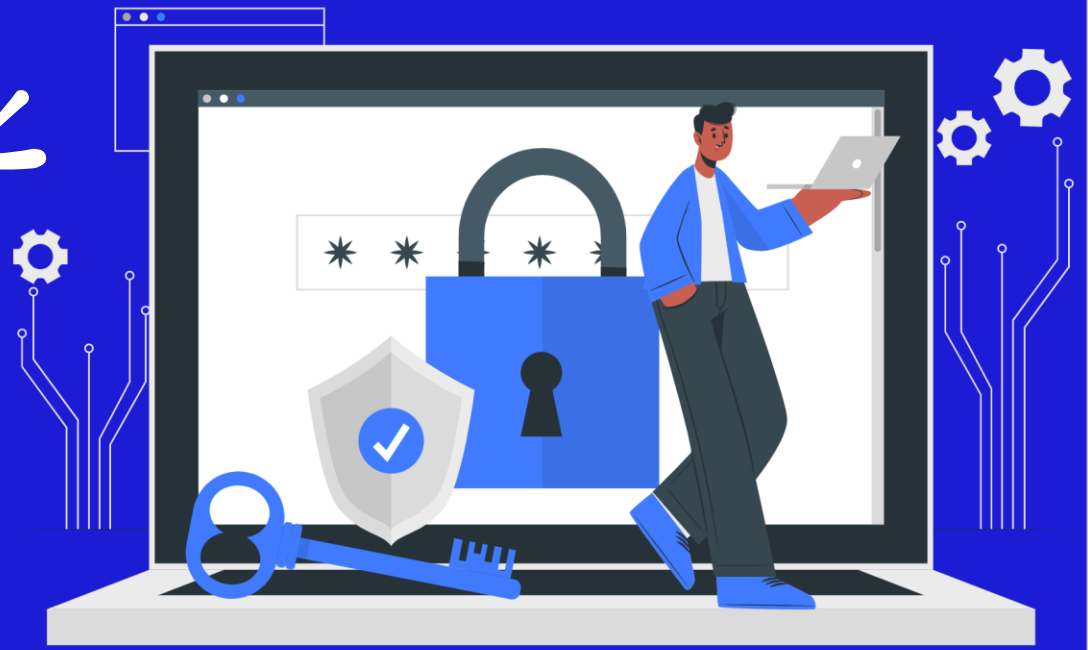
POLÍTICA DE Segurança Cibernética



PRÓXIMO

Sumário

#PraTodoVerem Acima quadro de navegação pelo documento, direcionando aos temas específicos ao clicar. Ao lado seta para direcionar ao próximo slide.

PRÓXIMO

Objetivos

Estabelecer os princípios e diretrizes que permitam o Grupo DM:

- Proteger os sistemas e ativos digitais contra ataques cibernéticos, assegurando a integridade, confidencialidade e disponibilidade das informações.
- Promover a melhoria contínua dos procedimentos em relação à segurança cibernética dos dados e informações, buscando identificar violações e estabelecer ações sistemáticas de detecção, tratamento, prevenção e redução a vulnerabilidades a incidentes relacionados ao ambiente cibernético;
- Atender aos requisitos legais regulamentares e às obrigações contratuais pertinentes as atividades do Grupo.

#PraTodoVerem Botões de navegação pelo documento presente nas páginas no canto direito ou esquerdo indicando seta para próximo slide e Menu Principal onde constam os links de direcionamento aos temas.

Abrangência

- Esta Política de Segurança Cibernética deve ser interpretada em conjunto com a NRM -SI - 006 - NORMA DE TRATAMENTO DE INCIDENTES SEGURANÇA DA INFORMAÇÃO e POL - SI - 001 - SEGURANÇA DA INFORMAÇÃO, bem como com todas as demais normas de privacidade e proteção de dados que compõe o programa de governança do Grupo DM.

