Política de Cibersegurança

Índice

1. INTRODUÇÃO

A Fundação Mendes Gonçalves e a Casa MG aprovaram a presente Política de Cibersegurança (doravante, a "Política") por considerar que a cibersegurança é um pilar fundamental para a proteção dos ativos digitais, dados sensíveis e continuidade operacional da Fundação Mendes Gonçalves e Casa MG, e por reconhecerem a crescente sofisticação dos ataques cibernéticos.

A presente Política tem como objetivo estabelecer de forma clara e inequívoca os princípios, as diretrizes e a abordagem adotada pela Fundação Mendes Gonçalves e Casa MG no que respeita à gestão dos riscos de cibersegurança, que são intrínsecos à sua atividade e operações, de modo a garantir a continuidade, integridade e confidencialidade dos dados e sistemas das organizações.

A Fundação Mendes Gonçalves e Casa MG estão comprometidas com a adoção das melhores práticas de cibersegurança e proteção de dados, em conformidade com as legislações, regulamentações e orientações nacionais e internacionais relevantes, incluindo o Quadro Nacional de Referência para a Cibersegurança e o Regulamento Geral de Proteção de Dados (RGPD), garantindo que todas as suas operações e processos estão em conformidade com as normativas legais e regulamentares relevantes. A política visa, ainda, apoiar o alcance dos objetivos estratégicos da organização, promovendo um ambiente seguro e resiliente, que favoreça a confiança dos clientes e beneficiários, colaboradoras, colaboradores e parceiros.

2. ÂMBITO DE APLICAÇÃO

A presente política aplica-se a todos os colaboradores da Fundação Mendes Gonçalves e de todas as entidades da Casa MG (titulares dos órgãos sociais e departamentos, e às pessoas ao serviço da Fundação Mendes Gonçalves e da Casa MG ao abrigo de contrato de trabalho, contrato de estágio ou de qualquer outra natureza) e todos os seus parceiros (Clientes ou Beneficiários, Fornecedores e Prestadores de Serviços) que tenham acesso a sistemas, redes, dispositivos e dados da Fundação Mendes Gonçalves e da Casa MG.

As diretrizes aqui estabelecidas abrangem toda a infraestrutura de Tecnologias de Informação (TI) da Fundação Mendes Gonçalves e Casa MG, nomeadamente:

- **Serviços digitais e aplicações**, como plataformas de gestão, sistemas de ERP, CRM e softwares especializados utilizados nas organizações;
- **Dispositivos**, como computadores, servidores, dispositivos móveis, tablets, impressoras e qualquer outro equipamento que aceda ou armazene dados das organizações;

- **Infraestrutura de rede e conectividade**, incluindo *Firewalls*, *Virtual Private Network* (VPNs), servidores físicos e virtuais, redes Wi-Fi, segmentação de rede e dispositivos de segurança;
- **Ambientes de trabalho remoto e híbrido**, garantindo que acessos externos à rede das organizações sigam os protocolos de segurança estabelecidos;
- **Armazenamento e gestão de dados**, abrangendo bases de dados locais e em nuvem, soluções de backup e políticas de retenção de dados;
- **Meios de comunicação digital**, como e-mails das organizações, ferramentas de videoconferência, aplicações de mensagens instantâneas e compartilhamento de arquivos.

3. OBJETIVOS DE SEGURANÇA

Para cumprir o seu compromisso com a promoção da cibersegurança e segurança da informação, a Fundação Mendes Gonçalves e a Casa MG adotaram os seguintes Objetivos de Segurança:

Identificar	• Compreender o contexto da Fundação Mendes Gonçalves e da Casa MG, dos ativos que suportam os processos críticos da sua atividade e dos riscos associados relevantes.
Proteger	• Implementar medidas destinadas a proteger os processos organizativos e os ativos da Fundação Mendes Gonçalves e da Casa MG, independentemente da sua natureza tecnológica.
Detetar	• Definir e implementar medidas destinadas a identificar, de forma atempada, os incidentes, i.e. efeitos adversos reais na segurança das redes e dos sistemas de informação.
Responder	• Definir e implementar medidas de ação apropriadas, em caso de deteção de um incidente.
Recuperar	• Definir e implementar atividades, que visam a gestão de planos e medidas de recuperação dos processos e serviços afetados por um incidente de cibersegurança.

