COIMBRA &
FERREIRA
Sociedade de Advogados

Rua Sete de Setembro, nº 99, 15º andar, Centro
Rio de Janeiro | RJ - CEP: 20050-005

+55 21 3513-5688

POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO

Versão: 2.4

SUMÁRIO

1. DADOS DO DOCUMENTO

1.1. RESPONSÁVEIS

Etapa	Responsável
Elaboração	Equipe de Segurança da informação
Revisão	Comitê Gestor de Segurança da Informação
Aprovação	Comitê Gestor de Segurança da Informação

1.2. REGISTRO DE ALTERAÇÕES

Versão	Item Alterado	Descrição Resumida das Alterações	Motivo	Data
1.0	Todos	Criação do Documento.	N/A	14/04/2022
2.0	-	-	Revisão periódica.	12/05/2023
2.1	14.	Atualização de Normas de Incidentes de segurança da Informação.	N/A	06/09/2023
2.2	15.	Criado Norma de Gerenciamento de Patches	N/A	08/09/2023
2.3	4., 12.3.-g.,	- Atualização de Normas de Controle de Acesso; - Definido regras para criptografia de dados em repouso.	N/A	12/10/2023
2.4	13.	Atualizado Normas de Gerenciamento de Chaves Criptográficas	N/A	14/10/2023
2.5	-	-	Revisão periódica.	20/10/2024

2. DIRETRIZES GERAIS DE SEGURANÇA DA INFORMAÇÃO

a) Esta Política aplica-se a todos os funcionários, estagiários ou qualquer outra categoria de colaborador, e também aos prestadores de serviços que atuam em quaisquer segmentos da empresa.

b) Esta Política define as Diretrizes para a Segurança da Informação, com intuito de manter a integridade, confidencialidade e disponibilidade das informações pertencentes a empresa ou sob sua gestão. Descreve a conduta considerada adequada para o uso, controle e proteção das informações contra destruição, modificação, divulgação indevida e acessos não permitidos, acidentais ou intencionais;

c) Esta Política se aplica às informações sob gestão da empresa, que podem existir de várias maneiras: impressa, escrita, armazenada e transmitida por meios eletrônicos, difundidas em áudio e/ou vídeo ou falada em conversas formais e informais. Seja qual for a forma apresentada ou o meio através do qual a informação seja apresentada ou compartilhada, ela deverá estar sempre protegida adequadamente, de acordo com controles definidos nesta política;

d) A Política deve ser conhecida e obedecida por todos os que utilizam os recursos de processamento de informação de propriedade ou controlados pela empresa, sendo o seu cumprimento de responsabilidade de cada um. A Política está disponível nos vários veículos de comunicação da empresa, sendo demonstrada aos funcionários, estagiários e demais colaboradores no momento da formalização de seus vínculos e a cada 12 meses a partir de então, o que implica diretamente na aceitação de seus termos;

e) No âmbito da empresa, somente é permitido aos usuários o uso de recursos de processamento da informação disponibilizados pela empresa, de forma a garantir que os requisitos de segurança sejam atendidos. Os Gerentes das Unidades Administrativas são responsáveis em tomar as medidas cabíveis para o cancelamento do acesso aos recursos quando estes não forem mais necessários. O uso de recursos de processamento de informação de terceiros em ambiente da empresa deve ser submetido à Diretoria e/ou Gerência de Segurança da Informação;

f) Somente atividades lícitas, éticas e administrativamente admitidas devem ser realizadas pelos usuários, quando na utilização dos recursos de processamento da informação da empresa;

g) Toda a informação produzida por intermédio dos recursos de processamento de dados da empresa é de propriedade da empresa e está sujeita a todos os termos desta política. De igual modo, os programas desenvolvidos por seus funcionários ou prestadores de serviço, bem como documentos e peças confeccionadas;

h) As informações de propriedade ou controladas pela empresa, disponibilizadas de acordo com permissões e critérios específicos, devem ser utilizadas somente para o desempenho de funções pertinentes e para a execução de processos estabelecidos pela

empresa. Os usuários não podem, em qualquer tempo ou sob qualquer propósito, apropriar-se dessas informações;

i) O cumprimento da Política de Segurança é auditado pela Gerência de Segurança da Informação, que se vale de processos de monitoria automáticos sobre o tráfego efetuado através das suas redes de comunicação, incluindo o acesso à Internet e o uso do Correio Eletrônico;

j) Aplicar o uso de segregação de funções, com o objetivo de assegurar a efetividade na execução das atividades, reduzir as oportunidades de modificação, não autorizada ou não intencional, ou uso indevido dos ativos da organização. As atividades de cada um devem ser bem definidas, de modo que a pessoa que realizou a operação não faça a conferência. Ninguém deve ter sob sua inteira responsabilidade todas as fases inerentes a uma operação.

k) Seguir, sempre que possível, os princípios da segregação de funções, que consiste nas funções de autorização, aprovação de operações, execução, controle e contabilização, de tal maneira que nenhum funcionário detenha poderes e atribuições em desacordo com este princípio de controle interno. Cada uma dessas fases deve, preferencialmente, ser executada por pessoas e setores independentes entre si.

l) Caso não seja possível aplicar a segregação de funções, controles compensatórios devem ser implementados para assegurar que os riscos sejam mitigados. Exemplos de controles de compensação são:

    - Utilização de trilhas de auditoria e/ou logs para monitoramento de acessos e atividades por outra pessoa;

    - Supervisão pela gestão, permitindo avaliação e tratativa apropriada e em tempo hábil de situações excepcionais.

m) Os recursos de processamento da informação disponibilizados aos usuários têm que ser suportados por um projeto a fim de evitar situações de risco à segurança da informação. Deve-se adotar esquema de segregação de funções e atividades, incluindo a separação dos ambientes de desenvolvimento, teste e produção, além de submeter à aprovação do Comitê Consultivo de Mudanças;

n) Todos os usuários ao tomarem conhecimento de qualquer incidente de segurança da informação devem notificar o fato, imediatamente, à Gerência de Segurança da Informação, através de e-mail (mauriciocoimbra@coimbraeferreira.com.br) ou por Comunicação Interna (CI);

o) É de responsabilidade da gestão de tecnologia da informação, garantir que estágios de um processo fiquem a cargo de dois ou mais indivíduos e que um indivíduo ou grupo possa verificar o trabalho de outro. A Gerência de Segurança da Informação deve garantir que não sejam exercidas pelo mesmo indivíduo as seguintes funções: usuário de sistema, gerenciamento de rede, administração de sistema, desenvolvimento de

sistema, gerenciamento de mudanças, administração de segurança e auditoria de segurança;

p) A não observância dos preceitos desta Política implicará na aplicação de sanções descritas no item 17 desta política.

3. COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO (CGSI)

Fica definido a constituição do **COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO** (CGSI), contando com a participação de, pelo menos, um representante da diretoria e um membro sênior das seguintes áreas: Tecnologia da Informação, Segurança da Informação, Recursos Humanos, Jurídico e Comunicação.

É responsabilidade do CGSI:

a) Analisar, revisar e propor a aprovação de políticas e normas relacionadas à segurança da informação;
b) Garantir a disponibilidade dos recursos necessários para uma efetiva Gestão de Segurança da Informação;
c) Garantir que as atividades de segurança da informação sejam executadas em conformidade com a PSI;
d) Promover a divulgação da PSI e tomar as ações necessárias para disseminar uma cultura de segurança da informação no ambiente.

4. NORMAS DE CONTROLE DE ACESSO

4.1. OBJETIVO

Direcionar o emprego adequado de medidas que viabilizem o completo controle de acesso às dependências e informações da empresa, para funcionários e não funcionários.

4.2. ABRANGÊNCIA

Esta norma se aplica a todas as instalações da empresa ou onde a mesma mantenha serviços ou ativos, para acessos físicos e remotos, para quaisquer finalidades.

4.3. DIRETIVAS DE AMBIENTE E CONTROLE

Garantir que as entradas e saídas das instalações da empresa sejam rigorosamente monitoradas e controladas, com o objetivo de assegurar a máxima segurança no ambiente.

Os responsáveis pelo controle de acesso devem receber orientações detalhadas sobre as normas internas de acesso, com a responsabilidade de manter e registrar todas as práticas estabelecidas.

Relatar qualquer atividade suspeita ou violações de segurança à equipe de segurança do condomínio.

Em caso de qualquer intrusão física nas instalações da empresa, é imperativo acionar imediatamente as autoridades policiais competentes.

4.3.1. SISTEMA DE VIGILÂNCIA POR VÍDEO (CFTV)

Os sistemas de vigilância por vídeo (CFTV) devem ser projetados para proporcionar, no mínimo, o monitoramento completo das entradas e saídas da organização, com a capacidade de armazenar, no mínimo, 30 dias de gravações.

4.3.2. SISTEMA DE RECONHECIMENTO FACIAL

O sistema de reconhecimento facial é uma tecnologia que utiliza algoritmos para analisar características únicas do rosto, como proporções e padrões de pele, criando um modelo facial exclusivo. Essa representação matemática é usada para autenticar a identidade de uma pessoa comparando-a com modelos armazenados, permitindo o acesso seguro a sistemas e locais protegidos.

4.3.2.1. PROCEDIMENTOS E FUNCIONALIDADE DO SISTEMA

- **Captura de Imagem:** O processo começa com a captura de uma imagem ou vídeo do rosto da pessoa que deseja acessar uma área ou serviço. Isso pode ser feito usando câmeras de segurança ou dispositivos de captura específicos.
- **Pré-processamento:** A imagem capturada é pré-processada para melhorar sua qualidade e remover ruídos, como variações de iluminação, sombras e distorções.
- **Detecção do rosto:** O sistema utiliza algoritmos de detecção de rosto para localizar a área do Rosto na imagem. Isso envolve identificar características como olhos, nariz, boca e contornos faciais.
- **Extração de características:** Após a detecção do rosto, o sistema extrai características distintas do rosto que são usadas para criar uma representação numérica única da pessoa. Essas características podem incluir distâncias entre pontos chave do rosto, texturas da pele e detalhes como rugas e cicatrizes.
- **Criação de modelo ou template facial:** Com base nas características extraídas, o sistema cria um modelo matemático ou uma representação numérica chamada de "assinatura facial" ou "template facial". Essa assinatura é única para cada indivíduo e serve como uma forma de identificação.
- **Armazenamento e comparação:** A assinatura facial é comparada com modelos armazenados anteriormente em um banco de dados. O banco de dados contém as assinaturas de pessoas autorizadas a acessar determinadas áreas.
- **Correspondência e verificação:** O sistema compara a assinatura facial do indivíduo em tempo real com as assinaturas armazenadas no banco de dados. Se houver uma correspondência dentro de um limite de tolerância, o acesso é concedido.
- **Feedback e acesso:** Com base na correspondência, o sistema toma uma decisão sobre o acesso. Isso pode resultar na abertura da porta de acesso as dependências da organização.

