Política
de Gestão de Acessos

Novembro 2024

V 1.0

Histórico do Documento

Versões

Versão	Data de Revisão	Sumário de Mudanças	Direcção
1.0	-	1. Versão inicial	GSI

Validação – Grupo de Trabalho de Validação de Políticas

Versão	Data de Validação
1.0	26-11-2024

Aprovação – Conselho de Administração

Versão	Data de Aprovação
1.0	29-11-2024

Distribuição

Área
Conselho de Administração
Comissão Executiva
Todas as Direcções do Banco Económico

Compromisso do Banco Económico

O Conselho de Administração do Banco Económico, ciente das suas responsabilidades perante os seus clientes, accionistas, parceiros e colaboradores, aprova e compromete-se a executar a presente Política

Pedro Filipe Pedrosa Pombo Cruchinho Presidente do Conselho de Administração	
Jorge Manuel Torres Pereira Ramos Presidente da Comissão Executiva	
Katila Perera Santos Rigal Administradora Executiva	
Elisa de Jesus Francês Baptista Administradora Executiva	
Victor Hariany Neves Faria Administrador Executivo	
Emanuel Maria Maravilhoso Buchartts Administrador não Executivo Independente	

Índice

1. ENQUADRAMENTO 6

2. ÂMBITO 6

3. ENQUADRAMENTO REGULAMENTAR 6

4. OBJECTIVO 7

5. DEFINIÇÕES 8

6. PRINCÍPIOS GERAIS 9

6.1. Identidade 10
6.2. Contas Privilegiadas 10
6.3. Princípio de Acessos Mínimos 10
6.4. Auditoria 10

7. PROCEDIMENTOS RELACIONADOS A GESTÃO E CONTROLO DE ACESSOS 11

7.1. Autenticação em Redes e Sistemas 11
7.2. Controlo de Acessos a Redes e Sistemas 11
7.3. Requisitos Críticos do Controlo de Acessos 12
7.3.1 Requisitos de Negócios, Legais e de Segurança para o Controlo de Acessos 12
7.3.2 Gestão de Acessos ao Utilizador 12
7.3.3 Controlo de Acessos à Rede 14
7.3.4 Controlo de Acessos ao Sistema Operacional 14
7.3.5 Controlo de Acessos aos Aplicativos e Outros Sistemas de Informação 15
7.3.6 Computação Móvel 15
7.3.7 Controlo de Acesso ao Ambiente Físico 15

8. ESTRUTURA ORGANIZACIONAL 17

8.1. Gabinete de Segurança da Informação 17
8.2. Direcção de Sistemas da Informação 17
8.3. Direcção de *Compliance* 17
8.4. Direcção de Risco 18
8.5. Direcção de Auditoria 18
8.6. Direcção de Património e Segurança 18

9. INCUMPRIMENTO 18

10. INTERPRETAÇÃO 19

11. DIVULGAÇÃO 19

12. ALTERAÇÕES E APROVAÇÃO **19**

1. CONSIDERAÇÕES FINAIS **19**

1. Enquadramento

A Política de Gestão de Acessos enquadra-se no nível tático da estrutura documental do Sistema de Gestão de Segurança da Informação (SGSI) do Banco Económico, doravante designado por Banco, a qual define e promove as considerações gerais de Segurança da Informação no que respeita a assegurar o acesso de colaboradores e partes interessadas autorizadas e prevenir o acesso não autorizado aos activos de informação da organização, tendo em conta os requisitos vertidos na Política de Segurança da Informação.

Todos os documentos enquadrados nos níveis tático e operacional da estrutura documental (e.g. normas, regulamentos, processos, procedimentos, modelos, evidências), no que respeita à temática de segurança na Gestão de Activos, devem ter como base o conteúdo vertido pelo presente documento e emanar as preocupações e considerações estabelecidas.

2. Âmbito

A Gestão de Acessos constitui um ponto fundamental para a Segurança da Informação do Banco Económico, na medida em que cada colaborador ou parte interessada só deve ter acesso à informação que está especificamente autorizado a utilizar no decorrer das suas funções laborais.

~~O~~ presente documento aplica-se directamente a todos os colaboradores do Banco Económico, independentemente da sua posição ou função, seja qual for o seu nível de responsabilidade e funções exercidas. Adicionalmente, também se aplica a entidades terceiras, parceiros, fornecedores e outras entidades ou utilizadores que possam ter acesso aos sistemas e serviços do Banco Económico.

