POLÍTICA DE GERENCIAMENTO DE INCIDENTES DE SEGURANÇA

Código: POL-TI-012
Revisão: 01
Data: 13/03/2023

WWW.DMSLOG.COM

1. DEFINIÇÕES

A Política de Gerenciamento de Incidentes da DMS LOGISTICS tem como objetivo principal definir as diretrizes estratégicas para as ações relativas à Segurança da Informação e Comunicações, com o intuito de preservar a confidencialidade, integridade, disponibilidade e autenticidade dos dados e informações produzidos, adquiridos, armazenados, em trânsito, descartados, de propriedade ou sob controle ou operação da DMS LOGISTICS.

O objetivo das regras para o Gerenciamento de Incidentes é primordialmente assegurar a proteção dos ativos de informação contra ameaças, internas ou externas, minimizar eventuais riscos à segurança das informações, reduzir a exposição a perdas ou danos decorrentes de falhas de segurança e garantir que os recursos adequados estarão disponíveis, mantendo um programa de segurança efetivo e conscientizando seus Colaboradores a respeito.

Deverá, assim, ser seguida por todos os seus Colaboradores, independentemente do nível hierárquico ou função na instituição, bem como de vínculo empregatício ou prestação de serviços.

2. PROPÓSITO

- “Ameaça” significa risco ou potencial perigo de um incidente, que pode resultar em dano à DMS LOGISTICS.
- “Área de Privacidade e Proteção de Dados” significa a área responsável pelo suporte ao DPO.
- “Ativo” significa qualquer coisa que tenha valor para a DMS LOGISTICS e precisa ser adequadamente protegido.
- “Autoridade Nacional de Proteção de Dados” ou “ANPD” significa a autoridade administrativa encarregada da Proteção de Dados Pessoais. Órgão da administração pública nacional responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados Pessoais em todo o território brasileiro.
- “Comitê de Segurança e Proteção de Dados Pessoais” significa um comitê especificamente dedicado a lidar com eventos de segurança da informação.

- “Colaboradores” significam todos os colaboradores da DMS LOGISTICS, incluindo diretores, estagiários, aprendizes e qualquer outra pessoa que possua vínculo direto com a DMS LOGISTICS.

- “Dados Pessoais” significam quaisquer dados relacionados a um indivíduo (pessoa natural) que é ou possa ser identificado a partir dos dados ou a partir dos dados em conjunto com outras informações.

- “Equipe de Resposta ao Incidente” significa pessoas ou área(s) nomeadas pela Gerência da Segurança da Informação para a identificação de Incidentes de Segurança internos ou externos, envolvendo ou não Dados Pessoais, seja na detecção de alertas provenientes dos sistemas de monitoramento da rede da DMS LOGISTICS ou por notificações realizadas por Usuários da Informação ou por qualquer pessoa relatando ser de seu conhecimento, ou mesmo vítima de atividade suspeita ou em desacordo com a Política de Segurança da Informação e demais políticas da DMS LOGISTICS.

- “Evento” significa qualquer ocorrência visível em uma rede ou sistema de informação. Exemplos: um usuário que acessa um arquivo compartilhado, um servidor que recebe uma solicitação para uma página da Web, um usuário que envia um e-mail ou um firewall que faz um bloqueio de uma tentativa de conexão, entre outros.

- “Evento adverso” (ou ofensivo) significa um evento, confirmado ou sob suspeita, com consequências negativas. Exemplos: falhas do sistema de informação, uso não autorizado de privilégios de sistema de informação, acesso não autorizado a dados confidenciais ou execução de malware que destrói dados, entre outros.

- “Encarregado de Dados” ou DPO significa a pessoa que na DMS LOGISTICS é a responsável por coordenar e por assegurar a conformidade com esta Política, com a Legislação de Proteção de Dados e que atuará como canal da DMS LOGISTICS com os Titulares de Dados e com a Autoridade Nacional de Proteção de Dados.

- “Incidente de Segurança” significa qualquer evento ou conjunto de eventos indesejados de segurança da informação, confirmado ou sob suspeita, que

tem possibilidade significativa de afetar as operações ou ameaçar as informações da DMS LOGISTICS e/ou que indica possível violação à PSI e suas normas e procedimentos agregados, falha de controles ou situação previamente desconhecida, que possa ser relevante à segurança da informação.

- “Incidente relevante de segurança” significa um incidente de segurança que afete sistemas ou serviços considerados como relevantes pela DMS LOGISTICS com consequências de interrupções de vários processos de negócio internos e/ou externos, não previsíveis e de difícil gerenciamento, causando grande impacto financeiro, bem como na imagem da DMS LOGISTICS.
- “Informação” significa o conjunto de dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato.
- “Risco” significa a combinação da probabilidade da concretização de um evento indesejado e seus potenciais impactos.
- “SI” significa a área de segurança da informação.
- “TI” significa a área de Tecnologia da Informação.
- “Usuário(s) de Informação” significa colaboradores, empregados, estagiários, aprendizes e qualquer outra pessoa que possua vínculo direto com a DMS LOGISTICS, bem como representantes, fornecedores, prestadores de serviços e terceiros a serviço da DMS LOGISTICS.
- “Violação de Dados Pessoais”, “Incidente de Segurança com Dados Pessoais” ou “Incidente de Violação de Dados Pessoais” significa Incidente de Segurança com o envolvimento de Dados Pessoais.
- “Black Team” é um grupo de cyber segurança destinado a realizar testes de segurança ofensiva em ambientes físicos.
- “Red Team” é um grupo de cyber segurança destinado a realizar testes de segurança ofensiva em ambientes digitais.
- “Blue Team” é um grupo de cyber segurança destinado a realizar operações

defensivas e fornecer segurança defensiva e resposta a incidentes.

- “Purple Team” é um grupo de cyber segurança destinado a maximizar a performance do red team e do blue team. Atua com uma combinação dos dois times.
- “Orange Team” é um grupo de cyber segurança destinado a auxiliar desenvolvedores a pensar como um atacante, utilizando informações do red team, de modo a criar aplicações e sistemas seguros e livres de possíveis ataques.
- “White Team” é um grupo de cyber segurança destinado a gerenciar os demais times, promovendo interação entre eles, estabelecendo regras, políticas e padrões de segurança e garantindo que estes requisitos sejam seguidos.
- “CISO” é a figura do Chief Information Security Officer, que é responsável por garantir a segurança dos dados como prioridade na organização.
- “DPO” é a figura do Data Protection Officer, na LGPD definido como encarregado de dados, responsável por manter padrões de segurança da informação na organização e fazer a comunicação com a Autoridade Nacional de Proteção de Dados (ANPD).

3. DIRETRIZES

O Gerenciamento de Incidentes visa garantir que os eventos confirmados ou sob suspeita, sejam comunicados, registrados e tratados de forma efetiva, ordenada e em tempo hábil.

Qualquer evento adverso, sob suspeita ou confirmação, relacionado a segurança de nossos sistemas ou de nossa rede, deverá ser documentado em nosso agrupamento de tarefas, descrito e evidenciado o evento, priorizando esta demanda como "Hotfix" (alta prioridade para resolução).

O responsável por notificar o evento deverá eleger um membro da equipe para se responsabilizar por todo o processo de resolução da tarefa e assegurar que ela seja resolvida e entregue em tempo hábil.

O processo de gerenciamento de incidentes e violação de dados deve ter o apoio da Alta Direção e deverá adotar as seguintes diretrizes:

3.1. PREVENÇÃO A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E DADOS PESSOAIS

- A DMS LOGISTICS realizará avaliações de impacto sobre proteção de dados, quebra da confidencialidade, integridade, autenticidade e não repúdio antes de iniciar qualquer projeto ou implementar qualquer tecnologia que processe Dados Pessoais. Nas avaliações de impacto serão apontados os riscos associados.

- Após determinar se existe um alto risco, o Comitê de Segurança - e se o Incidente de Segurança também envolver Dados Pessoais, o Encarregado de Dados - tomará as medidas técnicas e organizacionais apropriadas para proteger os Dados Pessoais contra a destruição acidental ou ilegal ou perda acidental, alteração, divulgação ou acesso não autorizado.

