PELOURO DE ESTABILIDADE FINANCEIRA

CIRCULAR N.º 03/EFI/2025

Maputo, 19 de Novembro de 2025

ASSUNTO: AUTO-AVALIAÇÃO DO RISCO CIBERNÉTICO

Mostrando-se necessário definir o modelo de reporte para o preenchimento do questionário de auto-avaliação do risco cibernético, o Banco de Moçambique, em conformidade com o disposto no número 1 do artigo 5 do Aviso n.º 02/GBM/2024, de 15 de Março, que aprova as Directrizes de Gestão do Risco e Resiliência Cibernética, determina:

1. As instituições de crédito e sociedades financeiras devem realizar a análise dos seus processos de gestão de risco e resiliência cibernética, com base no modelo de auto-avaliação constante em Anexo à presente Circular.
2. Na sequência do previsto no número anterior, as instituições de crédito e sociedades financeiras devem remeter ao Banco de Moçambique:
    a) O Relatório de auto-avaliação do risco cibernético, devidamente preenchido; e
    b) O Plano de remediação, indicando as medidas correctivas, prazos, responsáveis pela implementação e documentos de suporte.
3. Os documentos referidos no número anterior devem ser remetidos através do Portal BSA (*Banking Supervision Application*) ou por outros meios que venham a ser indicados pelo Banco de Moçambique.
4. Nos casos em que as instituições de crédito e sociedades financeiras não possuam, temporariamente, capacidade operacional para assegurar o envio pelos meios indicados, ou quando estes se encontrem indisponíveis, o reporte deve ser efectuado, a título excepcional, através do correio electrónico: dsp_riscocibernetico@bancomoc.mz
5. A presente Circular entra imediatamente em vigor.

As dúvidas relativas na interpretação e aplicação da presente Circular devem ser submetidas ao Departamento de Supervisão Prudencial do Banco de Moçambique.

BANCO DE MOÇAMBIQUE
Pelouro de Estabilidade Financeira

Benedita Guimino

Administradora

BANCO DE MOÇAMBIQUE

AUTO-AVALIAÇÃO DE GESTÃO DE RISCO E RESILIÊNCIA CIBERNÉTICA

Nome da Instituição:

Data de Submissão:

Responsável pelo preenchimento:

Designação/Função:

e-mail:

Instruções:

1. O questionário de auto-avaliação de gestão do risco e resiliência cibernética é uma ferramenta baseada no Aviso nº 02/GBM/2024, de 15 de Março, sobre Gestão de Risco e Resiliência Cibernética que pretende medir o risco cibernético intrínseco bem como avaliar a maturidade dos processos de segurança cibernética implementados a nivel institucional.

2. Este deve ser preenchido, anualmente, e remetido até 31 de Março, pelo executivo sénior responsável pela implementação, pela gestão de risco e resiliência cibernética e posteriomente, submetido ao Banco de Moçambique pelas vias indicadas.

3. O questionário tem 2 componentes: o risco intríseco e os processos distribuidos em 9 dominios, respectivamente:
*D1 - Governação
*D2 – Identificação
*D3 - Protecção
*D4 - Detecção
*D5 - Resposta e recuperação
*D6 - Consciencialização situacional
*D7 - Testes
*D8 - Terceirização
*D9 - Aprendizagem e Evolução

4. Para o risco intríseco este deve ser preenchido tendo em conta as categorias e níveis de risco:
4.1. Categorias do risco:

4.1.1.Características Organizacionais : fusões e aquisições, número de colaboradores directos e adjudicatários de cibersegurança, alterações no pessoal de segurança, o número de utilizadores com acesso privilegiado, alterações no ambiente das tecnologias de informação (TI), localizações da presença do negócio, e localização das operações e centro de dados.

4.1.2. Tecnologias e Tipos de Ligações: certos tipos de ligações e tecnologias podem expor a um risco intrínseco elevado dependendo da complexidade e maturidade das ligações e da natureza específica de produtos e serviços tecnológicos.

4.1.3. Canais: a diversidade de canais de oferta de produtos e serviços podem expor a um risco intrínseco elevado dependendo da natureza específica de produtos ou serviços oferecidos, podendo ser canais digitias e agentes.

4.1.4. Produtos e Serviços: diferentes produtos e serviços tecnológicos oferecidos pelas ICSF podem expor a um risco intrínseco elevado dependendo da natureza específica dos produtos ou serviços oferecidos.

4.1.5. Ameaças Externas: O volume e tipo de ataques (tentativas ou sucedidos) afectam a exposição ao risco intrínseco. Esta categoria considera o volume e sofisticação dos ataques cibernéticos contra a instituição.

4.2. Niveis de Risco Intríseco

Baixo: utilização limitada de tecnologia com poucos terminais, aplicações, sistemas e sem ligações. O conjunto de produtos e serviços é limitado. A instituição possui poucos colaboradores e uma pequena dispersão geográfica.

Médio: possui uma complexidade reduzida em termos de tecnologia utilizada. Oferece uma gama limitada de produtos e serviços de menor risco. Os sistemas críticos de negócio são terceirizados. As principais tecnologias utilizadas já estão estabelecidas. Ela possui poucos tipos de ligações de complexidade reduzida com clientes e entidades externas.

Critico: geralmente utiliza tecnologia com grau de complexidademoderado em termos de volume e sofisticação. A instituição poderá ter terceirizado alguns serviços críticos ou então suportar os mesmos internamente. Possuem diversos produtos e serviços, oferecidos através de vários canais.

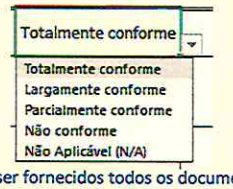
Alto: utiliza tecnologia complexa em termos do escopo e sofisticação. A instituição oferece produtos e serviços de risco elevado que podem incorporar tecnologias emergentes. A instituição poderá hospedar internamente um número significante de aplicações. A instituição permite a utilização de um número elevado de dispositivos pessoais ou uma diversidade de tipos de dispositivos. A instituição detém uma quantidade considerável de ligações com clientes e entidades externas. Uma diversidade de serviços de pagamentos são directamente oferecidos ao invés do recurso a entidades externas e podem reflectir um nível elevado do volume de transacções.

4.3. Fazer a leitura da afirmação declarativa de risco e determinar o nível apropriado de risco com base no critério descrito à direita da afirmação declarativa. Seleccione apartir da lista na coluna C o critério mais apropriado do ambiente da instituição.