3. Enquadramento Regulamentar

A presente Política foi elaborada com base nos seguintes diplomas:

- ISO/IEC 27000:2014 – Sistemas de Gestão de Segurança da Informação (Visão Geral e Vocabulário);
- ISO/IEC 27001:2022 – Sistemas de Gestão de Segurança da Informação (Requisitos);
- ISO/IEC 27001:2022 – Sistemas de Gestão de Segurança da Informação (Códigos de Prática Para Controlos de Segurança da Informação);

- ISO/IEC 27001:2022 – Sistemas de Gestão de Segurança da Informação (Cláusula A.9 – Controlo de Acesso);
- Aviso n.º 08/2020 – Política de Segurança Cibernética e Adopção da computação em Nuvem;
- Directiva n.º 05/DSB/DRO/2022 – Gestão dos Riscos Associados às Tecnologias de Informação e Comunicação e à Segurança Cibernética; e
- Política de Segurança de Informação – Define as regras processuais e operacionais da Governança da Segurança da Informação na Instituição.

4. Objectivo

Estabelecer diretrizes e procedimentos para assegurar que o acesso aos sistemas de informação e dados seja controlado adequadamente, alinhado com as necessidades de negócio e requisitos de segurança da informação.

Os controlos de acesso para esses ambientes devem ser seleccionados, não apenas com base nos requisitos de segurança, mas também nos requisitos de negócio e legais.

A Política descrita neste documento define um conjunto de controlos de segurança da informação, com o objectivo de:

- Garantir que apenas são realizados acessos autorizados às redes e sistemas de informação;
- Impedir o acesso não autorizado a serviços disponíveis na rede e nos sistemas de informação;
- Impedir o roubo de informação e que se comprometa as informações;
- Limitar o acesso à informação e aos recursos de processamento de informação ao mínimo indispensável;
- Tornar os colaboradores e partes interessadas responsáveis pela protecção da sua informação de autenticação nas redes e sistemas;
- Prevenir o acesso não autorizado ao ambiente e arquivos físicos;
- Prevenir o acesso não autorizado aos sistemas operacionais;
- Prevenir o acesso não autorizado à informação contida nos sistemas aplicacionais; e

Garantir o acesso seguro na utilização da computação móvel e dos recursos de trabalho remoto.

5. Definições

Para efeitos da presente Política, entende-se por:

- Administrador da Conta: trata-se de um colaborador que pode criar, activar ou desactivar contas do sistema, bem como atribuir privilégios ou permissões de acesso aos Utilizadores;
- Activos: Informações, hardware, software e serviços necessários para dar suporte ao negócio e identificados durante o processo de avaliação de riscos como activos que precisam ser protegidos;
- Autenticação: Verificação da identidade de um utilizador, processo ou dispositivo, geralmente como um pré-requisito para permitir o acesso a recursos em um Sistema de Informações;
- Bloqueio de Sessão: Uma acção temporária tomada por um Sistema de Informação para bloquear uma conexão a um aplicativo ou sistema em uma janela ou tela após um período de inactividade definido ou a pedido do utilizador até que o Utilizador restabeleça o acesso usando procedimentos de autenticação e identificação estabelecidos;
- Bloqueio da Tela: Um mecanismo de bloqueio de sessão dos Sistema de Informações, quando activado em um dispositivo com uma tela de exibição, coloca um padrão visível publicamente no monitor associado, ocultando o que estava visível anteriormente na tela.
- Computação Móvel: refere-se a vários dispositivos móveis (por exemplo, laptop, tablet ou smartphone) que permitem aos utilizadores acederem as informações de qualquer lugar e a qualquer momento;
- Controlo de Acessos: Processo de concessão ou rejeição de solicitações específicas:
    - Para obtenção e utilização de serviços de informações e processamento de informações relacionadas; e
    - Para entrar em instalações físicas específicas;
- Governance: garantia de que a Segurança da Informação se encontra alinhada com os objectivos de negócio, através do desenvolvimento de processos de gestão eficientes e eficazes que suportem a tomada de decisão;
- Informações: Dados processados que tenha significado e valor para o destinatário para suportar uma ação ou decisão;