3.2. IDENTIFICAÇÃO DO INCIDENTE

- Os membros do Comitê de Segurança, quando reportados pelos Usuários de Informação ou seus gestores sobre a suspeita de um Incidente de Segurança, deverá avaliar se o incidente envolve Dados Pessoais, hipótese em que notificará o Encarregado de Dados a esse respeito, por meio do e-mail: dpo@dmslog.com.

- Confirmada a ocorrência do Incidente de Segurança, a Equipe de Resposta ao Incidente deve ser acionada para categorizar e priorizar o atendimento com base: (i) no impacto potencial conforme avaliação de risco em segurança da informação realizada em conjunto com a Tabela de Classificação de Severidade de Incidente de Segurança (Anexo E); (ii) no tempo e recursos necessários para recuperar ativos impactados.

- Todo incidente categorizado como sendo de severidade crítica deve ser notificado imediatamente ao CISO (Chief Information Security Officer), que pode alocar os profissionais necessários para resolução do incidente.

- Caso a ocorrência configure um Incidente que envolva Dados Pessoais, o Encarregado de Dados deverá receber a notificação e preparará o Relatório

de Incidente de Violação de Dados Pessoais, com o apoio do Gestor de SI, TI e demais áreas impactadas.

- A Equipe de Resposta ao Incidente deve apresentar as ações que serão priorizadas com base na categoria e no impacto do cenário encontrado e realizar as comunicações necessárias.
- Todos os Incidentes de Segurança envolvendo Dados Pessoais serão avaliados pelo Comitê de Segurança e Proteção de Dados Pessoais, o qual deverá definir quais medidas serão adotadas.

3.3. REGISTRO DO INCIDENTE

- Caso o incidente envolva Dados Pessoais, o CISO, o Encarregado de Dados e demais membros do Comitê de Segurança realizarão o registro sobre o Incidente de Segurança ou Violação de Dados Pessoais, com a descrição do incidente, período de tempo, consequências, identificação das pessoas que avaliaram e para quem o incidente foi reportado, ações tomadas para resolver o incidente e as consequências que o incidente ocasionou, como a indisponibilidade, perda, divulgação ou alteração da Informação e/ou de Dados Pessoais.
- O Encarregado de Dados avaliará o tipo e o nível de risco criado pela violação e, então, registrará o incidente nos arquivos internos da DMS LOGISTICS.
- Tendo o Incidente de Segurança envolvimento de Dados Pessoais, o Encarregado de Dados determinará se existe um risco para os direitos e liberdades dos Titulares de Dados. Os riscos a direitos e liberdades incluem, entre outros, perda de controle ou confidencialidade dos Dados Pessoais, reversão não autorizada de pseudonimização, danos à reputação, discriminação, roubo ou fraude de identidade, perda financeira e outras desvantagens econômicas ou sociais.
- O Encarregado de Dados avaliará se a probabilidade e a gravidade dos riscos potenciais criam um risco alto. Essa avaliação deve envolver uma análise do tipo de violação; a natureza; sensibilidade e volume de Dados Pessoais afetados; a gravidade das possíveis consequências para os titulares de dados; o número e as características dos titulares de dados afetados; as

características do destinatário dos Dados Pessoais e a facilidade de identificação dos Titulares de Dados.

- O Comitê de Segurança e Proteção de Dados Pessoais definirá quais medidas serão adotadas, incluindo a notificação à ANPD e/ou aos Titulares de Dados.
- O Comitê irá repassar a situação para a direção, que então fará sua análise final antes de encaminhar para a ANPD.
- Sendo necessário, será feita a notificação para a ANPD e aos Titulares de Dados, com base no nível de risco, com o suporte do CISO, do Comitê de Segurança e Proteção de Dados Pessoais e do Encarregado de Dados.

3.4. CONTENÇÃO DO INCIDENTE DE SEGURANÇA

- O Encarregado de Dados, com o apoio de TI, SI e do Comitê de Segurança, deverá orientar os Gestores e áreas responsáveis/afetadas pelo Incidente de Segurança envolvendo Dados Pessoais quanto às medidas corretivas a serem tomadas para mitigação do risco ao máximo possível.
- No caso de Incidente de Segurança, o Encarregado de Dados deverá enviar relatório ao Comitê de Segurança para definição sobre quais ações serão tomadas pela DMS LOGISTICS.
- A TI, a SI e o Comitê de Segurança deverão fornecer apoio com as medidas técnicas necessárias para contenção/recuperação do incidente, a exemplo de efetuar coleta de evidências de forma legal ou isolar recursos de tecnologia de modo a não perder informações do incidente.

3.5. MITIGAÇÃO DOS INCIDENTES

3.5.1. PREPARAÇÃO

- Gerenciar as ferramentas para análise de incidentes, incluindo o conhecimento de todo o ambiente utilizado;
- Implementar mecanismos de defesa e controle de ameaças;
- Desenvolver procedimentos para lidar com incidentes de forma eficiente;

- Obter recursos e equipe necessária para lidar com os problemas;
- Estabelecer infraestrutura de suporte à atividade de resposta a incidentes.

3.5.2. DETECÇÃO

- Detectar o incidente, determinar o escopo e as partes envolvidas com o incidente;
- Identificar todos os sistemas e serviços afetados relacionados com o incidente;
- Avaliar o impacto do incidente e os potenciais riscos dos sistemas afetados (dados vazados, informações de instituições parceiras, impacto na própria organização e impacto na reputação);
- Identificar a existência de outros eventos e alertas relacionados com o incidente em questão;
- Identificar que tipo de informação e processos podem ter sido afetados;
- Identificar os responsáveis pelo sistema comprometido, equipes de suporte e donos das informações.

3.5.3. CONTENÇÃO

- Conter o incidente de maneira a atenuar os danos e evitar que demais recursos sejam comprometidos;
- Desconectar o sistema comprometido ou isolar a rede afetada;
- Desativar o sistema para evitar maiores perdas quando há perda ou roubo de informações durante o ataque;
- Alterar políticas de roteamento dos equipamentos de rede ou bloquear padrões de tráfego, interrompendo o fluxo malicioso;
- Desabilitar serviços vulneráveis, inibindo comprometimento de outros sistemas.

3.5.4. ERRADICAÇÃO

- Eliminar as causas do incidente, removendo todos os eventos relacionados;
- Garantir que as causas do incidente foram removidas, assim como todas as atividades e arquivos associados ao incidente;
- Assegurar a remoção de todos os métodos de acesso utilizados pelo atacante: novas contas de acessos; backdoors e, se aplicável, acesso físico ao sistema comprometido, etc.

3.5.5. RECUPERAÇÃO

- Restaurar o sistema ao seu estado normal;
- O Plano de Recuperação de Desastres deve ser iniciado conforme especificado no respectivo plano.
- Restaurar a integridade do sistema;
- Garantir que o sistema foi recuperado corretamente e que as funcionalidades estejam ativas;
- Implementar medidas de segurança para evitar novos comprometimentos;
- Restauração do último e íntegro backup completo armazenado.

3.5.6. AVALIAÇÃO

- Avaliar as ações realizadas para resolver o incidente, documentando detalhes, e discutir lições aprendidas;
- Caracterizar o conjunto de lições aprendidas de modo a aprimorar os procedimentos e processos existentes;
- Identificar características de incidentes que podem ser utilizadas para treinar novos membros da equipe;
- Prover estatísticas e métricas relativas ao processo de resposta a incidentes;
- Obter informações que podem ser utilizadas em processos legais.

3.6. ANÁLISE DE RISCOS

De forma a analisar os riscos envolvidos no Incidente de Segurança, deverá ser feita análise de riscos conduzida pelo Comitê de Segurança e Proteção de Dados Pessoais e pela Equipe de Resposta ao Incidente.

3.7. NOTIFICAÇÃO PARA A ANPD

Uma Violação de Dados Pessoais que provavelmente represente risco aos direitos e liberdades das Titulares deve ser relatada à ANPD sem demora injustificada, quando possível, dentro de 2 (dois) dias úteis depois que a DMS LOGISTICS tomar conhecimento da violação. Os motivos de eventual demora na comunicação à ANPD deverá ser justificada.