Categoria	Seleccione Nível de Risco para o Critério de Risco	Baixo	Médio 2	Alto 3	
Caracteristicas Organizacionais		**Baixo 1**	**Médio 2**	**Alto 3**	
Fusões e aquisições (incluindo desinvestimentos e *joint ventures*)	Médio	Nenhuma planeada	Em discussões com pelo menos uma entidade	Uma venda ou aquisição foi publicamente anunciada no ano anterior. em negociações com 1 ou mais entidades	N
Colaboradores directos (incluindo tecnologias de informação e subcontratadas de cibersegurança)	Baixo Médio Alto Crítico	Número total de funcionários é <50	Número total de funcionários entre 50 – 2.000	Número total de funcionários entre 2.001 – 10.000	Nim
Alterações nas funções de TI e pessoal de segurança de informação		Posições chave preenchidas; rotação baixa ou inexistente de	Alguma rotação nas posições chave ou de gestão	Rotação frequente do pessoal chave ou posições de gestão	Vag pos

5. Para preencher os dominios D1 até D9, para cada requisito, o utilizador deve escolher entre as seguintes opções de resposta:

Onde: ***Totalmente conforme*** : Adequado, implementado
Largamente conforme: Adequado e implementado, mas com pequenas falhas
Parcialmente conforme: Adequado mas em grande medida não implementado
Não conforme: Inadequado, não implementado



6. Em caso de resposta "Totalmente conforme" e "Largamente conforme", sempre que aplicável, devem ser fornecidos todos os documentos de suporte por via electrónica e indicar o(s) título(s) e a referência.

7. As dúvidas na interpretação e aplicação do presente Questionário devem ser submetidas ao Departamento de Supervisão Prudencial do Banco de Moçambique.

Categoria	Seleccione Nível de Risco para o Critério de Risco	Baixo 1	Médio 2	Alto 3	Crítico 4	Comentários
Características Organizacionais		**Baixo 1**	**Médio 2**	**Alto 3**	**Crítico 4**	
Fusões e aquisições (incluindo desinvestimentos e *joint ventures*)	Médio	Nenhuma planeada	Em discussões com pelo menos uma entidade	Uma venda ou aquisição foi publicamente anunciada no ano anterior, em negociações com 1 ou mais entidades	Múltiplas integrações em curso de aquisições estão em processo	
Colaboradores directos (incluindo tecnologias de informação e subcontratadas de cibersegurança)	Baixo	Número total de funcionários é <50	Número total de funcionários entre 50 – 2,000	Número total de funcionários entre 2,001 – 10,000	Número total de funcionários é >10,000	
Alterações nas funções de TI e pessoal de segurança de informação	Médio	Posições chave preenchidas; rotação baixa ou inexistente de pessoal	Alguma rotação nas posições chave ou de gestão	Rotação frequente do pessoal chave ou posições de gestão	Vagas nas posições de gestão ou chave por longos períodos; elevado nível de rotatividade de pessoal de TI ou segurança de informação	
Acesso privilegiado (Administradores de rede, base de dados, sistemas aplicacionais, etc.)	Médio	Número limitado de administradores; administradores externos inexistentes ou limitados	Nível de rotação de administradores afecta operações; pode utilizar alguns administradores externos	Dependência elevada dos administradores externos; número de administradores insuficientes para o volume de suporte ou demanda de alterações	Elevada rotação dos administradores; a maioria dos administradores são externos; experiência na administração é limitada	
Alterações no ambiente de TI (rede, infra-estrutura, aplicações críticas, tecnologias suportado novos produtos ou serviços)	Médio	Ambiente de TI estável	Alterações mínimas ou não frequentes no ambiente de TI	Adopção frequente de novas tecnologias	Volume de alterações significantes é elevado; Alterações substanciais nos provedores externos de serviços de TI.	
Locais dos balcões/presença	Médio	1 província	2-3 províncias	4-6 províncias	7- 11 províncias	
Locais das operações/centro de dados	Médio	1 província	2-3 províncias	4-6 províncias	7- 11 províncias	

Categoria	Seleccione Nível de Risco para o Critério de Risco	Baixo 1	Médio 2	Alto 3	Crítico 4	Comentários

Tecnologias e Tipos de Ligações		Baixo 1	Médio 2	Alto 3	Crítico 4	Comentários
Número total de ligações de provedores de serviços de Internet (ISP), incluindo ligações de	Baixo	Sem ligações	Complexidade Moderada (1- 20 ligações)	Complexidade significante (21 – 100 ligações)	Complexidade substancial (> 101 ligações)	
Acesso à rede sem fios	Baixo	Sem acesso à rede sem fios	Pontos de acesso a redes sem fios separados entre visitantes e corporativa; número limitado de utilizadores e pontos de acesso (1– 250 utilizadores; 1–25 pontos de acesso)	Redes sem fio de visitantes e corporativa estão logicamente separadas; Acesso à rede sem fios corporativa; número significante de utilizadores e pontos de acessos (251–1,000 utilizadores; 26– 100 pontos de acesso)	Acesso à rede sem fios corporativa; todos os colaboradores têm acesso; número substancial de pontos de acesso (> 1,000 utilizadores;> 100 pontos de acesso)	
Dispositivos pessoais com a permissão de ligação à rede corporativa.	Baixo	Apenas um tipo de dispositivo; permitido à <5% dos funcionários (colaboradores, executivos, gestores); apenas acesso ao correio electrónico	Múltiplos dispositivos utilizados; permitido à <10% dos funcionários (colaboradores, gestores) e a administração; apenas acesso ao correio electrónico	Múltiplos dispositivos utilizados; permitido à <25% funcionários autorizados (colaboradores, executivos, gestores) e administração; acesso ao correio electrónico e algumas aplicações	Quaisquer tipos de dispositivos utilizados; permitido à >25% dos funcionários (colaboradores, executivos, gestores) e administração; acesso à todas aplicações	
Ligações externas, número de ligações instanciadas (ex., protocolo de transferência de	Baixo	Poucas instâncias de ligações in (1–5)	Várias instâncias de ligações (6–10)	Instâncias de ligações significantes (11–25)	Instâncias substanciais de ligações (>25)	
Entidades externas, incluindo um número de instituições e funcionários de provedores de serviços e subcontratados, com acesso aos sistemas internos	Baixo	Número limitado de entidades externa (0 – 3) e número limitado de funcionários de provedores de serviços e subcontratados (<5) com acesso; complexidade baixa no modo de acesso	Número de entidades externas (4 – 6) e número de funcionários de provedores de serviços e subcontratados (6 – 15) com acesso; alguma complexidade no modo de acesso aos sistemas	Número de entidades externas (7 – 10) e número significante de funcionários de provedores de serviços e subcontratados (16 - 25) com acesso; nível de complexidade elevado no modo de acesso aos sistemas	Número de entidades externas (> 10) e funcionários de provedores de serviços e subcontratadas (> 25) com acesso; nível de complexidade elevado no modo de acesso aos sistemas	
Aplicações desenvolvidas por provedores de serviços, internamente hospedadas que suportam	Baixo	Aplicações limitadas (0 – 3)	Aplicações (4 – 7)	Número de aplicações (8 - 11)	Número de aplicações (> 11)	
Sistemas desenvolvidos internamente que suportam actividades críticas	Baixo	Nenhum sistema desenvolvido internamente	1-5 sistemas desenvolvidos internamente	6 - 10 sistemas desenvolvidos internamente	>11 sistemas desenvolvidos internamente	
Hardware no fim de vida (EOL)	Baixo	Inexistência de hardware em EOL ou que ultrapassaram o EOL	Hardware em EOL ou que ultrapassaram o EOL que tem impacto mínimo em caso de falha e as alternativas para substituição estão disponíveis.	Hardware em EOL ou que ultrapassaram o EOL que tem impacto no funcionamento do hardware mas com alternativas para substituição ou formas de mitigação a médio e longo prazo.	Hardware em EOL ou que ultrapassaram o EOL que tem impacto significativo no funcionamento do hardware em caso de falha mas com alternativas ou formas de mitigação a médio/longo prazo	