4.4. NORMAS PARA ACESSO FÍSICO

4.4.1. ACESSO DE FUNCIONÁRIOS

O acesso físico dos funcionários às dependências da organização se dará por meio do reconhecimento facial, sendo registrado e liberado após os trâmites do Departamento Pessoal para a sua contratação.

4.4.2. ACESSO DE NÃO FUNCIONÁRIOS

O acesso as dependências por qualquer pessoa que não seja um funcionário da organização, deverá ser registrado, mantendo dados de identificação, origem e motivo do acesso. Esse registro deve estar disponível para consulta sempre que necessário.

A área responsável pelo acesso deverá confirmar a necessidade do acesso e estará responsável pelo terceiro, mantendo o acompanhamento e orientação do mesmo sobre a conduta e regras que devem ser observadas na empresa, até sua saída.

O empregado de empresa e/ou pessoa prestadora de serviços depois de devidamente identificado pelo agente de portaria, receberá o crachá de identificação “prestador de serviços”, de uso obrigatório enquanto permanecer nas dependências da organização.

Os visitantes também serão cadastrados no sistema de reconhecimento facial, se atentando a definição/limitação de tempo de acesso às dependências.

4.4.3. REVOGAÇÃO DE ACESSO

Acesso de funcionários deve ser revogado em caso de demissão, término de contrato ou violações de segurança.

Visitantes que não cumpram as regras podem ter seu acesso revogado.

4.5. NORMAS PARA ACESSO À INFORMAÇÕES

Todo o acesso a informações da empresa ou mantidas por ela, se dará com base na observação das normas de classificação da informação, presentes neste mesmo documento.

4.6. NORMAS PARA ACESSO AOS ATIVOS TECNOLÓGICOS

O acesso às áreas onde existam ativos tecnológicos, físicos ou lógicos, é vedado a qualquer pessoa, seja funcionário próprio ou terceirizado, que não seja previamente autorizado pela gerência ou diretoria da área de tecnologia.

Os locais onde encontrarem-se os ativos físicos de tecnologia, destinados ao processamento, manutenção e disponibilização da informação, nos seus vários formatos, devem ser devidamente identificados, mantendo em local visível e de maneira clara os alertas pertinentes às restrições de acesso e procedimentos exigidos para o acesso. Estes locais devem dispor ainda de fechadura com senha eletrônica e o acesso a estes locais deve ser controlado diretamente pela gestão da área.

4.7. ACESSO REMOTO

4.7.1. ESCRITÓRIO

a) O acesso remoto aos equipamentos, softwares, banco de dados, informações, dados, programas de informática, e-mails, canais/endereços eletrônicos, ou a qualquer tipo de arquivo ou informação existente nos estabelecimentos da empresa (“Escritório”), somente será permitido quando realizados no equipamento de uso do colaborador para o exercício de sua função;
b) Não caracteriza invasão, pois o equipamento é de propriedade da empresa, e todas as informações contidas no mesmo são de propriedade da empresa;
c) O acesso remoto às informações e dados existentes no Escritório será restrito, sendo tratado como uma excepcionalidade e que somente será permitido mediante a prévia e expressa autorização da Diretoria.

4.7.2. DATA CENTER / NUVEM

a) O acesso remoto aos servidores alocados no data center ou nuvem pública será realizado exclusivamente através de uma conexão VPN – Virtual Private Network (rede privada virtual);
b) Acesso a consoles de gerenciamento de ambientes em nuvem, devem ter o recurso de múltiplo fator de autenticação obrigatoriamente habilitado;
c) Todos os acessos são realizados somente por colaboradores;
d) O controle de acesso é vinculado a um acesso exclusivo e intransferível para cada colaborador e autorizado previamente por cada área responsável;

e) O acesso remoto será restrito, sendo tratado como uma excepcionalidade, e somente será permitido mediante a prévia e expressa autorização pela Diretoria.

5. NORMAS DE CONTAS E SENHAS DE ACESSO

5.1. OBJETIVO

Estabelecer os procedimentos adequados para a correta utilização das contas de usuários no ambiente de Tecnologia da Informação e Comunicação (TIC).

5.2. ABRANGÊNCIA

Esta norma deverá ser aplicada a todos os usuários que possuam contas (sem privilégios de "administrador") nos ativos do tipo estações de trabalho e servidores do ambiente de Tecnologia da Informação e Comunicação (TIC).

5.3. CONCEITO

Segundo a nova norma ABNT NBR ISSO/IEC 17799:2005, item 11.2, convém que procedimentos formais sejam implementados para controlar a distribuição de direitos de acesso a sistemas de informação e serviços.

Convém ainda que a concessão e o uso de privilégios sejam restritos e controlados (item 11.2.2) e que a concessão de senhas seja controlada através de um processo de gerenciamento formal (item 11.2.3).

Portanto, a empresa elaborou esta norma de contas e senhas para usuários, de forma a evitar o uso inapropriado de senhas, que pode vir a ser um grande fator de contribuição para falhas ou violações de sistemas.

5.4. FORMAÇÃO DE CONTAS E SENHAS

a) As senhas para usuários finais deverão conter no mínimo 8 (oito) caracteres e usuários administrativos deverão conter no mínimo 15 (quinze) caracteres, sendo obrigatório o uso de letras minúsculas e maiúsculas, números e símbolos (tais como "$", "%", "&", "*", "@", "#", ...);

b) Deverá ser evitada a composição de senhas com sequências numéricas (123...) e/ou alfabéticas (abc...), além de senhas de fácil dedução (nome da máquina, login/ID, nome do usuário/mãe/pai/esposa/marido/filho, data de nascimento, ...);

c) Os sistemas e aplicações deverão prover algum mecanismo ou instrução que garanta o uso de senhas com as formações acima citado;

d) Os nomes de usuário não devem fazer alusões aos níveis de acessos dos mesmos (ex: admin, teste, poliana_admin, administração, gerencia).

5.5. TEMPO DE VIDA DE CONTAS E SENHAS

a) O usuário deverá ser forçado a trocar a senha no seu primeiro login;

b) Deverá ser guardado um histórico composto de, pelo menos, das 24 (vinte) últimas senhas;

c) O tempo mínimo para troca de senhas deverá ser de 1 (um) dia;

d) A conta deverá ser bloqueada após a 3ª (terceira) tentativa de login com falha;

e) Em caso de bloqueio de conta por falha na tentativa de login, a conta deverá ficar no mínimo 30 minutos bloqueada e após este tempo a conta é habilitada novamente de forma automática;

f) O tempo de vida das senhas deverá ser de, no máximo, 30 (trinta) dias, quando deverá ser forçada a sua troca no primeiro login após esse período;

g) Contas que ficarem inativas por mais de 60 (sessenta) dias deverão ser bloqueadas.

5.6. REINICIALIZAÇÃO DE SENHAS

a) As contas só poderão ser reinicializadas, por solicitação formal do seu detentor, à área responsável pela administração das contas;

b) Em casos de extrema necessidade de reinicializar uma senha em sistemas críticos, isto só poderá ocorrer mediante a confirmação de algumas informações de caráter pessoal do usuário. Nestes casos, o operador deverá retornar a ligação para confirmação desses dados;

c) Para casos considerados críticos, a solicitação de reinicialização de conta deverá ser feita através de contato com o Gerente/Diretor de Segurança da Informação;

d) Caso o usuário suspeite do comprometimento de sua senha, esta deverá ser modificada imediatamente.

5.7. CONTRATAÇÕES, DEMISSÕES e REMANEJAMENTOS

a) Para o novo usuário ou para aquele que esteja retornando após desligamento ou remanejamento, o Departamento Pessoal deverá solicitar a concessão de acesso mínimo necessário, para que este exerça suas respectivas tarefas (ex: conta de domínio);

b) O Departamento Pessoal deverá comunicar às áreas responsáveis pela administração das contas o desligamento ou remanejamento de qualquer usuário;

c) Obrigatório a suspensão de funcionários em ausência legal (ex. férias, licenças, etc.) por todo o período da ausência;

d) O período entre a notificação do desligamento e a exclusão dos acessos não deve exceder 24 horas;

e) Os acessos para sistemas de clientes e terceiros devem ser excluídos prioritariamente, de acordo com os manuais para administração de contas de cada instituição;

f) Política de Retirada de Direitos de Acesso deverá ser seguida rigorosamente pelas equipes do Departamento de Pessoal, juntamente com a equipe de T.I. responsável pela administração de contas de sistemas. Estes também deverão atualizar constantemente a documentação sempre que necessário, sob avaliações/revisões da equipe de segurança da informação.

5.8. DISPOSIÇÕES GERAIS

a) Os sistemas e aplicações deverão ter algum mecanismo que impeça a mesma conta de estar ativa, simultaneamente, em mais de uma estação;

b) Os sistemas e aplicações deverão ter algum mecanismo que impeça a exibição automática, na tela de login, da senha referente ao respectivo login em uso;

c) Os sistemas e aplicações deverão ter algum mecanismo de bloqueio automático por inatividade, em um prazo máximo de 1 minuto;

d) A senha é pessoal e intransferível, devendo ser mantida em sigilo. O usuário será responsabilizado pelo mau uso da mesma, conforme previsto na legislação;

e) É vedado o uso de contas compartilhadas, pois inviabilizam o rastreamento de atividades;

f) Deve-se atribuir o menor privilégio possível a uma conta, que deverá permitir apenas a realização das tarefas pertinentes ao seu usuário;

g) Os usuários finais não poderão ter contas com perfil de administrador, nem contas do domínio com privilégio de administrador local da estação;

h) Evitar a utilização da mesma senha para uso com finalidades profissionais e pessoais;

i) Os sistemas e aplicações deverão, sempre que possível, mostrar um aviso geral (banner) informando que somente pessoas autorizadas devem obter acesso ao computador ou sistema;

j) Evitar anotar senha (por exemplo, em papel, arquivos ou dispositivos móveis), a menos que esta possa ser guardada de forma segura, por exemplo, lacrado dentro de um cofre;

k) Tornar todas as senhas ilegíveis durante a transmissão e o armazenamento em todos os componentes usando a criptografia robusta.

6. NORMAS DE GESTÃO DE ATIVOS

6.1. OBJETIVO

Alcançar e manter a proteção adequada dos ativos (servidores, desktops, elementos de rede, sistemas operacionais, aplicativos de produtividade [como aplicativos de Office automation], software antivírus, softwares firewall e proxy, aplicações desenvolvidas, etc.) do ambiente de Tecnologia da Informação e Comunicação (TIC), definindo as responsabilidades dos proprietários e custodiantes de cada ativo tecnológico.

6.2. ABRANGÊNCIA

Esta norma deverá ser aplicada a todos os usuários que sejam proprietários e/ou custodiantes dos ativos tecnológicos da empresa ou por ela mantidos. Esta também se aplica a qualquer usuário que de alguma forma interaja com esses ativos.

