POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Gabinete de Tecnologias de Informação (GTI)

Sede, Versão 1

Versão	Data da Emissão	Entrada em Vigor	Aprovado	Entidade Responsável
01	29/11/2024	29/11/2024	Comissão Executiva (CE)	GTI

Histórico de revisões

Versão	Revisor	Revisão	Próxima revisão

1. OBJETIVOS

Esta política estabelece diretrizes claras e práticas por forma a garantir que todas as informações sensíveis e críticas da organização sejam protegidas contra acessos não autorizados, violações de dados, e outras ameaças potenciais. Além disso, esta política visa assegurar o cumprimento de regulamentações legais, promover a conscientização sobre segurança entre os colaboradores e definir processos para a gestão eficaz de riscos e resposta a incidentes.
Ao se implementar está política espera-se fortalecer a confiança de clientes, parceiros e stakeholders, por forma a garantir uma operação contínua e segura.

2. ESCOPO

Este documento é a principal ferramenta de gestão de segurança dentro da INDICO SEGUROS SA e este por sua vez se esforça para:

- Fornecer linhas de decisão clara e níveis de responsabilidade;
- Dar orientação em determinadas situações específicas;
- Certificar-se da conscientização de segurança da informação em todos os níveis dentro da organização;
- Reduzir o risco a um nível aceitável;
- Proteger a propriedade e reputação da INDICO SEGUROS SA;

O equilíbrio entre estes objetivos é cuidadosamente decidido em todos os níveis da organização. O foco principal é fornecer uma compreensão detalhada das informações e responsabilidades de segurança para todos os níveis de colaboradors, fornecedores, parceiros e terceiros.
Um dos fatores críticos de sucesso para esta Política é a aceitação e o cumprimento não opcional, mas sim obrigatório e em simultâneo com o início de qualquer tipo de trabalho.
Qualquer violação desta Política de Segurança ou de documentos e decisões relacionadas será considerado uma infração disciplinar e estará sujeita à ação disciplinar dentro das normas estabelecidas pela organização.

3. REVISÃO E ATUALIZAÇÃO

A Política de Segurança da Informação é revista e, se necessário atualizada, ao menos anualmente
A equipe responsável pela revisão e atualização é composta atualmente por:
ARSON RIBISSE Membro do Comitê de segurança da informação
ALIRIO MABILANA Membro do Comitê de segurança da informação
RUBEN CHIVALE Membro do Comitê de segurança da informação

4. DIRETRIZES

Para a definição da Política de Segurança da Informação, foram consideradas as seguintes diretrizes:

- segurança como uma responsabilidade de todos;
- importância da ética no trato de informações sigilosas e de caráter confidencial e restrito da organização;
- melhoria contínua de processos e procedimentos;
- capacitação constante das pessoas ao tratar a informação.

4.1 - DEFININDO AS FUNÇÕES

Quando se fala em informação, algumas funções precisam ser identificados e possuem importância fundamental. São eles:

- Proprietário/Owner

É o "dono" da informação, encarregado de sua criação e classificação, dos recursos de informação sob sua responsabilidade, da validação, liberação e cancelamento do acesso aos recursos e aos locais.

- Responsável

Designado pelo Proprietário para validar, liberar e cancelar o acesso aos recursos e aos locais restritos.

- Custodiante

Responsável pela guarda e armazenamento da informação, definido pelo Responsável da Informação.

- Usuário

Pessoa autorizada pelo Proprietário ou Responsável a ler, incluir ou atualizar informações.

4.2 - CLASSIFICAÇÃO DA INFORMAÇÃO

A informação deve ser classificada de acordo com a sua confidencialidade e os prejuízos que sua divulgação não autorizada ou acidental possa causar. De acordo com esses parâmetros, as informações são classificadas em:

Classificação	Definição	Exemplos
Confidencial Restrita	Informação associaa aos interesses estratégicos da organização. Quem tem acesso: alta direção e colaboradors que são obrigados a conhecê-las pela função que exercem. Sua divulgação pode trazer sérias conseqüências, por isso exige medidas mais rígidas de controle.	Estratégias, vantagens competitivas, detalhes sobre um produto em desenvolvimento;
Confidencial	Informação cujo conhecimento está limitado a pessoas que precisam ter acesso a ela no seu dia-a-dia profissional. Sua divulgação também pode trazer graves conseqüências à corporação, portanto esse tipo de informação necessita de controle e proteção contra acessos não autorizados.	Procedimentos internos, estudos e projetos.
Uso Interno	Toda informação restrita para uso dentro da organização. Disponível ao Usuário interno. Pode ser revelada ao público externo se o Responsável autorizar.	Circulares, manuais de procedimentos, resultados de metas.
Informação Pública	Tudo o que pode ou deve ser divulgado para o público	Informações de produtos, marketing, informativos, resultados de metas, código de ética da INDICO SEGUROS SA.

