HΣMΣRA

# Política de Segurança da Informação

## Sumário

## Introdução

Atualmente, a informação é um dos ativos mais valiosos para a HEMERA ("HEMERA DTVM"), devendo ser adequadamente utilizada e protegida contra ameaças e riscos. A adoção de políticas e procedimentos que visem garantir a segurança da informação deve ser prioridade constante da empresa, reduzindo-se os riscos de falhas, os danos e/ou os prejuízos que possam comprometer a imagem e os objetivos da instituição.

A informação pode existir e ser manipulada de diversas formas, por meio de arquivos eletrônicos, mensagens eletrônicas, WEB, FTP, bancos de dados, em meio impresso, verbalmente, em mídias de áudio e de vídeo etc.  pode estar armazenada localmente (em servidores no Data Center Local, estações de trabalho, mídias eletrônicas, etc.) ou ainda no ambiente de computação em Nuvem (Servidores em Data Center remoto – Microsoft Azzure).

Por princípio, a segurança da informação deve abranger três aspectos básicos, destacados a seguir:

1. **Confidencialidade**: somente pessoas devidamente autorizadas pela empresa devem ter acesso à informação.
2. **Integridade**: somente alterações, supressões e adições autorizadas pela empresa devem ser realizadas nas informações.

3. **Disponibilidade**: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado.

Para assegurar esses três pilares, a informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem, perda não intencional, acidentes e outras ameaças. A proteção da informação não é uma tarefa trivial. Em geral, o sucesso da Política de Segurança da Informação adotada por uma instituição depende da combinação de 3 elementos, que são:

- ✓ Políticas;
- ✓ Procedimentos, sistemas e rotinas; e
- ✓ Pessoas.

**Objetivo**

A Política de Segurança da Informação da HEMERA DTVM é uma declaração formal da empresa acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus colaboradores. Os objetivos de segurança cibernética da instituição são garantir a confidencialidade, integridade e disponibilidade das informações e sistemas críticos, bem como assegurar a resiliência operacional frente a incidentes cibernéticos. A instituição atua de forma contínua para prevenir, por meio de controles de acesso, criptografia e conscientização de usuários; detectar, por meio de monitoramento centralizado, sistemas de alerta e análise de logs; e reduzir a vulnerabilidade, por meio de testes de vulnerabilidades, atualizações de sistemas e gestão de riscos.

### Aplicação e Abrangência

A Política de Segurança Cibernética é disponibilizada integralmente a todos os funcionários e prestadores de serviços terceirizados por meio do portal corporativo e de treinamentos de integração. Para prestadores de serviços críticos, a política é complementada por orientações específicas sobre as obrigações de segurança aplicáveis ao contrato.

### Política Disponibilizada ao Publico

Um resumo contendo as linhas gerais da Política de Segurança da Informação é publicado no site institucional e mantido atualizado, permitindo que clientes, parceiros e o público em geral conheçam os princípios e compromissos adotados pela instituição na proteção das informações e na prevenção de incidentes cibernéticos. Link: Manuais e Políticas - Hemera DTVM

### Estrutura Normativa da Segurança da Informação

### Definição

A estrutura normativa da Segurança da Informação da HEMERA DTVM é composta por um conjunto de documentos com três níveis hierárquicos distintos, relacionados a seguir:

- ✓ **Política de Segurança da Informação (Política)**: constituída neste documento, define a estrutura, as diretrizes e as obrigações referentes à segurança da informação;
- ✓ **Normas de Segurança da Informação (Normas)**: estabelecem obrigações e procedimentos definidos de acordo com as diretrizes da Política, a serem seguidos em diversas situações em que a informação é tratada;

- ✓ **Procedimentos de Segurança da Informação (Procedimentos)**: instrumentalizam o disposto nas Normas e na Política, permitindo a direta aplicação nas atividades da HEMERA DTVM.

**Divulgação e Acesso à Estrutura Normativa**

A Política e as Normas de Segurança da Informação devem ser divulgadas a todos os colaboradores e fornecedores da HEMERA DTVM.

Os Procedimentos de Segurança da Informação, em sua grande maioria, são restritos ao ambiente de Tecnologia da Informação e devem ser divulgados às áreas diretamente relacionadas à sua aplicação.

**Aprovação e Revisão**

Os documentos integrantes da estrutura normativa da Segurança da Informação da HEMERA DTVM deverão ser aprovados e revisados conforme os seguintes critérios:

- ✓ **Política:** deve ser aprovada pelo Diretor Responsável pela área de Compliance e gestão de riscos, após validação conjunta com a área de tecnologia da informação.
- ✓ **Periodicidade de Revisão:** Anual
- ✓ **Normas:** deve ser aprovada pelo Gestor ou supervisor de tecnologia da informação e Diretor Responsável pela área de Compliance e gestão de riscos.
- ✓ **Periodicidade de Revisão:** Anual
- ✓ **Procedimentos:** devem ser aprovados pelo Gestor responsável pela área envolvida junto ao gestor de Compliance e gestão de riscos.
- ✓ **Periodicidade de Revisão:** Anual

**Atribuições e Responsabilidades na Gestão de Segurança da Informação**

Cabe a **todos os colaboradores (funcionários, estagiários e prestadores de serviços)** da HEMERA DTVM:

