EDMOND

Um novo ciclo para ir além

Política de Segurança da Informação e Cibernética

SUMÁRIO

Objetivo

Objetivo Edmond

Este documento tem por finalidade, formalizar as diretrizes da Política da Segurança Cibernética (“Política”) da EDMOND SOLUÇÕES E TECNOLOGIA S.A. (“Edmond”), visando a proteção dos ativos de informação de modo seguro e transparente, através da prevenção, detecção e redução dos riscos associados, de forma alinhada ao negócio, complexidade e porte da, assim como aos requisitos legais e exigências dos órgãos regulatórios de acordo com o negócio.

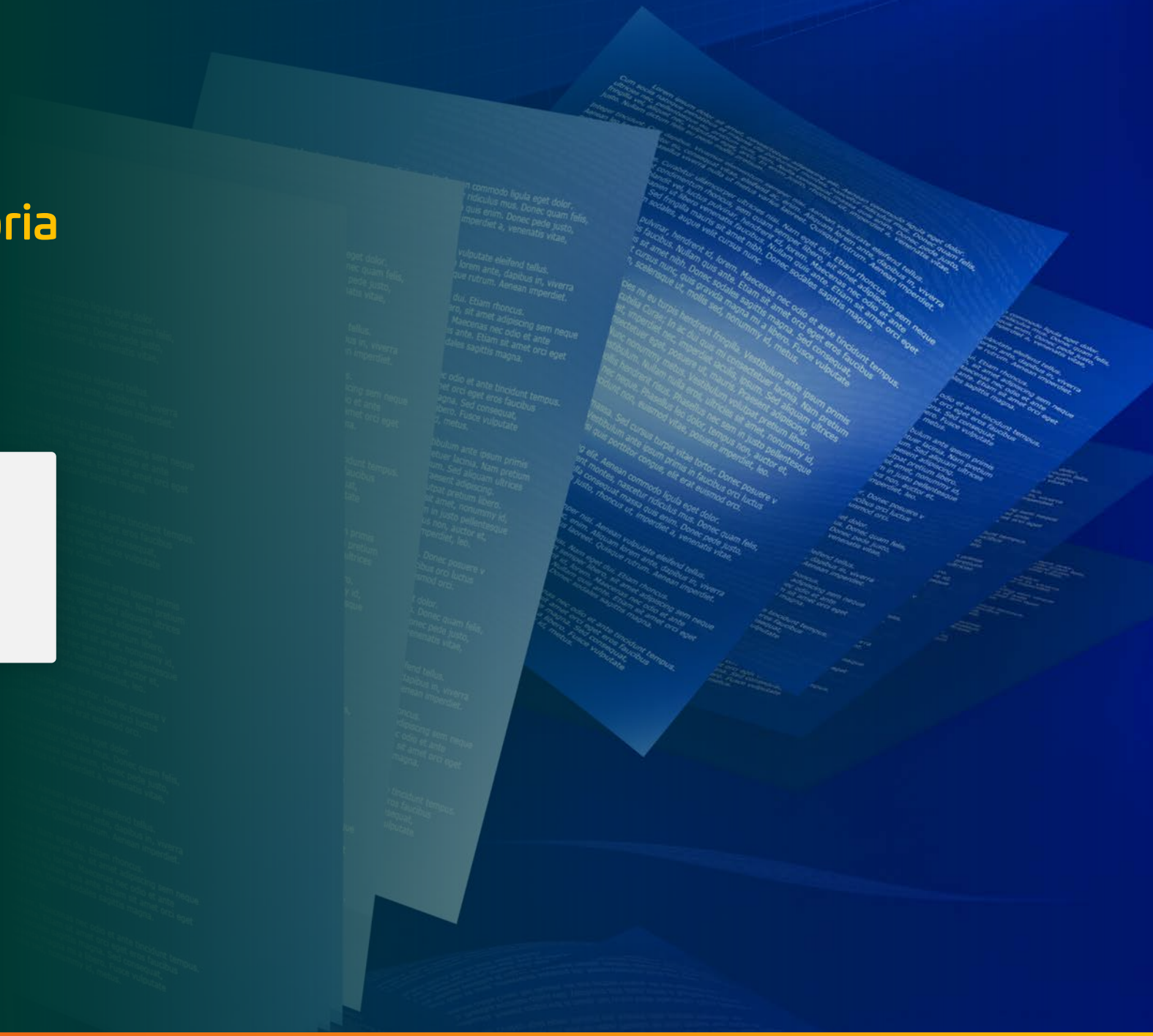
EDMOND

01. Base Legal e Regulatória

1 Base Legal e Regulatória

Esta Política cumpre fielmente a legislação concernente e as disposições do Banco Central do Brasil (“BCB”) e Conselho Monetário Nacional (“CMN”), em especial:

Resolução BCB nº 85, de 8 de abril de 2021 que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições de pagamento autorizadas a funcionar pelo Banco Central do Brasil.