- Abrange todas as ferramentas, aplicações e processos do ambiente de tecnologia e ambiente convencional do Grupo DM e deve ser aplicada, inclusive, no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias empregadas nas atividades da instituição de pagamento.

- Para os fins dispostos nesta Política, o termo “Colaboradores(as)” abrange: funcionários(as), estagiários(as), jovens aprendizes e administradores(as) do Grupo DM.

Vigência

Entra em vigor a partir da data de sua publicação, devendo ser revisada anualmente ou sempre que necessário pela área de Segurança da Informação.

Termos e Definições

Ameaça: Causa potencial de incidente indesejável que pode resultar em danos para o Grupo DM, para a sua informação ou sistemas de informação. Estas ameaças podem ser acidentais ou deliberadas;

ANPD - Autoridade Nacional de Proteção de Dados: Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) em todo o território nacional;

Ativo de Informação: Elemento com valor para o Grupo DM, para as suas atividades e para a continuidade destas, incluindo as tecnologias de informação e comunicação e os recursos de informação que a apoiam no desempenho das suas funções;

Confidencialidade: As informações são protegidas e são acessíveis somente às pessoas autorizadas;

Dado Pessoal: Qualquer informação relacionada a pessoa natural, direta ou indiretamente, identificada ou identificável;

Disponibilidade: As informações são acessíveis aos usuários autorizados sempre que necessário;

Incidente de Segurança de Informação: Qualquer evento que afete ou possa afetar a integridade, disponibilidade, privacidade, confidencialidade, autenticidade, auditabilidade e/ou fiabilidade da informação ou sistemas de informação do Grupo DM, incluindo qualquer ação ou omissão, deliberada ou não, que viole a regulação vigente em matéria de segurança de informação;

Informação: É um ativo estratégico e de alto valor para o Grupo DM, de sua propriedade ou sob sua responsabilidade e deve ser protegida, em conformidade com a legislação vigente, com os valores éticos e com as melhores práticas da segurança da informação;

Termos e Definições

Integridade: Garantia da exatidão e dos métodos de processamento das informações;

Informações Sensíveis: São aqueles dados que podem levar a discriminação de uma pessoa e, por tal motivo, devem ser considerados e tratados como dados sensíveis;

Prestador de Serviços: Pessoa física ou jurídica que presta qualquer tipo de serviços ao Grupo DM;

Riscos Cibernéticos: São aqueles associados a malwares, invasões, ataques de rede, violações de acessos e privacidade, ataques de rede, que podem desproteger o ambiente tecnológico, dados, redes causando danos financeiros e de imagem para o Grupo DM;