- ✓ Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação da HEMERA DTVM;
- ✓ Buscar orientação junto ao superior imediato ou junto à área de Compliance, em caso de dúvidas relacionadas à segurança da informação;
- ✓ Formalizar a ciência através da assinatura do Termo de Confidencialidade no momento de sua contratação e do aceite desta Política e das Normas de Segurança da Informação, assumindo responsabilidade por seu cumprimento;
- ✓ Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pela HEMERA DTVM;
- ✓ Cadastrar senhas confiáveis, com alto padrão de complexidade, e garantir que em hipótese alguma sejam disponibilizadas a terceiros ou compartilhadas com outros colaboradores.
- ✓ Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela HEMERA DTVM;
- ✓ Comunicar imediatamente à área de Tecnologia da Informação qualquer descumprimento ou violação desta Política e/ou de suas Normas e Procedimentos.
- ✓ Todos os colaboradores no exercício de suas funções devem estar atentos a ocorrência de situações de conflito de interesses, e comunicar imediatamente sobre sua existência, ao seu gestor e área de Compliance, antes de qualquer decisão relativa ao fato.

**Gestores e suas Responsabilidades**

Os gestores são responsáveis pelas definições dos direitos de acesso de seus colaboradores aos sistemas e informações da HEMERA DTVM, cabendo a eles verificar se estão acessando exatamente as rotinas compatíveis com as suas respectivas funções, usando e conservando adequadamente os equipamentos, e mantendo cópias de segurança de seus arquivos individuais, conforme estabelecido nesta política.

**Alta Administração**

A alta administração participa ativamente da definição e acompanhamento das iniciativas de segurança cibernética, aprovando planos de ação, recursos e indicadores de desempenho relacionados ao tema. Reuniões periódicas de comitê são realizadas para avaliar resultados, riscos emergentes e necessidades de aprimoramento, reforçando o compromisso institucional com a melhoria contínua dos procedimentos de segurança.

**Compliance e Controles Internos**

A área de Compliance e Controles Internos, junto a área de Tecnologia da Informação, , poderá realizar auditorias periódicas internas sobre o acesso dos usuários às informações e sua retenção, verificando:

- ✓ Que tipo de informação o usuário pode acessar;
- ✓ Quem está autorizado a acessar determinada rotina e/ou informação;
- ✓ Quem acessou determinada rotina e informação;
- ✓ Quem autorizou o usuário a ter permissão de acesso à determinada rotina ou informação;
- ✓ Que informação ou rotina, determinado usuário acessou;

- ✓ Quem tentou acessar qualquer rotina ou informação sem estar autorizado.

A área de Controles Internos é responsável pelo mapeamento dos Processos e Riscos inerentes a todas as áreas de negócio e áreas de suporte. O escopo abarca a identificação de sistemas e atividades críticas, acesso a informações sigilosas e posições que possam gerar conflito de interesses pelos colaboradores no desempenho de suas atribuições.

Qualquer modificação na estrutura de acessos da Hemera DTVM (novo acesso, exclusão de acesso, alteração de perfil) somente será realizada a partir da aprovação da área de Controles internos, que é responsável pela atualização da Matriz de Controle e Segregação de Acessos (Eletrônicos e Físicos).

**Programa de Capacitação e Orientação**

A cultura de segurança cibernética é disseminada de forma contínua por meio de treinamentos obrigatórios para todos os colaboradores e prestadores de serviço, campanhas de conscientização periódicas, simulações de phishing e comunicados internos sobre boas práticas e riscos emergentes. Essas ações têm como objetivo reforçar comportamentos seguros e reduzir a vulnerabilidade humana frente a incidentes. Tais diretrizes são seguidas conforme a Política de Conformidade e Controles Internos.

A instituição mantém ações contínuas de orientação aos usuários finais sobre precauções na utilização dos produtos e serviços oferecidos. Essas orientações incluem comunicações no portal institucional, materiais educativos, notificações preventivas sobre golpes e vulnerabilidades emergentes, e instruções para uso seguro de canais digitais. Sempre que um novo serviço ou funcionalidade é lançado, são disponibilizados guias e alertas de segurança específicos.

### Área de Tecnologia da Informação

- ✓ É responsabilidade da área de TI, em conjunto com a área de Compliance, estabelecer, publicar, manter atualizada e disseminar normas relevantes ao conjunto de mecanismos contidos na política de segurança da informação;
- ✓ Adotar medidas estruturais como plano de comunicação, autoavaliação e revisões de auditoria que possam assegurar a conformidade com as políticas de segurança;
- ✓ Revisar e publicar políticas e materiais de conscientização anualmente ou sempre que houver mudanças significativas;
- ✓ Divulgar as normas de segurança da informação apenas aos colaboradores da HEMERA DTVM e fornecedores que tenham real necessidade de conhecê-las;
- ✓ Exceções às políticas serão tratadas caso a caso pela área de Tecnologia da Informação em conjunto com a área de Compliance. Todas as exceções, caso sejam aprovadas, devem ser documentadas, arquivadas e revisadas anualmente. Para aprovação de exceções serão requeridas justificativas de negócio completas e dependendo da exceção requerida, a aprovação final deve ser apenas fornecida pela diretoria;
- ✓ Dar ciência a todos os colaboradores e prestadores de serviço que os ambientes, sistemas, recursos computacionais e as redes da empresa poderão ser monitorados e gravados.

