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 da Política de Segurança da Informação

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. Seu propósito é estabelecer as diretrizes a serem seguidas pela instituição no que diz respeito à adoção de procedimentos e mecanismos relacionados à segurança da informação. As

diretrizes e controles implementados e utilizados na HEMERA DTVM se estendem ao ambiente de computação em Nuvem, de forma que possa garantir a prevenção, detecção e mitigação dos riscos de incidentes de segurança.

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.

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).

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.

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

Aprovações da Política

Este documento foi aprovado pela Diretoria da HEMERA DTVM, no Comitê de Compliance e Riscos.

I. Norma de Uso do E-mail Corporativo

1. Objetivo

O objetivo desta norma é estabelecer regras e requisitos de segurança para o uso do e-mail corporativo da HEMERA DTVM.

2. Definição

O e-mail é a ferramenta de comunicação interna e externa necessária para realização dos negócios da HEMERA DTVM.

3. Utilização do E-mail

1. As mensagens enviadas devem ser escritas em linguagem profissional de forma que não comprometa a imagem da empresa, não viole a legislação vigente, os princípios éticos e nossos valores.
2. A utilização do e-mail é individual, sendo o usuário responsável pelo conteúdo enviado através dele. A utilização do e-mail deve ser feita apenas para fins profissionais.
3. Não devem ser enviados e-mails com mensagens ou imagens que:
    1. Possam prejudicar a imagem da HEMERA DTVM, de seus colaboradores ou de qualquer outra organização;
    2. Contenham declarações difamatórias ou ofensivas de qualquer natureza;
    3. Contenham informações preconceituosas com qualquer classe, como raça, sexo, idade, religião, condição física etc.;
    4. Contenham informações pornográficas, obscenas ou qualquer outra, inadequada para o ambiente profissional;
    5. Que incentivem atividades ilegais;
    6. Sejam classificadas como SPAM, correntes, etc.
4. Não deve ser reproduzido ou divulgado material que infrinja direitos autorais, sem a permissão do autor.
5. Não devem ser enviadas mensagens em nome da HEMERA DTVM que contenham opiniões pessoais ou políticas.
6. Uma mensagem eletrônica é considerada um documento formal da empresa.
7. O conteúdo do e-mail de cada usuário pode ser auditado pela HEMERA com o objetivo de garantir a segurança e integridade de seu negócio.

8. Mensagens recebidas de origens desconhecidas ou suspeitas devem ser removidas da caixa de entrada imediatamente desde que não sejam necessárias para análise e/ou registro de incidente de segurança.
9. Ao enviar uma mensagem, procure incluir apenas os destinatários interessados no assunto. Cópias desnecessárias sobrecarregam os recursos e causam excesso de conteúdo nas caixas de entradas.
10. Caso o colaborador cometa o equívoco de relacionar destinatários que não deveriam ter acesso ao conteúdo da mensagem, este deve notificar imediatamente seu gestor direto e, quando necessário, as áreas de Compliance e Segurança de Informação para que sejam tomadas as devidas providências.
11. **Ao enviar uma mensagem de correio eletrônico, ela está restrita a você e ao (s) destinatário (s). Porém, no caso de informações que exijam um maior sigilo, você deve indicar na primeira linha da mensagem o nível de classificação dessa informação, dentre os níveis de confidencialidade descritos na Política de Segurança - Classificação da informação.**
12. É proibida a edição e adulteração de e-mails ou cabeçalhos de e-mail, de forma que seja preservada a mensagem original em casos de resposta e encaminhamento.
13. Caso receba uma mensagem enviada por engano, proceder da seguinte maneira:
    1. caso seja uma mensagem do domínio ***hemeradtvm.com.br***, informe ao remetente o ocorrido e remova a mensagem da sua caixa;
    2. caso não seja do domínio ***hemeradtvm.com.br***, simplesmente remova a mensagem da sua caixa.

