POLÍTICA DE SEGURANÇA CIBERNETICA

MONTREAL

O FUTURO PRESENTE

SUMÁRIO

1. Objetivo

A Política de Segurança Cibernética tem por objetivo estabelecer diretrizes, controles e responsabilidades que permitam garantir a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados pela M.I. MONTREAL IINFORMÁTICA S/A e empresas do Grupo, bem como orientar a implementação de procedimentos e controles para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

Esta política está estruturada com base nas funções Identify, Protect, Detect, Respond e Recover do NIST CSF, complementadas pelos controles da ISO/IEC 27001/27002, CIS Controls e princípios de governança do COBIT.

2. Aplicabilidade

A Política de Segurança Cibernética é de caráter corporativo, aplicando-se a M.I. MONTREAL INFORMÁTICA S/A e empresas do Grupo. Cada regional deve observar integralmente as diretrizes aqui estabelecidas e, quando necessário, complementá-las com procedimentos locais específicos, respeitando suas particularidades operacionais, legais e tecnológicas, desde que não conflitem com as diretrizes corporativas.

Quaisquer alterações, adaptações ou complementações propostas pelas regionais deverão ser submetidas previamente ao Comitê de Segurança da Informação para análise, validação e aprovação formal, antes de sua implementação.

A Política se aplica a todos os ativos de informação da Montreal, incluindo dados, sistemas, aplicativos, dispositivos e redes. Seu escopo abrange todos os colaboradores, funcionários, contratados, parceiros e terceiros que acessam, utilizam ou processam informações da organização.

Esta política se aplica em todas as instalações físicas administradas ou utilizadas pela Montreal.

3. Termos e Definições

- **NIST Cybersecurity Framework (CSF)** é um conjunto de diretrizes, padrões e melhores práticas desenvolvido pelo National Institute of Standards and Technology (NIST) dos EUA, projetado para ajudar organizações de qualquer tamanho a identificar, proteger, detectar, responder e recuperar-se de riscos cibernéticos.
- **Identify (Identificar):** Desenvolve o entendimento organizacional para gerenciar riscos de segurança cibernética em sistemas, pessoas, ativos, dados e recursos. Define o contexto de negócio e prioridades.
- **Protect (Proteger):** Desenvolve e implementa salvaguardas apropriadas para garantir a entrega de serviços críticos. Foca na prevenção, controle de acesso, treinamento e proteção de dados.

- **Detect (Detectar):** Desenvolve e implementa atividades apropriadas para identificar a ocorrência de um evento de segurança cibernética, garantindo a detecção oportuna.
- **Respond (Responder):** Desenvolve e implementa ações para agir quando um incidente de segurança cibernética é detectado, visando conter o impacto.
- **Recover (Recuperar):** Desenvolve e implementa planos para a resiliência e para restaurar quaisquer capacidades ou serviços que foram prejudicados devido a um incidente de segurança cibernética.
- **COBIT (Control Objectives for Information and Related Technologies):** ramework de referência internacional, criado pela ISACA, focado na governança e gestão de TI empresarial.
- **Due diligence (ou diligência prévia):** Processo minucioso de investigação, análise e auditoria de uma empresa.
- **Autenticação Multifator (MFA):** Mecanismo de segurança que exige duas ou mais formas de verificação para acessar uma conta ou sistema, combinando senhas com fatores adicionais.
- **Threat Intelligence (ou Inteligência de Ameaças Cibernéticas):** É o conhecimento baseado em evidências—incluindo contexto, mecanismos, indicadores e conselhos práticos—sobre ameaças existentes ou emergentes à segurança de uma organização