Para tanto, a Fundação Mendes Gonçalves e a Casa MG definiram internamente um ***framework* de responsabilidades**, composto pelos respetivos Conselhos de Administração, pelo *Chief Information Security Officer* (CISO) nomeado pela Administração, pela Mendes Gonçalves - Sistemas e Tecnologias de Informação, Lda. e por prestadores de serviços externos.

4. IDENTIFICAR

O presente objetivo prende-se com a identificação pela Fundação Mendes Gonçalves e a Casa MG das diferentes dimensões das suas organizações, ao nível das suas redes e sistemas de informação, pessoas, ativos e dados.

Assim, para atingir este objetivo de segurança, ambas se comprometem a:

- ✓ **identificar e classificar os ativos de informação** (dados, colaboradores, equipamentos, sistemas e instalações) em função da sua relevância e criticidade para as atividades da Fundação Mendes Gonçalves e da Casa MG, de forma que possam ser adequadamente protegidos em todo o seu ciclo de vida;
- ✓ **identificar e tipificar os fornecedores**, nomeadamente os fornecedores que sejam considerados críticos pela Fundação Mendes Gonçalves e pela Casa MG, e assegurar que os mesmos se enquadram nas necessidades e requisitos de Cibersegurança;
- ✓ **identificar, avaliar e tratar os riscos de Cibersegurança inerentes à atividade** da Fundação Mendes Gonçalves e da Casa MG e aos quais os seus ativos se encontram expostos;
- ✓ **estabelecer um procedimento de identificação, avaliação e tratamento do risco** de acordo com a tolerância ao risco da Fundação Mendes Gonçalves e da Casa MG.

A Fundação Mendes Gonçalves e a Casa MG acreditam num processo de melhoria contínua dos seus procedimentos, políticas, planos e processos à luz da atualização das boas práticas da indústria e do setor fundacional e das referências e normas internacionais de Cibersegurança. Considerando isto, o objetivo ***Identificar*** tem em vista ainda (i) promover estratégias de implementação de oportunidades de melhoria, nomeadamente as propostas resultantes de auditorias, testes de intrusão ou outros projetos internos ou externos em matéria de Cibersegurança e (ii) definir indicadores que suportem modelos de reporte de Cibersegurança a ser apresentados internamente ao CISO e, quando aplicável, a outros órgãos da Fundação Mendes Gonçalves e da Casa MG.

5. PROTEGER

O objetivo ***Proteger*** tem em vista o desenvolvimento e a implementação de salvaguardas necessárias ao desenvolvimento da atividade da Fundação Mendes Gonçalves e da Casa MG, permitindo-lhes limitar ou conter o impacto da ocorrência de um incidente de cibersegurança. Para tanto, a Fundação Mendes Gonçalves e a Casa MG reconhecem a necessidade de:

- ✓ **estabelecer e implementar controlos para proteger os ativos de informação** da Fundação Mendes Gonçalves e da Casa MG de roubo, intrusão, abuso ou outras formas de tratamento ilícito;
- ✓ **assegurar a disponibilidade e fiabilidade dos equipamentos, infraestruturas** e sistemas que suportam a atividade da Fundação Mendes Gonçalves e da Casa MG;
- ✓ **promover uma cultura de sensibilização e compromisso para a Cibersegurança** entre os membros do Conselho de Administração, Responsáveis de Departamento e os Colaboradores, motivando-os a tomarem conhecimento e assumirem a responsabilidade pela sua intervenção, de forma a minimizar o risco de incidentes de segurança da informação;
- ✓ **assegurar a proteção de dados pessoais**, nos termos previstos na legislação aplicável;
- ✓ **promover a partilha de informação relevante em matéria de Cibersegurança**, através de canais seguros e em tempo útil, com as partes interessadas da Fundação Mendes Gonçalves e da Casa MG, entidades oficiais e outros grupos de interesse;
- ✓ **contribuir para a generalização da consciencialização sobre Cibersegurança**.

A Fundação Mendes Gonçalves e a Casa MG implementaram um conjunto de medidas de proteção no que concerne a proteção de equipamentos, sistemas e redes:

5.1. Segmentação e Proteção da Rede

A segmentação da rede é fundamental para evitar a propagação de ameaças e acessos não autorizados. A Fundação Mendes Gonçalves e a Casa MG implementaram ainda *firewalls* por forma a filtrar tráfego, bloquear acessos maliciosos e prevenir ataques de negação de serviço, nomeadamente ataques DoS (***Denial of Service*** - **Negação de Serviço**)[1] e DDoS (***Distributed Denial of Service*** - **Negação de Serviço Distribuída**)[2], como sistemas de IDS (***Intrusion***

[1] Um ataque de DoS ocorre quando um sistema, serviço ou rede é sobrecarregado com tráfego malicioso, tornando-o inacessível para utilizadores legítimos. Isso pode ser feito enviando um grande volume de requisições ou explorando vulnerabilidades do sistema.