Arquivos em anexo

1. Enviar arquivos anexados somente quando for imprescindível. Cuidado quando estiver repassando (Encaminhar/Forward) mensagens para não repassar desnecessariamente arquivos anexados.
2. Garantir que cada um dos arquivos anexados possua o seu nível de confidencialidade da informação de acordo com a Política de Segurança – Norma de Classificação da Informação.

3. Arquivos recebidos de remetentes desconhecidos não devem ser abertos e a mensagem deve ser removida. Salvo exceções de equipes capacitadas e autorizadas à análise. Acionar a Área de Tecnologia da Informação caso necessário.

Gestão do Correio Eletrônico

1. Não compartilhe a sua senha de acesso ao ambiente de rede e ao correio eletrônico com nenhum outro usuário.

4. 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.

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. 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

A Hemera DTVM se apresenta num contexto de negócios em que podem existir atividades conflitantes, informações sigilosas ou privilegiadas e diversos riscos inerentes ao modelo estrutural e operacional presentes no seu ramo de atuação.

Buscando atuar em conformidade e fiel cumprimento das obrigações assumidas junto aos órgãos reguladores, a instituição deve buscar:

1. Mitigar a ocorrência de atos ilícitos ou contrários à Regulação;
2. Promover a segregação funcional das áreas responsáveis pelas
3. Atividades de Serviços Qualificados das demais áreas que possam gerar potenciais conflitos de interesse, de forma a minimizar adequadamente tais conflitos, inclusive fisicamente, quando exigido pela Regulação aplicável;
4. Propiciar o bom uso de instalações, equipamentos e informações comuns a mais de um setor da empresa;

5. Preservar informações confidenciais e permitir a identificação das pessoas que tenham acesso a elas; e
6. Administrar e monitorar adequadamente as áreas identificadas como de potencial conflito de interesses.

Gestão de Acessos Eletrônicos

1. Objetivo

Tem como objetivo definir o processo de gestão de acessos de colaboradores, estagiários e prestadores de serviços aos sistemas e diretórios da HEMERA DTVM e do grupo de empresas participantes, além de estabelecer padrões para gerenciamento de contas e senhas.

2. Abrangência

Esta norma se aplica a todos os usuários da HEMERA DTVM, fornecedores ou pessoas que exerçam atividades junto as empresas participantes.

3. Responsabilidade

A gestão de acessos aos ambientes e sistemas fornecidos pela HEMERA DTVM é de responsabilidade da área de TI. Exceções deverão ser analisadas e documentadas.

4. Controle de Acessos Baseado em Função - RBAC

A estrutura da Hemera DTVM contempla a segregação de sistemas e dos arquivos referentes às atividades de administração, das funções exercidas pelo custodiante e controlador. Os acessos serão concedidos baseados na Matriz de Controle de Acessos Baseado em Função (RBAC).

Na matriz são definidas as funções existentes na área e os perfis de acesso e transações previamente autorizadas a sistemas, pastas de rede e demais recursos sistêmicos e computacionais pertinentes à função. As permissões de acesso, transações e perfis declaradas na Matriz RBAC são definidas pelo Gestor da área, e aprovadas pelas áreas de Controles Internos e Compliance.

Qualquer alteração nas permissões de acesso anteriormente acordadas e criação de novos perfis, será executada pela área de Tecnologia da Informação a pedido do Gestor responsável pela função, após autorização da área de Controles Internos, que irá avaliar a concessão ou não, a partir dos riscos mapeados, criticidade do processo e inexistência de conflito de interesses.

5. Concessão e Revogação de Acessos

5.1 Admissão e Movimentação Funcional de Colaboradores / Estagiários / Prestadores de Serviços

A área de Administração do Capital Humano da empresa ou o gestor responsável pela contratação deverá informar a área de Tecnologia da Informação, por meio de e-mail padronizado, toda e qualquer contratação, ausência, férias ou movimentação funcional (transferência de área) de colaboradores, estagiários e/ou prestadores de serviços. Deverá ser informado o nome do colaborador, estagiário ou prestador de serviço, a área onde irá desempenhar suas atividades, a função que irá exercer, a data de início na função.