Categoria	Seleccione Nível de Risco para o Critério de Risco	Baixo 1	Médio 2	Alto 3	Crítico 4	Comentários
Software no fim de vida (EOL)	Baixo	Inexistência de software em EOL ou que ultrapassaram o EOL	Sofware em EOL ou que ultrapassaram o EOL que tem impacto mínimo em caso de falhas e as alternativas para actualização estão disponíveis.	Software em EOL ou que ultrapassaram o EOL que tem impacto no funcionamento do sistema em causa mas com alternativas de actualização ou formas de mitigação disponíveis a	Software em EOL ou que ultrapassaram o EOL que tem impacto significativo no funcionamento do sistema e não existe a possibilidade de assistência por parte do provedor.	
Dispositivos de rede (inclui físicos e virtuais)	Médio	Dispositivos de rede limitados ou nenhum (<250)	Vários dispositivos (250 –500)	Número de dispositivos (501–1,000)	Número de dispositivos (> 1,001)	
Provedores de serviços externos que armazenam e/ou processam informação que suportam actividades críticas e não têm acesso aos sistemas internos, mas a instituição depende dos seus	Médio	Nenhuma entidade externa que suporte actividades críticas	1 - 3 entidades externas que suportam actividades críticas	4 - 6 entidades externas que suportam actividades criticas; 1 ou mais estão baseadas no estrangeiro	> 7 entidades externas que suportam actividades criticas; 1 ou mais estão baseadas no estrangeiro	
Serviços de computação em nuvem hospedados que suportam operações da instituição.	Médio	Nenhum provedor de computação em nuvem	Vários provedores de computação em nuvem; apenas computação em nuvem (1 – 3)	Vários provedores de computação em nuvem (4 – 7)	Número de provedores de computação em nuvem (8 – 10); os locais dos provedores de computação em nuvem incluem internacionais; utilização de	

Categoria	Seleccione Nível de Risco para o Critério de Risco	Baixo 1	Médio 2	Alto 3	Crítico 4	Comentários
Canais		**Baixo 1**	**Médio 2**	**Alto 3**	**Crítico 4**	**Comentários**
Serviços *online* (*Interbanking*, redes sociais)	Médio	Nenhuma aplicação baseada na Internet ou presença nas redes sociais	Website e/ou página nas redes sociais. Número de subscritores: <5,000	Website e/ou página nas redes sociais. Número de subscritores: 5,000 - 80,000	Website e/ou página nas redes sociais. Número de subscritores: > 80,000	
Serviços de telefonia móvel (aplicação móvel, USSD- *Unstructured Supplementary Service Data*)	Médio	Nenhum	Aplicações móveis e USSD para clientes que oferecem serviços. Número de subscritores <5,000	Aplicações móveis e USSD para clientes que oferecem serviços. Número de subscritores: 5,000 - 100,000	Aplicações móveis e USSD dpara clientes que oferecem serviços. Número de subscritores > 100,000	
Caixas Automáticas (ATM)	Médio	Sem ATM	Número de ATM < 25	Número de ATM: 25 - 100	Número de ATM > 100	
Ponto de Venda (POS)	Médio	Sem POS	Número de POS < 1,000	Número de POS : 1,000 - 8,000	Número de POS > 8,000	
Agentes (bancário, não bancários)	Médio	Não possui agentes.	Possui agentes; < 100 agentes	Possui agentes; entre 100 - 200 agentes.	Possui agentes; > 200 agentes.	
Produtos e Serviços		**Baixo 1**	**Médio 2**	**Alto 3**	**Crítico 4**	**Comentários**
Cartões (débito, crédito e pré-pagos)	Médio	Não possui cartões ou possui <10,000 cartões emitidos	Possui cartões: 10,000 - 499,000.	Possui cartões: 500,000 - 1,000,000	Possui cartões > 1,000,000	
Carteiras móveis (carteira de moeda electrónica e ourtras de moeda digital)	Baixo	Não possui serviço de carteira móvel.	Número de subscritores< 5,000,000	Número de subscritores: 5,000,000 - 8,000,000	Número de subscritores > 8,000,000	
Transferências electrónicas	Médio	Não efectua transferências electrónicas.	Volume de Transferências mensais < 250,000	Volume de Transferências mensais: 250,000 - 750,000	Volume de Transferências mensais > 750,000	
Ameaças Externas		**Baixo 1**	**Médio 2**	**Alto 3**	**Crítico 4**	**Comentários**
Ameaças de Ataques cibernéticos	Médio	Sem ameaças de ataques cibernéticos ou de reconhecimento	Poucas tentativas mensais (<100).	Várias tentativas mensais (100 – 500); pode ter sofrido tentativas de ataques de Negação de Serviços Distribuída (DDoS) no último ano;	Tentativas mensais > 500; pode ter sofrido múltiplas tentativas de ataques de Negação de Serviços Distribuída (DDoS) no último ano;	