- Programas utilitários: são projectados para auxiliar na gestão e ajuste de sistemas operacionais, hardware de computador e software aplicativo. Os programas utilitários executam uma tarefa específica relacionada a gestão de funções, recursos ou arquivos do computador (por exemplo, protecção por senha, gestão da memória, protecção contra vírus, etc.);

- SGSI (Sistema de Gestão de Segurança da Informação): abordagem sistemática para gerir e proteger os activos de informação do Banco Económico, sendo materializado por um conjunto de políticas, normas e procedimentos, bem como os controlos que definem toda a estratégia e operacionalização da Segurança da Informação. Os tipos de controlos que devem ser implementados são maioritariamente determinados com base nos resultados de avaliações de risco, mas também pelas exigências das partes interessadas, definidas pelo contexto do próprio Banco; e

- Utilizador: qualquer pessoa, entidade ou sistema que interage com, acede, utiliza ou gere sistemas de informação, recursos tecnológicos ou dados dentro de uma organização.

6. Princípios Gerais

O presente documento serve de referência para garantir o acesso de utilizadores autorizados e prevenir acessos não autorizados através do ambiente físico, as redes e sistemas à informação do Banco Económico, tendo como principal finalidade a salvaguarda da Informação. Assim, devem ser definidas e seguidas orientações no sentido de:

- Identificar e registar os utilizadores das redes e sistemas de informação;
- Restringir e gerir os acessos privilegiados atribuídos aos utilizadores;
- Rever periodicamente quais os utilizadores existentes, as suas permissões e os privilégios atribuídos;
- Gerir credenciais de acesso atribuídas aos utilizadores;
- Identificar os serviços e informação a disponibilizar aos colaboradores e partes interessadas de acordo com as suas funções laborais;
- Identificar controlos de acessos a implementar nas redes e sistemas de informação;
- Formar e instruir os colaboradores e partes interessadas na temática.

O Banco Económico providencia a todos os colaboradores e partes interessadas os acessos às redes e sistemas de informação estritamente necessários para a realização das suas funções laborais, tendo por base os seguintes princípios:

6.1. Identidade

- Os utilizadores das redes e sistemas são únicos, individuais e protegidos pelo colaborador, ou parte interessada, ao qual foi atribuído; e
- Os utilizadores genéricos ou de grupo são desaconselhados, salvo raras excepções onde os mesmos nunca devem permitir acessos a informação confidencial, restrita ou a informação pessoal de colaboradores, ou partes interessadas, do Banco Económico.

6.2. Contas Privilegiadas

- A atribuição de contas privilegiadas é baseada no mínimo necessário, cuidadosamente controladas e não atribuídas por defeito;
- As contas privilegiadas standard que são parte integrante dos sistemas, ou aplicações (e.g. *administrator, superuser, root, admin*), não são alteradas ou utilizadas para iniciar login. Como tal, são criadas contas com os mesmos privilégios ou associar esses privilégios a contas nominais. A identidade de quem realizou a acção é sempre conhecida.
- O processo de concessão de acessos privilegiados às redes e sistemas em geral são efectuados exclusivamente a utilizadores pertencentes a Direcção de Sistemas de Informação, a Direção de Compliance e ao Gabinete de Segurança da Informação; e
- A autorização de atribuição e utilização destas contas, sejam aplicações de negócio ou de acesso a infraestrutura deve ser explicitamente aprovada pelo Gabinete de Segurança da Informação, na sua ausência, pelo Grupo de Segurança da Informação.

6.3. Princípio de Acessos Mínimos

- A atribuição de acessos é sempre por base o Princípio de Acessos Mínimos de modo a garantir que os colaboradores e partes interessadas possuam somente os acessos necessários para desempenhar as suas funções na organização.

6.4. Auditoria

- As redes e sistemas de informação mantêm um registo dos acessos de utilizadores para os diferentes níveis, incluindo os afectos as equipas operacionais técnicas, tendo em conta as tentativas de login e as acções realizadas pelos mesmos; e

- Este registo é revisto periodicamente.