Os acessos serão atribuídos conforme definições da Matriz de Controle de Acessos Baseado em Função (RBAC). De posse dessas informações, a área de Tecnologia da Informação irá fazer a concessão dos acessos atribuídos à função, de acordo com perfil previamente estabelecido e repassar as credenciais de acesso ao colaborador. Demais acessos solicitados pelo gestor, serão fornecidos após aprovação da área de Controles Internos.

Nos casos de movimentação funcional, os acessos serão ajustados de acordo com a nova função desempenhada. Os acessos que não forem mais necessários para exercer a nova

função serão revogados, cabe ao gestor anterior cancelar os acessos desnecessários anteriormente concedidos e ao novo gestor providenciar os novos acessos caso necessário. No caso de prestadores de serviços deverá também ser informado o tempo em que o mesmo prestará serviço para a instituição, quando couber, para que na data de seu desligamento possam também ser encerradas as atividades relacionadas ao direito de seu acesso ao sistema. Cabe a área de Gestão de Pessoas dar conhecimento e obter as devidas assinaturas de concordância dos novos contratados em relação à Política de Segurança da Informação.

5.2. Desligamento de colaboradores / Estagiários / Prestadores de Serviços

No caso de desligamento ou afastamento de colaboradores, a área de Gestão do Capital Humano ou o gestor responsável pelo colaborador, estagiário ou prestador de serviço deverá comunicar o fato o mais rapidamente possível a área de Tecnologia da Informação, copiando Compliance e Controles Internos, para que os acessos internos e externos à HEMERA DTVM sejam revogados de maneira tempestiva. E caso seja necessário auditoria posterior, caberá ao gestor responsável solicitá-la.

6. Acesso a VPN

O acesso a VPN será autorizado e liberado para que os colaboradores possam acessar de maneira remota o ambiente da HEMERA DTVM. Todas as solicitações devem ser efetuadas pelo Gestor da área solicitante, via e-mail, para a área de Tecnologia da Informação, copiando Compliance e Controles Internos, informando o *login*, cargo ou função e a justificativa/necessidade. Os acessos serão concedidos após análise da área de Tecnologia da Informação. A área de Tecnologia da Informação irá orientar o usuário sobre os procedimentos necessários para utilização da VPN para acesso remoto do ambiente da empresa.

Gestão de Acessos Físicos

1. Objetivo

Tem como objetivo definir regras para prevenir acesso físico não autorizado, preservar a segregação das atividades de Administração de Recursos de Terceiros, Custódia, Escrituração e Controladoria, entre si, e das demais áreas da Instituição, prevenir danos e interferência nas instalações e informações da HEMERA DTVM.

2. Abrangência

Esta norma se aplica a todos os colaboradores e visitantes.

3. Definições

Colaborador: Refere-se a funcionários e estagiários em tempo integral ou meio período, empregados temporários e prestadores de serviços que estejam residentes nas dependências da HEMERA DTVM.

Visitante: É definido como um fornecedor, convidado de um colaborador, pessoal de serviços ou qualquer um que necessite entrar nas dependências da HEMERA DTVM por um curto período, normalmente não mais que um dia.

4. Perímetro de segurança física

1. O acesso às dependências da HEMERA DTVM deve ser restrito somente ao pessoal autorizado.

2. Os visitantes, durante permanência no ambiente do escritório, deverão estar acompanhados de um colaborador interno.

5. Controle de Acesso Físico

O ambiente físico da HEMERA DTVM possui segregação para que as atividades de administração fiduciária, sejam desempenhadas com total independência das atividades

de custódia de valores mobiliários, ou em relação a outras atividades atualmente desenvolvidas ou que venham a ser desenvolvidas pela instituição.

O controle de acesso é realizado através de Cartão de Proximidade, onde a leitora conta com um gerenciador embutido (Stand Alone), com exceção do Datacenter. Este também com acesso por cartão de proximidade tem gerenciador de acesso separado da leitora com registro e possibilidade de auditoria. Cada colaborador possui um cartão de proximidade com identidade única e cada ambiente controlado possui o seu controle de acesso.

