Política de Cibersegurança

ATLANTICO

BANCO MILLENNIUM ATLANTICO

INFORMAÇÃO DO DOCUMENTO

Política de Cibersegurança	
Documento atribuído à:	Direcção de *Cyber Security* (DCS)
Referência:	PL-ATL-029
Versão:	01
Elaborado por:	Direcção de *Cyber Security* (DCS)
Validado por:	Direcção de Processos e Organização (DPO)
Aprovado por:	Comissão Executiva (CE)
Data de Aprovação:	03/02/2021
Data de Publicação:	09/02/2021
Data da Última Revisão:	N/A
Classificação (Nível de confidencialidade):	Público
Local de Publicação:	Intranet e site Institucional

HISTÓRICO DE ALTERAÇÕES

Versão	Data de Publicação	Descrição das Alterações
01	09/02/2021	Versão Inicial

ÍNDICE

TÍTULO I - INTRODUÇÃO

A presente política define os requisitos e mecanismos para prevenir, detectar e responder aos riscos e ameaças de Cibersegurança nos Sistemas de Informação (SI) do ATLANTICO.

TÍTULO II – OBJECTIVO

A Política define as directrizes para regulamentar a segurança de informação do ATLANTICO, em linha com os princípios contidos na sua Missão, Visão e Valores, a fim de:

a) Contribuir para a manutenção da confiança dos clientes, colaboradores, accionistas e reguladores na capacidade do ATLANTICO proteger os activos sob sua responsabilidade, de ameaças associadas aos sistemas de informação ou outro tipo de ameaças, acidentais ou intencionais, que possam comprometer a sua confidencialidade, integridade e disponibilidade;

b) Cumprir as obrigações legais, regulamentares e contratuais aplicáveis ao ATLANTICO;

c) Detectar de forma oportuna os eventos que podem indicar acções que possam comprometer os activos do ATLANTICO;

d) Fornecer uma capacidade de resposta eficaz e eficiente em caso de incidentes de segurança de informação;

e) Operar a estratégia de segurança dos sistemas de informação do ATLANTICO, considerando os desafios actuais e futuros, a que o ATLANTICO tem de responder, em linha com o desenvolvimento tecnológico [ex: *Bring Your Own Device* (BYOD)], observando os princípios da:

   - **Confidencialidade** – salvaguardar que apenas quem está autorizado pode aceder à informação;
   - **Integridade** – assegurar que a informação e os seus métodos de tratamento e de processamento são exactos e completos;
   - **Disponibilidade** – garantir que os usuários autorizados tenham acesso à informação, estritamente necessária às suas funções e aos activos associados quando o solicitarem.

Deste modo, é uma obrigação legal e ética do ATLANTICO garantir, nos mesmos termos e conforme procedimentos em vigor, às instituições e aos organismos oficiais competentes, a informação estritamente necessária referente à sua actividade e aos seus clientes.

Sob estas premissas, a informação criada, processada e armazenada nos sistemas de informação interna, independentemente do seu suporte ou formato, é utilizada durante as actividades operativas e administrativas do seu negócio, considera-se um activo pertencente ao ATLANTICO. Inclui-se na definição anterior, a informação cedida ao ATLANTICO sob o âmbito legal estabelecido e que se considerará como activo próprio, inserido nos bens exclusivos em sua protecção.

Deve-se considerar igualmente como activos a proteger os diferentes recursos informáticos (hardware, software e produtos licenciados) utilizados para administrar, aceder e gerir a informação pertencente ao ATLANTICO.

TÍTULO III – ÂMBITO DE APLICAÇÃO

A Política é aplicável a todos os colaboradores, estagiários, parceiros, consultores e prestadores de serviço do ATLANTICO. Os requisitos para a protecção dos dados e das informações, conforme estabelecidos nesta política, também devem ser observados e cumpridos por parceiros externos e terceiros (inclusive consultores, contratados ou prestadores de serviços) sempre que prestarem serviços para o ATLANTICO, ou em seu nome.