EDMOND

02. Destinatários

2 Destinatários

Esta Política se aplica a todos os sócios, diretores, gestores, administradores, colaboradores, prestadores de serviços, prepostos, terceirizados e quaisquer demais pessoas físicas ou jurídicas contratadas ou outras entidades que participem, de forma direta ou indireta, das atividades diárias e negócios da Edmond ("Destinatários").

Os Destinatários devem atender a todas às diretrizes e procedimentos estabelecidos nesta Política, desde o momento de início do relacionamento, em que tomem ciência do mesmo, e, naquilo o que se prolongar no tempo, pelo prazo de 10 (dez) anos contados do término do vínculo do Destinatário com a Edmond.

EDMOND

03. Definições

3 Definições

Para os fins desta Política, consideram-se:

Confidencialidade: somente o usuário da informação, que esteja devidamente autorizado pelo gestor da informação, deve ter acesso às Informações respeitando os critérios de segregação de funções;

Adequação: garantir que informações não sejam alteradas desde a sua criação até seu uso. Eventuais alterações, supressões e/ou adições devem ser autorizadas pelo gestor da informação;

Disponibilidade: garantir que as informações estejam sempre disponíveis para o usuário da informação;

Autenticidade: garantir a identidade de quem está enviando a Informação, ou seja, gera o não-repúdio que se dá quando há garantia de que o emissor não pode se esquivar da autoria da mensagem (irretratabilidade);

Riscos Cibernéticos: riscos de ataques cibernéticos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets), fraudes externas, desprotegendo dados, redes e sistemas da empresa causando danos financeiros e de reputação consideráveis.

Negação de serviço: um ataque de negação de serviço (também conhecido como DoS Attack, um acrônimo em inglês para Denial of Service), é uma tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores. Alvos típicos são servidores web, e o ataque procura tornar as páginas hospedadas indisponíveis na rede. Não se trata de uma invasão do sistema, mas sim da sua invalidação por sobrecarga.

Fraudes Externas e invasões: realização de operações por fraudadores, utilizando-se de ataques em contas de pagamento, com o uso de conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Passphrase: é um tipo de senha que, ao invés de ser baseado em uma palavra, utiliza frases inteiras para aumentar a complexidade e segurança da senha, ao mesmo tempo que facilita o seu processo de memorização.

Restore: ato de restaurar os dados de uma cópia de segurança (Backup).

Short Message Service (“SMS”): serviço de telefones celulares digitais para envio de mensagens curtas.

Simple Network Management Protocol (“SNMP”): tipo de protocolo de gerenciamento e monitoramento de dispositivos de redes.

SPAM: termo utilizado para caracterizar mensagens indesejadas que são, normalmente, enviadas de forma automatizada para vários usuários diferentes.

Token: dispositivo que pode ser eletrônico (físico) ou virtual (aplicativo) que gera senhas de utilização única para serem utilizados em conjunto com as senhas pessoais de cada usuário.

Usuário da Rede: qualquer indivíduo ou instituição que tenha acesso autenticado aos recursos da rede corporativa da Edmond.

Usuário de Sistema: qualquer indivíduo ou instituição que tenha acesso autenticado aos sistemas disponibilizados pela Edmond.

Virtual Private Network (“VPN”): é uma rede de comunicações privada construída sobre uma rede de comunicações pública (por exemplo, a Internet).

WiFi / Wireless: redes de comunicação de dados que não necessitam de cabos.

EDMOND

04. Diretrizes

4 Diretrizes

O cumprimento da Política é de responsabilidade de todos os Destinatários, os quais devem seguir as diretrizes abaixo:

- Proteger as informações contra acesso, modificações, destruição ou divulgação não autorizada;
- Prover a adequada classificação da informação, considerando os critérios de confidencialidade, integridade e disponibilidade;
- Assegurar que os recursos utilizados para o desempenho da sua função sejam utilizados apenas para as finalidades desempenhadas a sua atividade;
- Garantir que os sistemas e as informações que estão sob a sua responsabilidade sejam adequadamente protegidos;
- Atender às leis e resoluções que regulamentam as atividades da Edmond e seu mercado de atuação;
- Selecionar os mecanismos de segurança da informação, balanceando fatores de riscos, tecnologia e custo;
- Garantir a continuidade do processamento das informações críticas de negócios;
- Comunicar imediatamente aos responsáveis quaisquer descumprimentos desta Política.