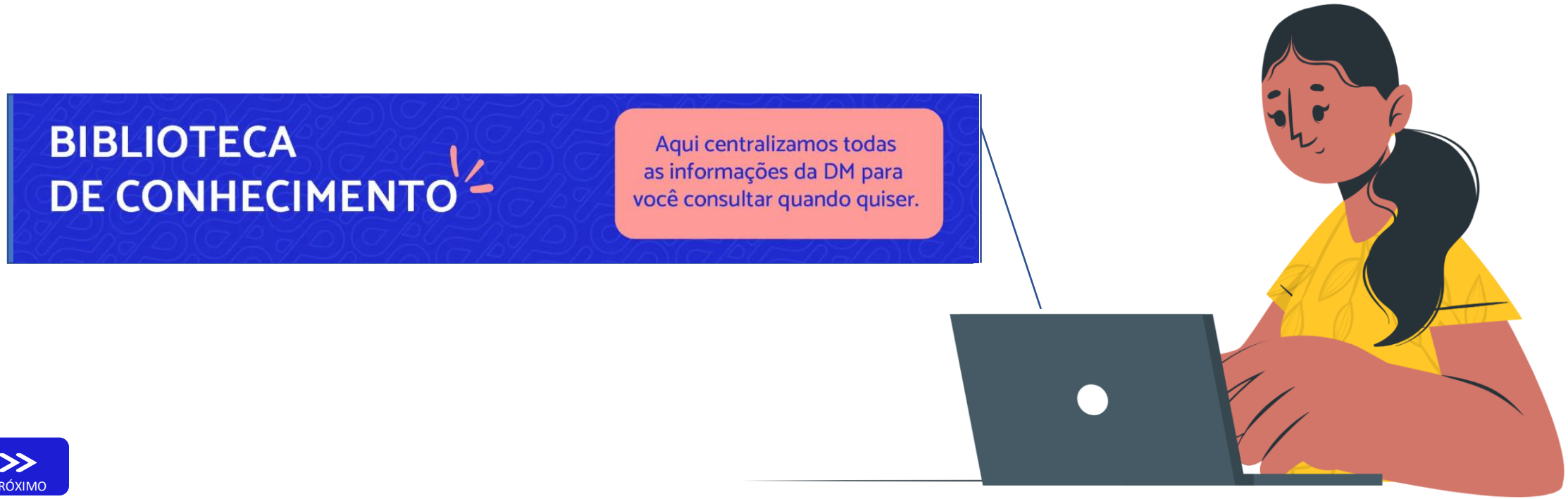
Segurança Cibernética: Conjunto de tecnologias, processos e práticas projetados para proteger redes, computadores, sistemas e dados de ataques, danos ou acesso não autorizado;

Segurança da Informação: Conjunto de conceitos, técnicas e estratégias, as quais visam proteger os ativos de informação do Grupo DM;

Vulnerabilidade de Segurança de Informação: Vulnerabilidade técnica, insuficiência a nível dos controles ou outra condição associada a um ativo ou conjunto de ativos de informação que pode ser explorada ou iniciada por ameaças, podendo dar origem ou potenciar a ocorrência de algum incidente de segurança de informação.

Adesão

- A adesão à esta Política implica estrita observância à legislação vigente e regras nela contidas, estando sujeito a sanções disciplinares em caso de descumprimento.
- Esta Política deve ser de conhecimento de colaboradores(as) e prestadores(as) de serviços do Grupo DM.
- Sempre que ocorrerem alterações relevantes e/ou que importarem obrigações adicionais aos(as) colaboradores(as) a atualização será informada por canal de comunicação interna.