FERRAMENTA DE AUTO-AVALIAÇÃO DO RISCO CIBERNÉTICO				
D1 - Governação	**Resposta da Instituição**	**Comentários da Instituição**	**Documento de Suporte (Título Ref)**	**Plano de Acção**
Órgão de administração				
Estão definidas as responsabilidades de todas as funções de gestão e fiscalização do risco cibernético, incluindo as linhas de defesa e os respectivos comités necessários.	Totalmente conforme			
O órgão de administração ou um comité delegado por este, assegura a fiscalização da implementação dos requisitos estabelecidos no Aviso nº 02/GBM/2024, de 15 de Março.	Largamente conforme			
Existe uma estrutura de recursos adequados para a função de segurança, com autoridade apropriada e acesso directo ao órgão de administração.	Largamente conforme			
Está assegurada a eficácia e eficiência da função auditoria interna na avaliação dos processos de gestão do risco cibernético e acompanhamento das recomendações, auditorias externas e certificações independentes.	Não conforme			
Gestão de Topo				
Foi indicado um executivo sénior responsável pela implementação da estratégia e estrutura de gestão de risco cibernético.	Totalmente conforme			
É apresentado, pelo menos, anualmente, um relatório ao órgão de administração sobre o estado global do risco e resiliência cibernética.	Largamente conforme			
O executivo sénior tem competências, conhecimento e experiência adequados em matéria de especialidade.	Largamente conforme			
O executivo sénior actua de forma independente e tem acesso directo ao órgão de administração.	Não conforme			
Estratégia de segurança cibernética				
A estratégia de segurança cibernética foi aprovada pelo órgão da administração e está alinhada à estratégia de negócio.	Totalmente conforme			
A estratégia de segurança cibernética incorpora: (i) importância da resiliência cibernética; (ii) requisitos de alto nível das part interessadas; (iii) visão e missão relativamente à resiliência cibernética; (iv) objectivos da resiliência cibernética; (v) apetite ao risco cibernético; (vi) metas de resiliência cibernética e o respectivo plano de implementação; (vii) âmbito de alto nível da tecnologia e dos activos utilizados para gerir a resiliência cibernética; (viii) iniciativas de resiliência cibernética; (ix) integração da resiliência cibernética em pessoas, processos, tecnologia; (x) gestão de dados; e (xi) consciencialização sobre segurança cibernética. **Caso tenha: 1 a 3 requisitos--> Parcialmente; 4 a 9 --> Largamente conforme.*	Largamente conforme			
A estratégia é revista, pelo menos, anualmente, de modo a incorporar as possíveis alterações ao nível do panorama de ameaças cibernéticas, alocar recursos, identificar e corrigir lacunas e incorporar as lições aprendidas.	Não conforme			
Framework de segurança cibernética				
O *framework* de segurança cibernética incorpora: (i) identificação, incluindo a classificação e risco de activos; (ii) protecção, incluindo os controlos lógicos e físicos;(iii) segurança de recursos humanos; (iv) gestão de alterações e *patches*; (v) gestão de terceiros; (vi) detecção; (vii) mecanismos de gestão de incidentes de segurança cibernética; (viii) resposta e recuperação; (ix) testes; e (x) consciência situacional. **Caso tenha: 1 a 3 requisitos--> Parcialmente; 4 a 8 --> Largamente conforme.*	Totalmente conforme			
O *framework* de segurança cibernética é consistente com o *framework* organizacional de gestão de risco.	Largamente conforme			
O *framework* é revisto, pelo menos, anualmente, de modo a verificar a adequação e eficácia dos controlos.	Largamente conforme			
O *framework* determina os controlos necessários para manter o risco dentro do apetite estabelecido.	Não conforme			
Políticas e procedimentos de segurança cibernética				
É definida e quantificada a tolerância do negócio, com periodicidade mínima anual, com relação ao risco cibernético e é assegurada a sua consistência com a estratégia e o apetite de risco organizacional.	Não Aplicável (N/A)			
Foram estabelecidas métricas para recolher informações que permitam a elaboração de relatórios, tanto ao nível técnico como executivo.	Totalmente conforme			
Gestão do risco cibernético				
A gestão do risco cibernético foi estabelecida como parte integrante do programa de gestão do risco organizacional, no qual as instituições avaliam o risco cibernético inerente às pessoas, processos, tecnologia, actividades, produtos e serviços identificados.	Não conforme			
O risco cibernético é devidamente identificado, classificado e mapeado através de um cenário que considere tanto o agente interno como externo.	Largamente conforme			
É avaliada a existência e eficácia dos controlos de protecção contra o risco identificado, com vista a apurar o risco residual.	Largamente conforme			

FERRAMENTA DE AUTO-AVALIAÇÃO DO RISCO CIBERNÉTICO				
D2 - Identificação	**Resposta da Instituição**	**Comentários**	**Documento de Suporte (Titulo_Ref)**	**Plano de Acção**
Identificação e classificação de activos				
São identificados os processos de negócio, as funções críticas e os activos de informação que suportam o negócio e a entrega de serviços, incluindo os geridos por provedores de serviços terceirizados.	Não Aplicável (N/A)			
Os processos de negócio e activos de informação são classificados em termos de criticidade e sensibilidade.	Não Aplicável (N/A)			
Os processos dependentes da relação com provedores de serviços terceirizados estão devidamente identificados, documentados e actualizados.	Parcialmente conforme			
As avaliações de risco sobre as funções críticas e activos de informação de suporte são realizadas anualmente.	Largamente conforme			
Inventário e gestão de activos				
O inventário das funções críticas, processos, activos de informação, fornecedores de serviços terceirizados e interligações é actualizado, pelo menos, anualmente.	Totalmente conforme			
O inventário das contas individuais e de sistemas é actualizado e revisto, pelo menos anualmente, de modo a incluir as contas com acesso remoto ou direitos de acesso privilegiado.	Largamente conforme			
A topologia de rede e conectividade interna e externa é mantida e actualizada e inclui recursos que suportam as funções críticas.	Parcialmente conforme			
Estão implementadas soluções automatizadas de gestão de activos que possibilitam a rastreabilidade e correlação entre os serviços, produtos prestados e os activos que os suportam, tanto *hardware* como *software*, de modo a possibilitar a identificação do ponto de falha.	Largamente conforme			