7. Procedimentos relacionados a Gestão e Controlo de Acessos

7.1. Autenticação em Redes e Sistemas

Para garantir a capacidade de identificar e autenticar um utilizador nas redes ou sistemas, assim como a capacidade de validar que um utilizador é quem diz ser, são analisados os seguintes requisitos:

- Garantir a utilização de identificadores organizacionais;
- Garantir que só é criado um identificador após a devida aprovação, sendo que o mesmo não pode ser reutilizado por outro colaborador, ou parte interessada;
- Definir mecanismos de autenticação que sejam suficientemente fortes para garantir a segurança da informação das redes e sistemas da organização;
- Manter o processo de autenticação utilizando sempre sessões e protocolos seguros (ex: HTTPS);
- Desactivar todos os protocolos que não garantam um início de sessão segura ou que transmitam as credenciais em plaintext (ex: HTTP, Telnet, FTP);
- Proteger e encriptar o conteúdo de autenticação de modificações ou divulgações não autorizadas;
- Garantir a validade dos certificados de autenticação; e
- Sempre que seja possível, implementar mecanismos com duplo factor de autenticação, preferencialmente com recurso a uma aplicação que gere tokens temporários (ex: Microsoft Authenticator), ao invés da utilização de SMS.

7.2. Controlo de Acessos a Redes e Sistemas

Para assegurar a segurança da informação armazenada nas redes e sistemas do Banco Económico, devem ser tidos em conta os seguintes requisitos:

- São utilizados mecanismos de segurança ao nível dos sistemas operativos para restringir ou prevenir o acesso não autorizado aos sistemas;
- O sistema de gestão de Palavra-Passe de acesso às redes e sistemas é interativo e garante a qualidade das mesmas;
- A utilização de aplicações privilegiadas que se sobreponham aos controlos existentes e sejam capazes de contornar os mecanismos de segurança das redes e sistemas está totalmente proibida;
- São considerados controlos de tempo das ligações no caso de sistemas que processem informação sensível, especialmente quando situados em localizações de

alto risco acesso, assegurando que a sessão é terminada após um período de inatividade pré-definido; e

- O acesso de utilizadores de suporte e fornecedores, às redes e sistemas da organização são geridos em conformidade com o contrato celebrado entre as partes.

7.3. Requisitos Críticos do Controlo de Acessos

7.3.1 Requisitos de Negócios, Legais e de Segurança para o Controlo de Acessos

Em consideração aos requisitos de negócios, legais e de segurança, o Proprietário da Informação orientará o processo de autorização e o acesso aos recursos de TI, assim como a outros activos de informação.

- A revisão dos requisitos do controlo de acessos é efectuada anualmente, ou a sua antecipação sempre que existir a necessidade de o fazer, e a ocorrência da mesma é sempre documentada.
- É validada a compatibilidade do acesso com os requisitos de Segurança dos activos dos sistemas sob gestão do Banco Economico.
- Os controlos de acesso são desenhados, implementados e validados em conformidade com todas as políticas, regulamentos, normas e diretrizes relevantes.

7.3.2 Gestão de Acessos ao Utilizador

A Gestão de Acessos do utilizador garante que utilizadores autorizados consigam ter acesso aos activos dos sistemas geridos pelo Banco Económico, enquanto os utilizadores não autorizados são impedidos de aceder ao mesmo. Cada activo do sistema gerido pelo Banco Económico deverá possuir procedimentos e controlos documentados específicos que cubram todas as fases do ciclo de vida do acesso do utilizador.

- Registo do Utilizador: O acesso aos activos dos sistemas deverá seguir os procedimentos formais.
    - Tipos específicos de conta são definidos (por exemplo, individual, grupo/compartilhado, serviço, convidado/anónimo, emergência e temporário).
        - Os utilizadores autorizados são associados a um grupo, função e às autorizações de acesso (por exemplo, privilégios) para cada conta.
    - As contas não devem ser criadas, activadas ou desactivadas sem obter o(s) nível(is) necessário(s) de aprovação. Esse processo incluí uma solicitação de acesso documentada.