4. Papeis e Responsabilidades

- **Colaborador:** seja no regime CLT, Prestador de Serviço ou temporário, ao assinar o contrato declara estar ciente e comprometido com a política de segurança cibernética da Montreal, e deverá cumprir a Política e demais normas específicas de segurança da informação, e torna-se inteiramente responsável por todo prejuízo ou dano que vier sofrer ou causar à Montreal e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.
- **Equipe de Cibersegurança:** Compete à equipe de Cibersegurança atuar de forma consultiva e técnica na sustentação do programa de segurança da informação, sendo responsável por definir diretrizes técnicas, padrões e controles de segurança, bem como assegurar sua efetividade ao longo de todo o ciclo de proteção: prevenção, detecção, resposta e recuperação de incidentes, em alinhamento com as políticas estabelecidas pela área de Governança de Segurança da Informação.
  A equipe de Cibersegurança deverá realizar reporte periódico ao Comitê Técnico de Segurança da Informação, assegurando visibilidade sobre o nível de risco, a efetividade dos controles e a evolução dos planos de ação, apoiando a tomada de decisão estratégica.
- **Equipe de Governança e Segurança da Informação:** A governança de segurança cibernética deverá estar alinhada aos objetivos estratégicos da Montreal, com reporte periódico ao Comitê de Segurança da Informação, acompanhamento de indicadores, exposição a riscos, planos de ação e decisões baseadas em criticidade e impacto ao negócio, é responsável pela criação, administração e supervisão de políticas e normas, garantindo que os riscos sejam identificados e gerenciados dentro dos níveis de tolerância definidos pela organização.

- **Comitê de Segurança da Informação (CSI):** O Comitê de Segurança da Informação, se compromete com uma abordagem integrada e alinhada às necessidades específicas de cada localidade.
  É responsabilidade do comitê aprovar e manter a Política de Segurança Cibernética atualizada. Assim como, avaliar e aprovar os planos de ação e resposta a incidentes, promover a melhoria contínua dos procedimentos relacionados com a segurança da informação, e comunicar a diretoria sobre a ocorrência de incidentes relevantes e das interrupções dos serviços relevantes que configurem uma situação de crise pela organização, bem como as providências para o reinício das atividades.

5. Diretrizes

- Esta Política de Segurança Cibernética foi elaborada em alinhamento com a Política de Segurança da Informação e Privacidade, assegurando consistência, integração e complementaridade entre os controles adotados pela organização.
- A proteção das informações deve ser orientada pelos princípios da Confidencialidade, Integridade e Disponibilidade, garantindo que os dados sejam acessados apenas por usuários autorizados, permaneçam íntegros e estejam disponíveis sempre que necessário ao negócio.
- As informações devem ser classificadas e tratadas de acordo com seu grau de criticidade e sensibilidade, considerando requisitos legais, regulatórios e de negócio ao longo de todo o seu ciclo de vida (criação, armazenamento, uso, compartilhamento e descarte).
- Deve ser assegurada a proteção das informações contra acessos, modificações, destruições ou divulgações não autorizadas, por meio da implementação de controles técnicos e administrativos adequados ao nível de risco.
- O acesso às informações deve ser concedido com base no princípio do menor privilégio e da necessidade de negócio, garantindo que sejam utilizadas exclusivamente para as finalidades para as quais foram coletadas.
- Terceiros que tratem, armazenem ou processem informações da MONTREAL devem ser submetidos a processos formais de avaliação de segurança, incluindo due diligence, definição de cláusulas contratuais específicas, monitoramento contínuo e requisitos obrigatórios de notificação e tratamento de incidentes de segurança.
- A gestão de riscos de segurança da informação deve ser realizada de forma contínua, contemplando a identificação, análise, avaliação e tratamento dos riscos, com base em metodologias reconhecidas de mercado.
- O não cumprimento das diretrizes estabelecidas nesta política estará sujeito às medidas administrativas e disciplinares cabíveis, conforme normas internas da organização.

6. Classificação dos dados das Informações

A informação será classificada de acordo com sua sensibilidade, impacto e necessidade de restrição de acesso, utilizando as seguintes categorias:

- **Pública:** Informações que podem ser livremente divulgadas ao público externo, sem causar qualquer prejuízo à empresa.

- **Interna:** Informações de uso exclusivo dos colaboradores e parceiros autorizados. Embora não críticas, sua divulgação externa não autorizada pode gerar impactos operacionais ou reputacionais.
- **Restrita:** Informações cujo acesso deve ser limitado a grupos específicos dentro da empresa. Sua exposição pode causar impactos significativos aos negócios.
- **Confidencial:** Informações altamente sensíveis, cujo acesso deve ser rigorosamente controlado. O vazamento pode gerar graves consequências legais, financeiras ou estratégicas.

7. Controles de acesso

O sistema dispõe de mecanismos de log, e fornece rastreabilidade dos acessos. As telas de sistema são segregadas de acordo com as funções estabelecidas aos usuários.