A DMS LOGISTICS é considerada ciente de uma violação quando existe um grau razoável de certeza de que ocorreu um Incidente de Segurança.

Um aviso parcial e incompleto pode ser enviado para a ANPD, com a maior brevidade possível, em algumas circunstâncias. Essas circunstâncias incluem violações complexas que requerem investigações detalhadas ou quando ocorrem várias violações semelhantes em um curto período.

A notificação para a ANPD deve incluir, dentre outros pontos descritos no anexo Notificação à Autoridade:

- A descrição da natureza dos Dados Pessoais afetados;
- As informações sobre os titulares envolvidos;
- A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- Os riscos relacionados ao incidente;
- As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo;
- A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- Os motivos da demora, no caso de a comunicação não ter sido imediata;
- Identificar pontos de contato para maiores detalhes;
- Descrever possíveis consequências do incidente de violação de dados;

- Descrever medidas para endereçar o incidente de violação de dados, incluindo medidas adotadas para mitigar possíveis efeitos adversos do incidente de violação de dados.

3.8. AVISO AOS TITULARES DE DADOS

O Encarregado de Dados comunicará às violações de alto risco aos titulares de dados afetados, sem demora injustificada.

A comunicação com o titular dos dados deve conter linguagem clara e simplificada, tomando como base orientações do Jurídico, Encarregado de Dados e do Comitê de Segurança.

A comunicação com os titulares de dados deve ser entregue em por meios disponíveis que maximizem as chances de comunicação, podendo exigir a utilização de vários métodos de comunicação e o fornecimento de informações em formatos.

3.9. DECISÃO DE NÃO NOTIFICAÇÃO

A DMS LOGISTICS está isenta do requisito de notificação obrigatória quando o risco para os titulares de dados é extremamente baixo ou não existir.

Se for tomada a decisão de não notificar, a justificativa para essa decisão deve ser documentada.

A DMS LOGISTICS deve continuar a monitorar as circunstâncias e os efeitos de uma violação e pode precisar fazer ou atualizar notificações à ANPD e ao Titular dos Dados à medida que novas informações surgirem.

Todas as ações tomadas relacionadas às violações devem ser totalmente documentadas, mesmo que nenhuma notificação seja necessária.

3.10. PÓS INCIDENTE

A etapa de pós Incidente de Segurança, ou violação de Dados Pessoais, tem o seu início após a resolução e encerramento do incidente, em que serão analisadas pela Equipe de Resposta ao Incidente, de SI, TI e Comitê de Segurança, as causas que motivaram o incidente e quais são as medidas que podem ser tomadas com objetivo que o fato não ocorra novamente.

3.11. RECOMENDAÇÕES E RESPOSTAS AOS INCIDENTES

Havendo recomendações a serem feitas aos usuários, administradores de sistemas ou a outras equipes de segurança, estas devem ser feitas no processo de fechamento do incidente.

3.12. LIÇÕES APRENDIDAS

O objetivo desta etapa é melhorar os procedimentos realizados na etapa de resposta e aprimorar os Ativos para protegê-los de futuros incidentes.

A Equipe de Resposta ao Incidente deve comunicar às partes interessadas do resultado da análise.

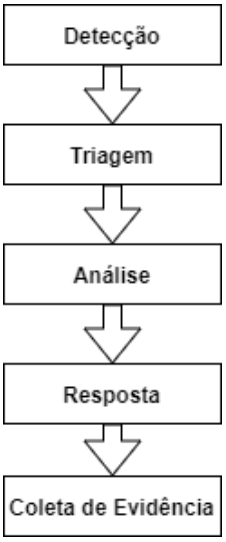
Os incidentes ocorridos devem ser analisados em conjunto com os procedimentos de continuidade de negócio da DMS LOGISTICS. Esta análise visa identificar o aprimoramento dos indicadores de probabilidade e consequência dos incidentes previstos e as ocorrências reais de incidentes.

Com base no relatório e nas informações obtidas durante a solução do incidente, a Equipe de Resposta ao Incidente deve criar um plano de ação que inclua os responsáveis, para garantir que todas as partes interessadas saibam o que se espera delas. As ações devem ser categorizadas como curto ou longo prazo.

Deve ser mantida uma base de conhecimento com o histórico dos incidentes tratados, para facilitar o tratamento de incidentes futuros com características semelhantes e para geração de indicadores.

4. FASES DO TRATAMENTO DE INCIDENTE

O tratamento de incidentes possui cinco fases, que devem seguir uma ordem definida, a saber:


Detecção
Triagem
Análise
Resposta
Coleta de Evidência

- **Detecção**: Reportar ou Identificar o evento.
- **Triagem:** Avaliar, Categorizar e Priorizar o evento.
- **Análise:** Entender o incidente.
- **Respostas:** Ações para resolver o incidente.
- **Coleta de Evidências:** Definir e aplicar procedimentos para a identificação, coleta, aquisição e preservação das informações que podem ser usadas como evidências do evento ocorrido

5. PRINCIPAIS AMEAÇA

Este plano deve ser acionado quando da ocorrência de cenários de incidentes que apresentam risco à continuidade da prestação dos serviços.

EVENTO / INCIDENTE	POSSÍVEIS CAUSAS
Interrupção do fornecimento de energia elétrica	Causada por fator externo à rede elétrica da empresa ou de sua localidade com duração da interrupção superior a 12 horas e/ou fator interno que comprometa a rede elétrica da empresa com curtos-circuitos, incêndio e infiltrações.
Falha na climatização do ambiente dois servidores	Superaquecimento dos ativos devido a falha no dimensionamento de carga na sala, principalmente nos servidores e switches.
Indisponibilidade de rede / Internet / Circuitos	Rompimento de cabos de interconexão decorrente de efeitos internos ou externos como a execução de obras, intempéries, desastres naturais ou acidentes.
Falha humana	Acidente ao manusear equipamentos críticos.
Ataques internos	Ataque aos ativos da empresa (Invasão nos bancos de dados de colaboradores).
Incêndio	Incêndios que comprometam os serviços da empresa.

Desastres Naturais	Terremotos, tempestades, alagamentos etc.
Falha de hardware	Falha que necessite reposição de peça ou reparo, cujo reparo ou aquisição dependa de processo de compra e/ou disponibilidade em fornecedores.
Ataque cibernético	Ataque virtual que comprometa o desempenho, os dados ou configuração dos serviços e sistemas que a empresa utiliza.
Vazamento de Informações	Usuário mal-intencionado ou invasor que consiga compartilhar informações de funcionários, terceiros e/ou de clientes.

6. PAPÉIS E RESPONSABILIDADES

6.1. COMITÊ DE SEGURANÇA E PROTEÇÃO DE DADOS PESSOAIS

- Avaliar o Plano de Continuidade de Negócios periodicamente e decidir pelo seu acionamento quando da ocorrência de incidentes, respondendo em nível institucional pela execução do plano e demais ocorrências relacionadas.
- Acompanhar as iniciativas relacionadas à temática de proteção de Dados Pessoais da DMS LOGISTICS, incluindo os treinamentos dos Usuários da Informação, eventos relacionados a Incidentes de Segurança e status do processo de implementação das ferramentas/softwares de privacidade.
- Analisar relatório(s) da DMS LOGISTICS quanto a incidentes de Segurança com o envolvimento de Dados Pessoais, com o apoio de SI e do Encarregado de Dados.
- É o responsável por todas as comunicações durante um desastre. Especificamente, eles se comunicarão com os funcionários, clientes, autoridades, fornecedores e até mesmo com a mídia, se necessário.
- O líder desta equipe é o CISO, que administrará e manterá o Plano de Administração de Crise. Ele deverá dar suporte para a Alta Administração da DMS LOGISTICS sobre decisões a tomar a respeito de tratamentos de Dados Pessoais que apresentem riscos, como resultados de avaliações de impacto

à proteção de Dados Pessoais, e a violação de Dados Pessoais.