### Logs e Rastreio

Todas as ações relevantes realizadas nos sistemas corporativos são registradas em logs imutáveis, contendo identificação do usuário, data, hora e detalhes da operação. Esses logs são armazenados em repositório seguro e monitorados por solução SIEM (Security Information and Event Management), com retenção mínima de 12 meses e alertas

automáticos para atividades fora do padrão. Tais diretrizes são seguidas conforme a Política de Retenção de Logs.

**Penalidades**

O não cumprimento desta Política implica em falta grave e poderá resultar nas seguintes ações: **advertência formal, suspensão, multa, rescisão do contrato de trabalho, outra ação disciplinar e/ou processo civil ou criminal.**

**Documentos Vinculados**

Fazem parte desta Política as seguintes normas que definem as regras e restrições para funcionamento dos serviços:

I. Norma de Uso de e-mail Corporativo;
II. Norma de Uso de Software;
III. Norma de Segregação de Acessos;
IV. Norma de Classificação da Informação;
V. Norma de Uso da Internet;
VI. Norma de Utilização de Senhas;
VII. Norma de Uso Aceitável de Estações de Trabalho, Notebooks e Demais Dispositivos;
VIII. Norma de Backup;
IX. Norma de Gestão de Incidentes de Segurança;
X. Norma de Criptografia e Gestão de Chaves
XI. Norma de Desenvolvimento de Sistemas
XII. Norma para Gerenciamento de Vulnerabilidades
XIII. Norma de Serviços de Computação em Nuvem

XIV. Norma de Acesso Remoto via VPN

## I. Norma de Uso do E-mail Corporativo, Internet e Estação de Trabalho

### 1. Objetivo

As diretrizes completas sobre o uso da Internet, estações de trabalho e e-mail corporativo estão descritas na Política de Uso Aceitável, a qual deve ser observada integralmente por todos os colaboradores e prestadores de serviço.

## II. Norma de Uso de Softwares

### 1. Objetivo

O objetivo desta norma é definir um padrão para utilização de programas de computador de forma legal e segura dentro da HEMERA DTVM.

### 2. Abrangência

Esta norma se aplica a todos os usuários (colaboradores e prestadores de serviço) que utilizam tanto localmente quanto remotamente o ambiente computacional da HEMERA DTVM.

### 3. Definições

**Direito autoral** - Referente ao rol de direitos aos autores de suas obras intelectuais. **Licença de software** - É uma definição de ações autorizadas ou proibidas, no âmbito do direito de autor de um programador de software de computador concedidas ou impostas ao usuário deste software.

**Disco Virtual -** Ferramenta online para armazenamento de arquivos em nuvens, ou seja, em um ambiente *Web* acessível por qualquer computador, de qualquer local.

**4. Utilização de Programas**

1. Todos os direitos autorais devem ser respeitados e jamais violados.
2. Todos os programas de computador devem estar devidamente licenciados e as mídias originais devem ser devidamente protegidas contra cópia (se aplicável).
3. A instalação somente poderá ser feita pela área de Tecnologia da Informação da HEMERA DTVM.
4. As estações de trabalho disponibilizadas para uso dos colaboradores ou prestadores de serviço serão auditadas e monitoradas conforme as premissas de segurança. Os equipamentos que não estiverem de acordo serão retirados da rede.
5. A utilização, para fins profissionais, de ferramentas online para armazenamento, colaboração e compartilhamento de informações em nuvem (discos virtuais), deverá ser feita com cuidado e apenas pelo período necessário. A informação deverá ser removida imediatamente após seu uso ou compartilhamento. Observar e respeitar a Política de Classificação da Informação.

**5. Uso de Antivírus**

Todo arquivo em mídia proveniente de entidade externa a HEMERA DTVM deve ser verificado por programa antivírus. Todo arquivo recebido / obtido através do ambiente WEB, FTP, HD Externo/PenDrive e similares ou por meio de email, deve ser verificado por programa antivírus. Todas as estações de trabalho devem ter um antivírus instalado. A atualização do antivírus será automática, agendada pela área de Tecnologia da Informação. O usuário não pode, em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

6. **Software desenvolvido na HEMERA DTVM**

Todo software, componente ou artefato de software produzido dentro da HEMERA DTVM ou pelo grupo de empresas participantes é de propriedade da empresa ou de seus sócios, sendo vedado a divulgação sem a devida autorização.

**7. Ativos de TI**

Todos os ativos corporativos são protegidos por solução antimalware com atualização automática de assinaturas e monitoramento centralizado. O bloqueio de execução de arquivos maliciosos é reforçado por políticas de controle de aplicativos (whitelisting). Tais diretrizes são seguidas conforme a Política de Ativos de TI.

**8. Conclusão**

O não cumprimento das regras descritas nesta norma constitui falta grave e o usuário está sujeito a penalidades administrativas e/ou contratuais.

Situações não previstas e sugestões devem ser encaminhadas à área de Tecnologia da Informação ou a área de Compliance.