TÍTULO IV – TRATAMENTO DAS INFORMAÇÕES DE RISCO EVCIBERSEGURANÇA

O ATLANTICO como um todo tem a responsabilidade de identificar, avaliar e gerir o amplo espectro de riscos aos quais está sujeito, sendo que adopta o modelo "Três linhas de defesa" para garantir que os riscos e controlos sejam geridos adequadamente pelos seus processos, pessoas e tecnologia de uma forma contínua e permanente:

- **Primeira Linha** – constituída por órgãos de Negócio e Suporte. Equipas técnicas especializadas responsáveis pela instalação e operação do ambiente de Tecnologias de Informação (TI) e uma equipa dedicada de segurança cibernética responsável por impulsionar a conformidade com as políticas e padrões sobre a utilização de sistemas, a implementação e a operacionalização de controlos de segurança na infraestrutura e nas redes de TI;
- **Segunda Linha** – as equipas de Risco Operacional, formulam e monitoram políticas e garantem a conformidade e a operação do controlo na primeira linha. As equipas de segunda linha também fornecem experiência no assunto para o desenvolvimento e implementação de controlos, ferramentas e projectos;
- **Terceira Linha** – os auditores internos fornecem uma revisão independente do estado de controlo da primeira e da segunda linha e da interacção entre elas.

TÍTULO V – PRINCÍPIOS E CONTROLOS DE SEGURANÇA DE INFORMAÇÃO

A Segurança de Informação consiste na protecção das informações e dos sistemas de informação contra o acesso e utilização indevida, divulgação, disrupção, modificação ou

destruição não autorizados, a fim de garantir sua confidencialidade, integridade e disponibilidade.

Esta Política apresenta os princípios que devem ser seguidos para a utilização aceitável e adequada de *hardware, software,* sistemas, aplicativos, dados, instalações e redes de tecnologia da informação, bem como equipamentos de telecomunicações, com base em exigências e objetivos de controlo de segurança das informações, por forma a proteger os activos do ATLANTICO.

4.1 Formação e Conscientização sobre Cibersegurança

O ATLANTICO dispõe de um programa contínuo de formação e consciencialização de segurança que emprega vários canais destinado aos seus colaboradores, prestadores de serviços e clientes, incluindo, conteúdos na netPHI e redes sociais, *e-mails* e educação de novos colaboradores. Anualmente deverá ser realizado um treino obrigatório de conscientização de Cibersegurança para os colaboradores, sendo que os resultados do mesmo deverão ser monitorizados.

4.2 Políticas

O ATLANTICO utiliza as boas práticas internacionais recomendáveis por meio da implementação de políticas, padrões e directrizes, com vista a cobertura dos riscos de Cibersegurança, estando contemplados nas diversas políticas os seguintes pontos:

a) Responsabilidades de segurança definidas;
b) Testes para identificar deficiências ou ausências de controlos;
c) Políticas de manuseamento ou utilização aceitável de sistemas e dispositivos dentro da Organização;
d) Critérios definidos para controlo de acesso, incluindo:
    - Ter acesso apenas a informação necessária para cumprimento das suas tarefas;
    - Princípio de menor privilégio;
    - ID exclusivo;
    - Complexidade de senhas;
    - Aprovações de acesso;
    - Processos de transferência;
    - Acesso privilegiado;
    - Controlos de acesso remoto.

e) Ciclos de vida de desenvolvimento de software para aplicativos, incluindo revisão de código, segregação de actividades, revisão de segurança de serviços web;
f) Controlo de alteração/mudança de requisitos e planeamento de Recuperação de Desastres e Plano de Continuidade de Negócios;
g) Procedimentos para classificação de informações definidas (sistema de classificação de informação de 5 (cinco) níveis: Público, Interno, Restrito, Confidencial e Secreto. Esses termos são mencionados neste documento);

h) Políticas e procedimentos bem definidos para tratamento, transmissão e destruição de informações de forma segura;
i) Políticas do ambiente do usuário final, abrangendo a fuga de dados, monitorização de aplicações cuja infraestruturas de processamento de dados não são geridos pelo ATLANTICO, classificação de informação e acesso remoto para teletrabalho;
j) Controlo das configurações técnicas efectuadas na infraestrutura, sistemas e redes do ATLANTICO;
k) Controlo físico.

4.3 Gestão de Riscos

O ATLANTICO aplica a gestão de riscos nas linhas de defesa para identificar, relatar e gerir riscos em toda a organização. As estruturas de segurança da informação no ATLANTICO seguem padrões internacionalmente reconhecidos para a aplicação das melhores práticas.