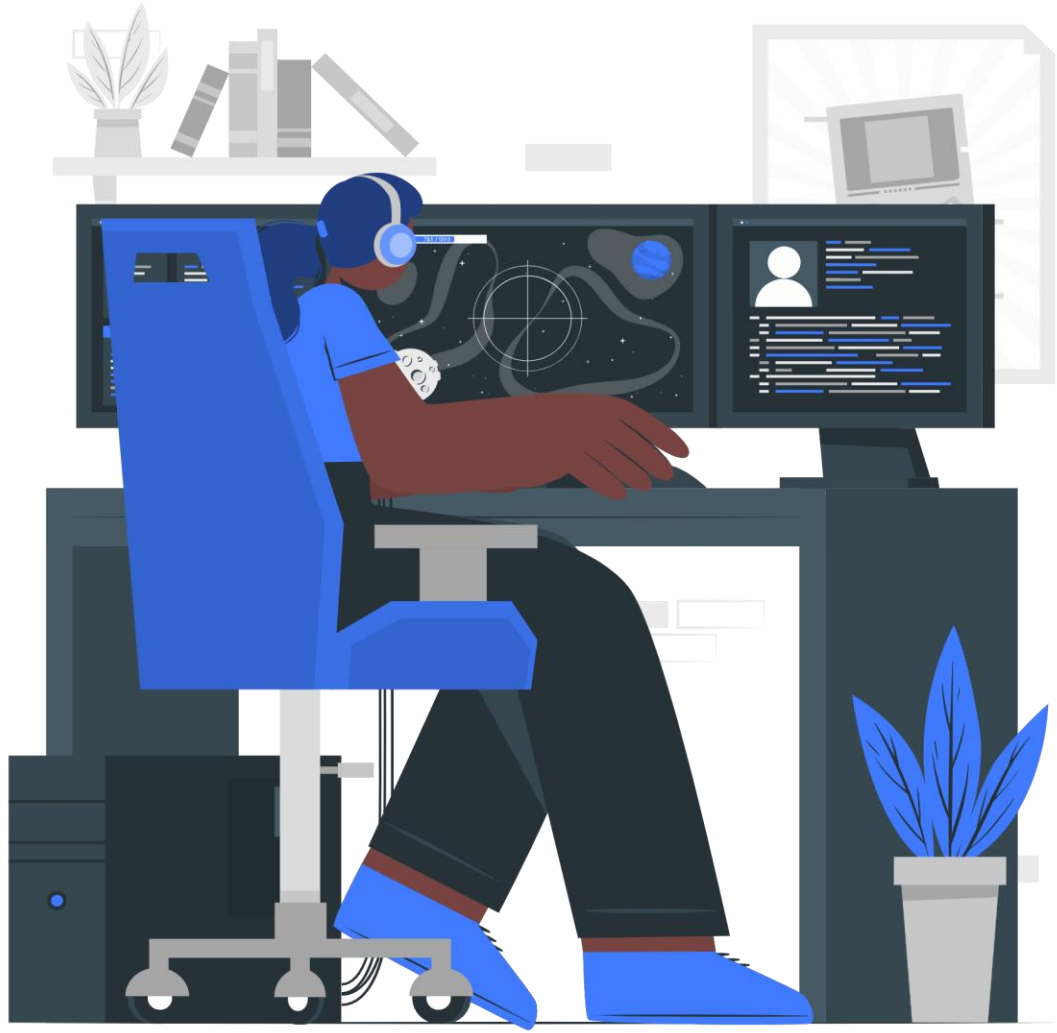


Plano de Segurança Cibernética

- A área de Segurança da Informação, adota procedimentos e controles para reduzir as vulnerabilidades e atender aos demais objetivos de segurança cibernética;

- A área de Segurança da Informação, atua para a disseminação da cultura de segurança cibernética visando garantir a integridade, confiabilidade e disponibilidade das informações;

- Para garantir o cumprimento dos princípios dispostos acima, o Grupo DM utiliza diversos meios como as políticas internas, instruções normativas, comunicados corporativos e a realização de treinamentos periódicos de segurança da informação e Compliance.



Procedimentos e Controles Específicos

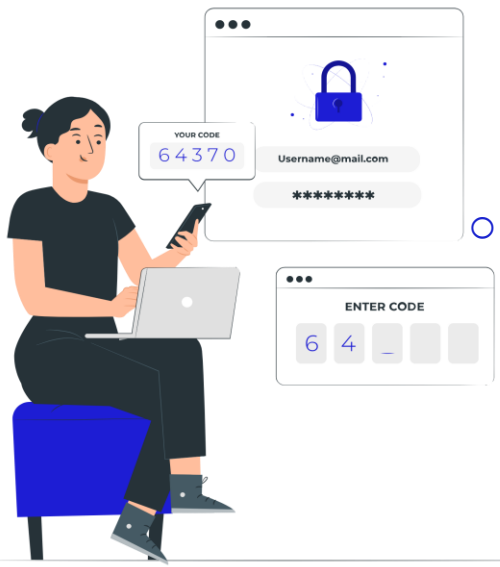
O Grupo DM possui diversos controles e procedimentos voltados para a rastreabilidade da informação de forma a garantir a segurança das informações sensíveis, conforme descrito nos tópicos abaixo:

- Controle de Acesso e Gerenciamento;
- Criptografia;
- Gerenciamento de Riscos e Tecnologia da Informação;
- Segurança e Gerenciamento de Ativos e Sistemas;
- Segurança de Rede;
- Gestão de Ameaças e Vulnerabilidade de T.I.;
- Segurança Física;
- Dispositivos e Controles de Mídia;
- Cópias de Segurança dos dados;
- Desenvolvimento de Sistemas.

