação</th><th>Dias para conclusão (máximo)</th></tr>
<tr><td>P1</td><td>Crítica</td><td>15 (máx. 30 dias)</td></tr>
</table>
</td>
<td>vulnerabilidades dos sistemas para realizarem ciberataques que podem resultar em danos regulamentares e para a reputação.</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td>
<table>
<tr><td>P2</td><td>Alta</td><td>60</td></tr>
<tr><td>P3</td><td>Média</td><td>180</td></tr>
<tr><td>P4</td><td>Baixa</td><td>Sem acordo de nível de serviço</td></tr>
</table>
Todos os problemas de segurança e vulnerabilidades passíveis de afetar substancialmente a infraestrutura de alojamento/aplicações 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 TPSecM – externalcyberassurance@barclayscorp.com).

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 controlos de gestão de vulnerabilidades adequados para salvaguardar o serviço Barclays -

• O cliente de serviços na nuvem deve solicitar informações ao fornecedor de serviços na nuvem sobre a gestão de vulnerabilidades técnicas que podem afetar os serviços na nuvem fornecidos. O cliente de serviços na nuvem deve identificar as vulnerabilidades técnicas pelas quais será responsável e definir claramente um processo para a gestão das mesmas.
</td>
<td></td>
</tr>
<tr>
<td>14. Gestão de patches</td>
<td>O Fornecedor tem de estabelecer um programa de Gestão de patches apoiado em políticas e procedimentos estabelecidos, processos empresariais/medidas organizacionais e técnicas para monitorizar/rastrear a necessidade de patching e de execução de patches de segurança para gerir todo o ambiente/património do Fornecedor.

O fornecedor deve garantir que os servidores, dispositivos de rede, aplicações e dispositivos de ponto final são mantidos atualizados com os patches de segurança mais recentes e em conformidade com as melhores práticas do setor, garantindo que:

• O fornecedor deve avaliar e 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 mesmo.
</td>
<td>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.</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td>Se o sistema não puder receber patches, será necessário implementar contramedidas adequadas.
• Todas as alterações essenciais de TI anteriores à implementação têm de ser registadas, testadas e aprovadas através de um processo de gestão de alterações aprovado e consistente para apoiar futuras auditorias, investigações, resolução de problemas e requisitos de análise.
• O fornecedor tem de verificar que os patches são refletidos nos ambientes de produção e de recuperação de desastre (DR).</td>
<td></td>
</tr>
<tr>
<td>15. Teste de penetração/avaliação de segurança de TI</td>
<td>O fornecedor tem de colaborar com um prestador de serviços de segurança qualificado e independente para realizar uma avaliação de segurança de TI/Teste de penetração que cubra a infraestrutura 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 segurança dos dados Barclays através de ciberataques. Todas as vulnerabilidades devem ser priorizadas e acompanhadas até à sua resolução. O teste tem de ser efetuado de acordo com as melhores práticas do setor.

Para serviços do fornecedor relacionados com infraestruturas de alojamento/aplicações em nome do Barclays (incluindo terceiros de alto risco comunicados)
• O Fornecedor tem de informar e acordar com a TPSecM o âmbito da avaliação de segurança com o Barclays, 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 TPSecM).
• O Fornecedor deve partilhar anualmente o mais recente relatório de avaliação de segurança com o Barclays (gabinete do Diretor de Segurança – Equipa TPSecM – externalcyberassurance@barclayscorp.com)
• O fornecedor tem de notificar imediatamente o Barclays caso sejam identificadas quaisquer vulnerabilidades críticas/altas.
• O fornecedor tem de corrigir as vulnerabilidades em linha com a tabela abaixo ou em acordo com o Barclays (gabinete do Diretor de segurança – Equipa TPSecM).
<table>
<tr><th>Prioridade</th><th>Classificação</th><th>Dias para conclusão (máximo)</th></tr>
<tr><td>P1</td><td>Crítica</td><td>15 (máx. 30 dias)</td></tr>
</table>
</td>
<td>Se este controlo não for implementado, o fornecedor pode não conseguir avaliar as ameaças cibernéticas com que se depara, 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 danos regulamentares ou para a reputação.</td>
</tr>
</table>