FERRAMENTA DE AUTO-AVALIAÇÃO DO RISCO CIBERNÉTICO				
D3 - Protecção	**Resposta da Instituição**	**Comentários**	**Documento de Suporte (Título_Ref)**	**Plano de Acção**
Objectivos de segurança cibernética				
Estão implementados controlos que permitem alcançar os objectivos de segurança cibernética.	Totalmente conforme			
Está assegurada a continuidade e disponibilidade dos sistemas de informação e a protecção da integridade da informação armazenada nos sistemas, tanto em utilização como em trânsito.	Totalmente conforme			
Está assegurada a protecção, integridade, confidencialidade e disponibilidade dos dados em estado de armazenamento, utilização e trânsito.	Totalmente conforme			
Os controlos de segurança cibernética são actualizados, pelo menos anualmente, por forma a assegurar que as abordagens adoptadas se mantêm proporcionais às suas funções críticas, ao cenário de ameaça cibernética e à importância sistémica.	Totalmente conforme			
Monitorização de sistemas e pessoal				
As actualizações dos sistemas são instaladas de forma atempada e segura, sendo mantidas, adequadamente, com o devido suporte.	Totalmente conforme			
As camadas adicionais de segurança cibernética estão implementadas e testadas, onde são identificadas vulnerabilidades nos sistemas.	Não Aplicável (N/A)			
Os sistemas desactualizados com vulnerabilidades que não podem ser corrigidas ou mitigadas são descartados e/ou substituídos.	Não Aplicável (N/A)			
Antes da contratação de novos colaboradores e terceiros estes são submetidos à processos de rastreios (*screening*) e verificações de antecedentes baseados no risco.	Não Aplicável (N/A)			
Gestão de acessos				
Está assegurada a limitação de acesso dos activos de informação e instalações associadas à utilizadores, processos e dispositivos autorizados, de acordo com o princípio da segregação de deveres e privilégios mínimos.	Não Sei (N/A)			
Estão implementados controlos que limitam e monitoram o pessoal com maior privilégio ou direitos de acesso.	Não Sei (N/A)			
Estão estabelecidos processos de monitoria de acesso aos sistemas e à informação e para accionar alertas em caso de tentativas de acesso não autorizado.	Não Sei (N/A)			
Em caso de mudança de responsabilidades do colaborador são revogados atempadamente todos os direitos de acesso relacionados com a posição anterior e não necessários para as novas funções.	Não Sei (N/A)			
Gestão de Acesso remoto				
Estão definidas regras de acesso remoto aos activos de informação a partir de dispositivos protegidos, de acordo com as normas de segurança em vigor.	Largamente conforme			
Os utilizadores com acesso remoto estão sujeitos à mecanismos de autenticação robusta, por forma a salvaguardar o acesso não autorizado.	Não conforme			
Os prestadores de serviços e terceiros com acesso aos activos de informação estão sujeitos à mesma monitorização e restrições de acesso concedida aos colaboradores.	Parcialmente conforme			
Em caso de actividades suspeitas ou não autorizadas, está estabelecido o processo de gestão e controlo de utilização de sistemas informáticos e contas de serviços.	Não Sei (N/A)			
Gestão de Alterações				
As políticas, procedimentos e controlos para a gestão de alterações incluem critérios de prioridade e classificação destas.	Largamente conforme			
As políticas, procedimentos e controlos de gestão de alterações estabelecem que, previamente a qualquer alteração, está assegurado que o pedido é: (i) revisto; (ii) aprovado pelo nível de gestão adequado; (iii) categorizado e avaliado por forma a identificar potenciais riscos; e (iv) definido um plano de retorno em caso de falha e/ou processo mal sucedido. **Caso seja assegurado: (i) e/ou (ii)--> Parcialmente; (i) e (ii) ou (iii) e (iv) --> Largamente conforme.*	Totalmente conforme			
As alterações aos sistemas de informação incluindo *hardware, software* ou *firmware* e definições de configuração do sistema e de segurança cibernética são testadas, validadas e documentadas antes da sua implementação em produção e incluem testes de integração e testes de aceitação pelo utilizador.	Largamente conforme			
Estão estabelecidos processos que permitem a programação da implementação das alterações e comunicação aos afectados antes da implementação efectiva, e incluem a sua consulta, sempre que aplicável.	Não Sei (N/A)			

FERRAMENTA DE AUTO-AVALIAÇÃO DO RISCO CIBERNÉTICO				
D3 - Protecção	**Resposta da Instituição**	**Comentários**	**Documento de Suporte (Título_Ref)**	**Plano de Acção**
Gestão de patches				
A política e processos de gestão de *patches* incluem: (i) identificação de *patches* apropriados para sistemas específicos; (ii) análise do impacto da sua instalação e no caso de se verificarem incumprimentos das recomendações dos fornecedores; (iii) regras que assegurem que os patches sejam instalados correctamente, previamente testados e monitorados após a instalação; e (iv) documentação de todos os procedimentos associados.	Totalmente conforme			
São adoptadas e previligiadas as configurações de base (*standard*) de recursos de tecnologias de informação.	Largamente conforme			
A instalação de novos *patches* tem aprovação prévia da gestão.	Não conforme			
Situações de Emergência				
São identificados, avaliados e aprovados, processos de alteração provenientes de situações de emergência.	Largamente conforme			
São conduzidas revisões pós-implementação que validam os procedimentos de emergência adoptados e determinam o impacto da alteração.	Largamente conforme			
Controlos de segurança de dados				
Os controlos de segurança de dados protegem os dispositivos terminais, previnem a perda de dados e detectam o acesso não autorizado, modificação, cópia ou transmissão dos dados sensíveis em trânsito, armazenados ou em utilização.	Totalmente conforme			
Os controlos de segurança de dados asseguram que os sistemas informáticos geridos por prestadores de serviços e terceiros estão sujeitos às mesmas normas de segurança cibernética implementadas ao nível da instituição.	Parcialmente conforme			
Os dados sensíveis armazenados em sistemas e dispositivos terminais são codificados e protegidos por mecanismos de controlo de acesso robustos e permanentemente apagados antes de serem descontinuados ou redistribuídos.	Parcialmente conforme			
Os controlos de segurança de dados previnem e detectam a utilização de serviços de *Internet* não autorizados.	Não Aplicável (N/A)			
Controlos de segurança de aplicações e sistemas				
Está implementada uma abordagem de segurança, por projecto, referente à incorporação de controlos de segurança em cada fase de desenvolvimento.	Parcialmente conforme			
Está definido o nível aceitável de segurança que satisfaça as necessidades de negócio e identifica potenciais ameaças e riscos relacionados.	Discordo totalmente			
Os requisitos de segurança relativos ao controlo de acesso ao sistema, autenticação, autorização de transacção, integridade dos dados dos *logs*, monitorização dos eventos de segurança e tratamento de excepções são especificados nas fases iniciais de desenvolvimento ou aquisição de sistemas.	Discordo			
As aplicações críticas de negócio são revistas e testadas, de modo a garantir que não exista impacto adverso nas operações ou na segurança.	Discordo			
Controlos de segurança de rede				
Estão instalados dispositivos de segurança para proteger a rede, entre elas e Internet e as ligações com prestadores de serviços.	Largamente conforme			
A arquitectura de rede é revista numa base periódica e inclui a concepção da sua segurança e das respectivas interligações.	Largamente conforme			
Está implementada a segregação física e/ou lógica dos dispositivos terminais que permite a restrição de acesso à Internet ou implementação de controlos equivalentes, proíbe e bloqueia o acesso dos terminais privilegiados.	Parcialmente conforme			
Estão implementados sistemas de detecção ou prevenção de intrusão quem detectam e bloqueiam o tráfego malicioso.	Parcialmente conforme			
As regras de controlo de acesso à rede em dispositivos de rede são revistas, pelo menos anualmente, de modo a assegurar que se mantêm actualizadas.	Largamente conforme			