- Os Administradores (DSI e DCP) da conta e o GSI, são sempre notificados quando:
  - Utilizadores são transferidos ou terminam o vínculo com a Instituição;
  - Existir a utilização indevida do Sistema de Informação ou necessidade de conhecer mudanças de requisitos; e
  - As contas, incluindo partilhada/grupo, emergência e temporária, não forem mais necessárias.
- Sempre que os Colaboradores forem transferidos, todos os acessos anteriores as suas funções específicas aos sistemas corporativos do Banco Económico, devem ser removidos, se aplicável ou revistos.
- A utilização de contas de grupo/partilhada, serviço, convidado/anónimo, de emergência e temporário é permitida somente se a utilização for explicitamente autorizada e monitorizada.
  - Quando contas de grupo/partilhadas são permitidas, um processo deve ser estabelecido para alterar as senhas quando os utilizadores são removidos do grupo. Além disso, um processo deve ser estabelecido para a responsabilidade individual dos utilizadores autorizados a utilizar o grupo/contas partilhadas.

- Arquivação da conta de utilizador: Com o objectivo de manter o histórico do utilizador e a capacidade da auditoria dos sistemas de informação do Banco Económico, as contas de utilizador não devem ser excluídas ou apagadas.
  - As contas de Utilizadores organizacionais podem ser arquivadas após noventa (90) dias de inatividade.
  - Contas de Utilizadores não-organizacionais/Parceiros/Fornecedores podem ser arquivadas após Cento e Vinte (120) dias de inatividade.
- Gestão de Privilégios: As regras de controlo de acessos incorporaram o princípio do privilégio mínimo, que concede o mais baixo nível de acesso, direitos, privilégios e permissões de segurança necessárias para o desempenho das tarefas autorizadas.
  - A Implementação de um sistema de controlo de acessos aceitável incluí a alocação de privilégios de Utilizador com base na necessidade de utilização, por sistema e por aplicação.
  - Os controlos de acesso estão alinhados para apoiar os requisitos de negócio e legais, incluindo a função de trabalho e a separação de tarefas.

- Revisão dos Direitos de Acesso do Utilizador: Os níveis de acesso do utilizador são revistos pelo GSI em alinhamento com o Proprietário da Informação (ou seus representantes) pelo menos uma vez por ano ou com mais frequência, conforme indicado pelos resultados dos requisitos de avaliação de risco dos Sistema de Informação e Classificação da Informação. A ocorrência de cada revisão deve ser documentada.

7.3.3 Controlo de Acessos à Rede

Os acessos internos e externos aos Sistemas de TI são fornecidos de maneira controlada e protegidos por uma combinação de controlos de segurança, incluindo segmentação, implementação de Firewalls e outros dispositivos de segurança, assim como mecanismos de autenticação forte, conforme apropriado.

Os controlos de segurança ajudam a prevenir e detectar o acesso não autorizado, enquanto fornecem acesso seguro para Utilizadores e sistemas autorizados.

- Identificação do Equipamento: Sempre que necessário, as conexões de locais e equipamentos específicos deverão ser autenticadas por um dos processos existentes e previamente definido; e
- Diagnóstico Remoto e Protecção da Porta de Configuração: As necessidades de funcionalidades de acesso remoto deverão ser validadas antes de activar qualquer capacidade de diagnóstico ou configuração remota.
- Segregação da Rede: Uma abordagem sobre o processo de segmentação deverá ser adoptada para separar os domínios lógicos da rede.

7.3.4 Controlo de Acessos ao Sistema Operacional

Os acessos aos sistemas operacionais são restritos a Utilizadores autorizados. Controlos de segurança deverão ser implementados para autenticar Utilizadores adequadamente, fornecer acesso apropriado por função (por exemplo, administrador), registar actividades e produzir notificações de eventos de segurança.

- Login Seguro: Procedimentos de login seguros que minimizem os riscos de acesso não autorizado devem ser adotados (por exemplo, acesso restrito a logins locais);
- Utilização de Utilitários do Sistema: O acesso e as permissões associadas a programas utilitários, incluindo programas com a capacidade de sobrepor controlos do sistema e aplicativos, devem ser estritamente controlados (por exemplo, documentados, verificados quanto a vulnerabilidades de segurança/códigos maliciosos, excluídos quando não forem mais necessários, etc.) e limitado a apenas à Utilizadores autorizados;
- Tempo Limite da Sessão: As sessões inactivas deverão ser bloqueadas ou encerradas após um período definido de inactividade.

- No mínimo, o Sistema de Informação deve ser configurado para:
  - Impedir o acesso não autorizado ao sistema;
  - Manter o bloqueio de sessão até que o Utilizador restabeleça o acesso utilizando procedimentos de identificação e autenticação pré-definidos (nome de utilizador e a palavra-passe); e
  - Iniciar um bloqueio da tela após um máximo de cinco (05) minutos de inatividade.