Visando o fortalecimento da cultura de Segurança da Informação e Cibernética através da disseminação dos princípios e diretrizes descritos nesta Política, a Edmond possui o documento "Treinamento e Conscientização em Segurança da Informação e Cibernética", que consiste no processo de capacitação e conscientização, de todos os níveis, ao que se refere à segurança da informação, contemplando segurança de dados, segurança cibernética, inclusive com relação aos terceiros e demais contrapartes.

A Edmond conta com ferramentas, mecanismos e controles adequados para garantir a efetividade do objetivo, diretrizes, princípios, regras, papéis, responsabilidades e demais conteúdos abordados nesta Política, dentre eles: processo, métricas, indicadores, trilhas de auditorias e testes. Esta Política e o seu conteúdo são parte integrante do plano de auditoria interna e, eventuais deficiências identificadas são tempestivamente tratadas.

Toda documentação que suporta e comprova o correto funcionamento do conteúdo aqui estabelecidos permanecerão a disposição da autoridade reguladora pelo prazo mínimo de 05 (cinco) anos.

A Edmond divulga a Política a todos os seus colaboradores, compartilhado via drive e no site, para dar acesso a consulta imediata quando necessário.

Na mesma linha, a Edmond divulga em seu website, resumo da Política de Segurança Cibernética, para acesso público.

EDMOND

05. Princípios e Regras

5 Princípios e Regras

A estratégia de Segurança da Informação da Edmond é baseada em arquitetura com os seguintes domínios:

- *Governança de Segurança da Informação;*
- *Segurança Cibernética Ofensiva;*
- *Segurança Cibernética Defensiva e Treinamento; e,*
- *Conscientização e Cultura.*

Todos os princípios adotados pela Edmond visam atingir as diretrizes e objetivos desta Política, reduzindo a sua vulnerabilidade quanto aos riscos de segurança cibernética.

Os procedimentos e os controles da segurança cibernética são implementados de modo a abranger a autenticação, criptografia, prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes de invasão e de outras metodologias de operações ofensivas para detecção e correção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores, a manutenção de cópias de segurança dos dados e das informações, e a prevenção e resposta de incidentes de segurança da informação.

ACESSO, CLASSIFICAÇÃO, MANUSEIO E ROTULAGEM DA INFORMAÇÃO:

Os acessos à informação são controlados, monitorados e restritos de forma a garantir sua utilização apenas para a realização das atividades inerentes a cada um dos Destinatários, sendo revisados periodicamente.

As concessões, revogações, transferências e revisões de acesso devem respeitar os fluxos de aprovação e execução determinados pela Edmond, bem como se utilizar das ferramentas oficiais disponibilizadas para estes processos, conforme definido em documento interno denominado *"Manual de Gestão de Identidade, Controle de Acesso e Segurança Física"*. Todos os acessos são rastreáveis, possibilitando auditoria e responsabilidade individual de um usuário.

O documento acima mencionado também compreende os procedimentos necessários para proteger equipamentos e informações contra Destinatários que não possuem autorização para acessá-los. Para a execução deste processo, são solicitadas autorizações aos gestores responsáveis e conferidos os titulares, quando aplicável, inclusive para a concessão de acesso às dependências da Edmond, segregando áreas com acesso restrito, por força de norma regulatória.

DADOS PESSOAIS

A Edmond possui a "*Aviso de Privacidade*" que define os procedimentos e controles relativos à coleta, processamento, proteção e compartilhamento de informações pessoais, respeitando os direitos de privacidade, à intimidade, honra, e outros direitos reservados ao titular dos dados, seguindo as leis e regulamentações de proteção de dados aplicáveis.