8. Autenticação

É utilizado o recurso da autenticação multifator (MFA), tendo como principal objetivo o gerenciamento de identidades digitais para os colaboradores, sistemas e processos, bem como na verificação de identidades que acessos os recursos da organização.

9. Criptografia

Os controles relacionados à criptografia são abrangidos pela Política de Privacidade e Proteção de Dados Pessoais, cujo objetivo é estabelecer requisitos de controle para proteger os dados em todos os ativos de informação da Montreal.

A Montreal deve manter inventário atualizado de ativos de hardware, software, serviços, contas privilegiadas e ativos críticos, bem como padrões seguros de configuração e processo formal de gestão de mudanças.

10. Prevenção e Detecção de Intrusão

Controles de mitigação são implementados nos perímetros da rede para limitar e conter o impacto de potenciais eventos de segurança cibernética.

O escopo inclui os perímetros da infraestrutura de rede em que são estabelecidas as conexões.

11. Realização periódica de testes e varreduras para detecção de vulnerabilidades

O objetivo é implementar, manter e atualizar frequentemente os requisitos de controle de detecção e prevenção para impedir que códigos maliciosos sejam executados e se infiltrem na rede da Empresa.

O código malicioso pode ser transportado por diferentes meios, incluindo, por exemplo, acessos à Internet, correio eletrônico, anexos de correio eletrônico e dispositivos de armazenamento portáteis. Os mecanismos de proteção contra códigos maliciosos incluem, por exemplo, o monitoramento de atividades de endpoints e controles de proteção de hardware.

12. Estabelecimento de mecanismos de rastreabilidade

A Montreal captura eventos relevantes para a identificação de possíveis incidentes de segurança cibernética (aqueles resultantes de atividades de intenção maliciosa). Os eventos são capturados e analisados pelo Centro de Operações de Segurança (SOC – Security Operations Center) e utiliza serviços/ferramentas de SEIM (Security Event and Incident Management) para monitorar e analisar os dados/alertas.

13. Controles de acesso e segmentação da rede

O programa de Gerenciamento de Identidade e Acesso implementa padrões e controles de acesso em toda a infraestrutura e aplicativos, especialmente aqueles que contêm informações de clientes. Esses controles são projetados para autenticar usuários, permitir acesso autorizado, garantir procedimentos consistentes, manter a segregação de funções e garantir atualizações tempestivas por meio de processos de inclusão/exclusão/transferência nos sistemas da Empresa.

14. Manutenção de cópias de segurança dos dados e das informações

O backup operacional abrange proteção de dados em nível de arquivo, retenção de dados e recuperação de arquivos para atender aos requisitos de recuperação operacional e inclui backup de dados, restauração e validação de backup.

A Montreal deve manter e testar periodicamente planos de continuidade de negócios e recuperação de desastres, responsabilidades e cenários de incidentes cibernéticos

15. Gerenciamento de Incidentes

Os recursos de gerenciamento de eventos e incidentes de segurança possibilitam o monitoramento, a detecção e a investigação de eventos e incidentes relacionados à segurança. Esses recursos se apoiam nos serviços de inteligência (threat intelligence), nas medidas de risco operacional e no contexto dos negócios para melhorar continuamente a detecção antecipada de ameaças e coordenar respostas integradas aos eventos relacionados à segurança.

A Montreal manterá processo formal de gestão de incidentes, com classificação, registro, escalonamento, tratamento, comunicação, análise de causa raiz, lições aprendidas e testes periódicos.

16. Referências

- NIST Cybersecurity Framework
- ISO/IEC 27001 e 27002
- CIS Controls
- COBIT (em menor grau, governança)

17. Disposições Finais

Esta política entra em vigor a partir da data de sua publicação e pode ser revisada e alterada a qualquer momento, sempre que necessário, visando garantir sua efetividade diante das mudanças tecnológicas, organizacionais e legais. Deve, obrigatoriamente, ser revisada a cada dois anos para assegurar sua atualização contínua.

Esta política se aplica a todas as empresas Montreal.
São elas PC Service Tecnologia, Mcare e Montreal Ventures.

Acesse nossos canais e saiba mais sobre este e outros temas.