[2] O ataque DDoS é uma variação do DoS, mas realizado de múltiplas origens simultaneamente, geralmente através de uma botnet (rede de dispositivos comprometidos). Isso torna o ataque mais difícil de bloquear, pois vem de vários locais ao mesmo tempo.

Detection System - Sistema de Deteção de Intrusão)[3] e IPS (*Intrusion Prevention System* - Sistema de Prevenção de Intrusão)[4].

5.2. Autenticação e Acesso Remoto

A Fundação Mendes Gonçalves e a Casa MG adotam um modelo robusto de segurança no acesso remoto, baseado em Autenticação Multifator (MFA) e VPN com criptografia avançada. Na Fundação Mendes Gonçalves e na Casa MG, a VPN é obrigatória para qualquer acesso remoto aos sistemas das organizações, impedindo acessos diretos que possam comprometer a segurança da rede e garantindo um ambiente digital protegido para Colaboradoras, Colaboradores e parceiros. Todos os dados que trafegam por essa conexão são criptografados com protocolos avançados.

5.3. Gestão de Dispositivos e Software

Todos os dispositivos utilizados pelos Colaboradores – incluindo computadores, portáteis, smartphones corporativos e tablets – são fornecidos, configurados e geridos exclusivamente pelo Departamento de IT comum à Fundação Mendes Gonçalves e à Casa MG, o que garante que padrões rígidos de segurança sejam aplicados a todo o *hardware* e *software* utilizado no ambiente corporativo. O uso de dispositivos pessoais para acesso à rede corporativa é estritamente proibido, seguindo a política de "No BYOD" (*No Bring Your Own Device*). Essa restrição é essencial para reduzir riscos de segurança, garantindo que todos os dispositivos que acedem aos sistemas da Fundação Mendes Gonçalves e da Casa MG sejam devidamente controlados e protegidos contra ameaças cibernéticas, malware e acessos não autorizados.

5.4. Controlo de Acesso Físico

O acesso a áreas críticas é restrito e controlado por autenticação biométrica e cartões MIFERE - tecnologia de cartões inteligentes baseada em *Radio Frequency Identification*, garantindo que apenas Colaboradores autorizados possam entrar em locais sensíveis ou de acesso restrito. Toda a infraestrutura física é ainda monitorizada por câmaras de CCTV 24/7, e equipas de segurança realizam rondas de vigilância para prevenir acessos indevidos.

[3] Um IDS monitora redes e sistemas em busca de atividades suspeitas ou maliciosas. Ele alerta os administradores de segurança, mas não interfere diretamente no tráfego da rede.

[4] Um IPS vai além do IDS, bloqueando automaticamente atividades suspeitas ou maliciosas assim que são detetadas. Ele pode impedir a propagação de ataques antes que causem danos.

5.5. Controlo de atualizações de Sistema

A Fundação Mendes Gonçalves e a Casa MG implementaram um programa que permite controlar que atualizações são instaladas em cada computador, garantindo que todos os sistemas estejam atualizados e protegidos contra vulnerabilidades de segurança.

5.6. Gestão de Dados e Informação Sensíveis

A Fundação Mendes Gonçalves e a Casa MG armazenam de forma segura e protegida os dados sensíveis a que tem acesso, incluindo informações financeiras e estratégicas. A retenção destes dados segue diretrizes rigorosas, garantindo que as informações sejam armazenadas apenas pelo tempo necessário e eliminadas de forma definitiva após esse período de acordo com toda a legislação em vigor.

6. DETETAR

A **deteção** da ocorrência de eventos de cibersegurança depende da monitorização contínua das redes e sistemas de informação e da implementação de processos de deteção. Para concretizar este objetivo, a Fundação Mendes Gonçalves e a Casa MG comprometem-se a:

- ✓ **monitorizar anomalias e eventos de Cibersegurança**, em tempo útil, e **compreender o impacto** potencial desses eventos;
- ✓ **monitorizar continuamente as redes e sistemas de informação** para identificar eventos de Cibersegurança e verificar a eficácia das medidas de proteção aplicadas;
- ✓ **implementar e manter processos de deteção de eventos anómalos**;
- ✓ **avaliar a eficácia dos controlos** implementados na Fundação Mendes Gonçalves e na Casa MG **para mitigação dos riscos identificados**;
- ✓ **identificar e mitigar as vulnerabilidades e oportunidades de melhoria na infraestrutura** da Fundação Mendes Gonçalves e da Casa MG.