Limite de Tempo de Conexão: O tempo de conexão é limitado com base em um período definido de inatividade.

7.3.5 Controlo de Acessos aos Aplicativos e Outros Sistemas de Informação

Os normativos de gestão de acesso devem ser aplicados às informações e funções do sistema, com o objectivo de proteger contra acesso não autorizado e evitar que sistemas dos quais informações são compartilhadas sejam comprometidos.

- Restrição ao Acesso às Informações: O acesso às informações e aos sistemas e seus aplicativos é gerido de acordo com os normativos de acesso.
  - Os sistemas de informação que requerem autenticação devem exibir uma mensagem de notificação ao se efectuar o login. A informações adicionadas as mensagens de notificação, serão definidas de acordo ao acesso/sistema.

7.3.6 Computação Móvel

Os controlos de segurança são implementados para proteger contra os riscos exclusivos introduzidos pelo acesso a recursos de ambientes potencialmente desprotegidos.

- Os métodos e controlos de acesso remoto e sem fio, incluindo o acesso à rede local com fio (*Wired*) e sem fio (WLAN), deverão utilizar somente métodos de acesso remoto aprovados, suportados e com os controlos de recursos necessários aplicados.
- Os utilizadores devem assinar/concordar com a declaração de utilização aceitável aplicável aos dispositivos móveis e ao acesso a informação antes de receberem acesso a recursos de computação móvel.

7.3.7 Controlo de Acesso ao Ambiente Físico

Os controlos de acesso ao ambiente físico deverão ser implementados com o objectivo de restringir o acesso a infraestrutura física da Instituição, a equipamentos, documentos e suprimentos.

- Cumprimento da Política de Segurança Física;

- Os recursos serão mantidos em ambientes reservados e controlados, e o acesso aos mesmos obrigado a uma validação por parte dos utilizadores; e
- Periodicamente os acessos são revistos pela DPS (Direcção de Património e Segurança) e acompanhadas pelo GSI (Gabinete de Segurança da Informação).

Deverão ser garantidos os seguintes objectivos:

- Regular e estabelecer os pilares base da Segurança Física e Ambiental, no que respeita às áreas físicas e aos equipamentos que devem ser protegidos; e
- Definir as linhas orientadoras para a definição de controlos de protecção de espaços físicos e para a salvaguarda de equipamentos contra perda, dano, roubo, acesso não autorizado, alteração da informação em arquivo físico e interrupção das actividades do negócio, causada quer por ameaças humanas quer por razões ambientais.

Em relação à segurança das instalações, áreas seguras e equipamentos do Banco Económico, deverão:

- Descrever os sistemas de segurança instalados nas instalações, e as respetivas regras de operação que os impactam;
- Descrever orientações para perímetros de segurança física, controlos de entrada física, segurança em escritórios, salas e outros tipos de instalações, protecção contra ameaças externas e ambientais, trabalho em áreas seguras e áreas de carga e descarga;
- Descrever orientações para colocação e protecção de equipamentos, serviços básicos de suporte, segurança da cablagem, manutenção de equipamentos, remoção de activos, segurança de equipamentos e activos foras das instalações, eliminação e reutilização segura e segurança de equipamentos não vigiados.
- Os acessos ao CPD devem requerer solicitação, análise, validação e aprovação e adição ao repositório de gestão de acessos, e estão sobre a responsabilidade das seguintes áreas: Direcção de Sistemas da Informação, em alinhamento com o Gabinete de Segurança da Informação.

Para o caso de existirem dados a serem processados em Centros de Processamento de Dados subcontratados, o Banco terá visibilidade sobre os acessos realizados as unidades pertencentes a instituição. As áreas que devem possuir esta visibilidade são a Direcção de Sistemas de Informação e o Gabinete de Segurança da Informação.