6.3. CONCEITOS

Segundo a nova norma ABNT NBR ISO/IEC 17799:2005, item 7.1, convém que todos os ativos sejam inventariados e tenham um proprietário responsável. Convém ainda que os proprietários dos ativos sejam identificados e a eles seja atribuída a responsabilidade pela manutenção apropriada dos controles. A implementação de controles específicos pode ser delegada pelo proprietário, conforme apropriado, porém o proprietário permanece responsável pela proteção adequada dos ativos.

Ademais, de acordo com o item 7.1.1 da mesma norma, convém que todos os ativos sejam claramente identificados e um inventário de todos os ativos importantes seja estruturado e mantido.

Portanto, a empresa elaborou esta norma de gestão de ativos, de forma a definir claramente quais as responsabilidades que os gestores terão ao serem designados como proprietário e/ou custodiante de algum ativo.

6.4. RESPONSABILIDADES

6.4.1. PROPRIETÁRIO

Todo ativo tecnológico do tipo servidor instalado no Datacenters terá designado um proprietário, que será responsável por:

a) Garantir o funcionamento/disponibilidade do ativo em regime 24x7x365;

b) Manter as informações cadastrais sobre o ativo atualizadas – hardware, sistema operacional, software, classificação de informação e serviços disponibilizados através daquele ativo, além das garantias e contratos de manutenção;

c) Manter o controle de versão das aplicações utilizadas e a guarda de suas fontes, configurações e demais materiais;

d) Garantir que todos os softwares proprietários sejam devidamente licenciados juntamente com o fabricante/desenvolvedor;

e) Atuar como suporte nível 3;

f) Delegar para um custodiante, mediante acordo prévio, as tarefas de administração diária daquele ativo;

g) Coordenar as ações em casos de comprometimento da segurança lógica do ativo – invasões de hackers, corrupção de sites, problemas na aplicação etc.;

h) Coordenar as ações em casos de comprometimento da segurança física do ativo – danos, furto, roubo ou qualquer ameaça física ou do meio ambiente; Obs.: Dependendo da natureza do incidente, como, por exemplo, roubo ou furto de equipamento, a empresa possui áreas exclusivas para tratar destes assuntos (segurança patrimonial). Porém, é de inteira responsabilidade do proprietário do ativo interagir com essas áreas a fim de garantir que todas as providências necessárias sejam tomadas;

i) Manter atualizado todos os softwares que rodem naquele ativo, desde upgrade de versão à aplicação de patches. Obs.: Como um ativo pode ter aplicações diversas pertencentes a diversas áreas (ex. Banco de dados, Sistema Operacional, Aplicações WEB), as atualizações de software necessárias serão feitas por essas áreas. Porém, cabe ao proprietário do ativo garantir que essas atualizações estão sendo realizadas e, em caso de não cumprimento deste item, notificar por escrito à Gerência de Segurança da Informação os problemas encontrados;

j) Ter chave de acesso com privilégio de leitura somente; Obs.: O proprietário do ativo poderá ter acesso com privilégios de administrador sempre que precisar. Para tal, é necessário solicitar formalmente ao custodiante que conceda este acesso, informando

sempre o período desejado e as tarefas que serão executadas, caso seja um servidor em produção. Para maiores informações sobre senhas de administrador, consultar o manual de normas e contas e senhas de administradores publicada na Intranet, seção Política de Segurança;

k) Definir e implementar novas funcionalidades. Ex. Upgrade de versão, configuração de um novo serviço, etc.;

l) Garantir que sistema operacional e aplicativos estejam sujeitos a rígido controle de gestão de mudanças, através do Processo de Mudanças estabelecido. Os seguintes aspectos devem ser considerados quando um ativo for sofrer qualquer tipo de modificação:

    - Identificação e registro das mudanças significativas;
    - Planejamento e testes das mudanças;
    - Avaliações de impactos potencias, incluindo impactos de segurança;
    - Procedimento formal de aprovação das mudanças propostas;
    - Comunicação dos detalhes das mudanças para todas as pessoas envolvidas;
    - Procedimento de recuperação, incluindo procedimentos e responsabilidades pela interrupção e recuperação de mudanças em caso de insucesso ou na ocorrência de eventos inesperados.

m) Criar e implantar os procedimentos para a geração de cópias de segurança (Backup) e sua recuperação (Restore) em um tempo aceitável. Garantir que os backups sejam armazenados em mídias adequadas para fins de backup e que as mesmas sejam mantidas em um ambiente seguro, monitorado e de acesso restrito;

n) Garantir que todo procedimento de backup deve contemplar diretórios ou arquivos necessários a qualquer tipo de investigação forense, conforme estabelecido, de acordo com as melhores práticas e normas de segurança da informação;

o) Garantir que registros (log) de auditoria contendo atividades dos usuários, exceções e outros eventos de segurança da informação sejam produzidos e mantidos por um período de tempo acordado para auxiliar em futuras investigações e monitoramento de controle de acesso;

p) Garantir o monitoramento adequado de recursos (processador, disco, memória e interface de rede, etc.) e serviços (up/down) através de softwares especializados, criando alertas visuais/sonoros/envio de e-mail ou SMS de forma automatizada, possibilitando a identificação de estados de normalidade, alertas ou falhas de sistemas e/ou hardwares, além da possibilidade de realizar diagnósticos de performance/desempenho do ativo;

q) Realizar estudos de planejamento de capacidade de forma a evitar sobrecarga nos sistemas suportados pelo ativo;

r) Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais;

s) Não permitir acesso direto e permanente a banco de dados ou outros repositórios de dados, por analistas de Suporte/TI ou usuários da aplicação;

t) Não liberar acesso a banco de dados, a partir de ferramentas com bases locais, como: excel, access ou similar;

u) Não liberar o acesso à terceiros, para fins de administração ou suporte, em aplicações/base de dados sem a prévia autorização de cliente proprietário dos dados.

v) Estar ciente que a não observância aos itens aqui apresentados sujeita-o às sanções previstas para o não cumprimento de suas responsabilidades, destacadas neste mesmo documento.

6.4.2. CUSTODIANTE

Todo ativo tecnológico do tipo servidor instalado no Datacenter terá designado um custodiante, que será responsável por:

a) Ajudar o proprietário a manter as informações cadastrais sobre o ativo atualizadas – hardware, software e serviços disponibilizados através daquele ativo;

b) Atuar como suporte nível 2;

c) Cuidar do ativo no dia-a-dia, notificando ao proprietário qualquer anomalia encontrada;

d) Comunicar imediatamente ao proprietário qualquer problema de segurança lógica do ativo – invasões de hackers, corrupção de sites, problemas na aplicação, etc. e as ações que foram tomadas para sanar/minimizar o problema;

e) Comunicar imediatamente, por escrito, qualquer incidência de dano, furto ou roubo dos equipamentos sob sua custódia;

f) Atualizar, a pedido do proprietário, os softwares de qualquer natureza que rodem no ativo, desde upgrade de versão à aplicação de patches. Obs.: Toda a documentação necessária para realizar as atualizações deverá ter sido previamente fornecida pelo proprietário;

g) Ter chave de acesso com privilégio de administrador nos ativos sob sua custodia;

h) Realizar as modificações necessárias nos ativos, de acordo com o planejamento de gestão de mudanças definido pelo proprietário, em concordância com o Processo de Mudanças;

i) Garantir a sincronização de hora dos ativos com servidores NTP;

j) Garantir que as cópias de segurança (backup) estão sendo geradas;

k) Monitorar os registros (log) de auditoria, avisando imediatamente ao proprietário qualquer problema encontrado;

l) Evitar o acesso aos ativos por pessoas não autorizadas ao serviço de sua área;

m) Estar ciente de que a instalação de software de qualquer natureza ou a modificação de qualquer configuração sem a autorização por escrito do proprietário do ativo não é permitida; Obs.: Para casos de suporte no ativo, esta cláusula não é válida;

n) Coibir qualquer modificação nos equipamentos e/ou software, por quem quer que seja, exceto quando autorizada por escrito, pelo proprietário do ativo;

o) Estar ciente que a não observância aos itens aqui apresentados sujeita-o às sanções previstas para o não cumprimento de suas responsabilidades, destacadas neste mesmo documento.

6.5. SUPORTE

Foram definidos 3 (três) níveis de suporte para os ativos dos tipos servidor instalados nos Datacenters, a saber:

6.5.1. SUPORTE 1º NÍVEL

Gerência de Infraestrutura:

- Testes de conectividade – Ex. ping, traceroute e similares;
- Monitoramento de serviços – up/down;
- Aviso ao custodiante e/ou proprietário em caso de falha no ativo;
- “Reboot” após autorização por escrito do proprietário outros – a serem acordadas entre os envolvidos.
- Gerenciar a retirada e devolução de equipamentos, contendo descrição do ativo e motivo da retirada, autorizada pelo responsável pelo ativo (no mínimo gerente)

6.5.2. SUPORTE 2º NÍVEL

Custodiante do ativo:

- Realizar todas as atividades definidas como responsabilidade do custodiante, neste mesmo documento. Quando na impossibilidade de resolução do problema, notificar imediatamente o suporte de 3º nível;

6.5.3. SUPORTE 3º NÍVEL

Proprietário do ativo:

- Realizar todas as atividades definidas como responsabilidades do proprietário, neste mesmo documento. Quando na impossibilidade de resolução do problema, este será responsável em acionar suporte externo;

6.6. ITEM ESPECIAL: ENTRADA EM PRODUÇÃO DE UM NOVO ATIVO

Todo ativo tecnológico do tipo servidor, para entrar em produção, deverá ter o formulário de checklist devidamente preenchido pelo proprietário. Este formulário encontra-se na INTRANET, seção formulários.

7. NORMAS DE CLASSIFICAÇÃO DA INFORMAÇÃO

7.1. OBJETIVO

Ser um guia para a determinação do nível de segurança necessário para cada informação ou sistema (sistema corporativo, redes locais e serviços da rede). Os responsáveis pelos sistemas devem usar este guia para determinar o nível de segurança adequado exigido pelas redes locais, sistemas corporativos e serviços da rede sob sua responsabilidade.

7.2. ABRANGÊNCIA

Estas normas devem ser empregadas em todas as formas de informação que estejam disponíveis dentro do ambiente, garantindo que nenhum ativo de informação deixe de receber a devida classificação.

7.3. DESIGNAÇÕES DOS NÍVEIS DE SEGURANÇA

Os esforços de classificação de informações são baseados na sensibilidade da informação contida em sistemas e na criticidade operacional de disponibilidade da capacidade de processamento dos sistemas corporativos, redes locais e serviços da rede. Designações dos níveis de segurança são usadas para definir as exigências destes esforços de segurança.