<table>
<tr><td></td><td></td><td><table>
<tr><td>P2</td><td>Alta</td><td>60</td></tr>
<tr><td>P3</td><td>Média</td><td>180</td></tr>
<tr><td>P4</td><td>Baixa</td><td>Sem acordo de nível de serviço</td></tr>
</table></td><td></td><td></td></tr>
<tr><td>16. Criptografia</td><td colspan="3">O Fornecedor tem de garantir a utilização adequada e eficaz da criptografia para proteger a confidencialidade, autenticidade ou integridade dos dados/informações do Barclays de acordo com os requisitos de segurança de informações e da empresa e tendo em consideração os requisitos legais, regulamentares e contratuais relativos à criptografia.

Ao usar criptografia, deve-se considerar o seguinte:
a política de criptografia específica de tópico definida pela organização, incluindo os princípios gerais para a proteção de informações. É necessária uma política específica de tópico sobre a utilização da criptografia para maximizar os benefícios e minimizar os riscos de utilização de técnicas criptográficas e evitar uma utilização inadequada ou incorreta.
identificar o nível de proteção necessário e a classificação das informações e, consequentemente, estabelecer o tipo, a força e a qualidade dos algoritmos criptográficos necessários.
a utilização de criptografia para proteção de informações mantidas em suportes de armazenamento e transmitidas através de redes a esses dispositivos ou suportes de armazenamento.
A abordagem da gestão de chaves, incluindo métodos para tratar da geração e proteção de chaves criptográficas e a recuperação de informações criptografadas em caso de chaves perdidas, comprometidas ou danificadas.
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 que detalhem os processos "ponto a ponto" para a gestão de chaves, desde a geração ao carregamento, distribuição e destruição. O Fornecedor tem de retirar as suas chaves após o período de serviço terminar ou configurar um programa de rotação de chaves obrigatório.</td><td>A atualização e a adequação da proteção de encriptação e dos algoritmos garantem a proteção ininterrupta dos ativos informacionais do Barclays.</td></tr>
</table>

	• 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.
	• 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.
	• Geração de chaves e "período de criptografia" - 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 ("período de criptografia") definido e limitado, sendo substituídas ou desativadas após este período. Este requisito também tem de estar em linha com os requisitos do "National Institute of Standards and Technology" (NIST) e melhores práticas 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.
	  o 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. Isto inclui:
	  o Chaves de serviços regulados nos quais os HSM são mandatados.
	  o Certificados que representam o Barclays nas CA públicas.
	  o Certificados de raiz, de emissão, OCSP e RA (autoridade de registo) utilizados para emissão de certificados que protejam os serviços Barclays.
	  o 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: o Equipa de suporte de TI o Ativos associados o 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, no mínimo, 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 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 a remoção de algoritmos fracos e que os algoritmos e o comprimento das chaves utilizadas estão em conformidade com os requisitos do National Institute of Standards and Technology (NIST) e melhores práticas do setor aplicáveis. • O fornecedor deve avaliar a utilização de algoritmos vulneráveis quânticos e planos de migração para resolver o problema.	
17. Computação em nuvem	O fornecedor (cliente de serviços na nuvem, CSC) tem de garantir que o serviço de nuvem utilizado para serviço(s) Barclays possui uma estrutura de controlos de segurança bem definidos para atingir os objetivos de confidencialidade, integridade e disponibilidade e para assegurar que os controlos de segurança estão implementados e funcionam eficazmente para serviço(s) Barclays. O fornecedor deve possuir uma certificação ISO/IEC 27017 ou 27001 ou SOC 2 ou estrutura de segurança de nuvem semelhante ou melhores práticas do setor como possuindo medidas de segurança estabelecidas e implementadas para garantir que toda a utilização de tecnologia de nuvem é segura. Assegurar que o prestador de serviço de nuvem possui certificação pelas melhores práticas do setor, incluindo controlos adequados equivalentes à mais recente versão da "Cloud Security Alliance", a "Cloud Controls Matrix" (CCM). O fornecedor é responsável por assegurar controlos de segurança de dados relativamente a ativos informacionais/dados Barclays, incluindo informações pessoais na nuvem, e o prestador de serviços na nuvem (CSP) é responsável pela segurança do ambiente de computação em nuvem. O fornecedor permanece responsável pela configuração e monitorização da implementação de controlos de segurança para proteger contra quaisquer incidentes de segurança, incluindo violações de dados. O Fornecedor tem de implementar medidas de segurança de modo transversal a todos os aspetos do serviço sendo prestado, incluindo o modelo de responsabilidade partilhada da nuvem, salvaguardando a confidencialidade, integridade, disponibilidade e acessibilidade através da minimização de oportunidade de pessoas não autorizadas obterem acesso a Informação do Barclays e aos serviços utilizados pelo Barclays. Os controlos de segurança na nuvem devem abranger, entre outros, os seguintes domínios de modelos de implementação (IaaS/PaaS/SaaS):	Se este controlo não for implementado, os dados do Barclays podem ficar comprometidos, o que pode resultar em danos regulamentares ou para a reputação.