As avaliações de riscos são realizadas periodicamente para tratar de alterações nos requisitos de segurança da informação ou no apetite ao risco institucional e/ou quando ocorrem alterações significativas. O ATLANTICO realiza avaliações de riscos em uma variedade de activos dentro da organização. Estes podem ser activos físicos, pessoas, processos, software e informações. Por exemplo: avaliações regulares de riscos à segurança das informações nas aplicações e infraestrutura para:

a) Identificar, quantificar e gerir riscos de segurança para atingir objectivos de negócio;
b) Fornecer meios para identificar atividades e factores que representam os maiores riscos de segurança para o ATLANTICO;
c) Garantir que a gestão das vulnerabilidades de segurança seja feita de acordo com a sua classificação de risco e que os controlos sejam proporcionais ao nível de risco descoberto;
d) Fornecer uma visão corporativa dos riscos de Cibersegurança e os respectivos planos de correção para desenvolver a estratégia de Cibersegurança;
e) Planear a implementação de recursos em áreas que proporcionem a maior redução de riscos nas informações dos clientes.

4.4 Gestão de Identidade e Acessos

A Gestão de Identidade e Acessos visa garantir que a eventual adição e/ou a modificação tempestiva e específica dos acessos seja adequada às atribuições dos utilizadores e que esteja em linha com o definido pelo Regulador e orientado por políticas ao longo do ciclo de vida dos controlos de suporte, sendo que estes incluem:

a) Os pedidos de criação, alteração, bloqueio e eliminação de acessos, que devem obedecer estritamente às regras definidas pelo ATLANTICO;
b) A criação de utilizadores deve obedecer a uma regra de nomenclatura de conta de utilizadores dos SI do ATLANTICO;

c) A atribuição de utilizadores privilegiados para a gestão dos SI do ATLANTICO é efectuada de acordo a função desempenhada;
d) Os utilizadores genéricos, de serviço e aplicacionais são criados e atribuídos de acordo com as regras internas definidas e seguindo um processo de aprovação;
e) A autenticação aos principais sistemas de informação é efectuada de forma centralizada e o acesso a informação é efectuado de acordo com os perfis de acessos atribuídos, seguindo o processo de atribuição de perfis de acessos definido no ATLANTICO;
f) A configuração e gestão de palavras-passe é efectuada de forma centralizada e os mesmos seguem os parâmetros de palavras-passe definidos na Política de Gestão de Identidade e Acessos do ATLANTICO;
g) A monitorização e revisão de utilizadores e perfis de acesso é efectuada e de forma sistemática e semiautomática, conforme definido no processo instituído.

4.5 Segurança de Aplicações

As equipas técnicas de gestão de Primeira e Segunda linha de defesa identificam ameaças, utilizam controlos e realizam testes incluindo:

a) Consultoria de segurança de aplicativos e avaliações de risco, para garantir que os riscos nos aplicativos e sistemas do ATLANTICO sejam geridos para um nível aceitável;
b) Assessoria técnica e de riscos à segurança da informação para empresas, projetos ou iniciativas de funções;
c) Definir e testar controlos relacionados a segurança nos sistemas e aplicativos;
d) Instalação e monitoração de controlos a nível aplicacional;
e) Desenvolvimento de padrões mínimos de segurança.

Realização de testes de segurança, ou seja, testes de intrusão aplicacionais (que incluem a utilização da *framework* OWASP) e revisões de código.

4.6 Segurança de Rede

Para permitir uma gestão eficaz e segura, o ATLANTICO utiliza várias tecnologias implementadas estrategicamente em toda a sua rede.

4.7 Intrusion Detection and Prevention Systems-IDS and IPS

O ATLANTICO tem implementado na sua rede e infraestrutura, um sistema de detecção e prevenção de intrusão. Esses sistemas são geridos pela primeira linha de defesa. A segurança das redes e infraestrutura do ATLANTICO estão sujeitas a monitorização 24/7.

4.8 Gestão de Redes Wireless

A infraestrutura de redes sem fio *(wireless)* nos serviços centrais e nas agências ATLANTICO são protegidas utilizando mecanismos de controlo, monitorização,

criptografia e autenticação de acessos e contam com recursos para protecção contra pontos de acesso sem fio não autorizados.