7.4. INTRODUÇÃO AOS NÍVEIS DE SEGURANÇA

A designação do nível de segurança, dentro do programa de segurança de redes locais, sistemas corporativos e serviços da rede, é baseada na:

A. Sensibilidade da informação; ou seja, na necessidade de proteção da informação contra exposição não autorizada, fraude, roubo ou abuso;

B. Criticidade Operacional da Disponibilidade de Processamento da Informação; ou seja, as consequências causadas pela interrupção das capacidades de processamento de informações. Existem quatro níveis de designação de segurança para sensibilidade da informação e quatro níveis para criticidade operacional. O responsável pelo sistema deve considerar a segurança para cada sistema sob estes dois pontos de vista, e depois escolher a taxa mais elevada para o nível de segurança do sistema como um todo. Um sistema de informação deve ser compartimentado,

pois geralmente conjuntos de informações ou processos são mais sensíveis do que outros dentro de um mesmo sistema. O responsável pelo sistema deve designar o nível mais alto de qualquer conjunto de informações ou Processos dentro do sistema como a designação final do nível de segurança como um todo. Esta prática deve suportar a Confidencialidade, Integridade, e disponibilidade necessárias para tais sistemas como descrito abaixo:

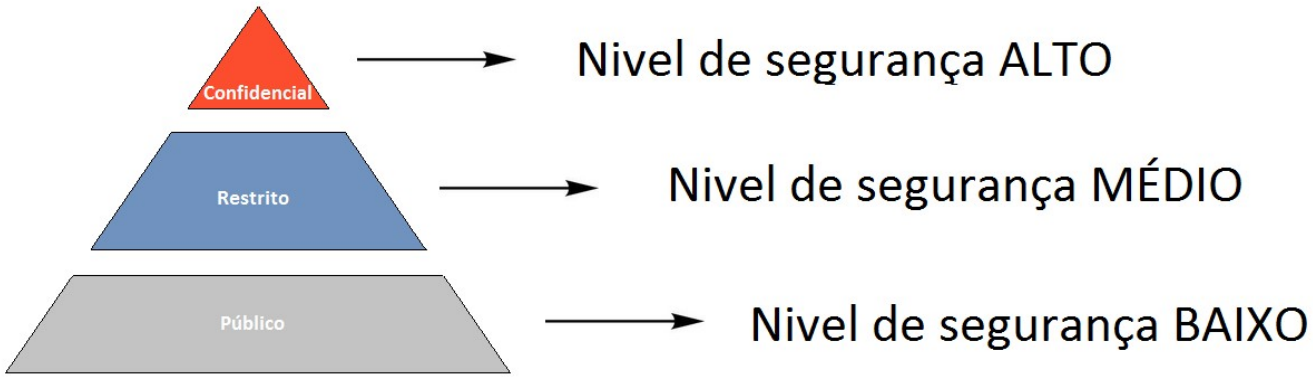
- **Confidencialidade**: O sistema contém informação que exige proteção contra exposição não autorizada.
- **Integridade**: O sistema contém informação que deve ser protegida contra modificação não autorizada, intencional ou não.
- **Disponibilidade**: O sistema contém informação ou fornece serviços que devem estar disponíveis o maior tempo possível baseado nas exigências da missão ou para evitar perdas substanciais.

Os profissionais responsáveis por redes locais, sistemas corporativos e serviços da rede devem certificar-se que as informações tratadas sejam acessadas somente por usuários autorizados que utilizem totalmente as exigências das salvaguardas do nível de segurança do sistema. Os Responsáveis por Redes locais, sistemas corporativos e serviços da rede devem tomar cuidados especiais quando especificarem o nível de segurança exigido para as redes locais, sistemas corporativos e serviços da rede, que utilizam serviços terceirizados de desenvolvimento do sistema e pessoal de suporte responsável pela manutenção dos sistemas. Ao especificarem o nível de segurança, os responsáveis por Redes locais, sistemas corporativos e serviços da rede deverão habilitar todos os registros possíveis de auditoria para que estes sejam auditados sempre que necessário.

A designação do nível de segurança de uma determinada classificação constitui a pilastra que vai possibilitar determinar as salvaguardas mínimas necessárias para proteger informações sensíveis e garantir a continuidade operacional crítica da capacidade de processamento das informações.

7.5. CLASSIFICAÇÃO DAS INFORMAÇÕES

As informações de propriedade da empresa, mantidas nos sistemas corporativos, devem ser classificadas de acordo com os níveis de segurança apresentados abaixo:



7.5.1. NÍVEIS DE SEGURANÇA DA INFORMAÇÃO

Os esforços de segurança de TI são baseados na sensibilidade de dados contidos nos sistemas, sejam as redes locais, os sistemas corporativos ou os serviços oferecidos pela rede e na disponibilidade de processamento destes sistemas. Designações de nível de segurança são usadas para definir exigências destes esforços de segurança.

7.5.2. CATEGORIA DE INFORMAÇÃO

As informações devem ser avaliadas de acordo com o critério de seleção descrito na tabela abaixo e devem ser associadas com o nível mínimo de segurança exigido.

Categoria	**Explicação e exemplos**	**Nível de segurança**		
		A	**M**	**B**
(1) Informação sobre indivíduos	Informação de pessoal, médica, e dados similares. Inclui todas as informações cobertas pela lei de privacidade tais como: salários, identificadores de usuários (ID's), perfil pessoal (endereço de casa e número telefônico), histórico médico, histórico do empregado e histórico de investigação (criminal/prisão).	A		

(2) Informações Financeiros, comerciais e contratuais.	Informações sobre movimentações financeiras e comerciais e informações de contratos firmados com clientes e parceiros. Informações sobre despesas e receitas de forma global.	A		
(3) Dados recebidos por intercâmbio eletrônico.	Quaisquer informações recebidas através de troca de dados eletrônica com os clientes e novas informações ou enriquecimentos gerados a partir destas.	A		
(4) Tecnologia nova.	Informação relacionada às ferramentas que estejam em desenvolvimento.	A		
(5) Informação sobre gerenciamento de configuração de sistemas.	Qualquer informação pertencente a operações da rede ou sistema computacional interno, tais como endereços de dispositivos de rede; esquemas de endereçamento de sistemas e protocolos implementados; protocolos de informação de gerenciamento de rede, pacotes de informação da rede, etc.; senhas de dispositivos e sistemas; informação de configuração de dispositivos e sistemas.	A		
(6) Diretrizes e manuais internos.	Qualquer documento disponibilizado pela empresa para fins de instrução/orientação/educação, nos vários setores da empresa, relativos a procedimentos internos.		M	
(7) Políticas e código de ética	Qualquer documento disponibilizado pela empresa para fins de instrução/orientação/educação, acerca das definições e diretrizes da empresa.			B

Legenda: A- Alta, **M**- Média, **B**- Baixo.

7.6. NÍVEIS DE SENSIBILIDADE PARA INFORMAÇÕES

Níveis de Sensibilidade classificam informações de acordo com o tipo de informação armazenada e necessidades específicas, governando a proteção ou exposição da informação armazenada.

7.6.1. INFORMAÇÃO PÚBLICA

Esta categoria classifica informações que exigem proteção mínima. Ameaças para estas informações são consideradas mínimas e somente as precauções mínimas do ambiente precisam ser tomadas para proteger a informação. Alteração não intencional ou destruição são as principais preocupações para esta classe de informação.

7.6.2. INFORMAÇÃO RESTRITA

Esta categoria classifica informações que devem estar restritas ao ambiente da empresa e que devem ser protegidas contra atos destrutivos e maliciosos.

Esta categoria inclui:

a) Informação gerencial sobre carga de trabalho, nomeação, e informações similares, geralmente em forma estatística, usadas para gerar relatórios. Acessos para estas informações precisam ser restritos somente para uma classe de usuários limitada;

b) Informações de e-mails e documentos que devem ser protegidos contra alteração ou exposição não autorizada. Estes tipos de informações incluem todas as correspondências, memorandos, e outros documentos que seu lançamento ou distribuição para fora da empresa precise ser controlado.

7.6.3. INFORMAÇÃO CONFIDENCIAL

Esta categoria classifica as informações mais sensíveis para a empresa. A informação nesta categoria exige o maior nível de proteção, salvaguarda e ambiente de usuário mais restrito.

Esta categoria inclui:

a) Informação sobre pagamentos e informação usada para autorizar ou fazer pagamentos para pessoas ou organizações. Estas informações são geralmente armazenadas em

redes locais, sistemas corporativos e serviços da rede em produção, e constituem informações privilegiadas, tais como a folha de pagamento;

b) Informação Proprietária que possui valor para a empresa e que deve ser protegida de exposição não autorizada;

c) Informações em e-mails e documentos considerados altamente sensíveis para a empresa, que devem ser protegidos de alteração não autorizada e/ou exposição antes do tempo;

d) Informações de registros de redes locais, sistemas corporativos e serviços da rede em que a exposição não autorizada constitua uma invasão;

e) Todas e quaisquer informações encaminhadas por clientes, via meios eletrônicos ou não.

8. NORMAS DE UTILIZAÇÃO DE MÍDIAS

8.1. OBJETIVO

Definir a utilização de todo o tipo de mídia de gravação de informações da empresa ou por ela mantidas.

8.2. ABRANGÊNCIA

Estas normas aplicam-se a todos os ativos de informação dentro da infraestrutura da empresa ou por ela mantidos.

8.3. DISPOSIÇÕES GERAIS

a) O controle sobre a utilização de mídias de armazenamento de dados é de responsabilidade da área de Infraestrutura de Tecnologia, que deve cuidar para que as normas aqui descritas sejam obedecidas nos processos da empresa;

b) Todos os dispositivos de armazenamento associados a servidores e computadores, fixos ou portáteis de todos os tipos, devem ser mantidos internamente nos respectivos dispositivos, evitando acesso indevido;

c) É vedado o uso de mídias removíveis dentro da infraestrutura da empresa, sendo bloqueados os meios de acesso para esse tipo de dispositivo (CDs, DVDs, *pendrives*, etc.);

d) Para qualquer necessidade específica de uso de mídias que não sejam fixas aos equipamentos da empresa, deverá ser registrado chamado para atendimento pela equipe de Suporte, que submeterá à avaliação da área de Segurança da Informação, que por sua vez – já garantido que a necessidade é válida – registrará a ocorrência junto à gerência da área solicitante. Todo o processo se dará pela área de tecnologia e não haverá liberação de uso dos dispositivos pelos solicitantes.

9. NORMAS DE DESCARTE DE MÍDIAS

9.1. OBJETIVO

Definir o tratamento de quaisquer mídias que possam conter informação, seja em seu descarte ou utilização para outra finalidade, garantindo que as informações anteriores não estejam acessíveis de qualquer forma.

9.2. ABRANGÊNCIA

Mídias óticas, eletrônicas e qualquer outro tipo de mídia onde possam registradas informações da empresa.