	• Mecanismos de governação e responsabilidade • Gestão de identidade e acesso • Segurança de rede (incluindo conectividade) • Proteção de dados (em trânsito/inativos/armazenados) • Eliminação/purga segura de dados • Criptografia, encriptação e gestão de chaves - CEK • Registo e monitorização • Virtualização • Segregação de serviços Os Ativos informacionais/Dados Barclays, incluindo informações pessoais armazenadas na nuvem como parte do serviço prestado ao Barclays, têm de ser aprovados pelo mesmo (gabinete do Diretor de Segurança – Equipa TPSecM). O fornecedor deverá fornecer ao Barclays localizações de zonas de dados e zonas de dados de ativação pós-falha onde os dados Barclays serão armazenados ou mantidos.	

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 é gerida pelo **fornecedor** ligando a gateways da extranet do **Barclays** - LAN, WAN e dispositivos de ambiente de trabalho são detidos e geridos pelo fornecedor.

Nível 3 (classe económica) - toda a infraestrutura de TI é gerida pelo **fornecedor** ligando a gateways da Internet do **Barclays** - LAN, WAN e dispositivos de ambiente de trabalho são detidos e geridos pelo fornecedor

18.1 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.
18.2 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 reguladas e monitorizadas por mecanismos de controlo de acesso físico a fim de garantir que apenas os funcionários autorizados dispõem de acesso (específico da função) e são aprovados (pelo responsável do serviço BDS). • 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 funcionários que cessem funções, que sejam transferidos ou que se ausentem (sendo mantidos os respetivos registos). • 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: Para funcionários autorizados: o Crachá com fotografia de identificação sempre visível o Leitores de cartões implementados nas proximidades o Mecanismo antirretorno ativado e monitorizado • O fornecedor tem de dispor de processos e procedimentos para o controlo e monitorização de pessoas externas, incluindo subcontratantes e subprocessadores com acesso físico às zonas do BDS para efeitos de manutenção e limpeza.
18.3 BDS - Videovigilância	• Implementar sistemas de videovigilância para as zonas do BDS a fim de registar ou alertar, de forma eficaz, qualquer acesso não autorizado e/ou atividade maliciosa e auxiliar nas investigações. • Todos os pontos de entrada e saída da zona BDS devem contar com videovigilância. • Testagem de câmaras para operação e qualidade, além de câmaras de segurança que 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.
18.4 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 (tokens de RSA) e trimestralmente o fornecedor tem de elaborar uma reconciliação. • O Barclays desativará as credenciais de autenticação após notificação de que o acesso já não é necessário (por exemplo, saída de funcionários, reatribuição de projetos, etc.) num prado de 24 (vinte e quatro) horas a contar da data de saída/último dia útil/data de LDIO recebida com o Fornecedor. • 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 remota através da aplicação Citrix Barclays têm de ser aprovados e autorizados pelo Barclays (gabinete do Diretor de segurança – Equipa TPSecM). O fornecedor tem de manter registos e realizar uma reconciliação trimestral. Consultar o ponto - 4. Trabalho remoto (Acesso remoto)
18.5 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 casa. Qualquer acesso remoto tem de ser aprovado pelas equipas do Barclays relevantes (incluindo o gabinete do Diretor de segurança – Equipa TPSecM). As capacidades de trabalho remoto (incluindo a partir de casa) são proibidas durante o decurso normal de negócios, quando terceiros sejam contratualmente obrigados a prestar serviços a partir do espaço dedicado do Banco ou das instalações do fornecedor ou quando são aplicáveis requisitos regulamentares. No entanto, são permitidas disposições em planos de continuidade de negócios de terceiros em caso de resposta a recuperação de desastres/crise/pandemia de acordo com o Barclays e quaisquer requisitos de segurança exigidos para o trabalho remoto no âmbito do acordo contratual.