6.1. Scans periódicos e auditoria

A deteção e mitigação de vulnerabilidades nos sistemas da Fundação Mendes Gonçalves e da Casa MG são executadas através da realização de ***scans* periódicos aos seus sistemas e redes** e uma **monitorização contínua** das suas redes e sistemas de informação.

A Fundação Mendes Gonçalves e a Casa MG realizam auditorias regulares nos seus sistemas, processos e infraestruturas tecnológicas para garantir que todas as diretrizes de segurança sejam cumpridas de forma eficaz. Essas auditorias têm como objetivo assegurar a conformidade com as políticas internas de cibersegurança, identificar oportunidades de melhoria contínua, detetar e corrigir vulnerabilidades antes que possam ser exploradas por ameaças cibernéticas e avaliar a eficácia das medidas de proteção de dados.

6.2. Mecanismos de proteção

A deteção resulta igualmente dos mecanismos adotados a propósito do objetivo *Proteger* e que permitem a deteção atempada da ocorrência de eventos de cibersegurança.

6.3. Formação e estabelecimento de canais de reporte

Para o efeito de potenciar a capacidade de deteção de incidentes, todos os Colaboradores da Fundação Mendes Gonçalves e da Casa MG recebem formação com vista a poderem identificar tentativas de *phishing* e ataques de engenharia social, e para reportarem qualquer e-mail suspeito à empresa Mendes Gonçalves – Sistemas e Tecnologias de Informação, Lda., de forma imediata.

7. RESPONDER

A Fundação Mendes Gonçalves e a Casa MG reconhecem que a resposta atempada a incidentes de segurança é primordial no sentido de mitigar o impacto dos incidentes de segurança e assegurar a conformidade com requisitos legais ou regulatórios.

O objetivo de segurança ***Responder*** corresponde ao compromisso de desenvolver e implementar práticas nesse sentido e, para tanto, a Fundação Mendes Gonçalves e a Casa MG comprometem-se a:

- ✓ **planear a resposta aos incidentes detetados**;
- ✓ **garantir que os incidentes de segurança da informação são reportados** em conformidade com a legislação em vigor e com os procedimentos internos definidos para o efeito;
- ✓ **garantir que a análise dos incidentes permite uma resposta efetiva** e o apoio às atividades de recuperação;
- ✓ **realizar os melhores esforços para conter, mitigar e/ou resolver o incidente ocorrido**;
- ✓ **reduzir os danos na atividade inerentes à ocorrência de incidentes de segurança da informação**, bem como minimizar o seu impacto para as partes interessadas da Fundação Mendes Gonçalves e da Casa MG (internas e externas);
- ✓ **acumular experiência e promover a melhoria contínua dos processos de resposta** a incidentes de cibersegurança.

O **CISO** estará dedicado ao acompanhamento destes temas, fortalecendo o seu compromisso com a proteção da segurança da informação. O processo de resposta é assegurado por prestador de serviços externo que oferece à Fundação Mendes Gonçalves e à Casa MG um plano robusto de resposta.

8. RECUPERAR

O objetivo ***Recuperar*** é marcado pelo compromisso de desenvolver e implementar práticas para restaurar qualquer capacidade e/ou serviço da Fundação Mendes Gonçalves e da Casa MG que tenha sido comprometido na sequência de um evento de cibersegurança e com vista a reduzir os impactos do incidente ocorrido. Assim, para atingir o objetivo de segurança, a Fundação Mendes Gonçalves e a Casa MG comprometem-se a:

- ✓ **assegurar que tem a capacidade de prosseguir a prestação dos seus serviços**, nomeadamente das suas funções de atividade críticas, caso ocorram incidentes de segurança da informação graves ou ciberataques, nas condições definidas na regulamentação, normas e procedimentos específicos aplicáveis;
- ✓ **assegurar a redundância de equipamentos, infraestruturas e sistemas de informação** que suportam as funções de atividade e de negócio críticas, evitando assim pontos únicos de falha;
- ✓ **minimizar os impactos negativos** que possam advir da ocorrência de incidentes de segurança graves, tanto para a reputação das organizações como para todas as suas partes interessadas.