Clique e veja o detalhamento por tópico!!

Controle de Acesso e Gerenciamento:

- A prática de Controle de Acesso e Gerenciamento tem o objetivo de prevenir o acesso de indivíduos não autorizados ao ambiente e aos sistemas, garantindo assim a confidencialidade, integridade, disponibilidade das informações bem como sua autenticidade.
- O Grupo DM adota as boas práticas, e:
  - Orienta que todos os usuários devem possuir acesso à informação de acordo com as necessidades de negócio. Esses acessos são concedidos considerando a segregação de função baseada em cargo/função.
    - Realiza periodicamente a revisão de acessos, conforme política, que tem como objetivo a atualização dos acessos e permissões, procedimento este, que é coordenado pela Área de Segurança da Informação.
    - Possui procedimentos formalizados e a descrição dos fluxos operacionais para a Concessão, Alteração, Revogação e Gerenciamento de acessos, sendo que para todos os procedimentos citados acima, é respeitado o princípio de menor privilégio e perfil mínimo restrito de acesso, conforme a matriz de segregação de função. Adicionalmente, os procedimentos de Concessão e Alteração devem ser aprovados pelo gestor responsável.



Criptografia:

O Grupo DM:

- Assegura o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação.
- Mantem uma política sobre o uso, proteção e ciclo de vida das chaves criptográficas (incluindo, a geração, armazenagem, arquivo, recuperação, distribuição, retirada e destruição das chaves), desenvolvidas e implementadas ao longo de todo o seu ciclo de vida.
- Utiliza a criptografia para a proteção de informações sensíveis transportadas em dispositivos móveis, mídias removíveis ou através de linhas de comunicação.

Gerenciamento de Riscos e Tecnologia da Informação:

O Grupo DM:

- Verifica periodicamente o controle de acessos à internet e controla os aplicativos instalados nos computadores.
- Ressalta que nenhum usuário possui acesso de administrador local, impossibilitando a instalação de qualquer aplicativo. Somente podem ser instalados aplicativos previamente testados e autorizados pela área de Tecnologia da Informação (T.I).
- Realiza o monitoramento da rede por meio de software específico.

Segurança e Gerenciamento de Ativos e Sistemas:

- Quando disponível, o acesso aos sistemas de informação do Grupo DM é integrado com o AD (Active Directory), que possui as suas especificidades definidas em políticas.
- Para os Sistemas de Informação que não estão integrados com AD, existe um pré-requisito mínimo para as parametrizações de senhas definido em política.
- Referente ao gerenciamento das parametrizações de segurança, somente a área de Segurança da Informação tem acesso para alterar as configurações de acesso e segurança nos Sistemas de Informação.

Segurança de Rede:

- A segurança é realizada através do monitoramento e gerenciamento da infraestrutura, sendo que todo acesso às redes internas e acessos à internet são controlados por Tecnologia da Informação.

Gestão de Ameaças e Vulnerabilidade de T.I.:

- O ambiente possui instalado software de antivírus para a proteção contra vírus, arquivos e softwares maliciosos, atualizados periodicamente.
- Todas as atualizações de segurança do Windows são gerenciadas e atualizadas frequentemente.

Segurança Física:

- Os recursos e instalações de processamento de informações críticas para as atividades do Grupo DM são mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas e recursos para controle de acesso.
- Os equipamentos críticos possuem proteção contra desastre físico e recursos para combate a incêndio.
- O Grupo DM possui sistema para controle do acesso de colaboradores(as), prestadores(as) de serviços ou fornecedores(as) aos locais restritos, que são monitorados por câmeras.
- O registro e análise dos efeitos de incidentes relevantes são atividades cruciais para minimizar impactos negativos para o Grupo DM , a nível operacional e reputacional. Os eventos de TI são registrados no sistema de chamados GLPI.