## III. Norma de Gestão e Segregação de Acessos

**1. Acessos ao ambiente**

Todos os acessos aos sistemas, aplicações e recursos tecnológicos da instituição são realizados por meio de mecanismos de autenticação seguros, contemplando, sempre que tecnicamente viável, a utilização de Autenticação Multifator (MFA) e parâmetros de senhas seguros. As credenciais são únicas, intransferíveis e mantidas sob responsabilidade do usuário, seguindo as diretrizes da Política de Gestão de Acessos.

**2. Acessos privilegiados**

A rede é microsegmentada em zonas de segurança distintas, sendo os acessos entre segmentos controlados de forma centralizada pelos firewalls implantados em todos os ambientes, complementados por controles de Segregação de Funções (SoD), de modo a reduzir riscos de uso indevido ou conflito de interesses.

## Norma de Classificação da Informação

**1. Objetivo**

Esta norma tem como objetivo definir requisitos para classificação da informação de forma a assegurar que as informações da HEMERA DTVM recebam um nível adequado de proteção.

**2. Escopo**

Todos os usuários da informação da HEMERA DTVM.

**3. Definições**

**Classificação da informação** - Processo através do qual o proprietário da informação atribui um grau de sigilo às informações.

**Grau de sigilo** – Graduação atribuída a ativos de informação considerados sigilosos em decorrência da sua natureza ou conteúdo.

**Informação** - Recursos de informação são definidos como qualquer dado criado, coletado, comunicado, usado ou observado por qualquer usuário de informação durante o seu período empregatício ou relacionamento com a HEMERA DTVM.

**Sigilo** - Segredo de conhecimento restrito a pessoas credenciadas e informação protegida contra revelação não autorizada.

## 4. Introdução

Toda informação, independente da forma como seja apresentada: arquivos eletrônicos, mensagens eletrônicas, WEB, bancos de dados, em meio impresso, verbalmente, em mídias de áudio e de vídeo (não se limitando apenas a estes), manipuladas no ambiente institucional ou fora dele, deverão indicar o nível de classificação da informação.

**Toda e qualquer outra forma de exposição da informação da HEMERA DTVM deve ser classificada e ter explícito o seu nível de confidencialidade.**

## 5. Gestor da informação

1. Todas as informações e ativos associados aos recursos de processamento da informação devem ter um gestor que será responsável por sua segurança.
2. É responsabilidade do gestor definir a classificação das informações e dos sistemas sob sua responsabilidade, realizar revisões periódicas e efetuar reclassificações quando necessário de forma a assegurar que os recursos de informação estejam no nível de classificação adequado.
3. As tarefas de rotina do gestor podem ser delegadas, por exemplo, para um custodiante que cuide do ativo/informação no dia a dia, porém a responsabilidade pela informação permanece com o gestor.

## 6. Níveis de classificação da informação

O grau de sigilo para os negócios da HEMERA DTVM considera os níveis descritos a seguir:

| **Níveis de classificação** | **Definição** |
|---|---|

| | |
|---|---|
| **Confidencial** | É o mais alto grau de sigilo e deve ser aplicado a informações estratégicas que somente devem ser de conhecimento de um grupo específico de pessoas. São considerados originariamente restritos, e devem ser classificados como tal, dados ou informações cujo conhecimento irrestrito ou divulgação possa acarretar qualquer risco, dano, dificuldade ou penalidade significativa para a HEMERA DTVM, seus clientes, parceiros comerciais ou colaboradores. Ex: Informações financeiras, planos estratégicos, informações jurídicas, dados de portadores de cartão, dados pessoais ou sensíveis que possam tornar uma pessoa identificável ou identificá-la. |
| **Interna** | São informações de uso interno, com circulação exclusiva dentro da empresa.<br>Estas informações podem estar disponíveis a alguns ou a todos empregados, terceiros, prestadores de serviço e parceiros comerciais a serviço da HEMERA DTVM. Exemplo: Documentos de serviços e produtos, o catálogo telefônico da empresa, procedimentos operacionais, organogramas, memorandos e manuais gerais internos são restritos ao uso exclusivo da empresa.<br>**Qualquer informação não rotulada deve ser considerada como "Proprietária".** |

| | |
|---|---|
| **Pública** | São passíveis de classificação Pública informações de circulação livre e domínio público. Esse tipo de informação não exige controles ou restrições de segurança com relação a acesso ou guarda. O sigilo da informação não é vital para a empresa.<br>Exemplo: Informações de marketing, notícias, site corporativo, relatórios anuais, etc. Material de propaganda e informativos, relatórios e outros devem ser considerados confidenciais até o momento de sua divulgação. |

**7. Mesa Limpa**

A Mesa Limpa é um programa que estabelece que todos os colaboradores têm responsabilidades ao manusear as informações da HEMERA DTVM. Por isso, nenhuma informação da HEMERA DTVM deve ser exposta sem cuidados especiais dentro ou fora do ambiente de trabalho, seja ela eletrônica ou em papel.

Todos os colaboradores, estagiários e prestadores de serviços devem assegurar que as informações internas restritas não sejam acessadas por pessoas não autorizadas.

Documentos contendo informações classificadas como Confidenciais ou Restritas devem permanecer dentro de gavetas ou armários trancados, evitando serem deixados sobre as mesas quando o colaborador, estagiário ou prestador de serviço se ausentar por períodos longos. Documentos que forem enviados para serem impressos nas impressoras devem ser recolhidos imediatamente por quem originou a impressão.