8. Estrutura Organizacional

A operacionalidade da Política é executada por vários intervenientes, a destacar:

8.1. Gabinete de Segurança da Informação

O GSI tem como principais responsabilidades:

- Efectuar a supervisão de todos os acessos (aplicações de negócio, infraestrutura e físico e ambiental), com base na matriz de acesso e validar o cumprimento dos requisitos;
- Emitir parecer sobre as solicitações de acesso excepcionais as aplicações de negócio e a infraestrutura de TI;
- Definir e submeter para validação os normativos de acesso aos vários segmentos da Infraestrutura do Banco Económico;
- Efectuar a gestão dos acessos a solução *swift* e seus produtos complementares;
- Garantir o cumprimento da política de gestão de acessos; e
- Acompanhar e validar o preenchimento dos repositórios de gestão de acessos a Infraestrutura, as aplicações de negócio e aos espaços físicos.

8.2. Direcção de Sistemas da Informação

A DSI tem como principais responsabilidades:

- Garantir e/ou configurar após a devida aprovação, o acesso a infraestrutura de TI, seus recursos e serviços;
- Proceder ao acompanhamento do procedimento de acesso final após a concessão do mesmo; e
- Adicionar informações o repositório de gestão de acessos a Infraestrutura.

8.3. Direcção de *Compliance*

O Grupo de Segurança de Informação tem como principais responsabilidades:

- Fazer o acompanhamento do ciclo da Política;
- Garantir a aplicabilidade da Política;
- Avaliar a Política de acordo com as necessidades do negócio e os Padrões Internacionais;
- Garantir a conformidade do processo de gestão de acessos de acordo com os normativos existentes;
- Efectuar a configuração dos acessos as aplicações de negócio, de acordo com as normas concernentes ao acesso as mesmas e/ou remeter as Direcções competentes as solicitações de acesso as aplicações de negócio;

- Adicionar informações o repositório de gestão de acessos as aplicações de negócio.

8.4. Direcção de Risco

A Direcção de Risco tem como principais responsabilidades:

- Efectuar a análise e a avaliação dos riscos que podem estar associados a actividades de Gestão de Acessos;
- Emitir parecer e opiniões sobre as acções de controlo de modo a mitigar os riscos.

8.5. Direcção de Auditoria

No âmbito das suas responsabilidades e de acordo com o respectivo Plano de actividades, a Direcção de Auditória tem como principais responsabilidades:

- Avaliar se as configurações dos sistemas (aplicações, base de dados, sistemas operativos, etc.) estão devidamente parametrizadas com o objectivo de reduzir a vulnerabilidade perante ameaças;
- Testar e avaliar os controlos dos processos de atribuição de acessos, remoção de acessos e revisão de acessos com o objectivo de verificar que os acessos são adequados, autorizados e estão de acordo com as suas respectivas funções e responsabilidades;
- Emitir junto da Comissão Executiva do Banco Económico as opiniões e pareceres sobre os resultados das avaliações e testes decorrentes do exercício de auditoria.

8.6. Direcção de Património e Segurança

A DPS tem como principais responsabilidades:

- Efectuar a gestão efectiva dos acessos ao ambiente físico, sempre que se observar o cumprimento dos requisitos necessários;
- Proceder a aprovação dos acessos ao ambiente físico solicitado em alinhamento com o GSI, dependendo da criticidade do ambiente/área, observando o processo de aprovação para o referido ambiente;
- Conceder o acesso sempre que se observar a aprovação do mesmo; e
- Adicionar informações o repositório de gestão de acesso físico e ambiental.

9. Incumprimento

O incumprimento das regras descritas nesta Política pode ser considerado violação grave dos deveres de conduta e, em consequência, pode dar lugar à aplicação de medidas disciplinares, sanções contratuais ou a eventual responsabilidade criminal.

10. Interpretação

A presente Política deve ser interpretada em conformidade com as normas legais e estatutárias que sejam aplicáveis cabendo, à Comissão Executiva resolver as dúvidas de interpretação que possam surgir.

11. Divulgação

A presente Política será objecto de divulgação, para consulta, no *site* de Intranet e Internet do Banco.

12. Alterações e Aprovação

A presente Política é revista com uma periodicidade mínima anual, podendo, no entanto, o Gabinete de Segurança da Informação propor ao Conselho de Administração a revisão da mesma num prazo inferior, sempre que se considere oportuno.

A Política de Gestão de Acessos foi aprovada pelo Conselho de Administração do Banco.

1. Considerações Finais

A coordenação e execução da Política de Gestão de Acessos é responsabilidade do Gabinete de Segurança da Informação, onde deve ser dirigida quaisquer questões relacionadas a mesma.