A configuração das permissões é realizada pelo departamento de Tecnologia da Informação, onde somente os colaboradores deste tem permissão para configurar os dispositivos de controle, mediante a liberação pelo gestor. O controle e mapeamento dos cartões de proximidade e acessos é efetuado na planilha "MatrizDeAcesso.xlsx". A planilha formulada é atualizada sempre que acontece uma contratação, movimentação funcional ou desligamento de colaborador.

6. Acesso ao Data Center

O acesso ao Data Center é permitido apenas a colaboradores previamente autorizados. Apenas os colaboradores da área de Tecnologia da Informação estão autorizados a acessar o Data Center. Além deles, o Gestor da área de Administração do Capital Humano também tem autorização para acessar o Data Center em situações excepcionais. A solicitação deve ser feita por e-mail, explicitando o tempo e motivo da demanda. Os visitantes somente podem ter acesso ao Data Center mediante autorização da prévia da área de Tecnologia da Informação junto a área de Compliance. A visita deverá ser acompanhada durante toda a permanência do visitante por colaborador da Área de Tecnologia da Informação. O registro contendo os dados do visitante, bem como data e horários de entrada e saída, devem ser feitos na Planilha de Visitante do Data Center.

7. Segurança de equipamentos

1. Os locais de armazenamento de informações confidenciais devem ser protegidos a fim de evitar o acesso não autorizado.

2. Não é permitido comer, beber ou usar ferramentas que possa produzir fumaça dentro das instalações do Data Center ou em salas que suportam a infraestrutura da instituição.

3. Caso se ausente do seu local de trabalho, o colaborador deve bloquear o acesso a sua estação de trabalho ou terminal, evitando que outras pessoas possam utilizá-lo em seu lugar.

4. O cabeamento de redes deve ser protegido contra interceptação não autorizada ou danos, por exemplo, pelo uso de conduítes ou evitando trajetos que passem por áreas públicas.

5. Dispositivos de segurança concedidos a Colaboradores são de uso individual e intransferível e devem sempre estar em posse do seu portador.

8. Remoção de propriedade

1. Equipamentos, informações ou softwares não devem ser movidos ou retirados do local sem prévia autorização.

2. Os colaboradores e/ou fornecedores que tenham autoridade para permitir a remoção de ativos devem ser claramente identificados.

3. Devem ser estabelecidos limites de tempo para retirada de equipamentos do local e a devolução deve ser controlada.

4. Deve ser feito um registro da retirada e da devolução de equipamentos, quando do seu retorno.

9. Circuito fechado de TV (CFTV)

1. Existe, no escritório, um sistema de circuito fechado de televisão (CFTV) para monitorar todas as dependências da HEMERA DTVM com gravação de imagens em 24x7.

2. Os arquivos ou cópias destes, com imagens gravadas somente poderão ser entregues a autoridades mediante ordem judicial, ou a quem requisitar após autorização do gestor da informação.

10. Gravação telefônica

1. Todos os ramais da HEMERA DTVM são gravados através do sistema automático de gravação.

2. Os arquivos com as gravações telefônicas devem ser guardados em local com controle de acesso e livre de agentes que possam causar danos as mesmas.

3. A liberação ou reprodução de qualquer mídia deve ser aprovada pelo diretor da área envolvida ou substituto aprovado mediante solicitação formal justificada.

11. Conclusão

O não cumprimento das regras descritas nesta Norma constitui em 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.

IV. 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. 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. **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. 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.

V. Norma de Uso da Internet

1. Objetivo

Definir os requisitos e as regras de segurança para o uso da Internet no ambiente da HEMERA DTVM.

2. Abrangência

Esta norma se aplica a todos os usuários (colaboradores, prestadores de serviço e estagiários) que utilizam o ambiente de tecnologia da instituição.

3. Proteção da informação

O ambiente de internet deve ser usado para desempenhar as atividades profissionais do usuário para a HEMERA DTVM. Os acessos realizados nesse ambiente são monitorados pela instituição com o objetivo de garantir o cumprimento dessa política. Os recursos de tecnologia disponibilizados para os usuários, tem como objetivo a realização de atividades profissionais. A utilização dos recursos de tecnologia com finalidade pessoal é permitida, desde que seja em um nível mínimo e que não viole a Política de Segurança.