18.6 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 Consulte o pontoo - 2. Segurança de limites e da rede
18.7 BDS - Rede sem fios	Desativação da rede sem fios para o fornecimento de rede BDS para serviços do Barclays.
18.8 BDS - Segurança de ponto final	Têm de ser configuradas construções de computadores (incluindo computadores portáteis) seguras segundo as melhores práticas do setor para computadores na rede do BDS. Têm de ser implementadas as melhores práticas do setor e a construção da segurança de dispositivos de ponto final BDS tem de incluir, entre outros:

	• Encriptação total do disco rígido. • Desativação de todo o software/serviços/portas desnecessários. • Desativação do acesso por direitos de administração para os utilizadores locais. • Os funcionários do fornecedor não poderão alterar as definições básicas, como o pacote de serviço predefinido e serviços predefinidos, etc. • Desativação da porta USB para não permitir copiar Informações/dados Barclays para suportes externos • Atualização com as assinaturas de antimalware e patches de segurança mais recentes. • Desativação do serviço spooler de impressão • A partilha/transferência de ativos informacionais/dados Barclays deve ser desativada utilizando ferramentas/software de mensagens instantâneas. • Deteção, interrupção e correção da presença e/ou utilização de software não autorizado, incluindo software malicioso. • O tempo limite do ecrã de bloqueio é ultrapassado, limita a ligação TCP IP apenas à rede corporativa, agente de segurança Advanced EPS para detetar comportamentos suspeitos. Consulte o ponto - 8. Segurança de ponto final

18.9 BDS - E-mail e Internet	• A conectividade da rede tem de 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 capacidade para 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.

18.10 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 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: 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 quaisquer subcontratantes ou subprocessadores que sejam exclusivamente dedicadas ao Barclays ou a partir das quais os serviços sejam prestados ou entregues.
Melhores práticas do setor	Utilização das melhores e mais atuais práticas, processos, normas e certificações líderes de mercado e aplicação do nível de competência e de cuidado que se esperaria de uma organização profissional líder no mercado, competente e experiente envolvida na prestação de serviços iguais ou semelhantes aos serviços prestados ao Barclays.
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.
Cibersegurança	Aplicação de tecnologias, processos, controlos e medidas organizacionais para proteger sistemas informáticos, redes, programas, dispositivos e dados contra ataques digitais que possam envolver (entre outros) divulgação não autorizada, destruição, perda, alteração, roubo ou danos em hardware, software ou Dados.

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.
TPSecM	Responsabilidade da equipa de gestão de segurança de terceiros em gerir a postura de segurança dos Fornecedores.
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.
Ativos informacionais	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 seja utilizado 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 (MFA)	Autenticação que requer 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).
Informações pessoais	Qualquer informação relacionada com uma pessoa singular identificada ou identificável ("titular dos dados"); uma pessoa singular identificável é uma pessoa que pode ser identificada, direta ou indiretamente, em particular através de 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.
Acesso privilegiado	Designação de acesso, permissões ou capacidades especiais (acima do padrão) a um utilizador, processo ou computador.
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
Acesso remoto	Tecnologia e técnicas utilizadas para conceder a utilizadores autorizados acesso a redes e sistemas de uma organização a partir de uma localização externa.
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 totalmente entendidas e cuidadosamente avaliadas.