4.9 Filtros de Acessos a Internet

Os colaboradores ATLANTICO apenas têm acesso à Internet para desempenho das suas actividades profissionais. O acesso é filtrado de acordo com regras definidas centralmente. É necessária uma aprovação de gestão adicional para qualquer acesso fora do padrão e pode estar sujeita a monitorização adicional.

4.10 Prevenção de Perda/Fuga de Dados

O Programa de Prevenção de Perda / Fuga de Dados do ATLANTICO está em vigor para reduzir a exposição ao risco de perda através da aplicação de controlos e processos técnicos, bem como a educação dos colaboradores. Inclui processos para detectar e proteger automaticamente informações restritas e altamente restritas, enviadas externamente pelo ATLANTICO, isto inclui *e-mails*, transferências de arquivos e *uploads* na *Web*. O ATLANTICO efectua monitorização de dados para se proteger contra os riscos de roubo, perda acidental ou exposição deliberada de informações confidenciais.

4.11 Testes de Segurança a Infraestrutura

O teste de segurança da infraestrutura é uma componente das análises técnicas de segurança do ATLANTICO e é utilizado para validar a postura de segurança de qualquer tecnologia. Os testes de intrusão na infraestrutura são realizados de forma regular por equipas internas, como parte dos processos de melhoria da tecnologia. Além disso, testes independentes por terceiros especializados, usando técnicas avançadas e os mais recentes padrões do sector para fornecer garantia adicional. As saídas de tais testes são geridas dentro do processo e da estrutura de gestão de riscos do ATLANTICO.

4.12 Criptografia

Os dados do ATLANTICO são classificados de acordo com a sua sensibilidade para determinar o nível de controlo necessário, incluindo, entre outros, a criptografia para manter a confidencialidade das informações, impedir a fuga não autorizada de dados ou fornecer verificações de integridade ou assinaturas digitais.

O ATLANTICO define claramente padrões criptográficos que exigem conjuntos de cifras apropriados e cumprimentos de chave (códigos de acesso a informação criptografada) para atender a objetivos específicos.

4.13 Estações de Trabalhos e Dispositivos Móveis

As estações de trabalho e *laptops* do ATLANTICO possuem, por padrão base, um *software* antivírus incorporado aos seus sistemas operativos, configurados para verificar automaticamente e de forma periódica os arquivos e obter actualizações assim que estiverem disponíveis.

Os *desktops* / *laptops* têm um único formato personalizado pré-instalado que limita o acesso administrativo dos utilizadores.

Todas as *Workstations* e *laptops* possuem uma solução de criptografia de disco que permite prevenir contra a fuga de dados em caso de furto ou roubo dos mesmos.

A utilização de dispositivos amovíveis é restrita a um conjunto limitado e pré-identificado de colaboradores autorizados e são aplicados automaticamente controlos de criptografia a estes dispositivos.

O acesso à rede interna do ATLANTICO fora das instalações é restrito aos dispositivos autorizados, que são controlados por conectividade remota.

Os dispositivos móveis fornecidos pelo ATLANTICO são geridos de forma centralizada através da aplicação de políticas e controlos para limitar a exposição de informações, sendo que também fornecem recursos de criptografia para dados em trânsito ou em repouso e recursos de segurança os dados de dispositivos perdidos ou roubados.

4.14 Gestão de Patches

As equipes de primeira linha efectuam verificações ou recebem notificações de vulnerabilidades do fornecedor do produto e respostas de *patch* recomendadas. A priorização para implementação de *patches* no ATLANTICO é determinada pela Política de Gestão de Vulnerabilidades que se baseia na *framework* para classificação de vulnerabilidade *Common Vulnerability System Standard* (CVSS).

Os *patches* são testados em ambiente de qualidade antes da implementação em sistemas de produção. Todas as implementações de *patch* são geridas de acordo com a Política de aquisição, desenvolvimento, manutenção de sistemas de informação do ATLANTICO.

A governança e a supervisão adequadas são exercidas por meio do envolvimento e da comunicação regular com todas as áreas do ATLANTICO e de acordo com a estrutura estabelecida. Mensalmente, são efectuados reportes de conformidade do *patch* de segurança e operacionais.