FERRAMENTA DE AUTO-AVALIAÇÃO DO RISCO CIBERNÉTICO				
D3 - Protecção	**Resposta da Instituição**	**Comentários**	**Documento de Suporte (Título_Ref)**	**Plano de Acção**
Criptografia				
Estão estabelecidas políticas, normas e procedimentos de gestão de chaves criptográficas que compreendem a geração, distribuição, instalação, renovação, revogação, recuperação e expiração de chaves.	Totalmente conforme			
As chaves criptográficas são geradas com segurança e protegidas contra divulgação não autorizada e a sua validade é determinada com base na sensibilidade dos dados, criticidade do sistema e ameaças e riscos a que os dados ou sistema estão expostos.	Totalmente conforme			
São preservadas cópias de segurança das chaves criptográficas e os algoritmos criptográficos são sujeitos à testes ou verificações.	Largamente conforme			
As ligações remotas são encriptadas.	Parcialmente conforme			

FERRAMENTA DE AUTO-AVALIAÇÃO DO RISCO CIBERNÉTICO				
D4 - Detecção	**Resposta da Instituição**	**Comentários**	**Documento de Suporte (Título Ref)**	**Plano de Acção**
Gestão de incidentes cibernéticos				
O perfil de base das actividades do sistema está definido e documentado.	Não Aplicável (N/A)			
Os processos e tecnologia estão implementados por forma a monitorizar e detectar actividades e eventos anómalos, definindo critérios, parâmetros e gatilhos apropriados para habilitar alertas.	Não conforme			
O pessoal com maior privilégio ou funções de administrador de sistemas ou redes são submetidos à formações e treinamentos personalizados.	Largamente conforme			
Estão estabelecidos processos de monitoria para detectar, de forma atempada, incidentes cibernéticos e avaliar, de forma contínua, a eficácia dos controlos por monitorização, testes, auditorias e exercícios à rede.	Totalmente conforme			
Monitorização das actividades dos sistemas informáticos e análise contínua				
Está estabelecido um Centro de Operações de Segurança (*Security Operations Center* - SOC) ou equivalente que possibilita a detecção e resposta a incidentes cibernéticos.	Totalmente conforme			
Estão definidos processos de recolha, revisão e retenção de *logs* de sistemas de segurança.	Largamente conforme			
São revistos, testados e actualizados os recursos de detecção e monitorização, as linhas de base de desempenho de sistemas, os critérios de activação e alertas, tendo em atenção o alinhamento com os outros testes dos sistemas.	Largamente conforme			
Estão implementadas ferramentas de monitorização contínua de vulnerabilidades, por forma a identificar, classificar e tratar, em tempo útil, as vulnerabilidades de risco alto e/ou crítico.	Não conforme			
Configuração de eventos ou alertas				
Estão configurados eventos ou alertas dos sistemas informáticos.	Totalmente conforme			
Os eventos ou alertas são activamente monitorizados o que possibilita a tomada de medidas imediatas para resolver os problemas detectados.	Largamente conforme			
É realizada a correlação de múltiplos eventos registados nos *logs* dos sistemas , como forma de identificar padrões de actividades suspeitas ou anómalas.	Não conforme			
Os controlos de detecção, incluindo pessoas, processos e tecnologia tem a capacidade de detectar ataques cibernéticos e isolar o ponto de comprometimento.	Largamente conforme			