9.3. DISPOSIÇÕES GERAIS

a) Implementar procedimentos formais para identificar as mídias que requerem descarte seguro;

b) Destruir, de forma segura e protegida, as mídias a serem descartadas que contenham informações sensíveis referentes a empresa e/ou clientes, usando métodos tais como incineração ou trituração. Garantir e total remoção/inutilização da informação anterior para a reutilização de qualquer mídia para outras finalidades;

c) O descarte das mídias deve ser baseado na norma de classificação da informação;

d) As regras de descarte de informações devem estar em concordância com os procedimentos de alienação ou reutilização de equipamentos;

e) CD's, DVD's, e documentos em papel deverão passar pelo triturador antes de serem encaminhados ao lixo;

f) Formatação de baixo nível através de software do fabricante para HD's (portáteis ou fixos) em desuso ou que servirão a outras funções através da técnica WIPE (Sobrescrever de todos os setores pelo o caractere '0');

g) No caso de dispositivos defeituosos que contenham informações sensíveis, se faz necessário uma análise/avaliação de riscos para determinar se convém destruir fisicamente o dispositivo em vez de enviá-lo para o conserto ou descarta-lo. No caso de destruição física, os dispositivos deverão ser abertos e as mídias destruídas;

h) Registrar o descarte de mídias contendo informações sensíveis para manter uma trilha de auditoria.

10. NORMAS DE “MESA LIMPA”

10.1. OBJETIVO

As normas de "Mesa Limpa" são uma forma eficaz para reduzir os riscos de acesso não autorizado, perda ou dano à informação durante e fora do horário normal de trabalho. Como consequência, pessoas mal-intencionadas podem divulgar, modificar ou furtar informações restritas.

As informações deixadas nas mesas de trabalho (papéis, mídias magnéticas, etc.) são também alvos prováveis de perda em desastres como incêndios, inundações ou explosões.

10.2. ABRANGÊNCIA

As normas de “Mesa Limpa” devem ser consideradas para todos os departamentos e seguidas por todos os funcionários/colaboradores, de forma a garantir a conformidade com as definições desta política e a segurança de informações diversas e importantes para o negócio.

10.3. DISPOSIÇÕES GERAIS

a) Papéis e mídias de computador devem ser guardados, quando não estiverem sendo utilizados, em lugares adequados, com fechaduras ou outras formas seguras de mobiliário, especialmente fora do horário normal de trabalho;

b) Informações sensíveis ou críticas ao negócio, quando não requeridas, devem ser guardadas em local distante, de forma segura e fechada, de preferência em um cofre ou arquivo resistente a fogo, especialmente quando o escritório estiver vazio;

c) Pontos de recepção e envio de correspondências e máquinas de fax e telex não assistidas devem ser protegidos;

d) Equipamentos de reprodução (fotocopiadoras, "scanners" e máquinas fotográficas digitais) devem ser travadas ou de alguma forma protegidas contra o uso não autorizado fora do horário de trabalho;

e) Definir os autorizados a utilizar impressoras e fax no ambiente de atendimento. Excluir quaisquer configurações de impressoras padrões, além de não permitir a inclusão de impressoras sem a autorização adequada de administradores de rede;

f) Informações sensíveis e classificadas, quando impressas, devem ser imediatamente retiradas da impressora e fax;

g) As salas devem ser mantidas limpas, sem caixa ou qualquer outro material sobre o chão de modo a facilitar o deslocamento dos funcionários/colaboradores;

h) Chaves de gavetas, armários, de portas de acesso às salas e laboratórios de informática devem ser guardadas em lugar adequado, e não deixadas sobre a mesa ou guardadas com funcionários/colaboradores não autorizados.

11. NORMAS DE “TELA LIMPA”

11.1. OBJETIVO

As normas de "Tela Limpa" são uma forma eficaz para reduzir os riscos de acesso não autorizado, perda ou dano à informação durante e fora do horário normal de trabalho. Como consequência, pessoas mal-intencionadas podem divulgar ou modificar informações restritas, por meio do acesso não autorizado ao sistema.

11.2. ABRANGÊNCIA

As normas de “Tela Limpa” devem ser consideradas para todos os departamentos e seguidas por todos os funcionários/colaboradores, de forma a garantir a conformidade com as definições desta política e a segurança de informações diversas e importantes para o negócio.

11.3. DISPOSIÇÕES GERAIS

a) Os computadores pessoais, terminais de computador e impressoras devem ser desligados quando desassistidos;

b) Os equipamentos devem ser protegidos por mecanismo de travamento de tela e teclado controlados por senhas, chaves ou outros mecanismos de autenticação quando não estiverem em uso.

12. NORMAS DE SEGURANÇA DE SISTEMAS E DE REDE

12.1. OBJETIVOS

As normas para Sistemas e Rede têm como objetivo estabelecer os parâmetros que devem ser observados na confecção e manutenção dos sistemas (desenvolvidos e/ou adquiridos) e também da infraestrutura e segurança de redes de comunicação utilizadas pela empresa.

12.2. ABRANGÊNCIA

Estas normas se aplicam a todos os sistemas e redes onde sejam mantidas ou por onde circulem informações da empresa ou por ela mantidas.

12.3. DISPOSIÇÕES GERAIS

a) Todo o acesso a sistemas e/ou dispositivos para armazenamento, trânsito ou processamento de dados da empresa ou por ela mantidos, deve estar devidamente identificado e autenticado;

b) Acessos às redes de comunicação da empresa ou por ela mantidas, realizados a partir de origens externas, somente serão concedidos para finalidades específicas e revogados imediatamente à sua conclusão. Estes devem ter permissão específica nos dispositivos de segurança de borda e serem submetidos a não menos que dois níveis de autenticação;

c) Devem estar em atividade nas redes da empresa ou por ela mantidas, sistemas de firewall de borda (roteadores) e locais (estações de trabalho), detecção de intrusão baseados em *host* e em rede (HIDS/IPS), firewall de aplicação WEB (proxy), antivírus e filtros anti-spam. Os sistemas acima listados, devem manter a equipe de segurança da informação atualizada sobre todos os alertas pertinentes;

d) Os sistemas de detecção de intrusão, antivírus e outras ferramentas de proteção devem ter suas bases de dados atualizadas em um prazo máximo de 7 dias. Quando possível, criar rotinas de automação para esta tarefa;

e) Todos os ativos em produção na infraestrutura da empresa ou por ela mantidos devem ser atualizados conformo normas de atualização de patches desta política;

f) Devem ser garantidos os níveis exigidos de criptografia das informações que transitam nas redes de comunicação da empresa ou por ela mantidas, de acordo com a classificação da informação, garantindo que não haja acesso não autorizado ao conteúdo. O acesso às informações deve utilizar protocolo seguro (SSH, SFTP, SSL, etc.);

g) Quando identificado a manipulação e armazenamento de dados sensíveis, o armazenamento de dados em repouso deve ser criptografado, seguindo a aplicação de algoritmos de criptografia de armazenamento robustos como o AES-256.

h) Todos os ativos em produção na infraestrutura da empresa ou por ela mantidos, para armazenamento, processamento ou trânsito de informações da empresa ou por ela mantidas, devem estar adequados aos procedimentos de *hardening*, conforme os apontamentos específicos da equipe de segurança da informação;

i) Para todos os ativos em produção na infraestrutura da empresa ou por ela mantida, deverá existir método adequado de prevenção a qualquer atividade de software malicioso, incluindo métodos de diagnóstico e notificação em caso de ocorrência.

12.4. AVALIAÇÃO DE SEGURANÇA EXTERNA

Deverão ser realizadas em períodos não superior a seis meses, avaliações de segurança por empresa externa, contemplando, mas não se limitando a testes de penetração e vulnerabilidades nos sistemas e dispositivos de borda da infraestrutura da empresa ou por ela mantida.

13. NORMAS DE GERENCIAMENTO DE CHAVES CRIPTOGRÁFICAS

13.1. OBJETIVO

O objetivo desta política é estabelecer um conjunto claro de diretrizes e procedimentos abrangentes, visando a governança completa das chaves criptográficas. Ela aborda aspectos cruciais como a geração, custódia, revogação, design criptográfico, seleção de algoritmos, estratégias de troca e as medidas de segurança indispensáveis para salvaguardar a integridade, confidencialidade e autenticidade das informações sensíveis e a garantia da eficácia das técnicas de criptografia.

13.2. ABRANGÊNCIA

Esta norma engloba toda a gestão das chaves criptográficas usadas para proteger informações sensíveis em sistemas, aplicativos e comunicações dentro da organização.

13.3. GERAÇÃO DE CHAVE

a) As chaves criptográficas serão geradas por um algoritmo seguro e robusto.
b) A geração de chaves deve ser realizada em ambientes controlados e seguros.
c) A força das chaves deve ser compatível com os requisitos de segurança da aplicação.

13.4. CUSTÓDIA DE CHAVE

a) As chaves criptográficas devem ser armazenadas em um repositório seguro e de acesso restrito.
b) Deve ser mantido um registro de todas as pessoas ou entidades que têm acesso às chaves.
c) Chaves de recuperação (se aplicável) devem ser armazenadas separadamente das chaves de uso.

13.5. REVOGAÇÃO DE CHAVE

a) Um processo de revogação deve estar em vigor para desativar chaves comprometidas ou não utilizadas.
b) O processo de revogação deve ser executado de forma rápida e eficaz.

13.6. PROTOCOLO DE DESIGN CRIPTOGRÁFICO

a) Deve-se seguir as melhores práticas de design criptográfico ao selecionar algoritmos e protocolos criptográficos.
b) O design deve considerar a resistência a ataques conhecidos, incluindo ataques de força bruta e criptoanálise.

13.7. ALGORITMOS UTILIZADOS

a) Devem ser utilizados algoritmos de criptografia amplamente reconhecidos e seguros.
b) A escolha dos algoritmos deve ser revisada periodicamente para garantir a adequação contínua.

13.8. TROCA DE CHAVE

a) As chaves criptográficas devem ser substituídas periodicamente de acordo com a política de troca de chaves.
b) As chaves antigas devem ser devidamente destruídas ou arquivadas.

13.9. SEGURANÇA DO SISTEMA DE GERAÇÃO E ARMAZENAMENTO DE CHAVE

a) Os sistemas envolvidos na geração e armazenamento de chaves devem ser protegidos contra ameaças físicas e lógicas.
b) Deve ser implementado um controle de acesso rigoroso aos sistemas de gerenciamento de chaves.

c) Auditorias regulares devem ser conduzidas para verificar a conformidade com as políticas de segurança.

14. NORMAS DE SISTEMA DE REGISTRO DE LOGS

14.1. OBJETIVOS

Os registros de eventos dos sistemas têm por objetivo manter informações que ajudam na identificação de ataques, fraudes e outros eventos de segurança.

14.2. ABRANGÊNCIA

Estas normas aplicam-se a todos os ativos de tecnologia da informação onde residam ou sejam processadas informações, da empresa ou sob sua gestão, de maneira automática ou operacional.