Dispositivos e Controles de Mídia:

- Somente pessoas previamente autorizadas pela Diretoria Executiva tem acesso aos dispositivos móveis e acessos ao leitor de DVD e USB do computador.

Cópias de Segurança dos dados:

- Todas as informações críticas do Grupo DM possuem cópias de segurança (backup) conforme definido em POLÍTICA DE BACKUP E RESTAURAÇÃO, as quais são testadas periodicamente.

Desenvolvimento de Sistemas:

- Os ambientes de desenvolvimento, homologação e produção devem ser separados para reduzir os riscos de acessos ou modificações não autorizadas.
- Alterações no ambiente de produção devem ser precedidos de processo de solicitação, análise e aprovação documentados.

Diretrizes Gerais

Os princípios e diretrizes desta Política são compatíveis com:

- O porte, o perfil de risco e o modelo de negócios do Grupo DM;
- A natureza das atividades do Grupo DM e a complexidade dos produtos e serviços oferecidos, e
- A sensibilidade dos dados e das informações sob responsabilidade do Grupo DM:
  - Teste de Continuidade de Negócios;
  - Fornecedores de Serviço de T.I.

Teste de Continuidade de Negócios:

O Grupo DM assume o compromisso de manter a continuidade dos negócios em caso de incidentes que possam comprometer o funcionamento normal de suas atividades, através do Plano de Continuidade de Negócios (PCN), sendo constantemente revisado com o objetivo contínuo de melhoria.

O programa possui o objetivo de identificar e elaborar os cenários que possam comprometer a continuidade da sua atividade, analisar o seu impacto e promover a resiliência organizacional, dotando a organização da capacidade de prevenir ou, na sua impossibilidade, responder de forma eficaz a estes eventos.

O PCN contempla as responsabilidades dos órgãos responsáveis pela coordenação do programa, as reponsabilidades das áreas envolvidas e os procedimentos para a realização da avaliação/revisão do Plano.

Fornecedores de Serviço de T.I.:

O Grupo DM adota procedimentos específicos em relação a proteção de dados e informações disponibilizadas às empresas que lhes prestam serviços. As informações recebidas por estas empresas são objeto de NDA (Non Disclosure Agreement), contempladas em registro específico e objeto de análise complementar no que se refere a impactos dos efeitos de incidentes e vulnerabilidades.

Os procedimentos e controles voltados à prevenção e ao tratamento de incidentes em relação aos(as) fornecedores(as) de serviço de T.I. são previamente definidos em contratos.

As diretrizes que permitem o Grupo DM gerenciar serviços relacionados a serviços de T.I. prestados por todos os tipos de fornecedores contratados para atender às necessidades organizacionais, incluindo a seleção de fornecedores, gestão de relacionamentos, gestão de contratos e revisão e monitoramento de desempenho de fornecedores(as) para a efetividade e conformidade, são formalizadas em Política específica denominada “Política de Gestão de Fornecedores(as) de Serviços de Tecnologia da Informação”.

Disseminação da Cultura de Segurança Cibernética

O Grupo DM incentiva e promove uma cultura de segurança dentro da instituição, visando proteger os objetivos citados nesta política, e principalmente proteger a informação.

A cultura de Segurança Cibernética é disseminada internamente através de programas de capacitação ministrados periodicamente para colaboradores(as), garantindo assim estejam cientes das possíveis ameaças e vulnerabilidades que ocorrerem no âmbito da Segurança Cibernética, bem como quais são os procedimentos que devem ser adotados em casos de incidentes.

O Grupo DM tem consciência que as atividades no âmbito de Segurança Cibernética, estão em constante evolução, sendo assim, os procedimentos e controles relacionados com o tema, devem ser revistos com periodicidade, promovendo uma melhoria contínua do ambiente de Segurança Cibernética.