Incidente de segurança	Os incidentes de segurança são definidos como aqueles eventos que incluem, entre outros: • Tentativas (falhadas ou bem-sucedidas) de obter acesso não autorizado a um sistema ou seus dados. • Interrupção indesejada ou ataques de recusa de serviço. • Utilização não autorizada de um sistema para o processamento ou armazenamento de dados. • Alterações às caraterísticas 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.
Máquina virtual:	O ambiente completo que suporta a execução de software convidado. NOTA – uma máquina virtual é um encapsulamento completo do hardware virtual, dos discos virtuais e dos metadados associados à mesma. As máquinas virtuais permitem multiplexar a máquina física subjacente através de uma camada de software chamada hipervisor.

Segredo bancário

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

Versão final 14.0 Outubro de 2024

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 a CID após qualquer modificação substancial no modelo de operação (ou negócio) do fornecedor ou, pelo menos, anualmente e de os distribuir na 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, processos e procedimentos 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 e testado regularmente 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. Deve ser oportunamente tomada uma ação corretiva pelo fornecedor. 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 penalizações e à perda da licença bancária na Suíça ou no Mónaco

3. Formação e sensibilização	Os funcionários 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 funcionários 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 risco 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 as leis e a regulamentações aplicáveis na 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 B: 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 afeta ao Fornecedor como colaborador permanente ou qualquer pessoa prestando serviços ao Fornecedor por um período limitado (tal como um 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 funcionário do fornecedor, consultor, contratante ou colaborador de agência que tenha acesso autorizado a um sistema detido pelo Barclays sem privilégios elevados.

Anexo C: 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/potencial 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. UK)

1. Nome do cliente

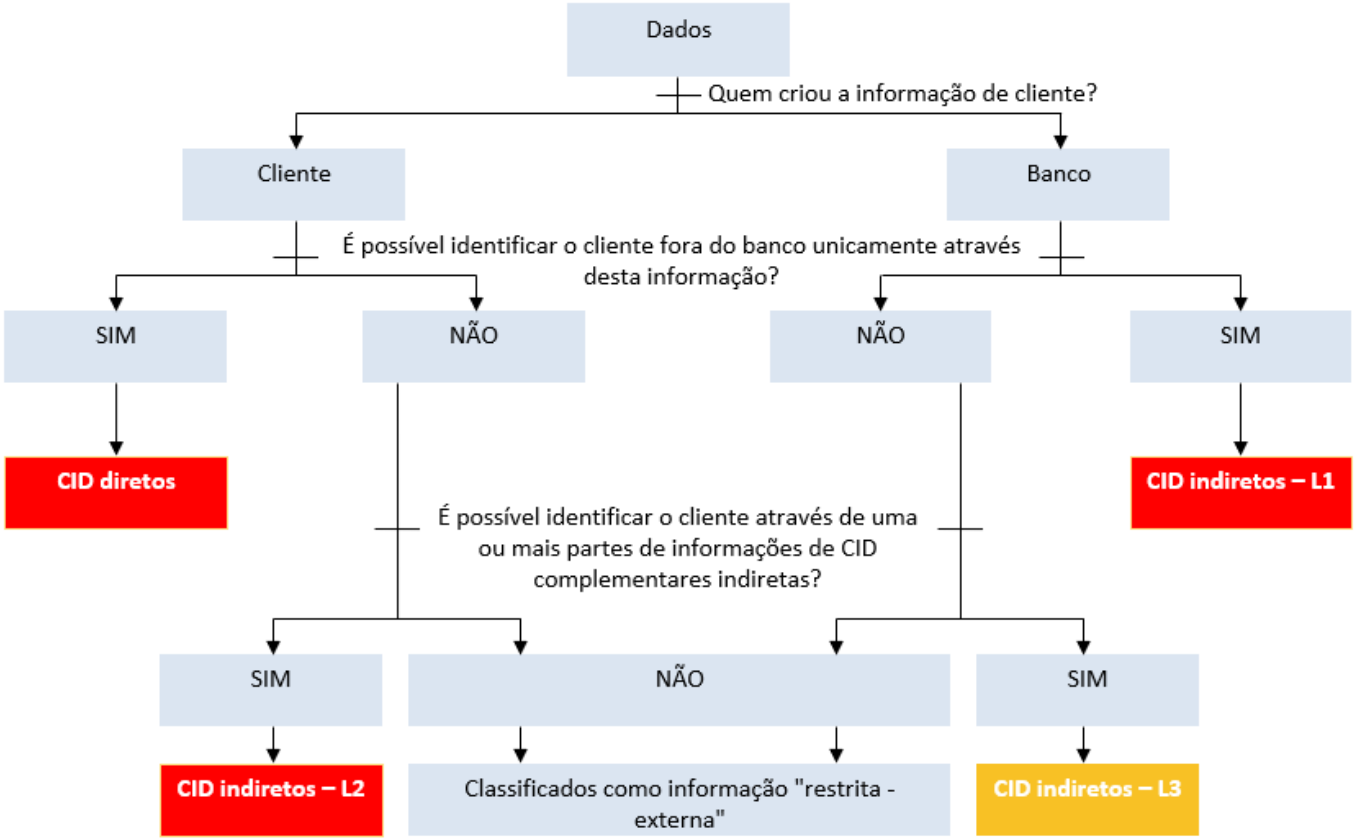
   (DCID) = Violação do segredo bancário