4. Regras para os usuários

1. O usuário não deve alterar a configuração do navegador da sua máquina no que diz respeito aos parâmetros de segurança.
2. Quando estiver acessando a internet o usuário não deve acessar sites ou executar ações que possam infringir direitos autorais, marcas, licença de software ou patentes existentes.

3. Nenhum material com nível de sigilo "Confidencial" pode ser disponibilizado fora do ambiente monitorado da HEMERA DTVM.
4. Nenhum material ofensivo ou hostil pode ser disponibilizado no ambiente da HEMERA DTVM.
5. É proibido e considerado abuso:
    1. A visualização, compartilhamento, *streaming*, cópia e acesso WEB de conteúdos que não estejam relacionados à atividade profissional, tais quais:
        1. de cunho sexual, pornográfico e de pedofilia;
        2. que defendam atividades ilegais;
        3. que menosprezem, depreciem e incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, religião, nacionalidade.
    2. A transferência ou cópia de grandes quantidades de arquivos de vídeo, som, ou gráficos não relacionados aos interesses de negócios da companhia. Este tipo de ação afeta diretamente os recursos de rede.
    3. Participação em:
        1. qualquer discussão pública sobre os negócios da companhia, através do uso de salas de chat, comunidades virtuais, grupos de discussão, ou qualquer outro tipo de fórum público, a menos que autorizado pela Diretoria.
    4. Distribuição de informações confidenciais da HEMERA DTVM.
    5. Transferência e compartilhamento (downloads/uploads) de arquivos e programas ilegais.

5. Conclusão

O não cumprimento das regras descritas nesta Norma constitui em 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 e Compliance.

VI. Norma de Utilização de Senhas

1. Objetivo

Esta norma tem como objetivo definir regras para uso de *login* e senhas para acesso a sistemas da HEMERA DTVM.

2. Abrangência

Esta norma se aplica a todos os colaboradores, estagiários e prestadores de serviços com acessos autorizados a sistemas e ambientes computacionais e de rede da HEMERA DTVM.

3. Credenciais para acesso a sistemas e ambiente de rede

As contas devem ser únicas, nominais e de uso individual e não devem ser compartilhadas em hipótese alguma.

As senhas são confidenciais e não devem ser divulgadas a nenhuma pessoa. Nenhum colaborador está autorizado a solicitar ou divulgar senhas de acesso de outras pessoas ou suas. Caso isso ocorra, será necessária comunicação ao Gestor.

Recomenda-se a utilização de senhas complexas, ou seja, utilizar estas quatro opções: letras maiúsculas, minúsculas, caractere especial e ou número. As senhas utilizadas em outros locais, como bancos e sites específicos não devem ser reutilizadas na HEMERA DTVM, além disso, não devem ser utilizadas senhas com informações pessoais, como datas ou nomes conhecidos.

A senha deve ter no mínimo 8 caracteres.

Toda senha deve ser trocada periodicamente.

Sistemas de autenticação deverão expirar as senhas periodicamente (90 dias).

As senhas que forem armazenadas em qualquer ferramenta de gestão de senhas, devem ser criptografadas. A senha jamais deve estar disponível para a leitura de outras pessoas. Se for impossível aplicar criptografia as senhas gravadas, o gestor deve comunicar a área de compliance para que juntos decidam quais medidas devem ser tomadas para garantir a segurança. A criação de uma conta privilegiada para tarefas administrativas deve ser aprovada pelo time responsável pelo sistema. As senhas administrativas ou de usuários com privilégios elevados (*root*, *admin*, etc.) não devem ser armazenadas de forma insegura. São considerados exemplos de forma insegura de armazenamento (não se limitando a eles): arquivos texto, arquivos que não estejam criptografados, de forma escrita, etc. Recomenda-se usar gerenciador de senhas com senha mestra. A sessão da estação ou servidor deverá ser bloqueada assim que o usuário ou administrador se ausentar do local, independente do tempo. O titular da conta será o único e exclusivo responsável por qualquer ocorrência que envolva o servidor.