São realizadas divulgações internas sobre os temas de segurança da informação e cibernética ao público externo através de blog e lives.

A política de segurança cibernética é divulgada aos(as) colaboradores(as), às empresas prestadoras de serviços a terceiros e ao público geral através de divulgação no site do Grupo DM.

Compartilhamento de Informações

O Grupo DM busca atuar com transparência e objetivando a melhoria dos seus procedimentos relacionados à Segurança Cibernética, tem o compromisso de compartilhar com as Instituições Financeiras Parceiras, com o Banco Central do Brasil (“BACEN”) e com a Autoridade Nacional de Proteção de Dados - ANPD todos os incidentes relevantes, tempestivamente, sempre que solicitado e quando afetar os direitos fundamentais de privacidade de seus clientes pessoas físicas.

As formas de comunicação, de maneira mais detalhada, às autoridades e órgãos competentes são definidas e formalizadas em documento específico denominado “Plano de Ação e de Resposta a Incidentes”.

Processamento e Armazenamento de dados e de Computação em Nuvem

Toda contratação de serviços de processamento e armazenamento de dados e de computação em nuvem devem estar aderentes com as diretrizes indicadas pelo Bacen a ser observadas pelas Instituições autorizadas a funcionar pelo BACEN.

Caso o Grupo DM decida estrategicamente pela contratação de fornecedores(as) para prestação de serviços de T.I. relacionados ao processamento e armazenamento de dados e de computação em nuvem, além da adoção das medidas e análises contidas na “Política de Gestão de Fornecedores(as) de Serviços de Tecnologia da Informação” também deverá observar as diretrizes constantes da Política da Segurança da Informação.

Os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem conter cláusulas específicas conforme Resolução Bacen.

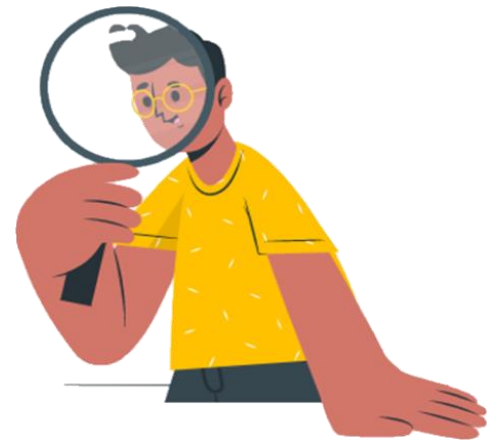
Plano de Ação e Resposta de Incidentes

O Grupo DM entende que é de extrema importância a existência de um procedimento que possibilita a detecção tempestiva e a pronta comunicação de incidentes e vulnerabilidades, assegurando assim, a eficácia das medidas a serem tomadas na sequência. Possui os controles que permitem detectar e identificar os incidentes e vulnerabilidades que afetam o ambiente de Segurança Cibernética.

As responsabilidades em relação ao registro, análise e comunicação dos incidentes estão devidamente detalhadas em normativos específicos. O plano de ação e de resposta a incidentes devem ser documentados e revisados, no mínimo, anualmente.

O Grupo DM mantém em seus registros, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes e vulnerabilidades para as atividades da instituição.

Caso ocorra um incidente, ele deve ser analisado e, após análise, é elaborado um plano de ação para corrigir e/ou melhorar o ambiente e/ou processo com o objetivo de minimizar a possibilidade de nova ocorrência.



Plano de Ação e Resposta de Incidentes

A elaboração e acompanhamento do plano de ação são coordenados pela Área de Segurança da Informação, com participação de outras Área.