CONTROLES DE ACESSO

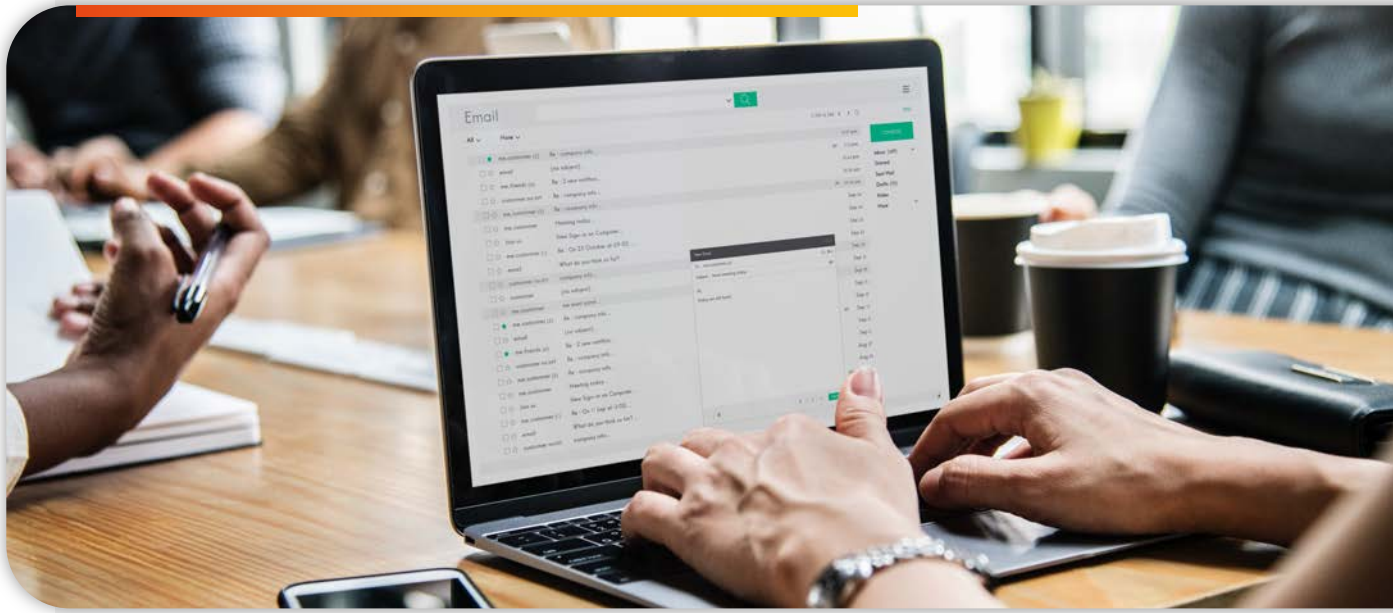
Os Destinatários deverão adotar medidas de prevenção para garantir o acesso seguro a ativos e serviços de informação, incluindo:

- Os acessos lógicos, locais ou remotos, à Rede Corporativa da Edmond deverão ser realizados somente para os interesses específicos dos negócios da empresa;
- O acesso à Rede Corporativa deverá ser realizado através de diferentes perfis de acesso, específicos para cada Destinatário, sendo o responsável pelo setor por definir as atribuições e atualizações dos perfis em questão;
- Cada perfil terá suas atribuições que concederão acesso aos diferentes recursos tecnológicos da rede corporativa, conforme definição e orientação do responsável pelo setor;
- As redes e recursos destinados aos visitantes da empresa deverão ser utilizados somente pelo seu público alvo;
- As técnicas de autenticação e autorização para validar a identidade dos usuários na rede são: nome de usuário e senha pessoal. Em alguns casos, pode ser solicitado um segundo fator de autenticação, que poderá ser enviado ao usuário via SMS ou token, que deverá ser apresentado no momento da autenticação em conjunto com a Senha Pessoal;
- Os acessos realizados a sistemas que exijam técnicas de autenticação e autorização deverão ser sempre encerrados quando finalizados ou bloqueados temporariamente durante interrupções no serviço ou em ausências dos profissionais responsáveis;
- O acesso à rede corporativa e os seus recursos, seja de forma cabeada ou via wireless, deverá ser evitada fora dos horários comerciais, salvo em momentos onde seja de interesse dos negócios da Edmond.