Da mesma forma, dispositivos de armazenamento de dados devem estar trancados em local seguro quando não estiverem em uso. Qualquer violação da política deve ser relata

imediatamente ao superior. O acesso à tela do monitor e o acesso ao microcomputador deve ser bloqueado sempre quando o colaborador se ausentar de sua mesa. Automaticamente após algum tempo o sistema operacional é bloqueado sendo necessário entrar com o *login* para desbloquear.

**8. Compartilhamento de Informações**

Não é permitido o compartilhamento de pastas locais dos micros dos colaboradores da HEMERA DTVM. Todos os dados deverão ser armazenados nos Servidores da Rede, e o controle de acessos e credenciais é gerenciado pela equipe de infraestrutura. A área de Tecnologia da Informação verifica periodicamente todos os compartilhamentos locais existentes nas estações de trabalho a fim de garantir que dados considerados confidenciais e/ou restritos deixem de estar armazenados na rede.

**9. Descarte das Informações**

As informações armazenadas em arquivos e diretórios e que não serão mais utilizadas deverão ser apagadas e removidas das lixeiras do sistema operacional.

Mídias contendo informações confidenciais ou sensíveis que não devam ser mantidas por mais tempo devem ser descartadas de forma segura, conforme disposto abaixo:

- ✓ Discos rígidos: formatação segura (no mínimo 7 passagens) ou inviabilizar fisicamente a utilização do disco.
- ✓ Discos magnéticos flexíveis: desintegrar, incinerar, triturar ou derreter.
- ✓ USB “thumb” drives, smart cards, e mídia digital: incinerar, pulverizar ou derreter.
- ✓ Discos óticos (CDs e DVDs): destruir a superfície ótica, incinerar, pulverizar, triturar ou derreter.
- ✓ Cópias impressas (recibos de papel, relatórios e faxes): fragmentação, fragmentação cruzada, incineração ou transformação em polpa.

**10. Conclusão**

As situações específicas devem ser registradas junto à Área de Tecnologia da Informação da HEMERA DTVM.

Fica estabelecido que qualquer informação de cliente será sempre classificada como confidencial e só poderá ser divulgada, mesmo para pessoas da HEMERA DTVM, com expressa autorização.

Informações da HEMERA DTVM que não estejam em áreas públicas devem, da mesma maneira, serem tratadas como informação confidencial e somente podem ser divulgadas, com expressa autorização do detentor da informação.

## IV. Norma de Backup

### 1. Objetivo

Definir as diretrizes sobre backup de dados e informações da HEMERA DTVM.

### 2. Diretrizes

Todos os dados da HEMERA DTVM deverão ser protegidos através de rotinas sistemáticas de Backup. Cópias de segurança do sistema integrado e servidores de rede são de responsabilidade da área de Tecnologia da Informação e deverão ser feitas diariamente. Todos os backups são enviados para o serviço de armazenamento Microsoft *Azzure,* fora da estrutura interna da instituição. Os backups só podem ser acessados e restaurados pela área de Tecnologia da Informação, através de *login* e senha, para evitar que pessoas não autorizadas tenham acesso a estes dados em caso de perda ou roubo da mídia. Deverá haver permanentemente um conjunto completo de sistema de backup capaz de restaurar todos os

dados da HEMERA DTVM em caso de sinistro. Para o servidor de arquivos, diariamente é realizado um backup Diferencial dos dados do servidor de arquivos e guardados devidamente no servidor externo de backup. O acesso a estes arquivos é direto, sem necessidade de descompactação. Somente a área de Tecnologia da Informação tem permissão de acesso aos arquivos de backup para fazer restauração e testes.

### *Cópia de Segurança de Arquivos em Desktops*

Não é política da HEMERA DTVM o armazenamento de dados em desktops individuais, entretanto, existem alguns programas que não podem ser acessados via URL e que não permitem o armazenamento diretamente em rede. Nestes e em outros casos, o setor de Tecnologia da Informação deverá alertar ao usuário que ele deve fazer backup dos dados de sua máquina periodicamente ou enviar os mesmos para o servidor de arquivos da HEMERA DTVM.

Há casos em que existe a necessidade de se fazer backups de e-mails de gerenciadores de e-mails com caixas de correio antigas do tipo POP.

É responsabilidade dos próprios usuários a elaboração de cópias de segurança ("backups") de dados e outros arquivos ou documentos, desenvolvidos pelos colaboradores, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos negócios da HEMERA DTVM.

No caso das informações consideradas de fundamental importância para a continuidade dos negócios da HEMERA DTVM o Setor de Tecnologia da Informação disponibilizará um espaço nos servidores onde cada usuário deverá manter estas informações. Estas informações serão incluídas na rotina diária de backup.