A área de Segurança da Informação realiza monitoramento de segurança do ambiente tecnológico, analisando os eventos e alertas a fim de identificar e precaver a possíveis incidentes;

A área de Segurança da Informação, é responsável por estabelecer um processo de tratamento e comunicação, onde se mantém o registro dos incidentes identificados, e a avaliação quanto a causa, impacto, e a classificação;

É responsabilidade e prerrogativa da área de Segurança da Informação, coletar logs dos sistemas, processá-los e gerar insumos para resposta a incidentes.

Os procedimentos detalhados de resposta de incidentes são definidos no “Plano de Ação e de Resposta a Incidentes”.

A área de Tecnologia da Informação disponibiliza bimestralmente o KRI (Key Risk Indicator) de acompanhamento de incidentes ao Comitê responsável e por solicitação da área de Risco Operacional e Controles Internos do Grupo DM.

Emissão de Relatórios Anuais

A área de Segurança da Informação irá elaborar relatório anual sobre a implementação do plano de ação e de resposta a incidentes (data-base de 31 de dezembro) e apresentar para aprovação da diretoria até 31/03 do ano seguinte a base. O relatório irá conter:

- a efetividade da implementação das ações do plano de ação e de resposta a incidentes;
- o resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes;
- os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período; e
- os resultados dos testes de continuidade, considerando cenários de indisponibilidade ocasionada por incidentes.

Armazenamento e Guarda

Serão mantidos por 5 anos e à disposição do Bacen:

- política de segurança cibernética;
- plano de ação e de resposta a incidentes;
- relatório anual sobre a implementação do plano de ação e de resposta a incidente;
- procedimentos de análise de contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem;
- a documentação prevista para serviços prestados no exterior;
- análise de cláusulas dos contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem;
- a documentação dos critérios que configurem uma situação de crise;
- mecanismos de acompanhamento e controle para assegurar a implementação e a efetividade da política de segurança cibernética, do plano de ação e de resposta a incidentes e dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

Responsabilidades

Alta Administração:

- Apoiar na melhoria contínua dos procedimentos relacionados com a segurança cibernética e aderência à Política de Segurança da Informação e à Política de Segurança Cibernética de acordo com os objetivos e estratégias do negócio.

Diretor de Risco:

- Definir estratégias e ações para cumprimento da política de segurança cibernética e pela execução do plano de ação e de resposta a incidentes.

Gerência e Coordenação de Segurança da Informação:

- Tratar todos os assuntos relacionados à Segurança da Informação e à Segurança Cibernética de maneira efetiva e consistente;
- Manter atualizada e divulgar esta Política.

Liderança:

- Cabe a liderança assegurar o cumprimento da Política para colaboradores(as) diretos;
- Assegurar que os contratos e serviços sob sua responsabilidade estejam aderentes à esta Política e demais Normas e Procedimentos de Segurança da Informação; e
- Comunicar imediatamente eventuais casos de violação à área de Segurança da Informação.

Colaboradores(as) e Prestadores(as) de Serviços:

- Cabe aos(as) colaboradores(as) e prestadores(as) de serviços cumprirem as diretrizes estabelecidas na Política de Segurança da Informação e nesta Política de Segurança Cibernética;
- Reportar qualquer situação que configure desvio ou violação da segurança de informação, pelo canal privacidade@vocedm.com.br.

Documentos Relacionados

NBR/ISO 27001

Lei 13.709/2018 - LGPD

Lei 12.965/2014 – Marco Civil Internet

Resolução BCB 85/2021

Resolução CMN 4893/2021

POL – SI – 001 – SEGURANÇA DA INFORMAÇÃO

POL – TIS – 008 – POLÍTICA DE GESTÃO DE FORNECEDORES DE SERVIÇOS DE T.I

NRM -SI - 006 - NORMA DE TRATAMENTO DE INCIDENTES SEGURANÇA DA INFORMAÇÃO

COBIT – 2019

Os documentos relacionados encontram-se no ambiente do Sharepoint (Políticas)

O conteúdo deste documento foi classificado de acesso PÚBLICO.