- Fornece a infraestrutura de servidor necessários para que a equipe de TI execute suas operações e processos essenciais durante uma contingência.
- Garante que as atividades essenciais funcionam como exigido para atender aos objetivos de negócios em caso de descontinuidade das atividades por alguma razão;
- Providência que os colaboradores assinem um termo de responsabilidade e confidencialidade de informações;
- Faz divulgação ampla e monitora o uso correto de informações e segurança de dados da empresa, de colaboradores e de clientes, para atender e cumprir a Lei 13.709/2018 – Lei Geral de Proteção de Dados (LGPD) e a ISO 27001.
- Aprova e empreende ações ou investimentos que promovam a melhoria contínua do processo.
- Apoia sempre que necessário na interação e no escalonamento com as demais áreas a fim de prover um atendimento mais rápido ao processo.
- Apoia os procedimentos de averiguação interna, quando necessário.
- Cria e gerencia equipe de resposta a incidentes de segurança.

6.2. SI

- Revisar esta Política e propor alterações.
- Criar um plano de resposta a Incidentes de Segurança.
- Classificar a gravidade dos Incidentes de Segurança ocorridos.
- Estabelecer e aprimorar programas e sistemas de prevenção de Incidentes de Segurança.
- Monitorar os sistemas de segurança da informação.
- Elaborar relatórios periódicos sobre Incidentes de Segurança ocorridos.
- Analisar e efetuar a coleta de evidências técnicas nos casos de incidentes de segurança.

- Investigar incidentes de segurança, reportando as informações pertinentes ao evento envolvendo Dados Pessoais ao Encarregado de Dados, sugerindo as medidas técnicas a serem adotadas.
- Analisar Reporte de Incidentes de Segurança, bem como apoiar o Encarregado de Dados nos processos de investigação do incidente e na elaboração do Relatório de Incidente de Violação de Dados Pessoais.
- Caso o Incidente de Segurança envolva Dados Pessoais, notificar o Encarregado de Dados para reportá-lo ao Comitê de Proteção de Dados.
- Determinar o monitoramento contínuo do ambiente tecnológico do ponto de vista de segurança da informação, visando identificar eventos que possam causar impacto na disponibilidade, integridade e confidencialidade de Dados Pessoais que sejam tratados pela DMS LOGISTICS.
- Seguir todas as fases descritas neste documento, desde a identificação até a solução do incidente.
- Comunicar às áreas responsáveis pelo gerenciamento de mudanças em caso de incidentes de violação de Dados Pessoais que envolvam impactos no ambiente de produção.
- Apoiar com as medidas técnicas necessárias para contenção/recuperação do incidente.
- Monitorar o cumprimento desta Política.

6.3. ENCARREGADO DE DADOS

- Após análise do Reporte de Incidente de Segurança por SI e ter sido notificado a respeito de possível Incidente de Violação de Dados Pessoais, elabora o Relatório de Incidente de Violação de Dados Pessoais, com o apoio do Gestor, bem como TI e SI.
- Elaborar relatório sobre riscos a tratamentos de Dados Pessoais e incidentes de violação de Dados Pessoais ao Comitê de Segurança e Proteção de Dados Pessoais.
- Iniciar processos de investigação do Incidente de Violação de Dados e indicar as áreas envolvidas que deverão participar do processo.

- Avaliar a necessidade de comunicação do Incidente de Violação de Dados Pessoais para a Autoridade Nacional de Proteção de Dados e aos Titulares de Dados Pessoais, com o reporte prévio ao Comitê de Segurança e a Diretoria.
- Acompanhar e apoiar a implementação dos planos de ação para correção de gaps das iniciativas de privacidade.
- Orientar a área de SI sobre medidas de segurança que deverão ser implementadas nos sistemas, conforme diretrizes da ANPD.
- Responsabilizar-se pela interface com a ANPD, sempre que for necessário.

6.4. DIRETORIA

- Tomar conhecimento, por meio do Comitê de Segurança e Proteção de Dados Pessoais, e providências sobre casos de Incidentes e Violação de Dados Pessoais que tiverem desdobramentos para fora da DMS LOGISTICS e que envolvam a imprensa ou comunidade externa.
- Caso os incidentes de Segurança envolvam Dados Pessoais, o respectivo conhecimento pela Diretoria se dará por meio do Comitê de Segurança da Informação.

6.5. TI

- Aprovar e empreender ações ou investimentos que promovam a melhoria contínua do processo.
- Auxiliar na análise dos incidentes de violação de Dados Pessoais por meio da apresentação das trilhas de auditoria dos sistemas sob sua gestão.
- Analisar e efetuar a coleta de evidências técnicas nos casos de incidentes de segurança.
- Investigar incidentes de segurança com envolvimento de Dados Pessoais, reportando as informações pertinentes ao evento ao Encarregado de Dados, SI e Comitê de Segurança, sugerindo as medidas técnicas a serem adotadas.
- Auxiliar nos processos de investigação dos incidentes quando requerido.
- Apoiar com as medidas técnicas necessárias para contenção/recuperação dos incidentes.

7. ACIONAMENTO DAS EQUIPES DE GERENCIAMENTO DE INCIDENTES

Este plano será acionado quando da ocorrência de algum dos cenários de incidentes, a insurgência ou ocorrência de um risco desconhecido ou caso uma vulnerabilidade tenha grande possibilidade de ser explorada. O plano também poderá ser acionado em casos de testes ou por determinação da alta administração da empresa para avaliar sua eficiência, eficácia e efetividade.

Em caso de incidente, devem ser acionados os responsáveis abaixo elencados:

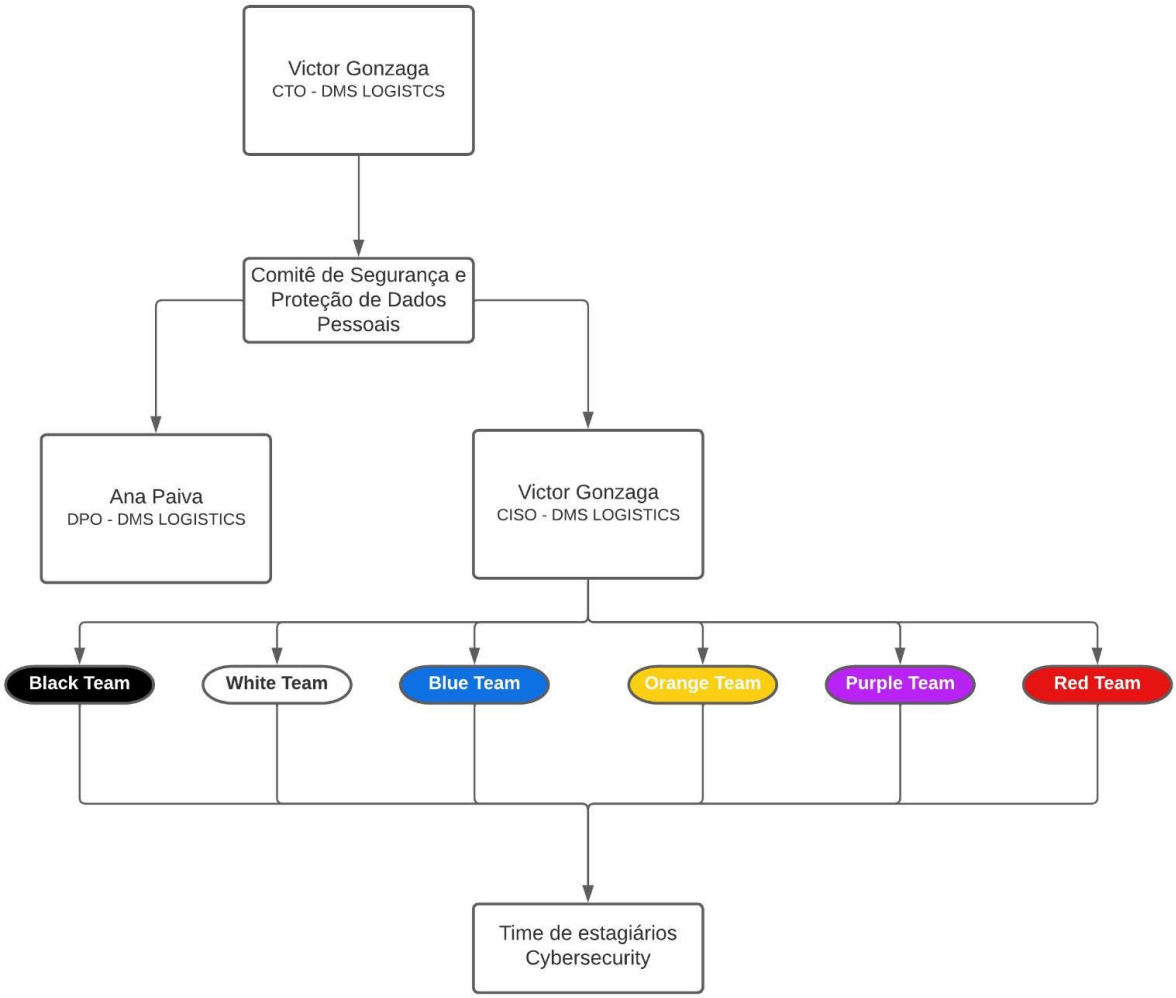
Integrantes do Comitê de Segurança e Proteção de Dados Pessoais