*Segurança e Integridade de Dados*

O gerenciamento dos bancos de dados, incluindo backup, restauração e sincronização, é de responsabilidade da área de Tecnologia da Informação da HEMERA DTVM, ainda que sejam utilizados serviços nativos do provedor de public cloud para automação e orquestração dessas rotinas. Os backups completos serão realizados diariamente e preservados conforme a política de retenção estabelecida, enquanto os diferenciais e incrementais deverão ser configurados de acordo com a criticidade de cada banco de dados. Para aqueles que armazenarem informações de alta relevância operacional ou dados de terceiros, deverá ser assegurada a realização de backups incrementais em periodicidade mínima de hora em hora, por meio de mecanismos como log shipping ou soluções equivalentes oferecidas pelo provedor de public cloud, podendo tal configuração ser ajustada segundo as necessidades de segurança da informação e da aplicação. Todos os backups deverão estar catalogados, armazenados em repositórios criptografados e sujeitos a controle de acesso restrito, sendo administrados em conformidade com o modelo GFS (*Grandfather, Father and Son*) de rotação de backups ou equivalente disponibilizado pelo provedor. O acesso a esses arquivos e rotinas de backup e restauração será restrito exclusivamente aos profissionais autorizados da área de Tecnologia da Informação e Infraestrutura de Sistemas.

## V.Norma de Gestão de Incidentes de Segurança

### 1. Objetivo

Esta norma tem como objetivo definir regras para a gestão de incidentes de segurança da informação de forma que eles sejam identificados, filtrados, analisados e respondidos em tempo hábil e que medidas apropriadas sejam tomadas para que estes incidentes não ocorram novamente.

Todos os incidentes de segurança cibernética classificados como relevantes para as atividades da instituição são registrados de forma estruturada, incluindo data, hora, sistemas e dados afetados, usuários envolvidos e a origem do incidente, inclusive informações recebidas de prestadores de serviços terceirizados.

A causa de cada incidente é analisada detalhadamente, identificando vulnerabilidades exploradas, falhas de procedimento ou eventuais deficiências de controles, e avaliando o impacto sobre a operação, clientes, dados sensíveis e imagem institucional. Os efeitos dos incidentes são controlados por meio de planos de ação corretivos e medidas de mitigação imediatas, incluindo isolamento de ativos, restauração de serviços, comunicação interna e, quando aplicável, comunicação a órgãos reguladores e entidades setoriais.

### 2. Definições

**Incidente de segurança** - Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas ou de redes que tragam riscos para nossos ativos e os ativos de nossos clientes.

**Vulnerabilidade** - Falha no projeto, implementação ou configuração de uma aplicação ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança.

**3. Relevância**

A avaliação da relevância de incidentes considera a gravidade do impacto, o alcance dos sistemas ou dados afetados, a possibilidade de violação de informações sensíveis, o potencial de indisponibilidade de serviços críticos e a exposição à imagem institucional. Incidentes classificados como relevantes são tratados com prioridade máxima e comunicados aos órgãos reguladores conforme a legislação aplicável.

Tais diretrizes são seguidas conforme o Plano de Continuidade de Negócios.

**4.Controles para Proteção de Informações Sensíveis.**

O ambiente corporativo conta com controles específicos para garantir a segurança das informações sensíveis, incluindo mecanismos de rastreabilidade completos. Todas as interações com dados classificados como confidenciais são registradas em logs invioláveis, contendo identificação do usuário, data, hora, origem e tipo de ação executada. Esses registros são coletados de forma centralizada por solução SIEM, com retenção mínima de 12 meses e alertas automáticos para atividades fora do padrão. O acesso a informações sensíveis é restrito por perfis de autorização pré-definidos e controlados pelo diretório corporativo, com trilhas de auditoria que permitem a reconstituição de qualquer evento.

**5.Compartilhamento de Incidentes Relevantes**

Os incidentes de segurança cibernética classificados como relevantes são reportados de forma estruturada e tempestiva às demais instituições financeiras e entidades setoriais com as quais a organização mantém relacionamento ou participa de fóruns de cooperação. Esse compartilhamento é realizado por meio de canais seguros, respeitando a confidencialidade das informações e as restrições legais aplicáveis. Sempre que possível, são incluídos detalhes

técnicos do incidente e medidas corretivas adotadas, visando contribuir para a prevenção de ocorrências semelhantes no setor.

**5. Registro e Notificação de Incidentes**

1. O gerenciamento de incidentes de Segurança da informação deve incluir, mas não se limitar aos seguintes eventos:
    1. Vazamento de Informações;
    2. Fraude;
    3. Comportamento anormal de sistemas (ex. reinicialização não programada do sistema, mensagens inesperadas, erros anormais em arquivos de log do sistema ou em terminais)
    4. Compartilhamento de senha;
    5. Notificações sobre eventos de segurança (ex. alertas de integridade de arquivos, alarmes de detecção de intrusos, alertas de antivírus, alarmes de segurança física).
    6. Uso indevido de recursos de tecnologia;
    7. Detecção de redes wireless no ambiente da HEMERA DTVM, etc.