A Fundação Mendes Gonçalves e a Casa MG desenvolveram neste contexto uma **política de *backups*** e uma estratégia robustas, que asseguram a proteção contínua das informações essenciais, garantindo que ambas possam recuperar dados rapidamente e manter as suas operações ininterruptas, mesmo diante de cenários adversos. Estas passam por:

- ✓ Adicionar aos *backups* as configurações dos sistemas críticos;
- ✓ Automatizar os sistemas de *backup* e recuperação, garantindo eficiência e consistência do seu funcionamento;
- ✓ Separar o armazenamento dos *backups* da rede corporativa, protegendo-os de ameaças à rede interna;
- ✓ Duplicar os *backups* críticos para uma localização distinta;
- ✓ Realizar *backups* diários para garantir a recuperação rápida e segura de dados críticos, assegurando a continuidade operacional em caso de falha de sistema, ataque cibernético ou erro humano;
- ✓ Armazenar os *backups* por 14 dias e replicar os mesmos em locais seguros para aumentar a resiliência, garantindo redundância e proteção contra perda de informações;
- ✓ Criptografar todos os *backups* para impedir acessos não autorizados e seguir rigorosos protocolos de segurança, garantindo que os dados sejam recuperáveis sem comprometer a integridade das informações;

- ✓ Realizar testes regulares de restauração, verificando a eficácia das cópias armazenadas e garantindo que possam ser recuperadas com rapidez e precisão sempre que necessário.

A Fundação Mendes Gonçalves e a Casa MG implementaram ainda um **Plano de Recuperação de Desastres** que consideram essencial para manter a resiliência e a continuidade das suas operações. O plano tem como objetivos (i) minimizar o tempo de inatividade e reduzir o impacto operacional em caso de falha grave, (ii) assegurar a integridade e a recuperação dos dados, garantindo que informações essenciais não sejam perdidas, (iii) proteger a continuidade dos serviços críticos, permitindo que as organizações voltem a operar rapidamente e (iv) evitar prejuízos financeiros e danos à reputação causados por falhas prolongadas.

9. COMUNICAÇÃO E SENSIBILIZAÇÃO

A Fundação Mendes Gonçalves e a Casa MG disponibilizam a presente Política ao seus Colaboradores, fornecedores e parceiros e desenvolvem internamente formações e ações de sensibilização aos seus Colaboradores, por forma a potenciar uma cultura de cumprimento e de resiliência, garantindo a compreensão e cumprimento das boas práticas de segurança implementadas pela Fundação Mendes Gonçalves e pela Casa MG.

10. APROVAÇÃO, MONITORIZAÇÃO E REVISÃO DA POLÍTICA

O Conselho de Administração da Fundação Mendes Gonçalves e da Casa MG é responsável pela definição e aprovação da Política, bem como pela revisão da mesma. A revisão da Política é feita a cada dois anos, com o apoio do Departamento de IT, considerando a sua adequação às exigências legais e regulamentares, à eficácia das medidas implementadas e a ocorrência de alterações organizativas que justifiquem a sua revisão.

A Fundação Mendes Gonçalves e a Casa MG realizam auditorias regulares aos seus sistemas, processos e infraestruturas tecnológicas para garantir que todas as diretrizes de segurança sejam cumpridas de forma eficaz e que os objetivos de segurança estão a ser atingidos. As auditorias têm como objetivo assegurar a conformidade com as políticas internas de cibersegurança, identificar oportunidades de melhoria, detetar e corrigir vulnerabilidades antes que possam ser exploradas por ameaças cibernéticas e avaliar a eficácia das medidas de proteção de dados.

As auditorias serão conduzidas internamente, pela Mendes Gonçalves - Sistemas e Tecnologias de Informação, Lda., ou por empresas especializadas externas, garantindo uma avaliação imparcial sobre riscos e oportunidades de aprimoramento.

Além disso, a Fundação Mendes Gonçalves e a Casa MG adotam sistemas de monitorização contínua, analisando tentativas de acesso não autorizado, padrões anômalos de tráfego e possíveis violações de dados. A partir dessas análises, são gerados relatórios de conformidade, permitindo que a Fundação Mendes Gonçalves e a Casa MG estejam sempre alinhada às melhores práticas e regulamentações de segurança.

Os Colaboradores devem reportar qualquer incidente ou vulnerabilidade que identifiquem ao Departamento de IT, enviando um e-mail para: ciberseguranca@casamg.pt.

HISTÓRICO DE REVISÕES DO DOCUMENTO

N.º da Versão	Data	Resumo das Alterações
01	23/04/2025	Primeira versão.