CONTATO	FUNÇÃO / ÁREA	E-MAIL
Victor Gonzaga	CISO	victor.gonzaga@dmslog.com
Ana Paiva	DPO / Head do RH e DP	dpo@dmslog.com
Natalie Corrêa	Membro / Team Leader Suporte e Qualidade	natalie.correa@dmslog.com
Monique Pestana	Membro / Team Leader DevOps e QA	monique.pestana@dmslog.com
Felipe Lage	Membro / Team Leader Desenvolvimento	felipe.lage@dmslog.com
Leonardo Sabbadim	Membro / Team Leader Garantia de Qualidade	leonardo.sabbadim@dmslog.com

Integrantes da Equipe de Gerenciamento de Incidentes

CONTATO	FUNÇÃO / ÁREA	E-MAIL
Victor Gonzaga	CISO	victor.gonzaga@dmslog.com
Ana Paiva	DPO / White Team	dpo@dmslog.com
xx	Blue Team Leader	dpo@dmslog.com
xx	White Team Leader	dpo@dmslog.com
xx	Orange Team Leader	dpo@dmslog.com
xx	Red Team Leader	dpo@dmslog.com

8. ORGANOGRAMA DA EQUIPE DE GERENCIAMENTO DE INCIDENTES DE SEGURANÇA



9. PRIORIZAÇÃO DOS INCIDENTES

São os seguintes serviços considerados essenciais, por ordem de priorização, para o acionamento e execução deste plano.

Serviço / Área	Criticidade
Segurança da Informação e TI	Alta
Monitoramento com recursos tecnológicos	Alta
Barramento de serviços e controle de senhas	Alta
Links de Internet	Alta
E-mail institucional/webmail	Baixa

RH	Média
VPN	Baixo

10. SANÇÕES E PUNIÇÕES

As violações, mesmo que por mera omissão, negligência, imprudência ou tentativa não consumada de violação a esta Política bem como demais normas e procedimentos de segurança, serão passíveis de medidas disciplinares.

O Comitê de Segurança e Proteção de Dados Pessoais, em Incidentes de Segurança e Violação de Dados Pessoais, e o Encarregado de Dados, em casos de Violação de Dados Pessoais, apoiarão os procedimentos de averiguação interna, quando necessário.

Os procedimentos de averiguação e aplicação de medidas disciplinares obedecerão aos normativos internos e decisões da Diretoria.

No caso de terceiros contratados ou prestadores de serviço, a estrutura de Segurança da Informação deve analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato.

11. CASOS OMISSOS

Os casos omissos serão avaliados pelo Comitê de Segurança e Proteção de Dados Pessoais para posterior deliberação.

As diretrizes estabelecidas nesta Política e nas demais normas e procedimentos de segurança, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui rol taxativo, sendo obrigação do usuário da informação da DMS LOGISTICS adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção às informações da DMS LOGISTICS.

12. IMPLEMENTAÇÃO E ATUALIZAÇÃO

A Política de Gerenciamento de Incidentes de Segurança da DMS LOGISTICS deve ser atualizada sempre que necessário ou em um intervalo não superior a 01 (um) ano.

13. ANEXO A – FORMULÁRIO DE REPORTE DE INCIDENTES DE SEGURANÇA

Nome:

Cargo:

Área/Departamento:

Descrição do Incidente ou suspeita de Incidente:

Data e hora que o incidente foi descoberto:

Natureza do dado envolvido (quando possível):

Informações sobre os titulares impactados (quando possível):

Locais e sistemas afetados:

O incidente foi solucionado? Em quanto tempo? De que maneira?

Potenciais impactos do incidente: [Danos aos sistemas/perda de dados/violação da legislação/violação de políticas internas]

Há ou se desconfia que haja o envolvimento de algum Colaborador no incidente de segurança? Se sim, qual o nome e qual foi a participação deste Colaborador?

14. ANEXO B – FORMULÁRIO DE INCIDENTE DE VIOLAÇÃO DE DADOS PESSOAIS

Parte 1 - Notificação de Violação de Dados Pessoais	
Informações	**DADOS A SEREM PREENCHIDOS PELA ÁREA**
Data do incidente	
Data de descoberta do incidente	
Local do incidente	

Países afetados (se aplicável)	
Nome do colaborador responsável por identificar os incidentes	
Detalhes de contato do colaborador responsável por identificar o incidente	
Breve descrição do incidente	
Número de titulares de Dados Pessoais afetados	
Dados Pessoais foram colocados em risco? Favor detalhar	
Breve descrição das medidas adotadas após descoberta do incidente	
Preenchimento pelo Encarregado pela Proteção de Dados Pessoais	
Recebido por:	
Data de recebimento:	
Áreas a serem envolvidas:	
Data de notificação de envolvimento das demais áreas:	
PARTE 2 – AVALIAÇÃO DE SEVERIDADE	
Detalhes de sistemas, equipamentos, registros envolvidos no incidente	
Detalhes de quais dados foram alvo de violação (destruição, alteração indevida, compartilhamento indevido etc.)	

Natureza/categoria dos dados alvo do incidente de Dados Pessoais (tipos de dados envolvidos)	
Volume de dados afetados pelo incidente	
Há salvaguarda desta informação? Caso não haja, esta Violação de Dados Pessoais pode ter feitos operacionais, legais e reputacionais para a Empresa?	
Quantos indivíduos foram afetados?	
Há Dados Pessoais sensíveis envolvidos?	
Há Dados Pessoais de menores envolvidos?	
Foi possível identificar todos os envolvidos no incidente ocorrido?	
A violação de Dados Pessoais afeta algum direito ao titular, que é garantido pela legislação de proteção de dados?	
A Informação caso acessada por terceiros pode ser utilizada para fins ilícitos? Ex.: cadastros, compras e abertura de contas em banco.	
PARTE 3 – MEDIDAS TOMADAS	
Medidas técnicas e legais adotadas	
Planos de ação recomendados	

Necessária notificação para Autoridade Nacional de Proteção de Dados? De quais países? (se necessário)	
Necessária notificação para Titulares de Dados Pessoais?	
Necessária notificação para outras partes interessadas?	
Quais medidas de segurança são aplicáveis à área/recurso originário do incidente?	
ASSINATURAS	
Usuário da Informação:	
Encarregado de Dados:	
Data:	
Avaliação e decisão do Comitê de Proteção de Dados:	

15. ANEXO C – NOTIFICAÇÃO À AUTORIDADE

15.1. COMUNICAÇÃO

- Tipo de comunicação:
  - Completa.
  - Parcial.
- Para comunicação parcial:
  - Preliminar.
  - Complementar.

- Critério para a comunicação:
    - O incidente de segurança pode acarretar risco ou dano relevante aos titulares.
    - Não tenho certeza sobre o nível de risco do incidente de segurança.

15.2. AGENTE DE TRATAMENTO

O notificante é:

- Controlador.
- Operador.

Se operador, informar se já houve comunicação ao controlador: [Resposta]

Dados do agente de tratamento:

Número do CPF ou CNPJ: [XXX]

Nome ou Razão Social: [XXX]

Natureza da Organização (Pública ou Privada): [Resposta]

Endereço: [Resposta]

Cidade: [Resposta]

Estado: [Resposta]

CEP: [Resposta]

Telefone: [Resposta]

E-mail: [Resposta]

Dados do notificante:

Nome: [Resposta]

E-mail: [Resposta]

Telefone: [Resposta]

Dados do encarregado:

-Mesmos dados do notificante.