2. ID da partição

   (ICID L1) = Violação do segredo bancário

3. Situação patrimonial + Nacionalidade

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


Dados
Quem criou a informação de cliente?
Cliente
Banco
É possível identificar o cliente fora do banco unicamente através desta informação?
SIM
NÃO
NÃO
SIM
CID diretos
CID indiretos – L1
É possível identificar o cliente através de uma ou mais partes de informações de CID complementares indiretas?
SIM
NÃO
SIM
CID indiretos – L2
Classificados como informação "restrita - externa"
CID indiretos – L3

Anexo D: Esquema de classificação de informações do Barclays

Tabela D1: 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 funcionários, 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 penalizações 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 funcionários 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 funcionários e informações pessoais. • Avaliações de vulnerabilidade. • Resultados e relatórios de auditorias.
Restrito – Externo	As informações têm de ser classificadas como restritas-externas se os destinatários previstos forem funcionários autenticados do Barclays e MSP do Barclays com contrato vigente e se estiverem limitadas a um público específico ou terceiros autorizados pelo responsável pela informação. A divulgação não autorizada teria um impacto negativo no Barclays, avaliado segundo o ERMF, como "importante" ou "limitado" (financeiro ou não financeiro). As informações não se destinam a distribuição geral, mas podem ser encaminhadas ou partilhadas pelos destinatários de acordo com o princípio da necessidade de tomar conhecimento.	• Planos de novos produtos. • Contratos com clientes. • Contratos legais. • Pequenas quantidades de informação/informações individuais de clientes/consumidores destinadas a serem enviadas externamente. • Comunicações de clientes/consumidores. • Nova emissão de materiais de oferta (p. ex. brochuras, prospetos de oferta). • Documentos finais de investigação. • Informações não públicas relevantes (MNPI) externas ao Barclays. • Todos os relatórios de investigação • Alguns materiais de marketing. • Comentários de mercado.
Não restrito	Informações destinadas a distribuição geral ou cuja distribuição não teria impacto na organização.	• Materiais de marketing. • Publicações. • Anúncios públicos. • Anúncios de emprego. • Informações sem impacto no Barclays.