14.3. DISPOSIÇÕES GERAIS

a) Padronizar os registros ("logs") de auditoria para as atividades de usuários, exceções e outros eventos de segurança da informação, incluindo: identificação dos usuários, datas e horários como detalhes de eventos-chave, identidade e localização da estação de trabalho, registros das tentativas de acesso aceitas e rejeitadas e outras informações relevantes;

b) Os administradores de sistemas não devem ter permissão de exclusão ou desativação dos registros ("log") de suas próprias atividades, seguindo as orientações estabelecidas nas regras de segregação de funções;

c) Definir, para cada conjunto de registros ("logs") de auditoria, uma periodicidade de retenção baseada em determinações de órgãos reguladores;

d) Manter um histórico da trilha de auditoria por pelo menos um ano, com um mínimo de três meses imediatamente disponível para análise (por exemplo, online, arquivado ou recuperável a partir do backup);

e) Armazenar os registros ("log") de auditoria em locais adequados, providos de controle de acesso, pelos períodos definidos;

f) Ter uma atenção especial à mídia de armazenamento dos registros, que deve ter validade superior ao período de retenção definido, de forma que as qualidades das evidências sejam mantidas;

g) Os servidores de "log" devem estar localizados em uma área de segurança, contendo uma console de gerenciamento;

h) Os servidores de "log" devem estar em uma rede segmentada da rede local, com proteção de dispositivos de segurança ("Firewall" e VLAN);

i) Os relógios dos servidores de "log" devem estar sincronizados;

j) Registrar todas as atividades executados nos servidores de "log";

k) Devem-se aplicar medidas de segregação de funções para assegurar que as pessoas autorizadas que realizam atividades nos servidores de "log" sejam diferentes daquelas que realizam a auditoria;

l) O acesso remoto aos servidores de "log" deve ser feito através de utilização de protocolos seguros (por exemplo: SSL/SSH); documentar todos os procedimentos dos servidores de "log", tais como: configuração e instalação, administração e operação, backup e manutenção, acessos a todas as trilhas de auditoria, inicialização dos registros de auditoria;

m) Alertas de sucesso e falhas de logins administrativos nos servidores deverão ser enviados para equipe de segurança (via e-mail, dashboards de monitoramento, etc.), para que qualquer acesso indevido seja identificado imediatamente.

15. NORMAS DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

15.1. OBJETIVO

Assegurar que os eventos de segurança de informação sejam tratados de forma efetiva, permitindo o adequado registro, investigação e tomada de ação corretiva em tempo hábil para mitigar o impacto negativo.

15.2. ABRANGÊNCIA

As normas para incidentes de segurança da informação devem ser observadas nas definições de todos os ativos, físicos e/ou lógicos, relacionados à informação da empresa ou sob sua gestão.

15.3. TIME DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

O time de resposta a incidentes de segurança da informação deverá ser composto por, no mínimo, representantes das seguintes áreas:

- Gerência de tecnologia da informação;
- Gerência de infraestrutura;
- Gerência de recursos humanos;
- Gerência jurídica.

Conforme a natureza do incidente, colaboradores de qualquer setor podem ser convocados a participar do time de resposta a incidentes de segurança da informação.

15.4. PROCEDIMENTO

Procedimento Formal de Gerenciamento de Incidentes de Segurança:

15.4.1. DETECÇÃO/IDENTIFICAÇÃO DO INCIDENTE

A detecção de incidentes pode se manifestar por meio de uma variedade de métodos e fontes, incluindo:

- Monitoramento Contínuo de Sistemas: A observação constante de sistemas e redes em busca de padrões incomuns, atividades suspeitas ou vulnerabilidades.
- Relatórios de Usuários: Comunicações dos próprios usuários da organização que identificam atividades anômalas ou comportamentos suspeitos em sistemas ou aplicativos.
- Análise de Logs: A análise detalhada dos registros (logs) gerados pelos sistemas e aplicativos para identificar eventos incomuns ou indicativos de intrusões.
- Identificação de Ameaças: O uso de soluções de segurança, como sistemas de detecção de intrusões (IDS) e sistemas de prevenção de intrusões (IPS), para identificar atividades maliciosas ou potencialmente prejudiciais.

Procedimentos/Ações:

- Receber a comunicação sobre o incidente.
- Detectar o incidente.
- Solicitar esclarecimentos ao informante, quando necessário.
- Registrar o incidente de forma completa e detalhada, incluindo informações relevantes como data, hora, localização, ativos/sistemas afetados, descrição do incidente e seus impactos e quaisquer evidências coletadas.
- Verificar a necessidade de autorização prévia do Comitê Gestor de Segurança da Informação (CGSI), conforme as políticas internas estabelecidas.

15.4.2. CATEGORIZAÇÃO/CLASSIFICAÇÃO DO INCIDENTE

Após a detecção, é imperativo que os incidentes sejam meticulosamente categorizados e classificados de acordo com sua gravidade e impacto.

Esta etapa é essencial para priorizar a resposta e alocar recursos eficazmente para mitigar o incidente, permitindo à equipe de resposta a incidentes compreender rapidamente a natureza do evento e tomar medidas proporcionais à ameaça identificada.

Além disso, a classificação apropriada dos incidentes contribui para a elaboração de relatórios precisos e a criação de registros históricos.

Esses registros são valiosos para análises de tendências e para aprimoramentos contínuos na postura de segurança da organização.

A tabela a seguir ilustra uma classificação geral de gravidade e impacto para alguns tipos comuns de incidentes:

Incidente	Gravidade	Impacto
Violação da Política de Segurança da Informação	Alta	Médio
Ocorrência de execução de malware	Alta	Alto
Comprometimento de credenciais	Alta	Alto
Identificação de vulnerabilidade	Média	Médio
Ocorrência de Intrusão/ataque	Alta	Alto
Discussão de assuntos sigilosos em ambientes públicos	Média	Médio
Violação de informações sensíveis (confidencial ou restrita)	Alta	Alto
Violação de Dados Pessoais (LGPD)	Alta	Alto

Neste contexto:

- **Gravidade:** denota a gravidade inerente do incidente, ou seja, a severidade intrínseca do evento.
- **Impacto:** reflete o impacto potencial do incidente na organização, incluindo suas implicações financeiras, legais, reputacionais, entre outras.

Essa tabela de classificação serve como um guia geral e deve ser personalizada de acordo com as políticas e prioridades específicas.

15.4.3. FLUXOS DE ESCALONAMENTO

Incidentes devem ser escalonados de acordo com sua gravidade e complexidade para as equipes encarregadas de seu tratamento. Esse processo pode incluir a ativação de equipes internas de segurança ou a colaboração com outras áreas da empresa, conforme necessário.

Esse procedimento visa assegurar que os incidentes sejam gerenciados de maneira eficaz e apropriada, com a devida atenção dada à sua natureza e potencial impacto.

15.4.3.1. COMUNICAÇÃO/NOTIFICAÇÃO

A comunicação desempenha um papel crítico, sobretudo nos incidentes envolvendo dados pessoais. Deve existir canais de comunicação dedicados para informar prontamente os clientes e a autoridade local de privacidade/proteção de dados, conforme exigido pelas regulamentações pertinentes. Essas notificações devem ser conduzidas em estrita conformidade com os prazos estipulados pelas normativas aplicáveis, garantindo a transparência e o cumprimento das obrigações legais relacionadas à gestão de incidentes de segurança.

15.4.3.2. HORÁRIOS DE COMUNICAÇÃO

Os horários de comunicação devem ser definidos de acordo com a gravidade do incidente e as exigências regulatórias. Incidentes graves podem exigir comunicação imediata, 24 horas por dia, enquanto incidentes menos críticos podem seguir um cronograma de comunicação definido.

15.4.3.3. CANAIS DE COMUNICAÇÃO

Devem ser estabelecidos canais de comunicação dedicados para notificação de incidentes, incluindo números de telefone, endereços de e-mail e contatos de emergência.

15.4.4. TRATAMENTO DE INCIDENTES

O tratamento de incidentes engloba um processo composto pelas seguintes etapas:

15.4.4.1. INVESTIGAÇÃO

Com base nas informações iniciais coletadas, em colaboração com outras áreas, a equipe de investigação tem a responsabilidade de investigar e determinar a causa raiz do incidente. Isso envolve a identificação se o incidente foi desencadeado por fatores externos, como vírus, ataques de hackers, ou se foi resultado de atividades internas, como acesso não autorizado ou vazamento de dados.

É essencial analisar quais ativos de informação foram afetados pelo incidente e compreender o alcance total do impacto. Isso inclui identificar os danos causados aos sistemas, dados e processos envolvidos.

Essa etapa é fundamental para subsidiar as decisões e ações necessárias para conter o incidente ou encaminhá-lo adequadamente.

15.4.4.2. CONTENÇÃO

Isolar o incidente de modo a impedir sua disseminação e a minimização de danos adicionais.

Dependendo da natureza das ações propostas, será necessário a autorização prévia do Comitê Gestor de Segurança da Informação (CGSI) antes de prosseguir com a implementação.

15.4.4.3. MITIGAÇÃO

Realização das medidas necessárias para resolução ou contenção do incidente.

Verificar se o resultado das ações aplicadas foi positivo ou negativo. Em caso negativo, novas medidas deverão ser adotadas.

15.4.4.4. RECUPERAÇÃO

Restaurar os ativos/sistemas afetados ao seu estado operacional, mesmo que de forma parcial, restabelecendo a integridade e a funcionalidade das operações.

15.4.4.5. GERAR EVIDÊNCIAS E/OU RELATÓRIOS

Em qualquer incidente e durante toda sua tratativa, evidências digitais devem ser coletas pois podem ser cruciais para investigações futuras ou para fins legais. Isso pode envolver a identificação dos dados necessários para esclarecer o incidente e a subsequente coleta e compilação desses dados, incluindo a geração de relatórios de logs de acesso, conforme apropriado.

15.4.5. ANÁLISE DO INCIDENTE

Após contenção do incidente, o mesmo deverá ser analisado como um todo, a fim de que o processo seja finalizado e não haja novas ocorrências similares.

A análise do incidente deve ser realizada em todas as áreas/setores, e em caso onde o incidente foi oriundo de uma ação interna ou descumprimento da Política de Segurança Interna, os responsáveis serão passíveis de sanções que incluem advertência verbal, advertência por escrito, suspensão e a demissão por justa causa, a depender de cada caso.

15.4.5.1. ANALISAR A CAUSA-RAIZ DO INCIDENTE

Auditoria de todo o cenário do incidente e identificar a porta de entrada do incidente. Verificar as vulnerabilidades exploradas, quais ameaças envolvidas, riscos e impactos.

15.4.5.2. PROPOSTAS DE MELHORIAS

Após auditoria do cenário, propor ações de melhorias, de forma a evitar novas ocorrências.

15.4.5.3. ELABORAÇÃO DO RELATÓRIO DE INCIDENTE

Elaboração do relatório de análise e caso necessário, encaminhar para o Encarregado de Dados, posteriormente para a deliberação da Diretoria.