Nome: [Resposta]

E-mail: [Resposta]

Telefone: [Resposta]

15.3. INCIDENTE DE SEGURANÇA

Descreva de forma resumida como o incidente de segurança com dados pessoais ocorreu.

[Resposta]

Quando o incidente ocorreu?

[Data e hora]

-Não tenho conhecimento. Justifique: [Resposta]

-Não tenho certeza. Justifique: [Resposta]

Quando a organização teve ciência do incidente de segurança?

[Data e hora]

Descreva como a organização teve ciência do incidente de segurança.

[Resposta]

Se a comunicação inicial do incidente não foi comunicada no prazo sugerido de 2 dias úteis após ter tomado ciência do incidente, justifique os motivos.

[Resposta]

Se o incidente não foi comunicado de forma imediata após a sua ciência, justifique os motivos da demora.

[Resposta]

Qual a natureza dos dados afetados?

- Origem racial ou étnica.

- Convicção religiosa.
- Opinião política.
- Filiação a sindicato.
- Filiação a organização de caráter religioso, filosófico ou político.
- Dado referente à saúde.
- Dado referente à vida sexual.
- Dado genético ou biométrico.
- Dado de comprovação de identidade oficial (Por exemplo, n° RG, CPF, CNH).
- Dado financeiro.
- Nomes de usuário ou senhas de sistemas de informação.
- Dado de geolocalização.

Outros: [Resposta]

Qual a quantidade de titulares afetados?

[Resposta]

Qual a categoria dos titulares afetados?

- Funcionários
- Prestadores de serviço
- Clientes
- Consumidores
- Usuários
- Pacientes de serviço de saúde
- Crianças ou adolescentes

Outros: [Resposta]

15.4. MEDIDAS DE SEGURANÇA UTILIZADAS PARA A PROTEÇÃO DOS DADOS

Quais medidas de segurança, técnicas e administrativas, foram tomadas para prevenir a recorrência do incidente de segurança?

[Resposta]

Quais medidas de segurança, técnicas e administrativas, foram tomadas após a ciência do incidente de segurança?

[Resposta]

Quais medidas de segurança, técnicas e administrativas, foram ou serão adotadas para reverter ou mitigar os efeitos do prejuízo do incidente de segurança aos titulares dos dados?

[Resposta]

O agente de tratamento realizou relatório de impacto à proteção de dados pessoais?

[Resposta]

15.5. RISCOS RELACIONADOS AO INCIDENTE DE SEGURANÇA

Quais as prováveis consequências do incidente de segurança para os titulares afetados?

[Resposta]

Considerando os titulares afetados, na sua avaliação, o incidente pode trazer consequências transfronteiriças?

[Resposta]

15.6. COMUNICAÇÃO AOS TITULARES DE DADOS

Os titulares foram comunicados sobre o incidente de segurança com dados pessoais?

- Sim
- Não
- Não sei

Forneça detalhes.

[Resposta]

Caso os titulares afetados não tenham sido informados, quais são os motivos que justificam a não comunicação ou o seu retardo?

[Resposta]

Atenciosamente,

DMS LOGISTICS

16. ANEXO D – NOTIFICAÇÃO AO TITULAR

[DESTINATÁRIO]

[ENDEREÇO]

Prezado [Titular dos Dados Pessoais],

Lamentamos informá-lo sobre uma violação da segurança que resultou na [destruição OU perda OU alteração OU divulgação acidental [ou ilegal] OU acesso não autorizado] de seus Dados Pessoais.

A violação foi descoberta em [DATA] e provavelmente ocorreu em [DATA].

Como resultado de nossa investigação, concluímos que referida violação afeta os seguintes tipos de informações:

- [TIPOS DE INFORMAÇÃO. POR EXEMPLO, DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS].

A violação ocorreu nas seguintes circunstâncias e pelas seguintes razões:

- [CIRCUNSTÂNCIAS].
- [RAZÕES].

Tomamos as seguintes medidas para mitigar quaisquer efeitos adversos:

- [MEDIDAS].

Recomendamos que você tome as seguintes medidas para mitigar possíveis efeitos adversos:

- [MEDIDAS].

Informamos a Autoridade de Proteção de Dados sobre a violação em [DATA].

Eventuais esclarecimentos adicionais poderão ser obtidos por meio dos contatos abaixo indicados:

- [NOME DO CONTROLADOR DE DADOS]
- [NOME DO ENCARREGADO PELO TRATAMENTO DE DADOS]
- [ENDEREÇO]
- [NÚMERO DE TELEFONE]
- [ENDEREÇO DE E-MAIL]
- [ENDEREÇO DO WEBSITE].

Atenciosamente,

DMS LOGISTICS

17. ANEXO E – CLASSIFICAÇÃO DE INCIDENTES DE SEGURANÇA

Severidade	Legalidade	Confidencialidade	Integridade	Disponibilidade	SLA
Crítica	Falta legal de alto impacto que pode resultar em processo e multas altas. Não atendimento a dispositivos legais. Possibilidade de litígio de grande impacto. Ocorrência de descumprimento contratual com	Em caso de um incidente que afete sistemas ou serviços considerados relevantes pela DMS LOGISTICS, há consequências para vários processos de negócio internos e/ou externos, não previsíveis e de difícil gerenciamento. Possibilidade de exploração de vulnerabilidades por	Em caso de um incidente de segurança que afete sistemas ou serviços considerados como relevantes pela DMS LOGISTICS, há consequências para um ou mais processos de negócio internos e/ou externos, parcialmente previsíveis e de	Em caso de um incidente de segurança que afete sistemas ou serviços considerados como relevantes pela DMS LOGISTICS, há consequência para um ou mais processos de negócio interno e/ou externo, parcialmente previsível e de difícil gerenciamento. Paralisação das atividades de uma unidade de negócio da	0 a 2 horas

	terceiros e clientes.	atacantes decorrente do uso de informações tornadas públicas devido a incidente de segurança.	difícil gerenciamento. Possibilidade de tomada de decisão errônea por parte da DMS LOGISTICS devido à falta de integridade de informações afetadas por incidente de segurança.	DMS LOGISTICS ou de várias Áreas. Descontentamento dos colaboradores e clientes. (> 50 %).	
Alta	Falta legal de alto impacto que pode resultar em processo e multas altas. Não atendimento a dispositivos legais. Possibilidade de litígio de alto impacto. Ocorrência de descumprimento contratual com terceiros e clientes.	Em caso de um incidente de segurança que afete sistemas ou serviços pela DMS LOGISTICS, há consequências para vários processos de negócio interno e/ou externo, não previsíveis e de difícil gerenciamento. Possibilidade de exploração de vulnerabilidades por atacantes decorrente do uso de informações tornadas públicas devido a incidente de segurança.	Em caso de um incidente de segurança que afete sistemas ou serviços pela DMS LOGISTICS, há consequências para um ou mais processos de negócio internos e/ou externos, parcialmente previsíveis e de difícil gerenciamento. Possibilidade de tomada de decisão errônea por parte da DMS LOGISTICS devido à falta de integridade de informações afetadas por incidente de segurança.	Em caso de um incidente de segurança que afete sistemas ou serviços pela DMS LOGISTICS, há consequências para um ou mais processos de negócio internos e/ou externos, parcialmente previsíveis e de difícil gerenciamento. Paralisação das atividades de uma unidade de negócio da DMS LOGISTICS ou de várias Áreas. Descontentamento dos colaboradores e clientes (> 50 %).	0 a 2 horas
Média	Falta legal de alto impacto que pode resultar em processo e multas altas. Falta Legal com procedimentos de investigação de incidentes e/ou ilícitos.	Em caso de um incidente de segurança que afete sistemas ou serviços pela DMS LOGISTICS, há consequências para um ou mais processos de negócio internos e/ou externos, parcialmente previsíveis e gerenciáveis.	Em caso de um incidente de segurança que afete sistemas ou serviços pela DMS LOGISTICS, há consequências para um ou mais processos de negócio internos e/ou externos, parcialmente previsíveis e gerenciáveis.	Em caso de um incidente de segurança que afete sistemas ou serviços pela DMS LOGISTICS, há consequências para um ou mais processos de negócio internos e/ou externos, parcialmente previsíveis e gerenciáveis. Paralisação das atividades de uma unidade de negócio da DMS LOGISTICS. Descontentamento dos colaboradores e clientes (> 25 %).	Até 24 horas