Contas de usuários desligados devem ser imediatamente bloqueadas.

Novas senhas (iniciais ou reinicializadas) devem ser transmitidas de maneira segura, utilizando-se ferramentas ou métodos que garantam o sigilo das mesmas.

4. Conclusão

Qualquer tentativa de executar operações não permitidas poderá ser tipificada ou caracterizada como violação da Política de Segurança da Informação e é passível de sanção.

VII. Norma de Uso Aceitável de Estações de Trabalho, Notebooks e Demais Dispositivos

1. Objetivo

Esta norma tem como objetivo definir as regras para uso dos recursos de computação oferecidos pela HEMERA DTVM a seus colaboradores, estabelecer padrões de uso de Software (Programas, Sistemas) e Hardware (Estações de Trabalho e Notebooks).

2. Utilização de Equipamentos – Estações de Trabalho e Notebooks

Os usuários de computadores (desktops, notebook e/ou dispositivos móveis), ou qualquer outro equipamento computacional, de propriedade da HEMERA DTVM, devem estar cientes que:

- ✓ Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo a realização de atividades profissionais;
- ✓ A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário;
- ✓ É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo;
- ✓ O usuário não deve alterar a configuração do equipamento recebido sem autorização e/ou acompanhamento da área de Tecnologia da Informação.

Alguns cuidados devem ser observados:

Fora do escritório (com ou sem acesso remoto a rede interna da HEMERA DTVM):

- ✓ Mantenha o equipamento sempre com você;
- ✓ Atenção em hall de hotéis, aeroportos, aviões, táxi etc.
- ✓ Quando transportar o equipamento em automóvel utilize sempre o porta-malas ou lugar não visível;
- ✓ Não solicitar ajuda de estranhos;
- ✓ Manter sempre o equipamento com acesso bloqueado caso não esteja distante ou não utilizando o equipamento, mesmo que temporariamente;
- ✓ Atenção ao transportar o equipamento na rua.

Em caso de furto ou perda

- ✓ (Furto) Registre a ocorrência em uma delegacia de polícia;
- ✓ Comunique ao seu superior imediato e a área de Tecnologia da Informação;

- ✓ (Furto) Envie uma cópia da ocorrência para as áreas de Tecnologia da Informação e Administrativo.

Utilização de Dispositivos Pessoais

A utilização de dispositivos pessoais (notebooks laptops) no ambiente computacional da HEMERA DTVM é permitida somente em casos excepcionais ou para os colaboradores chave da instituição. No entanto, o acesso só será concedido feito via VPN após prévia comunicação a área de infraestrutura da instituição.

VIII. 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 responsabilidade exclusiva do setor de Tecnologia da Informação, assim como a manutenção, alteração e atualização de equipamentos e programas. Ao longo do dia, um ou mais, backups diferenciais serão realizados e armazenados pelo período de 24 horas nas mesmas condições de segurança do backup completo. Para os bancos de dados que armazenarem informações de alta relevância operacional e ou informações de terceiros deverão sofrer, BACKUP INCREMENTAL que ocorrerá por padrão de hora em hora,

mas pode ser ajustado segundo as necessidades de segurança da informação e da aplicação. Todos os backups deverão estar catalogados, armazenados em mídias criptografadas e serão administrados segundo o modelo GFS (*Grandfather, Father and Son*) de rotação de backups.

O acesso aos arquivos de BACKUP será restrito apenas ao responsável pelas áreas de tecnologia da informação e infraestrutura de sistemas.

IX. 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.

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. 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;

4. 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.

5. 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.

6. 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.

X. Norma de Criptografia e Gerenciamento de Chaves

1. Objetivo

Esta norma tem como objetivo definir meios criptográficos para proteger a confidencialidade, autenticidade e a integridade das informações da HEMERA DTVM.

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.