FERRAMENTA DE AUTO-AVALIAÇÃO DO RISCO CIBERNÉTICO				
D5 - Resposta e recuperação	**Resposta da Instituição**	**Comentários**	**Documento de Suporte (Título_Ref)**	**Plano de Acção**
Mecanismos de resposta				
As políticas e processos de gestão de incidentes aprimoram a resiliência, asseguram a continuidade de funções e/ou serviços críticos, melhoram a confiança dos clientes e de partes interessadas e reduzem impactos.	Não Aplicável (N/A)			
Estão implementados mecanismos para responder e recuperar de ataques cibernéticos bem como mitigar potenciais riscos.	Não conforme			
Após a detecção de um ataque cibernético ou de uma tentativa é conduzida uma investigação para determinar a sua natureza e extensão, danos ocorridos e são tomadas medidas imediatas para conter a situação, com base no plano de resposta.	Largamente conforme			
Estratégia de backup				
Está estabelecida uma estratégia de *backup* e o respectivo plano de execução.	Totalmente conforme			
Os dados sensíveis armazenados nos dispositivos de *backup* são protegidos, dentre outros mecanismos, através da encriptação.	Largamente conforme			
Os dispositivos de *backup* são armazenados em local externo que não é sujeito aos mesmos riscos que a fonte de dados.	Largamente conforme			
Os Objectivos de Ponto de Recuperação (*Recovery Point Objectives* - RPO) e de Tempo de Recuperação (*Recovery Time Objectives* - RTO) estão definidos de forma proporcional às necessidades do negócio e ao papel sistémico no ecossistema económico-financeiro.	Não conforme			
Estratégia de comunicação				
Está estabelecida uma estratégia de comunicação com os clientes afectados por ataques cibernéticos.	Totalmente conforme			
Esta inclui canais de comunicação directos, fiáveis e seguros com as partes interessadas.	Largamente conforme			
Plano de resposta e gestão de incidentes cibernéticos				
Define funções e responsabilidades e estabelece opções para redireccionar ou substituir funções ou serviços críticos que possam estar afectados por um ataque cibernético bem-sucedido por um período significativo.	Totalmente conforme			
Estabelece o isolamento e neutralização de ameaças cibernéticas e prevê mecanismos de reestabelecimento dos serviços afectados.	Largamente conforme			
Descreve os procedimentos de comunicação, coordenação e resposta para lidar com cenários de ameaças cibernéticas.	Totalmente conforme			
Prevê o alcance dos objectivos de recuperação, prioridades de restauração e determina as capacidades necessárias para a disponibilidade contínua do sistema, com base em diferentes cenários cibernéticos.	Totalmente conforme			
Estes planos são testados regularmente, devendo a periodicidade estar alinhada com os testes realizados no Plano de Continuidade de Negócios.	Totalmente conforme			
Processos de resposta e recuperação				
Estes processos incluem a simulação de incidentes cibernéticos integrados com a gestão de crises, continuidade do negócio, planeamento da recuperação de desastres e operações de recuperação.	Não Aplicável (N/A)			
Estão estabelecidos procedimentos para recolher e rever a informação de incidentes de segurança cibernética e resultados de testes.	Totalmente conforme			
Estão adoptados processos para realizar análises das causas dos incidentes de segurança cibernética, devendo os resultados estarem integrados nos planos de resposta, retoma e recuperação de incidentes cibernéticos.	Parcialmente conforme			
Estão estabelecidos procedimentos para a retoma da actividade.	Totalmente conforme			

FERRAMENTA DE AUTO-AVALIAÇÃO DO RISCO CIBERNÉTICO				
D6 - Consciencialização situacional	**Resposta da Instituição**	**Comentários**	**Documento de Suporte (Título_Ref)**	**Plano de Acção**
Cultura de consciencialização e formação				
É promovida uma cultura institucional para assegurar a resiliência cibernética através de uma comunicação interna que inclui a partilha de informação relevante sobre a estratégia e *framework* cibernético a todos os colaboradores.	Não Aplicável (N/A)			
É promovida uma cultura de consciencialização em matérias de risco cibernético para os seus clientes.	Não conforme			
Existe um programa de formação contínua e testes de consciencialização sobre o risco e resiliência cibernética para todos colaboradores, que inclui a realização de testes de engenharia social, como as falsas campanhas de e-mails de *phishing*.	Largamente conforme			
Os clientes são treinados em técnicas de detecção de comunicações fraudulentas através de programas de consciencialização e educação em matérias de literacia cibernética.	Totalmente conforme			
Recolha e partilha de informação				
Estão estabelecidos processos de recolha de informação de fontes internas e externas de riscos cibernéticos.	Totalmente conforme			
Estão adoptados protocolos de partilha de informação com grupos inter-profissionais, inter-governamentais e transfronteiriços para recolher, partilhar e avaliar informação sobre práticas e ameaças cibernéticas.	Largamente conforme			
Estão definidas metas e objectivos de partilha de informação de acordo com os objectivos de negócio e o respectivo quadro de resiliência cibernética.	Largamente conforme			
Os objectivos de partilha incluem a recolha e troca de informação de forma atempada de modo a facilitar a detecção, resposta, retoma e recuperação dos sistemas e de outros integrantes do sector durante e após um ataque cibernético.	Não conforme			

FERRAMENTA DE AUTO-AVALIAÇÃO DO RISCO CIBERNÉTICO				
D7 - Testes	**Resposta da Instituição**	**Comentários**	**Documento de Suporte (Titulo_Ref)**	**Plano de Acção**
Testes de resiliência cibernética				
A natureza e a frequência dos testes é proporcional à: (i) ritmo a que as vulnerabilidades e ameaças mudam; (ii) criticidade e sensibilidade dos sistemas informáticos; (iii) consequências de um incidente de segurança; (iv) riscos associados à exposição a ambientes em que não há capacidade de aplicar as políticas de segurança; e (v) materialidade e frequência das alterações aos activos de informação. **Caso tenha: 1 a 2 elementos--> Parcialmente; 3 a 4 --> Largamente conforme.*	Não Aplicável (N/A)			
São realizados os seguintes testes: (i) avaliações de vulnerabilidades; (ii) Baseados em cenários e (iii) testes de intrusão. **Caso realize: (i) e/ou (ii)--> Parcialmente; (i) e (iii) ou (ii) e (iii) --> Largamente conforme.*	Não Aplicável (N/A)			
O órgão de administração é comunicado sobre os resultados de testes que identificam deficiências de controlo de segurança que não possam ser corrigidas em tempo útil.	Não Aplicável (N/A)			
Avaliações de vulnerabilidades				
São realizadas avaliações nos sistemas informáticos para identificar vulnerabilidades de segurança e assegurar que os riscos decorrentes das mesmas são tratados atempadamente.	Não Aplicável (N/A)			
A frequência das avaliações de vulnerabilidades é proporcional à criticidade dos sistemas informáticos e aos riscos de segurança a que estes estão expostos.	Não Aplicável (N/A)			
Os processos de avaliações são realizados de forma periódica. *Para instituições domésticas de importância sistémica -->trimestralmente; outras ICSF: semestralmente.*	Não Aplicável (N/A)			
As ferramentas de avaliação de vulnerabilidades possuem perfis de *scanning* actualizados mensalmente.	Não Aplicável (N/A)			
Testes baseados em cenários				
São realizados exercícios de simulação baseados em cenários, com periodicidade anual, para validar as capacidades de resposta e recuperação, bem como os planos de comunicação, contra as ameaças cibernéticas prevalecentes.	Não Aplicável (N/A)			
A concepção do exercício de simulação baseados em cenários tem em consideração: (i) os agentes susceptíveis de representar ameaça e as tácticas; (ii) técnicas e (iii) procedimentos a serem utilizados em tais ataques. *Caso (i) e/ou (ii) --> Parcialmente; (i) e (iii); (ii) e (iii); (i) e (iii) -->Largamente Conforme.*	Não Aplicável (N/A)			
Testes de intrusão				
São realizados com base em factores como a criticidade e a exposição a riscos cibernéticos, pelo menos, anualmente ou sempre que os sistemas e activos sofram alterações.	Não Aplicável (N/A)			
É assegurada a combinação de testes de *black box, grey box* e *white box* para sistemas informáticos e activos de informação e os resultados são documentados e definidos no planos de acção.	Não Aplicável (N/A)			
Testes de Red Teaming				
São realizados, pelo menos anualmente, exercícios independentes de r*ed teaming*, nomeadamente, a execução de ataques controlados de engenharia social e instalação de dispositivos.	Não Aplicável (N/A)			
A *red team* (equipa independente da equipa de segurança cibernética) testa a forma como a equipa de segurança da instituição responde às várias ameaças.	Não Aplicável (N/A)			
Controlos de gestão de remediação				
Após a realização dos testes ou exercícios de segurança cibernética são estabelecidos processos de remediação com base nas avaliações de terceiros, das auto-avaliações e das constatações de avaliações internas e externas.	Não Aplicável (N/A)			
São rastreados os problemas identificados a partir dos testes ou exercícios de segurança cibernética, as deficiências de *software* detectadas a partir da revisão do código fonte e dos testes de segurança da aplicação e remediados antes da colocação em produção.	Não Aplicável (N/A)			
É efectuado o registo das actualizações e vulnerabilidades de *software* de terceiros e de código aberto.	Não Aplicável (N/A)			
O processo de remediação inclui: (i) avaliação da criticidade e classificação dos problemas; (ii) prazos para remediar os problemas de acordo com a criticidade ; (iii) avaliações de risco; e (iv) estratégias de mitigação para gerir desvios do *framework* de segurança cibernética. *Para o caso de (i) e/ou (ii), (iii) --> Parcialmente; (i); (ii) e/ou (iii), (iv) --> Largamente Conforme.*	Não Aplicável (N/A)			