4.15 Trabalho Remoto

O ATLANTICO oferece suporte a recursos de trabalho remoto quando apropriado, necessário e conforme processo em vigor. Controlos e orientações adicionais para os colaboradores e prestadores que trabalham remotamente incluem, mas não estão limitados a:

a) Sensibilização sobre os riscos do trabalho remoto e termo de responsabilidade antes que o acesso remoto seja fornecido;
b) Criptografia de disco em *laptops*;
c) Utilização de VPN para conexão com a infraestrutura interna;

d) Utilização de uma solução centralizada para a gestão de dispositivos não pertencentes ao ATLANTICO.

4.16 Segurança Física

Medidas de segurança física são implementadas para impedir o acesso não autorizado às instalações, recursos ou informações do ATLANTICO. Estas medidas são revistas regularmente. As medidas implementadas pelo ATLANTICO incluem, mas não estão limitadas a:

a) Barreiras físicas e pessoal de protecção física;
b) Sistemas de controlo de acesso e cartões de identidade;
c) Sistemas de vídeo vigilância;
d) Sistemas de detecção de intrusão.

4.17 Resposta a Incidentes de Cibersegurança

O plano de gestão e resposta a incidentes de segurança cibernética do ATLANTICO visa:

- Coordenar a gestão de incidentes de segurança cibernética para garantir que todas as tarefas necessárias sejam concluídas e evitar que as mesmas sejam duplicadas;
- Garantir que os incidentes de segurança cibernética sejam investigados no mínimo tempo possível;
- Garantir que o risco associado a um incidente seja devidamente identificado, mensurado e controlado;
- Certificar de que as notificações internas e relatórios externos necessários sejam efectuados;
- Garantir que todos os incidentes de segurança cibernética sejam monitorizados para análise e reportados a gestão de topo.

4.18 Acordos de Confidencialidade de Informação

O ATLANTICO apenas divulga informações a terceiros se os controlos apropriados forem considerados e implementados, conforme aplicável, para gestão de acessos de terceiros, utilização e armazenamento de informações do ATLANTICO. Os controlos podem incluir:

- Acordar perviamente e por escrito (exemplo via assinatura de *NDA*) as obrigações de confidencialidade e segurança da informação com o terceiro;
- Fazer avaliações adequadas da informação, como e por que ela deve ser divulgada;
- A transferência de informações é protegida por meio de controlos técnicos, conforme exigido pelo ATLANTICO, para que terceiros possam atender às nossas responsabilidades legais, obrigações e requisitos regulamentares.

4.19 Gestão de Segurança de Prestadores de Serviços

O ATLANTICO tem políticas e processos de gestão de Prestadores de Serviços (incluindo: Avaliação, identificação e selecção de prestadores de serviços e fornecedores) associados aos contractos com prestadores.

O ATLANTICO exige que estes observem pelo menos o mesmo nível de segurança, de acordo com as políticas e padrões internacionalmente recomendados, cobrindo os requisitos legais e regulatórios que se aplicam às informações ou sistemas do ATLANTICO cedidos durante a prestação de serviço.

Os prestadores de serviços com acesso à infraestrutura ou informações do ATLANTICO estão sujeitos a análises de devida diligência de segurança da informação com base em seu risco potencial para a organização. Cláusulas específicas de Cibersegurança estão incluídas nos termos e condições dos contratos com os prestadores de serviços.

TÍTULO X – APROVAÇÃO E REVISÃO DA POLIÍTICA

A Política de Cibersegurança é aprovada pela Comissão Executiva (CE) e será objecto de revisão ou actualização com a periodicidade mínima anual ou sempre que se considere necessário, sob proposta da DCS, responsável pela sua aplicação.

TÍTULO VI – VIGÊNCIA E VALIDADE

A presente Política vigora a partir da data da sua publicação, podendo ser actualizada com base nas modificações inerentes a novos serviços, novas ameaças e alterações na Política Interna do ATLANTICO.

Banco Millennium Atlântico

ATLANTICO
Valores para a vida.

Cidade Financeira Via S8,
Talatona – Luanda Sul, Angola
Código Postal nº 195

(+244) 226 432 400
www.atlantico.ao