XI. Norma de Desenvolvimento de Sistemas

1. Objetivo

Esta norma tem como objetivo definir mecanismos de segurança para o desenvolvimento seguro dos sistemas.

2. Abrangência

Esta norma se aplica a todos os sistemas desenvolvidos pela HEMERA DTVM ou os sistemas desenvolvidos para a HEMERA DTVM por prestadores de serviços de terceiros especificados para esta função.

3. Definições

Alta disponibilidade - Técnicas de aumento da resistência a falhas em sistemas, visando aumentar sua disponibilidade.

4. Desenvolvimento e Manutenção de Sistemas

1. Todas as atividades de desenvolvimento e manutenção de sistemas executadas por pessoal interno estão sujeitas às políticas, padrões, procedimentos e outras convenções de desenvolvimento;
2. Princípios de desenvolvimento seguro e práticas específicas e atualizadas pelo gerenciamento devem ser usados para todos os sistemas desenvolvidos ou mantidos internamente.
3. Para todo sistema utilizado por clientes devem ser implementados métodos de alta disponibilidade.
4. Todos os sistemas desenvolvidos internamente ou desenvolvidos para atender a HEMERA DTVM deverão, em sua fase de homologação, passar por uma avaliação de segurança com o objetivo de identificar possíveis vulnerabilidades ou desvios dos controles de segurança.
5. Para sistemas já existentes antes da publicação desta política, deve ser feita uma análise de custo e de risco para avaliar quais itens devem ser aplicados.

6. Nenhum processo de desenvolvimento de sistemas deve alterar informações dos ambientes de produção. Os dados utilizados em ambiente de testes devem ser mascarados ou fictícios.
7. Dados confidenciais de produção (ex: CPF, RG, endereço) não devem ser usados para testes ou desenvolvimento. Nos casos onde houver necessidade incontornável de utilização de dados de produção no ambiente de testes, será necessário obter aprovação formal do gestor da informação antes da utilização dos dados.
8. Solicitações de regra no firewall deverão ser avaliadas e autorizadas pela área de TI.
9. Os critérios para seleção de softwares de terceiros ou desenvolvimento terceirizado de software devem incluir os controles de segurança da Política e do Padrão de Desenvolvimento de Sistemas, bem como seguir as determinações da Norma de Uso de Software da HEMERA DTVM. Exceções devem ser analisadas pela Área de TI.
10. Não é permitida a publicação de sistemas no ambiente de produção que não tenham passado por todas as fases do processo de homologação e análise da área de Segurança. Entende-se por ambiente de produção sistemas acessíveis de uma rede externa e/ou com dados reais.

5. Segregação de Ambientes e Controle de Mudanças

1. Mudanças em sistemas de produção devem ser executadas apenas por administradores de sistemas autorizados.
2. Devem ser implementados controles apropriados para garantir a inexistência de conflito de funções quando do desenvolvimento, manutenção e promoção de sistemas para o ambiente de produção. Para tanto, os colaboradores das áreas de desenvolvimento, homologação e produção não podem executar funções em duas dessas três áreas ao mesmo tempo. Isto somente estará autorizado, caso o colaborador mude oficialmente de área e após a certificação de que este colaborador não carrega nenhum acesso da antiga área.

3. Os ambientes de desenvolvimento e produção devem ser segregados por um ambiente de testes, de forma que as aplicações desenvolvidas ou adquiridas não entrem em produção sem estar devidamente testadas e documentadas.
4. Sistemas em fase de desenvolvimento ou homologação não deverão ser hospedados em ambiente público. No caso de desenvolvimento por terceiros, o ambiente deve ser limitado via firewall.

6. Código Fonte

1. Todos os sistemas desenvolvidos internamente deverão ter um repositório no servidor oficial da HEMERA DTVM.
2. Consultores e prestadores de serviço terão acesso restrito no repositório oficial da HEMERA DTVM, devendo ter permissão para acessar única e exclusivamente os repositórios dos projetos em que estejam alocados.