IMPORTANTE: Sempre que o relatório envolve dados pessoais, o documento deverá ser protegido e armazenado em local restrito.

15.4.6. NOTIFICAÇÃO ANPD E TITULAR DOS DADOS

Deve-se analisar se o incidente envolve dados pessoais. Em caso positivo, necessário notificação formal à ANPD e ao titular dos Dados.

15.4.6.1. ANÁLISE DO IMPACTO AOS DADOS PESSOAIS

Com o incidente evidenciado, é necessário análise para averiguação se houve dano ao dados pessoais de colaboradores e/ou clientes. Avaliar internamente o incidente, e apurar a natureza, categoria e quantidade de titulares de dados afetados. Além disso, na avaliação interna também devem constar as consequências concretas e prováveis do incidente.

15.4.6.2. NOTIFICAÇÃO À ANPD E AO TITULAR DOS DADO

Constatado que no incidente de Segurança da Informação houve danos em Dados Pessoais, é necessário enviar relatório de notificação a ANPD e ao titular dos dados, com as circunstâncias e impacto da violação. Notificação realizada pelo Encarregados de Dados.

15.4.6.3. NOTIFICAÇÃO AO TITULAR DOS DADOS

Constatado que no incidente de Segurança da Informação houve danos em Dados Pessoais, é necessário enviar relatório de notificação ao titular dos dados, com as circunstâncias e impacto da violação. Notificação deve ser realizada pelo Encarregados de Dados.

15.4.7. ATIVIDADES PÓS-INCIDENTE (LIÇÕES APRENDIDAS)

Após a resolução do incidente, realizar uma análise para identificar lições aprendidas e melhorias necessárias no processo. Isso pode incluir a revisão das ações tomadas, identificação de pontos fracos e atualização das políticas e procedimentos de segurança.

15.4.8. DISPOSIÇÕES GERAIS

Este procedimento formal de gerenciamento de incidentes de segurança deve ser documentado, treinado e periodicamente revisado e testado por meio de simulações de incidentes para garantir sua eficácia.

16. NORMAS DE GERENCIAMENTO DE PATCHES

16.1. INTRODUÇÃO

A Política de Gerenciamento de Patches é o processo que identifica e instala continuamente atualizações de software para aplicativos, sistemas operacionais, dispositivos de rede, firmware e quaisquer outros recursos de TI aplicáveis utilizados pela organização.

16.2. OBJETIVO

A Política de Gerenciamento de Patches tem como objetivo monitorar quais patches foram aplicados anteriormente, instalar novos, bem como verificar se os patches foram instalados corretamente e se entregaram com êxito a correção prometida, garantindo segurança, continuidade, proteção e conformidade.

16.2.1. Benefícios do Gerenciamento de Patches:

- **Segurança aprimorada:** alguns patches fornecem correções importantes para problemas de segurança. Se não forem aplicados rotineiramente, aumenta o risco de ataques ligados a vulnerabilidades conhecidas.
- **Continuidade de negócios:** os patches podem fornecer atualizações que corrigem problemas de confiabilidade ou desempenho que, se deixados sem solução, podem causar erros e interromper as operações de negócios.
- **Proteção proativa:** o gerenciamento de patches ajuda a aplicar patches proativamente.
- **Cumprindo as regras de conformidade:** Mantém os softwares atualizados garantindo conformidade com organizações que têm como requisito de segurança que os softwares sejam atualizados.

16.3. ABRANGÊNCIA

Esta norma se aplica a todos os ativos, serviços e sistemas de informação que façam parte do ambiente de tecnologia da organização e que possuam potencial para impactar a segurança de seus sistemas e dados. A abrangência inclui, mas não se limita a:

- **Sistemas de TI:** Todos os sistemas, servidores, estações de trabalho e dispositivos de rede em uso pela organização, incluindo hardware, sistemas operacionais, aplicativos e serviços relacionados.
- **Aplicativos e Software:** Todos os aplicativos e software desenvolvidos internamente ou adquiridos de terceiros que são utilizados para fins comerciais ou operacionais.
- **Infraestrutura de Rede:** Todos os dispositivos de rede, como roteadores, switches, firewalls e gateways que fazem parte da infraestrutura de rede da organização.
- **Dados e Armazenamento:** Todos os dados sensíveis, informações de clientes, registros de transações e sistemas de armazenamento que contêm informações críticas.
- **Serviços Terceirizados:** Qualquer serviço de terceiros que esteja integrado ao ambiente de TI da organização e que possa afetar a segurança dos sistemas ou dados.
- **Dispositivos Móveis:** Dispositivos móveis, como smartphones e tablets, que se conectam à rede corporativa ou acessam recursos da organização.
- **Terceiros e Parceiros:** Qualquer sistema ou recurso controlado por terceiros ou parceiros comerciais que tenha um impacto direto ou indireto na segurança da organização.

A norma de gerenciamento de patches de segurança se aplica a todas as áreas e departamentos da organização e é de responsabilidade de todos os funcionários e partes envolvidas garantir o cumprimento dessas diretrizes. A abrangência pode ser ajustada conforme necessário para incluir novos ativos, serviços ou sistemas que sejam incorporados ao ambiente de tecnologia da organização.

16.4. DIRETRIZES DE GERENCIAMENTO DE PATCHES

16.4.1. GESTÃO DE ATIVOS

A gestão de ativos desempenha um papel fundamental no processo de gerenciamento de patches de segurança. É crucial que a organização tenha uma visão abrangente e precisa de todos os seus recursos de TI para garantir que nenhum ativo crítico seja negligenciado no ciclo de aplicação de patches. Portanto, a identificação dos recursos de TI existentes na organização deve ser realizada de maneira minuciosa e eficaz.

16.4.2. IDENTIFICAÇÃO E COLETA DE PATCHES

A equipe de segurança da informação deve monitorar fontes confiáveis de notificações de patches, como fornecedores de software, órgãos de segurança cibernética e grupos de discussão.

Patches devem ser categorizados com base em sua criticidade, impacto e aplicabilidade aos sistemas da organização.

A coleta de patches deve ser feita de forma sistemática e registrada em um repositório seguro.

16.4.3. AUDITORIA E ANÁLISE

Avaliações periódicas e varreduras contínuas nos ativos de TI para avaliar quais vulnerabilidades de segurança ou outros problemas podem impactar o ambiente devido a atualizações insuficientes.

16.4.4. CLASSIFICAÇÃO DE GRAVIDADE E PRAZOS DE ATUALIZAÇÃO

Caso um patch não possa ser atualizado imediatamente, a classificação de gravidade determina um tempo máximo para atualização.

- **Impacto crítico: 15 dias**

  Essa classificação é dada a falhas que podem ser facilmente exploradas por um invasor remoto não autenticado e levar ao comprometimento do sistema (execução de código arbitrário) sem exigir interação do usuário. É recomendável que se apliquem as atualizações Críticas imediatamente.

- **Impacto importante: 15 dias**

  Esta classificação é dada a falhas que podem facilmente comprometer a confidencialidade, integridade ou disponibilidade de recursos. É recomendável que se apliquem as atualizações Importantes assim que possível.

- **Impacto moderado: 20 dias**

  Essa classificação é dada a falhas que podem ser mais difíceis de explorar, mas ainda podem levar a algum comprometimento da confidencialidade, integridade ou disponibilidade de recursos. É recomendável que se apliquem as atualizações de segurança.

- **Baixo impacto: 30 dias**

  Essa classificação é atribuída a todos os outros problemas que podem ter um impacto na segurança, mas são considerados menos críticos. É recomendável que se apliquem as atualizações.

16.4.5. PRIORIZAÇÃO E AGENDAMENTO

Com base na classificação de gravidade, deve-se determinar quais patches priorizar e, em seguida, fazer um cronograma para aplicá-los.

Patches para correção de vulnerabilidades críticas de “dia zero” devem ser tratados com prioridade máxima.

Um procedimento de resposta a incidentes deve ser acionado para lidar com patches urgentes.

A implementação de patches urgentes deve ser monitorada de perto e revisada após a aplicação.

16.4.6. INSTALAÇÃO DE PATCH

Os patches devem ser atualizados de forma manual ou automática.

Sempre que a implementação não seja possível nos prazos acima descritos, deverão ser tomadas medidas apropriadas e temporárias que mitiguem os riscos expostos pelas respectivas vulnerabilidades.

As mudanças devem ser documentadas e rastreadas em um sistema de gerenciamento de mudanças.

Deve haver um processo de comunicação para informar aos usuários finais e partes interessadas sobre as interrupções planejadas.

16.4.7. TESTE E VERIFICAÇÃO

Todos os patches deverão ser testados em máquinas de teste antes de serem aplicados em sistemas de produção.

Após a instalação dos patches, deve ser feita análise em cada sistema e verificar os arquivos de log de instalação para confirmar se a instalação foi bem-sucedida.

16.4.8. RASTREAMENTO E MONITORAMENTO

A equipe de segurança da informação deve monitorar continuamente a eficácia do processo de gerenciamento de patches.

Deve-se controlar quais patches foram instalados e em quais sistemas.

Em caso de uma violação de segurança, deve ser possível verificar se ocorreu antes ou depois da atualização.

16.4.9. REVISÃO

A norma deve ser revisada periodicamente para incorporar melhorias e refletir as mudanças nas ameaças de segurança.

16.4.10. TREINAMENTO E CONSCIENTIZAÇÃO

Funcionários envolvidos no processo de gerenciamento de patches devem receber treinamento adequado.

A conscientização sobre a importância do gerenciamento de patches deve ser promovida em toda a organização.

17. NORMAS DE UTILIZAÇÃO DA INTERNET

17.1. OBJETIVO

Estabelecer responsabilidades e requisitos básicos de utilização da Internet no ambiente de Tecnologia da Informação e Comunicação (TIC).

17.2. ABRANGÊNCIA

Esta norma deverá ser aplicada a todos os usuários que possuam contas (sem privilégios de "administrador") nos ativos do tipo estações de trabalho e servidores do ambiente de Tecnologia da Informação e Comunicação (TIC).

17.3. CONCEITO

Sob o aspecto de proteção e integridade dos sistemas de informação, a Internet é classificada como conexão de alto risco. Os Usuários devem estar cientes, portanto, da peculiaridade da navegação na Internet, antes de acessá-la e de utilizar os seus recursos. Considerando que o uso da INTERNET, no âmbito da empresa, é uma concessão e não um direito, é de extrema importância que se estabeleça um conjunto de regras que possibilitem a utilização adequada desse importante recurso tecnológico.

Todos os Usuários dos ativos de informação de propriedade ou controlados pela empresa, ao utilizarem esse serviço, deverão fazê-lo no estrito interesse da empresa, mantendo uma conduta profissional.