Baixa	Falta legal de baixo impacto que pode resultar em processo e multas baixas.	Em caso de um incidente de segurança que afete sistemas ou serviços pela DMS LOGISTICS, há consequências para um ou mais processos de negócio internos e/ou externos, previsíveis e facilmente gerenciáveis.	Em caso de um incidente de segurança que afete sistemas ou serviços pela DMS LOGISTICS, há consequências para um ou mais processos de negócio internos e/ou externos, previsíveis e facilmente gerenciáveis.	Em caso de um incidente de segurança que afete sistemas ou serviços pela DMS LOGISTICS, há consequências para um ou mais processos de negócio internos e/ou externos, previsíveis e facilmente gerenciáveis. Paralisação das atividades de um pequeno grupo de usuários. Descontentamento dos colaboradores e clientes (> 25 %).	Até 48 horas

18. ANEXO F – PROCEDIMENTOS OPERACIONAIS EM CASO DE INCIDENTE

Está normativa indica quais os procedimentos operacionais devem ser adotados nos cenários apontados a seguir:

EVENTO / INCIDENTE	POSSÍVEIS CAUSAS
Interrupção do fornecimento de energia elétrica	Causada por fator externo à rede elétrica da empresa ou de sua localidade com duração da interrupção superior a 12 horas e/ou fator interno que comprometa a rede elétrica da empresa com curtos-circuitos, incêndio e infiltrações.
Falha na climatização do ambiente dos servidores	Superaquecimento dos ativos devido a falha no dimensionamento de carga na sala, principalmente nos servidores e switches.
Indisponibilidade de rede / Internet / Circuitos	Rompimento de cabos de interconexão decorrente de efeitos internos ou externos como a execução de obras, intempéries, desastres naturais ou acidentes.
Falha humana	Acidente ao manusear equipamentos críticos.
Ataques internos	Ataque aos ativos da empresa (Invasão nos bancos de dados de colaboradores).
Incêndio	Incêndios que comprometam os serviços da empresa.
Desastres Naturais	Tempestades, alagamentos etc.
Falha de hardware	Falha que necessite reposição de peça ou reparo, cujo reparo ou aquisição dependa de processo de compra e/ou disponibilidade em fornecedores.
Ataque cibernético	Ataque virtual que comprometa o desempenho, os dados ou configuração dos serviços e sistemas que a empresa utiliza.

Vazamento de Informações	Usuário mal-intencionado ou invasor que consiga compartilhar informações de funcionários, terceiros e/ou de clientes.

18.1. INTERRUPÇÃO DO FORNECIMENTO DE ENERGIA ELÉTRICA

Estas indicações são voltadas para a orientação e padronização dos procedimentos operacionais, em caso de falta de energia elétrica nas instalações físicas da DMS LOGISTICS. Elas devem ser seguidas por todos os colaboradores, independentemente da posição hierárquica.

A DMS LOGISTICS, em suas instalações físicas, utiliza a energia elétrica proveniente da concessionária de energia elétrica. Para minimizar o risco de perdas de dados e paralisação abrupta das atividades por falta de energia, a empresa utiliza nobreaks dimensionados à demanda atual.

Todos os equipamentos do DMS LOGISTICS estão conectados aos nobreaks, permitindo uma operação de desligamento segura.

Caso ocorra interrupção no fornecimento de energia elétrica, eles entram automaticamente em funcionamento, permitindo que os colaboradores tenham tempo para salvar o trabalho e desligar os equipamentos em segurança.

As ações a serem tomadas neste plano de contingência se dividem em quatro etapas:

1. Verificar se a pane elétrica atingiu as edificações vizinhas adjacentes. Se sim, ir para o passo 3. Se não, ir para o passo 2;
2. Verificar se a chave geral está desarmada. Em caso afirmativo, a causa poderá ter sido uma sobrecarga e poderá ser necessário desligar os equipamentos não essenciais que demandam mais energia, como ar-condicionado. Se o problema não foi identificado, acionar a concessionária de energia conforme passo 3;
3. Com o número de instalação em mãos ou cópia da conta de energia elétrica, ligar e informar a situação à Concessionária, registrar o número de protocolo e verificar a previsão de restabelecimento de energia. Em seguida, proceder o passo;
4. Desligar os equipamentos de acordo com os protocolos de segurança e retirá-los das tomadas, para evitar a sobrecarga quando a energia retornar.

A retomada das atividades está condicionada ao restabelecimento da energia elétrica e ao horário de funcionamento da empresa. Sendo assim, a gestão/coordenação deve avaliar a viabilidade de retomada das atividades para o mesmo dia ou para outro dia.

Após o retorno da energia elétrica, os equipamentos devem ser observados. Caso exista alguma anormalidade, ela deverá ser informada ao líder do setor. Se necessário, o líder comunicará o Comitê de Segurança e Proteção de Dados Pessoais sobre o problema, solicitando uma análise no equipamento.

A DMS LOGISTICS faz a manutenção preventiva dos seus equipamentos. Eles são revisados a cada 06 (seis) meses.

18.2. INDISPONIBILIDADE DE REDE/INTERNET

Estas indicações são voltadas para a orientação e padronização dos procedimentos operacionais, em caso de indisponibilidade de rede e/ou internet nas instalações físicas da DMS LOGISTICS. Elas devem ser seguidas por todos os colaboradores, independentemente da posição hierárquica.

Todos os colaboradores devem conhecer o passo-a-passo nessa normativa e estarem capacitados para executá-la.

Em caso de indisponibilidade de rede e/ou internet, os colaboradores deverão seguir o passo-a-passo abaixo:

Ao primeiro indício de indisponibilidade de rede e/ou internet, verifique a ocorrência de interrupção no fornecimento de energia elétrica; Caso afirmativo, com o número de instalação em mãos ou cópia da conta de energia elétrica, ligar e informar a situação à Concessionária, registrar o número de protocolo e verificar a previsão de restabelecimento de energia;

Caso seja identificado a interrupção no fornecimento de energia elétrica, verificar se no-breaks e geradores estão ativos;

Caso os no-breaks e geradores não estejam ativos, ativá-los e aguardar pelo período necessário para utilização dos equipamentos de rede e/ou internet e verificar se a indisponibilidade cessou;

Caso não haja interrupção no fornecimento de energia elétrica e/ou os no-breaks e geradores estejam ativos e seja identificado que a indisponibilidade da rede e/ou internet permanece:

Verificar se a indisponibilidade da rede e/ou internet se limita apenas a um dispositivo ou todos os dispositivos;

Desligar o(s) dispositivo(s) da rede elétrica por 1 (um) minuto e religá-los. Aguardar pelo período necessário para utilização dos equipamentos de rede e/ou internet

Caso a indisponibilidade da rede e/ou internet persista, acionar o departamento de Tecnologia da Informação (TI) para verificar condições de acesso, serviços de firewall e links de internet.

Detectado problema externo de internet, abrir um chamado de suporte com o provedor de serviços de internet, visando o restabelecimento do serviço. Informar a previsão do conserto ou solução aos demais servidores.

O Comitê de Segurança e Proteção de Dados Pessoais será convocado e determinará as ações para a recuperação do desastre e a continuidade de negócios, de acordo com a gravidade do caso.

18.3. FALHA HUMANA POR IMPRUDÊNCIA, IMPERÍCIA OU NEGLIGÊNCIA

Estas indicações são voltadas para a orientação e padronização dos procedimentos operacionais, em caso de falha humana nas instalações da DMS LOGISTICS. Elas devem ser seguidas por todos os colaboradores, independentemente da posição hierárquica.

Todos os colaboradores devem conhecer o passo-a-passo nessa normativa e estarem capacitados para executá-la.