2. O processo de registro e escalonamento de incidentes de segurança deve considerar, mas não se limitar a:
    1. Estabelecimento de processo adequado de registro de incidentes e descrição detalhada de todas as ações para solução de cada incidente de segurança, através do formulário de Registro de Ocorrências, disponibilizado pelo setor de Compliance aos gestores das áreas;
    2. Análise e identificação da causa do incidente;

3. Notificação do incidente aos membros do comitê de Compliance e risco e à diretoria para avaliação de instauração dos procedimentos para tratativas da ocorrência.
4. A comunicação a clientes, entidades externas e órgãos reguladores, quando aplicável, ficará sob responsabilidade da área de Compliance.;
5. Notificação da ação para os envolvidos;
6. Definição e divulgação do comportamento correto a ser tomado;

**6. Comunicação de Incidentes de Segurança**

1. A área de TI deve estabelecer um ponto de contato que seja conhecido de toda a organização e esteja disponível em regime 24x7 e em condições de assegurar uma resposta adequada e oportuna para os incidentes de segurança.
2. Um processo deve ser estabelecido para identificar vulnerabilidades recentemente descobertas. Procedimentos e padrões devem ser atualizados para endereçar as novas vulnerabilidades se necessário.
3. Procedimentos e padrões devem ser implementados especificando quando, por quem, as autoridades e as agências regulatórias que devem ser notificadas em caso de incidentes ou vulnerabilidades.
4. Todos os colaboradores devem ser conscientizados sobre os procedimentos para notificação dos diferentes tipos de eventos e vulnerabilidades que possam causar incidentes de segurança.
5. É esperado que os colaboradores permaneçam vigilantes a respeito de possíveis atividades fraudulentas.
6. Todos os incidentes e/ou vulnerabilidades de segurança devem ser imediatamente reportados ao ponto de contato designado na área de TI.

7. Quaisquer erros de software descobertos ou suspeitas de vulnerabilidades em sistemas devem ser reportados imediatamente para o gestor do sistema e para o responsável pela segurança da informação.
8. Deve ser estabelecido procedimento formal de registro e escalonamento estabelecendo a ação a ser tomada ao se receber a notificação de um evento de segurança da informação.
9. Informações relacionadas a incidentes de segurança devem ser divulgadas somente por pessoas autorizadas.

**7. Tratamento de Incidentes de Segurança**

1. Devem ser estabelecidos procedimentos que limitem o tempo de exposição de dados de clientes no caso de perda, roubo ou uso indevido.
2. Pessoal treinado e qualificado deve investigar incidentes/vulnerabilidades pesquisando a natureza e escopo dos mesmos e identificando que sistemas de informações sensíveis e tipos de informações sensíveis foram acessados ou usados indevidamente. Este pessoal deve tomar passos apropriados para conter e controlar o incidente e prevenir mais acessos não autorizados ou uso de informações sensíveis.
3. Incidentes de segurança gerados por falhas de sistema devem ser investigados por técnicos competentes.
4. Os colaboradores responsáveis pelo gerenciamento de incidentes devem ser suportados pelo gerenciamento em todas as solicitações razoáveis de assistência e ferramentas de forma a responder efetivamente a incidentes / vulnerabilidades.
5. O responsável pela Segurança da Informação deve responder de forma rápida e cautelosa aos incidentes de segurança significantes.

6. Caso seja constatada a possibilidade de processo jurídico quando um evento de segurança da informação for detectado, deve-se envolver o departamento jurídico imediatamente para obter consultoria sobre as evidências necessárias.
7. Informações específicas sobre incidentes de segurança, como, por exemplo, detalhes de uma invasão recente de sistema, não devem ser compartilhados com pessoas que não tiverem necessidade de saber justificável.

**8. Coleta de Evidências**

1. Devem-se estabelecer processos para coleta de evidências relacionadas a vulnerabilidades e incidentes.
2. Evidências relacionadas a suspeitas de vulnerabilidades devem ser registradas e tratadas de acordo com procedimentos de segurança estabelecidos.
3. A divulgação e/ou armazenamento de evidências só poderá ser feito por pessoas autorizadas.

**9. Prevenção de Vazamento de Informações**

A prevenção de vazamento de dados é realizada por meio de solução DLP (Data Loss Prevention) integrada ao gateway de e-mail e ao endpoint corporativo, com políticas específicas para bloqueio de envio de informações confidenciais para domínios externos não autorizados.

## VI. Norma de Criptografia e Gerenciamento de Chaves

**1. Objetivo**

Todas as informações classificadas como sensíveis ou confidenciais são protegidas por criptografia AES-256 quando em repouso, e por TLS 1.2 ou superior quando em trânsito, garantindo a integridade e a confidencialidade dos dados.

## 2. Definições

**Algoritmo de criptografia** - É um conjunto de funções matemáticas que, executadas em um texto, determinam de que forma a mensagem será cifrada.

**Criptografia** - Métodos de proteção de informações pelos quais apenas os detentores de um determinado segredo denominado "chave", têm acesso a elas. Informações criptografadas, mesmo quando capturadas em trânsito pela rede, não podem ser lidas por quem não conhece a chave necessária.

**Chave de criptografia** - É um parâmetro que controla a operação do algoritmo de criptografia. A chave especifica a transformação do texto aberto em texto cifrado ou a transformação do texto cifrado em texto aberto.

**Confidencial (informação)** - Informação que não pode estar disponível ou ser divulgada a indivíduos, entidades ou processos sem autorização.

## 3. Gerenciamento de Chaves

1. Chaves de criptografia são confidenciais e devem receber tratamento adequado de acordo com o as regras de manuseio, armazenamento e transmissão de informações.
2. Chaves de criptografia não devem ser reveladas para consultores, contratantes ou outros terceiros.
3. Deve haver cópias de backup das Chaves de criptografia.
4. Se for utilizada criptografia para proteger dados sensíveis armazenados em mídia, as chaves criptográficas e os materiais usados no processo de criptografia não devem ser armazenados em qualquer local desta mídia de armazenamento.