ACESSO À INTERNET E UTILIZAÇÃO DE E-MAIL CORPORATIVO

A Edmond fornece o serviço de e-mail para o desempenho das atividades profissionais relacionadas à Empresa. Quando o usuário fizer uso do serviço de e-mail da Edmond, o mesmo deverá seguir o abaixo:

- *A vigência do acesso à conta de e-mail corporativo deve ser vinculada ao período estipulado no contrato firmado entre o usuário e a Edmond;*
- *O acesso à internet e a conta de e-mail corporativo disponibilizado aos usuários da rede (WiFi e cabeada) da Edmond são de uso pessoal e intransferíveis, sendo o seu titular o único e total responsável pelas ações e possíveis danos causados à Instituição ou a terceiros por meio de seu uso;*
- *A utilização da internet e do e-mail corporativo é uma concessão da Edmond, não um direito do usuário da rede e será obrigatoriamente cancelada quando do desligamento ou ao final da vigência do contrato firmado com o profissional;*
- *É vetada a utilização dos serviços concedidos pela Edmond para acessar, receber, armazenar ou enviar mensagens com códigos maliciosos, materiais pornográficos, ofensas, ações criminosas ou ilegais, que façam apologia ou incitação à violência, que não respeitem os direitos autorais, os objetivos comerciais particulares ou que contribuam com a continuidade de correntes de mensagens eletrônicas e SPAM;*
- *O acesso à internet e ao e-mail corporativo poderá ser monitorado e restringido pela Edmond;*
- *Todos os usuários deverão se submeter aos controles implementados nas redes corporativas, de forma que a utilização de sistemas que forneçam formas de evasão destes controles seja considerada uma infração grave desta Política;*
- *A utilização de soluções de VPN deverá ser previamente solicitada e justificada por escrito ao CSI;*
- *Nos casos de suspeita de infração das Diretrizes Gerais da Política de Segurança das Informações em vigor, a Edmond poderá acessar a caixa postal corporativa do usuário da rede em questão, bem como solicitar um relatório com informações detalhadas dos sites acessados e todas as ações realizadas por ele durante a utilização dos serviços corporativos.*



GESTÃO DE ACESSO

Todo colaborador ao ingressar nas dependências da Empresa para a suas atividades é orientado sobre o seu acesso, sendo esse acesso intransferível. O acesso fora do horário de serviço deverá ser autorizado expressamente pelo responsável do setor e com a devida justificativa.

O responsável de cada setor, indicará ao profissional autorizado para fazer os acessos de senhas, login nos sistemas mais importantes e restritos e passar os acessos caso seja autorizado.

O responsável de cada setor, indicará o colaborador autorizado para fazer os acessos aos servidores e informará o método de acesso aos sites e softwares para uso diário com a devida segurança necessária.

PROTEÇÃO E UTILIZAÇÃO DE SENHAS

As senhas associadas às contas de acesso a ativos/serviços de informação ou recursos computacionais da Edmond são de uso pessoal e intransferível, sendo dever do usuário zelar por sua guarda e sigilo. A Edmond adota padrões seguros para geração de senhas de acesso a seus ativos/serviços de informação ou recursos computacionais.

PROTEÇÃO DE DADOS

- Nenhum usuário deverá manter armazenado em suas máquinas cópias de arquivos sensíveis, assim como armazenar e receber cópias de correio eletrônico. A Edmond fornece ferramentas de uso online para esse fim. É dever do usuário dar fim adequado a qualquer arquivo que receber e após isso destruir o mesmo removendo inclusive da lixeira de sua máquina. Todas as máquinas utilizadas por usuários deverão possuir instalados e ativos os sistemas de segurança designados pela organização;

- Todos os dispositivos que tiverem acesso às informações da empresa, como por exemplo notebooks, celulares ou tablets, sejam eles de propriedade da organização ou particulares, deverão ser protegidos com senhas e possuir tempos de bloqueio automático;

- Colaboradores remotos ou em viagem, ao acessar ou manipular recursos da organização, não devem fazê-lo através de redes públicas (hotéis, restaurantes, cafés, etc.), principalmente redes Wireless, exceto nos casos em que se faça o uso da VPN corporativa.

DESENVOLVIMENTO DE APLICAÇÕES E SISTEMAS

A Edmond possui princípios que garante o desenvolvimento seguro de aplicações e sistemas, cujos procedimentos seguem as boas práticas de mercado, como segregações de função, testes, homologação, e gestão de mudanças, garantindo que a segurança da informação esteja projetada e implementada no ciclo de vida do desenvolvimento dos sistemas de informação.

PROCESSAMENTO, ARMAZENAMENTO DE DADOS E COMPUTAÇÃO EM NUVEM

As contratações de serviços de terceiros para o processamento e armazenamento de dados, e de computação na nuvem seguem todos os requisitos de segurança, avaliando a relevância do serviço contratado, criticidade, e a sensibilidade dos dados e das informações a serem processadas, armazenadas e gerenciadas pelo serviço.