Tabela D2: 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 rotulagem	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 pelos ativos informacionais.	• Os ativos têm de ser atribuídos a um responsável pelos ativos informacionais.	• Os ativos têm de ser atribuídos a um responsável pelos ativos informacionais.
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., 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.	• 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
Partilha	• Os ativos em papel têm de integrar uma etiqueta de informação visível. A etiqueta tem de encontrar-se pelo menos na página do título. • Os ativos eletrónicos têm de integrar uma etiqueta de informação bem visível.	• Os ativos em papel têm de ter uma etiqueta de informação visível. A etiqueta tem de encontrar-se pelo menos na página do título. • Os envelopes que contenham ativos em papel têm de incluir uma etiqueta de informação visível na parte da frente	• Os ativos em papel têm de incluir uma etiqueta de informação visível em todas as páginas.

	• Os ativos só podem ser distribuídos utilizando sistemas, métodos ou fornecedores aprovados pela organização. • Os ativos só podem ser distribuídos a pessoas empregadas pela empresa, ou ao abrigo de uma obrigação contratual adequada para com a empresa, ou no âmbito de uma necessidade comercial inequivocamente reconhecida, por exemplo, negociação contratual.	• Os ativos eletrónicos têm de integrar uma etiqueta de informação bem visível. As cópias eletrónicas de documentos com várias páginas têm de integrar uma etiqueta de informação visível em todas as páginas. • Os ativos só podem ser distribuídos utilizando sistemas, métodos ou fornecedores aprovados pela organização. • Os ativos só podem ser distribuídos a pessoas empregadas pela empresa, ou ao abrigo de uma obrigação contratual adequada para com a empresa, ou no âmbito de uma necessidade comercial inequivocamente reconhecida, por exemplo, negociação contratual. • Os ativos só podem ser distribuídos a pessoas com uma necessidade comercial de os receberem. • 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.	• Os envelopes que contêm ativos em papel têm de incluir uma etiqueta de informação na parte da frente e de ser selados através de um sistema que não permita a violação. Antes da distribuição, têm de ser colocados no interior de um segundo envelope sem etiquetas. • Os ativos eletrónicos têm de integrar uma etiqueta de informação bem visível. As cópias eletrónicas de documentos com várias páginas têm de integrar uma etiqueta de informação visível em todas as páginas. • Os ativos só podem ser distribuídos utilizando sistemas, métodos ou fornecedores aprovados pela organização. • Os ativos só podem ser distribuídos a pessoas empregadas pela empresa, ou ao abrigo de uma obrigação contratual adequada para com a empresa, ou no âmbito de uma necessidade comercial inequivocamente reconhecida, por exemplo, negociação contratual. • Os ativos só podem ser distribuídos a pessoas especificamente autorizadas a recebê-los pelo responsável pelos ativos informacionais.

			• Os ativos não podem ser enviados por fax. • Os ativos eletrónicos têm de ser encriptados com recurso a um mecanismo de proteção criptográfico aprovado, sempre que estiverem a ser distribuídos fora da rede interna. • Tem de ser mantida uma cadeia de custódia para ativos eletrónicos.
Arquivo e eliminação	• Os ativos em papel têm de ser eliminados com recurso a um serviço de eliminação confidencial. • As cópias de ativos eletrónicos também têm de ser eliminadas dos "cestos de reciclagem" do sistema ou dispositivos semelhantes em tempo útil	• Os ativos em papel têm de ser eliminados com recurso a um serviço de eliminação confidencial. • As cópias de ativos eletrónicos também têm de ser eliminadas dos "cestos de reciclagem" do sistema ou dispositivos semelhantes em tempo útil.	• Os ativos em papel têm de ser eliminados com recurso a um serviço de eliminação confidencial. • As cópias de ativos eletrónicos também têm de ser eliminadas dos "cestos de reciclagem" do sistema ou dispositivos semelhantes em tempo útil. • Os suportes onde ativos eletrónicos secretos tiverem sido guardados têm de ser devidamente limpos antes ou durante a eliminação.