**4. Geração e armazenamento de chaves**

1. As chaves de criptografia devem preferencialmente ser geradas por um software homologado pela organização e quando forem geradas manualmente, devem ser manuseadas por um grupo restrito de pessoas.
2. O uso de algoritmos proprietários de criptografia não é permitido, a menos que seja explicitamente aprovado pela Segurança da Informação.
3. As chaves armazenadas nos dispositivos de criptografia não devem ser mostradas em texto aberto.
4. Os equipamentos utilizados para gerar, armazenar e guardar as chaves devem ser fisicamente protegidos.
5. As chaves de criptografia devem ser armazenadas em local seguro no menor número de localidades possível.

**5. Custódia e distribuição de chaves**

1. Acesso a chaves de criptografia deve ser limitado a aqueles que tenham necessidade de negócio comprovada.
2. Antes de ter acesso a uma chave de criptografia, o custodiante deve assinar um termo de responsabilidade fornecido pela HEMERA DTVM declarando comprometimento com a confidencialidade das referidas informações.
3. A distribuição de chaves deve ser realizada preferencialmente de maneira automatizada.

**6. Revogação, substituição e recuperação de chaves**

1. Toda vez que um novo certificado digital for gerado, o certificado antigo correspondente deve ser revogado.
2. Chaves criptográficas que tenham sido comprometidas ou reveladas devem ser imediatamente revogadas ou substituídas.

## VII. Norma de Desenvolvimento de Sistemas

### 1. Referência

As diretrizes e controles relacionados ao desenvolvimento seguro de sistemas e aplicações, incluindo práticas, padrões, responsabilidades e requisitos técnicos, estão descritos de forma detalhada na Política de Desenvolvimento Seguro da HEMERA DTVM, a qual deve ser observada integralmente por todos os colaboradores e terceiros envolvidos no ciclo de vida do software.

## VIII. Norma para Gerenciamento de Vulnerabilidades

### 1. Infraestrutura

A infraestrutura de rede é protegida por firewalls configurados com regras de acesso restritivas e monitoramento de tráfego em tempo real. São utilizados sistemas de detecção e prevenção de intrusão (IDS/IPS) integrados à solução de segurança centralizada, com alertas enviados automaticamente ao time de segurança.

### 2. Testes de invasão

Em paralelo, são realizados testes de invasão por fornecedor especializado e são realizadas varreduras de vulnerabilidades mensais por ferramenta automatizada, abrangendo servidores, estações e aplicações críticas. As vulnerabilidades identificadas são tratadas conforme procedimento interno de gestão de vulnerabilidades. Tais diretrizes são seguidas conforme a Política de Gestão de Vulnerabilidades

## IX. Norma de Serviços de Computação em Nuvem

### 1. Referência

As diretrizes, requisitos e responsabilidades para a utilização segura de serviços, plataformas e infraestruturas de computação em nuvem pela HEMERA DTVM estão descritos na Política de Segurança em Nuvem. Este documento deve ser consultado para orientações sobre seleção de provedores, configuração de ambientes, controle de acessos, proteção de dados, monitoramento e conformidade com exigências legais e regulatórias aplicáveis.

## X. Norma de Gestão de Continuidade de Negócios

### 1. Referência

Os testes de continuidade contemplam cenários de incidentes que afetam a operação dos serviços de pagamento e sistemas críticos, incluindo indisponibilidade de data center, ataques de ransomware, falhas de conectividade, indisponibilidade de prestadores de serviços essenciais e corrupção de dados. Esses cenários são revisados anualmente para refletir mudanças no ambiente tecnológico e nas ameaças cibernéticas. Tais diretrizes são seguidas conforme a Política de Gestão de Continuidade de negócios.

## XI. Norma de Gestão de Terceiros

### 1. Referência

Os contratos com prestadores que manuseiam dados sensíveis ou que executam atividades relevantes para as operações incluem cláusulas obrigatórias de segurança cibernética, exigindo a adoção de procedimentos e controles equivalentes aos aplicados internamente. Isso abrange uso de autenticação multifator, criptografia, monitoramento de acessos e

registro de atividades etc. O cumprimento dessas obrigações é avaliado por meio de auditorias periódicas e relatórios de conformidade enviados pelo prestador.

Tais diretrizes são seguidas conforme a Política de Contratação de Serviços Terceirizados.

**Verificação e Atualização**

- ✓ Esta política será atualizada a cada 12 (doze) meses, ou sempre que houver alterações, e tal atualização seguirá o mesmo fluxo de aprovação e divulgação.
- ✓ A área de *Tecnologia da Informação* é a responsável final por toda e qualquer alteração, atualização e divulgação.
- ✓ Este documento foi aprovado pela Diretoria da HEMERA DTVM, no Comitê de Compliance e Riscos.

**Controle de Versão**

O controle de versão deste documento, incluindo a identificação dos responsáveis pela sua elaboração, revisão e aprovação, encontra-se disponível no sistema gerencial de Compliance, garantindo rastreabilidade, transparência e adequada governança do processo.