Todos os prestadores deste tipo de serviço que são contratados pela Edmond passam por uma rígida avaliação de sua capacidade, garantindo sua conformidade (com a legislação e regulamentação em vigor, com as certificações exigidas e com os critérios de qualidade desejados), confidencialidade, integridade, disponibilidade e capacidade de recuperação. Estes prestadores garantem o acesso da Edmond, sempre que solicitado, aos seus relatórios de auditoria e as evidências dos controles de identificação e segregação dos dados.

Ainda, a Edmond avalia o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados, se é realizada a identificação e a segregação dos dados dos usuários finais da instituição por meio de controles físicos ou lógicos; e a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos usuários finais da Edmond pelo prestador de serviço.

Os documentos relativos às análises realizadas pela Edmond para tomada de decisão relativa à contratação do prestador de serviço que atua com o processamento e armazenamento de dados e computação em nuvem resta arquivado pelo período de 10 (dez) anos, a contar do término da relação com o prestador de serviço.

Em cumprimento à Resolução CMN nº 4.893/2021, quando aplicável, toda nova contratação relevante, ou alteração contratual, de serviços de processamento e/ou armazenamento de dados na nuvem por parte da Edmond são comunicadas ao Banco Central do Brasil no prazo de até 10 (dez) dias após a contratação do serviço, contendo minimamente as seguintes informações:

- nome da empresa contratada;
- serviços contratados; e,
- indicação dos países e regiões onde os serviços poderão ser prestados e os dados poderão ser processados, armazenados e gerenciados.

Caso a operação do serviço contratado seja no exterior, a Edmond deve verificar a existência de um convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços poderão ser prestados. No caso da inexistência de um convênio, a Edmond deverá solicitar autorização para uso do serviço diretamente com o Banco Central do Brasil com no mínimo 60 (sessenta) dias de antecedência.

Antes da assinatura do contrato com o prestador de serviços, deve ser definido quais são os países e as regiões dos países que podem ser utilizadas para processamento e armazenamento das informações, certificando que todos os requisitos estão sendo cumpridos.

A Edmond mantém à disposição do Banco Central, por ao menos 5 (cinco) anos, as informações contratuais e todos os documentos relativos ao contrato de prestação de serviços.

Ainda, a Edmond define que os prestadores de serviços que atuem com armazenamento de dados devem comunicar a Edmond, imediatamente, a tomada de conhecimento de incidentes relativos aos dados armazenados, para que, em conjunto, tomem as providências cabíveis.

CÓPIAS DE SEGURANÇA (BACKUP)

A Edmond possui possui procedimentos relacionados à extração de cópias de segurança das informações, dos softwares e dos sistemas. A Edmond mantém o registro completo e exato das cópias de segurança, provendo documentação apropriada sobre os procedimentos de restauração da informação.

GESTÃO DE RISCOS E INCIDENTES DE SEGURANÇA

Os riscos de segurança da informação são identificados e acompanhados através de um processo de análise de vulnerabilidades, quantificando e qualificando as ameaças e seus respectivos impactos sobre os ativos de informação, para associação dos níveis de proteção adequados.

O processo de respostas aos incidentes de segurança da informação está definido no Plano de Resposta a Incidentes de Segurança da Informação, que estabelece diretrizes para garantir o tratamento e a resposta adequada a cada tipo de incidente de segurança da informação que possa impactar ativos/serviços de informação ou recursos computacionais da instituição.

Todas as ocorrências que possam vir a ter impacto negativo sobre a confidencialidade, integridade ou disponibilidade das informações/ativos/serviços da Edmond são caracterizadas como um incidente de segurança da informação, devendo as referidas ocorrências serem tratadas de maneira a minimizar qualquer tipo de impacto e recuperar as características de segurança da informação dos itens afetados o mais rápido possível.

Todos os incidentes, ou suspeitas de incidentes, devem ser imediatamente comunicados à equipe de segurança da informação através dos canais disponíveis. Cabe a esta equipe determinar a criticidade do incidente e, quando pertinente, comunicar às partes interessadas (alta administração, colaboradores, clientes, órgãos regulamentadores etc.).