FERRAMENTA DE AUTO-AVALIAÇÃO DO RISCO CIBERNÉTICO				
D8 - Terceirização	**Resposta da Instituição**	**Comentários**	**Documento de Suporte (Titulo_Ref)**	**Plano de Acção**
Avaliação Preliminar				
Antes da celebração de contratos com terceiros é avaliada a criticidade e sensibilidade das actividades, dados ou processos a terceirizar bem como é conduzida uma avaliação de risco.	Não Aplicável (N/A)			
Antes da assinatura de contratos são realizadas diligências e documentados os seus resultados.	Não conforme			
Na avaliação do perfil do prestador de serviços de terceiros são acedidos os relatórios de auditoria ou resultados de certificações de avaliações independentes.	Largamente conforme			
O risco cibernético associado à utilização de prestadores de serviços de terceiros é identificado e actualizado, pelo menos anualmente.	Totalmente conforme			
Contratação de terceiros				
Os contratos celebrados com terceiros incluem: (i) papéis e responsabilidades de cada parte envolvida relativamente ao acesso aos dados; (ii) resposta e comunicação de incidentes; (iii) gestão da continuidade do negócio; (iv) cessação do contrato; (v) portabilidade dos dados e (vi) acesso aos relatórios de auditoria e relatórios de certificações de avaliações independentes. **Caso tenha: 1 a 3 requisitos--> Parcialmente; 4 a 5 --> Largamente conforme.*	Totalmente conforme			
Os prestadores de serviços informam pontualmente sobre as sub-contratações feitas.	Largamente conforme			
Os contratos têm em conta a portabilidade e interoperabilidade dos dados e aplicações, por forma a evitar o bloqueio (*lock-in*) por parte do prestador de serviços.	Largamente conforme			
Em caso de rescisão de contrato está prevista a devolução ou transferência segura de dados ou, caso esta devolução seja impossível, estão previstos mecanismos que permitem a destruição segura dos suportes de armazenamento.	Não conforme			
Gestão de terceiros				
Estão implementados controlos de segurança para detectar e prevenir possíveis intrusões decorrentes de ligações de terceiros.	Totalmente conforme			
O acesso aos dados confidenciais pelos colaboradores de prestadores de serviços é activamente rastreado e controlado, com base no princípio de privilégios mínimos.	Largamente conforme			
O plano de resposta integra terceiros que prestam serviços para as suas funções críticas.	Não conforme			
Para as funções críticas, o Plano de Continuidade de Negócio contemplam mecanismos de transição para prestadores de serviços alternativos ou de realização interna das funções.	Largamente conforme			

FERRAMENTA DE AUTO-AVALIAÇÃO DO RISCO CIBERNÉTICO				
D9 - Aprendizagem e Evolução	**Resposta da Instituição**	**Comentários**	**Documento de Suporte (Titulo_Ref)**	**Plano de Acção**
Lições aprendidas				
Estão definidos procedimentos que permitem identificar e avaliar ameaças e vulnerabilidades de segurança.	Não Aplicável (N/A)			
Estão identificadas e classificadas as lições estratégicas, tácticas e operacionais aprendidas e as principais partes interessadas a quem estas se aplicam.	Não conforme			
As lições estratégicas, tácticas e operacionais aprendidas são incorporadas na melhoria do *framework* e nas capacidades de resiliência cibernética, numa base contínua.	Largamente conforme			
As lições aprendidas são incorporadas na formação do pessoal, nos programas e materiais de sensibilização, de forma contínua e dinâmica.	Totalmente conforme			
Definição de indicadores				
Estão definidos os indicadores e informação de gestão para medir e monitorar a efectiva implementação da estratégia e *framework* de resiliência cibernética, numa base anual, e a sua evolução ao longo do tempo.	Totalmente conforme			
Dos indicadores existentes, incluem: (i) percentagem do pessoal que recebeu formação em segurança cibernética; (ii) percentagem de incidentes reportados dentro do prazo exigido por categoria; (iii) percentagem de vulnerabilidades mitigadas dentro de um período de tempo definido após a descoberta; e (iv) relatórios anuais de monitorização do progresso dos indicadores. **Caso tenha: 1 indicador --> Parcialmente; 2 a 3 --> Largamente conforme.*	Largamente conforme			