17.4. NORMAS PARA UTILIZAÇÃO DA INTERNET

a) A empresa possui mecanismos de autenticação, que determinam a titularidade de todos os acessos à Internet feitos por seus usuários;

b) É expressamente proibida a divulgação e/ou o compartilhamento indevido de informações sigilosas em listas de discussão ou bate-papo;

c) Usuários com acesso à Internet não podem efetuar upload de qualquer software licenciado ou de dados de propriedade da empresa e/ou de seus clientes sem a autorização expressa da Diretoria ou do responsável pelo software/dado;

d) Os usuários poderão fazer download de arquivos da Internet que sejam necessários ao desempenho de suas atividades desde que observado os termos de licença de uso e registro desses programas/dados;

e) A Internet, no âmbito da empresa, é uma concessão e não um direito. Portanto, sua utilização, deve ser exclusivamente para atividades ligadas ao trabalho desempenhado na e para a empresa. Caso o usuário necessite utilizar à INTERNET para atividades não relacionadas com os negócios da organização e receba esta permissão, o mesmo deverá fazê-lo, preferencialmente, fora do horário do expediente;

f) Haverá geração de relatórios gerenciais dos sites acessados por usuários num determinado período. A Diretoria poderá ter acesso a essas informações a qualquer tempo;

g) O usuário deve utilizar a Internet de forma adequada e diligente;

h) O usuário deve utilizar a Internet observando a conformidade com a lei, a moral, os bons costumes aceitos e a ordem pública;

i) O usuário deve abster-se de utilizar a Internet como meio para a prática de atos ilícitos, proibidos pela lei ou pela presente norma, lesivos aos direitos e interesses da empresa ou de terceiros, ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, de seu uso ou de uso de terceiros;

j) O Usuário é pessoalmente responsável por todas as atividades realizadas por intermédio de sua chave de acesso;

k) É vedada a utilização de “modem” em máquinas que estejam conectadas ao ambiente da rede da empresa;

l) Os usuários que desejarem utilizar outras conexões, além daquelas já estabelecidas, deverão obrigatoriamente informar à Gerência de Segurança da Informação, de forma a não comprometer a segurança da rede da empresa;

m) Será de responsabilidade de cada usuário zelar pelo fiel cumprimento ao estabelecido na presente Norma;

n) É vedado o uso de sistemas de mensagens instantâneas (*instant messenger – IM*), tais como MSN Messenger, ICQ, mIRC e afins;

o) É vedado o uso de software de compartilhamento de dados ponto-a-ponto (*peer-to-peer - P2P*), tais como Kazaa, Emule e afins;

p) Não é permitido o acesso a sites de relacionamento, tais como Orkut, Twitter, Facebook e afins;

q) A empresa inibi o acesso a sites de pornografia, pedofilia, racismo e outros contrários à lei. O acesso a esses sites é terminantemente proibido no âmbito da empresa, mesmo que, por falha ou outro motivo, algum conteúdo dessa natureza não esteja bloqueado;

r) A não observância de qualquer item acima implicará nas sanções previstas nesta norma.

17.5. SANÇÕES

A monitoração do cumprimento das normas de utilização da INTERNET dar-se-á da seguinte forma:

a) Técnicos da Gerência de Segurança da Informação identificarão os usuários - doravante chamados de infratores - que violarem qualquer item desta norma de segurança;

b) Na primeira transgressão, esses infratores serão notificados, via e-mail, do descumprimento das Normas estabelecidas neste documento (Caso na infração cometida esteja caracterizado qualquer tipo de crime – acesso a sites de pedofilia, racismo, etc. –, aplicar-se-á a sanção especial desta norma);

c) Caso haja uma segunda transgressão da Norma, num período de 90 dias, esses infratores serão novamente notificados, via e-mail, sendo que uma cópia da notificação será enviada para o Gerente da área e para o Diretor;

d) Na terceira transgressão, as sanções administrativas previstas nas diretrizes gerais da Política Interna de Segurança da Informação da empresa serão aplicadas.

17.6. SANÇÃO ESPECIAL

Qualquer acesso a sites que tiverem conteúdo de pedofilia, racismo ou qualquer outro assunto contrário à lei que, eventualmente, não esteja bloqueado no sistema de proteção da empresa, é terminantemente proibido. A violação deste item implica em abertura de inquérito policial na delegacia competente.

18. NORMAS DE UTILIZAÇÃO DE E-MAIL

18.1. OBJETIVO

Estabelecer responsabilidades e requisitos básicos de uso dos serviços de Correio Eletrônico no ambiente de Tecnologia da Informação e Comunicação (TIC).

18.2. ABRANGÊNCIA

Esta norma deverá ser aplicada aos ativos de informação e comunicação da empresa.

18.3. CONCEITO

Prover a comunicação é, sem dúvida, a essência das redes. As pessoas sempre procuraram corresponderem-se da maneira mais rápida e fácil possível. O correio eletrônico (e-mail) é a aplicação que mais ilustra esta procura, pois reúne, entre outros, estes atributos. Entretanto, a facilidade de correio eletrônico fornecido pela empresa, deve ser usada no interesse do serviço, podendo ser, ocasionalmente, utilizada para mensagens pessoais curtas e pouco frequentes.

Considerando que o uso dos serviços de Correio Eletrônico, no âmbito da empresa, é uma concessão e não um direito, é de extrema importância que se estabeleça um conjunto de regras que possibilitem a utilização adequada desse importante recurso tecnológico.

Todos os usuários dos ativos de informação de propriedade ou controlados pela empresa, ao utilizarem esse serviço, deverão fazê-lo no estrito interesse da empresa, mantendo uma conduta profissional.

18.4. ACESSO AO CORREIO ELETRÔNICO

A liberação de acesso ao serviço, só será realizada com a devida autorização do gestor do setor pertinente, seguindo as orientações de segurança e possíveis autorizações dos clientes envolvidos.

Todas as contas de correio eletrônico terão uma titularidade, determinando a responsabilidade sobre a sua utilização.

Os usuários poderão ser titulares de uma única caixa postal individual no Servidor de Correio Eletrônico, com direitos de envio/recebimento de mensagens, via Intranet e Internet, enquanto perdurar o seu vínculo com a empresa.

Contas com inatividade por um período igual ou superior a 60 (sessenta) dias serão bloqueadas, a fim de evitar o recebimento de novas mensagens. Esta regra não se aplica as contas vinculadas aos cargos/funções, por serem inerentes às atribuições desses cargos/funções.

18.5. REGRAS PARA UTILIZAÇÃO DO CORREIO ELETRÔNICO (E-MAIL)

a) O usuário é o responsável direto pelas mensagens enviadas por intermédio do seu endereço de correio eletrônico;

b) O usuário deve utilizar o Correio Eletrônico de forma adequada e diligente;

c) É vedada a utilização do Correio Eletrônico, nas situações abaixo:

d) Envio de mensagens não autorizadas divulgando informações sigilosas e/ou de propriedade da empresa ou sob sua gestão;

e) Acesso não autorizado à caixa postal de outro usuário;

f) Uso de contas particulares dos usuários, através dos serviços Post Office Protocol - POP, Internet Message Access Protocol - IMAP e Simple Mail Transfer Protocol - SMTP de provedores externos;

g) Envio, armazenamento e manuseio de material que contrarie o disposto na legislação vigente, a moral e os bons costumes e a ordem pública;

h) Envio, armazenamento e manuseio de material que caracterize a divulgação, incentivo ou prática de atos ilícitos, proibidos pela lei ou pela presente Norma, lesivos aos direitos e interesses da empresa ou de terceiros, ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, do usuário ou de terceiros;

i) Envio, armazenamento e manuseio de material que caracterize:

- Promoção, divulgação ou incentivo a ameaças, difamação ou assédio a outras pessoas;
- Assuntos de caráter obsceno;
- Prática de qualquer tipo de discriminação relativa à raça, sexo ou credo religioso;
- Distribuição de qualquer material que caracterize violação de direito autoral garantido por lei;

- Uso para atividades com fins comerciais e o uso extensivo para assuntos pessoais ou privados;

j) Envio de mensagens do tipo “corrente” e “spam”;

k) Envio intencional de mensagens que contenham vírus eletrônico ou qualquer forma de rotinas de programação de computador, prejudiciais ou danosas;

l) Envio de mensagens que contenham arquivos com código e/ou extensão executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança de acordo com os critérios estabelecidos pela Gerência de Segurança da Informação da empresa;

m) Utilização de listas e/ou caderno de endereços da empresa ou de qualquer empresa para a distribuição de mensagens que não sejam de estrito interesse funcional e sem a devida permissão do responsável pelas listas e/ou caderno de endereços em questão;

n) Todo e qualquer procedimento de uso do Correio Eletrônico não previsto nesta Política, que possa afetar de forma negativa a empresa.

18.6. MANUTENÇÃO DE CONTAS

A equipe de tecnologia da informação (Setor de Helpdesk) é a área responsável pela inclusão, exclusão e alteração dos usuários de correio eletrônico. Esta tarefa será realizada de acordo com o procedimento definido na política de segurança da informação.

18.7. DISPOSIÇÕES FINAIS

A empresa se reserva o direito de verificar, sempre que julgar necessário, a obediência às normas e procedimentos citados neste documento.

As mensagens eletrônicas trafegam de forma aberta na Internet, passíveis de visualização. Para evitar que pessoas não autorizadas possam ter acesso a essas mensagens, a empresa fez uso de técnicas e ferramentas de criptografia.

O uso indevido dos serviços de Correio Eletrônico, tratados neste documento, é passível de sanção disciplinar, de acordo com a legislação vigente e demais Normas aplicadas à matéria.

Será de responsabilidade de cada usuário zelar pelo fiel cumprimento ao estabelecido na presente Norma, devendo também assinar o “Termo Individual de Responsabilidade”.

19. SANÇÕES E PUNIÇÕES

As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como demais normas e procedimentos de segurança, serão passíveis de penalidades que incluem advertência verbal, advertência por escrito, suspensão não remunerada e a demissão por justa causa.

A aplicação de sanções e punições será realizada conforme análise do Comitê Gestor de Segurança da Informação (CGSI), devendo-se considerar a gravidade da infração, efeito alcançado, recorrência e as hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, podendo o Comitê Gestor de Segurança da Informação, no uso do poder disciplinar que lhe é atribuído, aplicar a pena que entender cabível quando tipificada a falta grave.

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

Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano a empresa, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes sem prejuízo aos termos descritos nos parágrafos descritos anteriormente.

20. CASOS OMISSOS

Os casos omissos serão avaliados pelo Comitê Gestor de Segurança da Informação para posterior deliberação.

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

21. REVISÕES E ATUALIZAÇÕES

Esta política é revisada com periodicidade anual ou a qualquer tempo, conforme o entendimento da Equipe de Segurança da Informação.

22. DISPOSIÇÕES FINAIS

Quaisquer exceções as políticas aqui relacionadas deverão ser levadas à deliberação junto à diretoria e alta gerência da área responsável para análise de riscos e aprovação, que deverá ser devidamente documentada para registro.

_____

Diretoria de T.I.