A extensão dos danos do incidente de segurança é avaliada de maneira tempestiva para, em seguida, ser identificado o melhor curso de ação para a resolução completa do incidente e restauração dos ativos de informação afetados. Durante a avaliação são verificados planos de ações previstos. Durante o tratamento os envolvidos devem preservar, quando possível, todas as evidências, para que seja efetuada uma análise de causa raiz. Identificar o nível real de impacto, vulnerabilidades exploradas, a efetividade do tratamento aplicado e a necessidade de maiores ações para evitar a recorrência do incidente.

Quando completamente tratado, os envolvidos devem preencher o Relatório de Incidente de Segurança da Informação para controle interno, divulgação às partes interessadas e serão consolidados e farão parte do relatório anual enviado ao BCB. Tal relatório é enviado anualmente até o dia 31 de março, com data base 31 de dezembro, apresentado à alta administração, e contém, dentre outros assuntos: resumo das implementações do plano de ação, resumo dos resultados obtidos, incidentes relevantes e resultado dos testes de continuidade.

PLANO DE CONTINUIDADE DE NEGÓCIOS

A Edmond possui documento específico intitulado “Plano de Continuidade de Negócios” que visa garantir que existam planos de continuidade de negócios e recuperação de desastres que contemplem alocação de profissionais, os principais processos e ativos de tecnologia e negócio da Edmond, bem como a possibilidade de elaboração de cenários de incidentes a serem considerados em testes de continuidade dos serviços de pagamento prestados pela Edmond.

AUDITORIA E CONFORMIDADE

Um auditor auditor deverá realizar, periodicamente, inspeções independentes dos registros e atividades com objetivo de testar a adequação dos recursos de tecnologia da informação, para assegurar o cumprimento das Diretrizes Gerais da Política de Segurança das Informações e também para recomendar quaisquer mudanças nos controles, políticas e procedimentos adotados.

Com o intuito de aumentar o controle e facilitar os momentos de auditoria, todos os recursos de tecnologia da informação, quando compatíveis, deverão ser configurados para manter os registros (logs) de todos os eventos significativos para a segurança (logins, tentativas de acesso, alterações em geral, etc.).

Sempre que possível, os recursos de tecnologia da informação devem ser configurados de forma que a trilha de auditoria seja protegida contra remoção e alteração.

Os recursos de tecnologia da informação devem ser configurados de forma a verificar automaticamente a geração dos registros de auditoria e, caso não tenham suporte a esta funcionalidade, deverão ser estabelecidas rotinas de verificação manual com periodicidade mensal. Os registros de auditoria deverão ser armazenados de forma centralizada ou em suas origens pelo período mínimo de 06 (seis) meses.

EDMOND

06. Papéis e Responsabilidades

6 Papéis e Responsabilidades

HEAD RESPONSÁVEL

Todos os Destinatários e a Edmond são responsáveis por adotar e cumprir as diretrizes, deveres, controles e práticas a eles aplicáveis contidas nesta Política, zelando para que todas as normas éticas e legais sejam cumpridas por todos aqueles com quem são mantidas relações de cunho profissional, e comunicando imediatamente qualquer violação ao Responsável, para adoção das respectivas providências, de acordo com sua gravidade.

Ao Head Responsável cabe:

- *Analisar, revisar e propor a aprovação de políticas e normas relacionadas à segurança cibernética;*
- *Garantir a disponibilidade dos recursos necessários para uma efetiva gestão de segurança cibernética;*
- *Garantir que as atividades de segurança cibernética sejam executadas em conformidade com esta Política e com as demais normas de segurança da informação;*
- *Promover a divulgação de todas as políticas cujos conteúdos abordem a segurança cibernética e tomar as ações necessárias para disseminar uma cultura cibernética no ambiente da Edmond.*

DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO

Dentre as demais funções relacionadas à operação da Edmond, ao Departamento de Tecnologia da Informação cabe:

- Receber e analisar solicitações para criação de contas de acesso ou fornecimento de privilégios para colaboradores e/ou prestadores de serviços;
- Conceder, quando autorizado, o acesso aos colaboradores e/ou prestadores de serviços, conforme indicado pelos gestores da informação;
- Revogar, quando solicitado, o acesso dos colaboradores e/ou prestadores de serviço, conforme indicado pelos gestores da informação;
- Apoiar a revisão periódica da validade de credenciais de acesso dos colaboradores e/ou prestadores de serviço fornecendo informações sobre os privilégios atualmente efetivados em ativos/sistemas de informação;
- Executar procedimentos de descarte de informações ao término da vida útil dos ativos no âmbito tecnológico, utilizando as boas práticas e técnicas que tornem as informações originais irrecuperáveis;
- Preparar e manter o inventário dos equipamentos fornecidos pela Edmond aos seus colaboradores para o desempenho de suas atividades segundo as normas definidas pelo Responsável;
- Documentar e monitorar todas as contas bem como analisar atividades suspeitas reportada pelas ferramentas disponíveis;