- Em caso de falha humana, os colaboradores deverão seguir o passo-a-passo abaixo:
- Ao primeiro indício de falha humana, entrar em contato com o Comitê de Segurança e Proteção de Dados Pessoais e relatar os acontecimentos;
- Em seguida, seguir as orientações do Comitê;
- Na ausência ou demora nas orientações, isolar o dispositivo da rede,

desligando o dispositivo e desconectando todos os seus cabos;

O Comitê de Segurança e Proteção de Dados Pessoais será convocado e determinará as ações para a recuperação do desastre e a continuidade de negócios, de acordo com a gravidade do caso.

18.4. ATAQUES INTERNOS

Estas indicações são voltadas para a orientação e padronização dos procedimentos operacionais, em caso de ataques internos nas instalações da DMS LOGISTICS. Elas devem ser seguidas por todos os colaboradores, independentemente da posição hierárquica.

Todos os colaboradores devem conhecer o passo-a-passo nesta normativa e estarem capacitados para executá-la.

Em caso de ataque interno, os colaboradores deverão seguir o passo-a-passo abaixo:

- Ao primeiro indício de ataque interno, entrar imediatamente em contato com o Comitê de Segurança e Proteção de Dados Pessoais e relatar os acontecimentos;
- Em seguida, seguir as orientações do Comitê;
- Na ausência ou demora nas orientações, isolar o dispositivo da rede, desligando o dispositivo e desconectando todos os seus cabos;

O Comitê de Segurança e Proteção de Dados Pessoais será convocado e determinará as ações para a recuperação do desastre e a continuidade de negócios, de acordo com a gravidade do caso.

18.5. INCÊNDIO

Estas indicações são voltadas para a orientação e padronização dos procedimentos operacionais, em caso de incêndio nas instalações físicas da DMS LOGISTICS. Elas devem ser seguidas por todos os colaboradores, independentemente da posição hierárquica.

Todos os colaboradores devem conhecer o passo-a-passo nessa normativa e estarem capacitados para executá-la.

Em caso de incêndio, os colaboradores deverão seguir o passo-a-passo abaixo:

- Ao primeiro indício de incêndio, transmitir o alarme geral e chame imediatamente o Corpo de Bombeiros pelo telefone 193;
- Caso seja identificado um curto-circuito, desligar a chave elétrica geral;
- Tirar todos os equipamentos da tomada;
- Se for possível, utilizar o extintor de incêndio para combater as chamas no estágio inicial;
- Utilize o equipamento de combate ao fogo disponível nas áreas comuns da DMS LOGISTICS;
- Não sendo possível eliminar o fogo, abandonar o edifício rapidamente, pelas escadas. Ao sair, feche todas as portas atrás de si, sem trancá-las;
- Não utilizar o elevador como meio de escape;
- Não sendo possível abandonar o edifício pelas escadas, permanecer no pavimento em que se encontra, aguardando a chegada do Corpo de Bombeiros;
- Em condições de fumaça intensa cubra o rosto com um lenço molhado;
- Depois de estar em segurança, entrar em contato com o Comitê de Segurança e Proteção de Dados Pessoais e relatar os acontecimentos.

O Comitê de Segurança e Proteção de Dados Pessoais será convocado e determinará as ações para a recuperação do desastre e a continuidade de negócios, de acordo com a gravidade do caso.

18.6. DESASTRES NATURAIS (ALAGAMENTOS, TEMPESTADES)

Estas indicações são voltadas para a orientação e padronização dos procedimentos operacionais, em caso de alagamentos e tempestades que possam comprometer as instalações físicas da DMS LOGISTICS.

Elas devem ser seguidas por todos os colaboradores, independentemente da posição hierárquica.

Todos os colaboradores devem conhecer o passo-a-passo nessa normativa e estarem capacitados para executá-la.

- Desligar a chave elétrica geral;
- Desligar todos os equipamentos da rede elétrica.

Em caso de inundação, além dos passos acima, deve-se:

- Fechar imediatamente o registro da água, em caso de desastre causado por rompimento de tubulação hidráulica;
- Remover todos os equipamentos eletrônicos, a começar pelos mais sensíveis, do local do dano;
- Remover o acervo analógico como papéis e arquivos, para fora do local;
- Informar o Comitê de Segurança e Proteção de Dados Pessoais;
- Chamar auxílio - Corpo de Bombeiros, Defesa Civil, concessionária de energia elétrica ou profissional habilitado em hidráulica, de acordo com a situação.

18.7. FALHA DE HARDWARE

Estas indicações são voltadas para a orientação e padronização dos procedimentos operacionais, em caso de falha de hardware nas instalações da DMS LOGISTICS. Elas devem ser seguidas por todos os colaboradores, independentemente da posição hierárquica.

Todos os colaboradores devem conhecer o passo-a-passo nessa normativa e estarem capacitados para executá-la.

Em caso de falha de hardware, os colaboradores deverão seguir o passo-a-passo abaixo:

- Ao primeiro indício de falha de hardware, abrir chamado para o departamento de Tecnologia da Informação (TI), informando o equipamento, tipo de falha e data da ocorrência;
- Depois de abrir o chamado para TI, entrar em contato com o Comitê de Segurança e Proteção de Dados Pessoais e relatar os acontecimentos;

O Comitê de Segurança e Proteção de Dados Pessoais será convocado e determinará as ações para a recuperação do desastre e a continuidade de negócios, de acordo com a gravidade do caso.

18.8. ATAQUE CIBERNÉTICO

Estas indicações são voltadas para a orientação e padronização dos procedimentos operacionais, em caso de ataque cibernético nas instalações da DMS LOGISTICS. Elas devem ser seguidas por todos os colaboradores, independentemente da posição hierárquica.

Todos os colaboradores devem conhecer o passo-a-passo nesta normativa e estarem capacitados para executá-la.

Em caso de ataque cibernético, os colaboradores deverão seguir o passo-a-passo abaixo:

- Ao primeiro indício de ataque cibernético, entrar imediatamente em contato com o Comitê de Segurança e Proteção de Dados Pessoais e relatar os acontecimentos;
- Em seguida, seguir as orientações do Comitê;
- Na ausência ou demora nas orientações, isolar o dispositivo da rede, desligando o dispositivo e desconectando todos os seus cabos;

O Comitê de Segurança e Proteção de Dados Pessoais será convocado e determinará as ações para a recuperação do desastre e a continuidade de negócios, de acordo com a gravidade do caso.

18.9. VAZAMENTO DE INFORMAÇÕES

Estas indicações são voltadas para a orientação e padronização dos procedimentos operacionais, em caso de vazamento de informações nas instalações da DMS LOGISTICS. Elas devem ser seguidas por todos os colaboradores, independentemente da posição hierárquica.

Todos os colaboradores devem conhecer o passo-a-passo nesta normativa e estarem capacitados para executá-la.

Em caso de vazamento de informações, os colaboradores deverão seguir o passo-a-passo abaixo:

- Ao primeiro indício de vazamento de informações, entrar imediatamente em contato com o Comitê de Segurança e Proteção de Dados Pessoais e DPO

relatando os acontecimentos;

- Em seguida, seguir as orientações do Comitê e/ou DPO;
- Na ausência ou demora nas orientações, isolar o dispositivo da rede, desligando o dispositivo e desconectando todos os seus cabos;

O Comitê de Segurança e Proteção de Dados Pessoais e DPO serão convocados e determinarão as ações para a recuperação do desastre e a continuidade de negócios, de acordo com a gravidade do caso.

19. HISTÓRICO DE REVISÃO

Revisão	Data	Descrição
00	17/02/2023	Emissão do documento.
01	13/03/2023	Revisão e padronização do documento.

20. APROVAÇÃO E CLASSIFICAÇÃO DA INFORMAÇÃO

Elaborado por:	CyberSecurity Team	
Revisado por:	Leonardo Sabbadim	
Aprovador por:	Victor Gonzaga	
Nível de Confidencialidade:	x	**Informação Pública**
		Informação Interna
		Informação Confidencial
		Informação Sigilosa

NUNCA COLOCAMOS EM RISCO A QUALIDADE E NEM A ÉTICA NOS NEGÓCIOS

WE NEVER COMPROMISE ON QUALITY AND BUSINESS ETHICS