7. Licença

1. Os códigos de programação desenvolvidos por colaboradores internos ou terceiros contratados para esta finalidade são de propriedade da HEMERA DTVM e cabe ao gestor responsável definir o tipo de licença e condições de uso.

XII. Norma para Gerenciamento de Vulnerabilidades

1. Objetivo

Esta norma tem como objetivo estabelecer um processo periódico de identificação, análise e correção de vulnerabilidades.

2. Definições

Ambiente de produção - Infraestrutura ligada diretamente aos produtos e serviços oferecidos aos clientes.

Baseline de Segurança - São determinações de segurança que devem ser aplicadas aos elementos de infraestrutura para garantir que não estejam vulneráveis a ameaças.

Evidência de falso-positivo - É a prova que uma determinada vulnerabilidade não existe para o alvo específico.

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

3. Responsabilidades

TI

1. Executar periodicamente "scan de vulnerabilidades" no ambiente de produção.
2. Gerar relatório de vulnerabilidades.
3. Analisar as evidências para as vulnerabilidades consideradas como falso-positivos.
4. Definir / negociar prazos para correção do ambiente de acordo com sua criticidade.
5. Monitorar a execução das atualizações de acordo com o SLA definido.
6. Avaliar o impacto da mudança para os clientes.
7. Elaborar estratégias para realização das correções de segurança com mínimo impacto para clientes - idealmente, sem nenhum impacto.
8. Executar as correções de segurança nos ambientes sob sua responsabilidade.
9. Organização de planos de ação para descontinuidade de produtos ou funcionalidades legados.
10. Garantir que os baselines definidos estejam aplicados no ambiente.

Todos os colaboradores

1. Notificar imediatamente a área de TI caso identifique vulnerabilidades em qualquer ativo da empresa.

XIII. Norma de Serviços de Computação em Nuvem

1. Objetivo

Esta norma tem como objetivo definir conceitos e regras para a gestão dos serviços em Nuvem utilizados pela HEMERA DTVM, garantindo que todos as diretrizes da Política de Segurança da Informação sejam aplicadas e estendidas a esse ambiente. Os controles implementados e utilizados na HEMERA DTVM garantem também no ambiente em Nuvem a prevenção, detecção e mitigação dos riscos de incidentes de segurança.

2. Descrição dos Serviços de Computação em Nuvem

Utilizamos um VPC (Virtual Private Cloud) da Azzure, localizado em São Paulo.

O acesso é restrito por VPN Site-Host.
A definição do prestador de serviço foi baseada nos critérios descritos a seguir:

- ✓ A infraestrutura em Nuvem da Azzure possui controles robustos de segurança e proteção de dados;
- ✓ Conformidade com as principais regulamentações, normas e práticas de mercado
- ✓ Garantia da Confidencialidade, Integridade e Disponibilidade da Informação;
- ✓ Reconhecimento da qualidade dos serviços prestados por todo o mercado.

3. Procedimentos

O gerenciamento dos serviços de computação em Nuvem abrange, não se limitando:

1. Gerenciamento dos servidores e outros ativos já ativos;
2. Provisionamento de novos servidores para atender novas demandas;
3. Gestão de Incidentes de Segurança no Ambiente em Nuvem;
4. Implementação e Gestão de Controles de Segurança da Informação, de forma a impedir, prevenir, detectar ou mitigar eventuais vulnerabilidades que possam causar incidentes de segurança;
5. Gerenciamento de Billing;
6. Comunicação com Órgãos Reguladores.

4. Comunicação ao BACEN

A contratação de serviços **relevantes** de processamento e armazenamento de dados em nuvem ou alterações contratuais relevantes devem ser previamente comunicadas ao BACEN.

Devem ser indicados nessa comunicação:

1. Nome da empresa contratada;
2. Serviços que estão sendo contratados;
3. Indicação da localidade (País, estado, cidade) onde o serviço será prestado;
4. Alterações contratuais (quando aplicável).

A comunicação deverá ser realizada no prazo máximo de 10 (dez) dias após a contratação ou alteração contratual do serviço.

Controle de Versão

Histórico de Atualizações: Segunda Versão.