- Implementar e manter os controles de segurança definidos pelo Responsável no âmbito tecnológico;
- Durante o desligamento de colaboradores da Edmond, revogar as contas de acesso;
- Auxiliar na disseminação da cultura de segurança cibernética;
- Conduzir a gestão e operação da segurança cibernética, tendo como base esta Política e demais resoluções editadas pelo Responsável;
- Apoiar o Responsável em suas deliberações;
- Elaborar e propor ao Responsável as normas e procedimentos de cibernética, necessários para se fazer cumprir esta Política e com as demais normas de cibernética;
- Identificar e avaliar as principais ameaças à segurança cibernética, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco;
- Tomar as ações cabíveis para se fazer cumprir os termos desta Política;
- Realizar a gestão dos incidentes de segurança cibernética, garantindo tratamento adequado.

DESTINATÁRIOS

- Ler, compreender e cumprir integralmente os termos desta Política, bem como as demais normas e procedimentos de segurança aplicáveis;
- Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre esta Política, suas normas e procedimentos ao Departamento de Tecnologia da Informação ou, quando pertinente, ao Responsável;
- Comunicar ao Responsável qualquer evento que viole esta Política ou coloque/possa vir a colocar em risco a segurança das informações ou dos recursos computacionais da Edmond.

EDMOND

07. Efetividade e Violação

7 Efetividade e Violação

Além de contar com mecanismos de controles que buscam garantir e assegurar a correta implementação das diretrizes, princípios e regras formalizados nesta Política, a Edmond realiza, anualmente, a Avaliação de Efetividade desta Política, a fim de analisar e validar se a estratégia prevista estão sendo efetivas e suficientes para a Segurança Cibernética.

Para tanto, a Edmond realiza:

- a definição de processos, testes e trilhas de auditoria;
- a definição de métricas e indicadores adequados; e,
- a identificação e a correção de eventuais deficiências.

Todo colaborador é responsável por garantir a segurança cibernética, com o objetivo de evitar que ela possa ser acessada por pessoa não autorizada. Sendo assim, é vedado:

- Expor a Edmond à uma perda monetária efetiva ou perda potencial por meio do comprometimento da segurança de dados ou de informações ou, ainda, por meio da perda de equipamento;
- Revelar dados confidenciais e negociações;
- Usar indevidamente e sem autorização direitos autorais, patentes e dados corporativos;
- Utilizar dados para propósitos ilícitos que violem qualquer lei, regulamento ou seja qual for outro dispositivo governamental.

Em caso de **violação** desta Política, será avaliada a severidade, a amplitude e o tipo de infração cometida. **A punição para tal pode resultar desde advertência verbal ou escrita até em uma ação judicial.**

EDMOND

08. Vigência e Controle de Versões

Esta Política entra em vigor a partir da data de sua publicação e disponibilização aos Destinatários e será periodicamente revisada e atualizada pelo Responsável, com a frequência mínima a cada 3 (três) meses.

EDMOND

09. Aprovação

9 Aprovação

A Diretoria da Edmond, ao aprovar esta Política de Segurança Cibernética, institui um compromisso para com a melhoria contínua dos procedimentos relacionados com a segurança cibernética, buscando sempre manter a Edmond em conformidade com normas legais e regulamentares sobre os referidos temas, guiada pelos princípios, conceitos, valores e práticas aqui adotados, com o objetivo de assegurar a confidencialidade, a integridade e a disponibilidade dos dados da Edmond ou por ela controlados e dos sistemas de informação por ela utilizados, permitindo à Edmond prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados à segurança da informação e ao ambiente cibernético e proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

EDMOND

Um novo ciclo para ir além

Muito Obrigado!

company/edmond-tech

edmond.tech

edmond.tech

Edmond Soluções e Tecnologia S.A.

Av. Andrômeda, 885 - sala 2901 - Green Valley Alphaville

Barueri - SP - CEP - 06473-000

Tel.: + 55 11 5199-0983

Site: edmond.com.br

E-mail: contato@edmond.com.br