Observações:

- O Proprietário ou o Responsável da Informação deve definir o nível da informação quanto à confidencialidade;
- A informação deverá ser reclassificada caso necessário.

4.3- RESPONSABILIDADES

Para garantir a implementação e a continuidade da Política de Segurança da Informação, formaram-se grupos onde cada um deles tem uma responsabilidade específica, confoorme abaixo.

Comitê de Segurança da Informação
• elaborar, divulgar e revisar periodicamente as normas de Política de Segurança da Informação;
• prover ações para disseminação e dar suporte ao cumprimento das normas;
• esclarecer eventuais dúvidas.

Corpo Gerencial
• garantir o cumprimento das normas pelos colaboradors de sua área;
• indicar o Responsável da Informação;
• divulgar a importância da política de senha segura;
• restringir o acesso às informações confidenciais.

Custodiante
• controlar o acesso às informações;
• adotar procedimentos de segurança;
• monitorar as informações sob sua custódia.

Comitê de Infra-estrutura de Tecnologia
• providenciar recursos de segurança;
• fornecer ferramentas para controle de acesso às informações.

Auditoria Interna
• realizar trabalhos para determinar o nível de cumprimento das normas.

Proprietário ou Responsável da Informação
• classificar/reclassificar informações sob sua responsabilidade;
• controlar acessos;
• criar controles.

Usuário
• conhecer e cumprir os controles de segurança estabelecidos;
• reportar ao superior imediato a exposição indevida das informações confidenciais.

4.4- MATRIZ RACI

Atividades	Corpo Gerencial	Custodiante	Comitê de Segurança da Informação	Usuário
Desenvolver e realizar treinamento	A	I	R	I
Revisar Política de Segurança da Informação	I	I	R	I
Compliance	R	C	I	I

5. FLUXO DE INFORMAÇÕES

Todas as informações devem obedecer aos critérios de classificação.

5.1 Fotocopiadoras

Todo usuário deverá utilizar a sua senha de impressão que é de uso pessoal e intransferível

Ao enviar o arquivo para impressão, o usuário deverá imediatamente verificar se o que foi solicitado já está disponível na impressora, não deixando documentos nas bandejas das impressoras mais tempo do que o necessário.

5.2 Estações de Trabalho

A política de Segurança de Estação de Trabalho define quatro níveis descritos abaixo:

Nível 1 - Padrão Básico de Segurança

Destinado aos equipamentos que não se enquadram nos demais níveis. Devem ser tratados como exceções e disponibilizados provisoriamente. É necessário aprovação do diretor da área.

Nível 2 - Padrão Intermediário de Segurança

Destinado aos equipamentos utilizados por Colaboradores que precisam de maior flexibilidade no uso de recursos sem deixar de atender as Políticas de Segurança da Informação. É necessário aprovação do diretor da área.

Nível 3 - Padrão Avançado de Segurança

Destinado a todos os equipamentos. Este é o nível padrão de segurança exigido nas estações de trabalho da Organização.

Nível 4 - Padrão Especial de Segurança

Destinado aos equipamentos utilizados exclusivamente para o acesso a determinadas aplicações

corporativas, não ocorrendo armazenamento de dados.

O quadro a seguir apresenta os recursos disponíveis na Política de Segurança de Estação de Trabalho:

Características	Nível 1	Nível 2	Nível 3	Nível 4
Bloquear execução de download da internet		X	X	
Bloquear compartilhamentos (arquivos ou pastas)		X	X	
Customização especial				X

5.3- Base de dados

Devem ser definidos critérios e perfis de acesso. Esses acessos devem ser revistos periodicamente, os usuários e senhas devem obedecer às boas práticas de utilização.

As aplicações deverão ter logs que registam os acessos dos usuários e modificações dos dados. Apenas usuários com acesso privilegiado podem acessar dados estratégicos, deverá haver uma lista de aplicativos separados pelo grau de criticidade para operação.

Deve ser implementada técnica de "mascaramento" de dados críticos, onde os campos de maior importância são mascarados com caracteres especiais.

7. Segurança nos recursos humanos

Embora o GTI seja responsável pela gestão da Segurança Corporativa, cabe a todos os colaboradores zelar pela segurança do seu local de trabalho.

Todos os colaboradores devem guardar ou descartar adequadamente materiais confidenciais, manter gavetas e armários fechados, desligar ou bloquear estações de trabalho e notebooks, zelar pelos bens e ativos da Organização, entre outras ações que vem detalhadamente explicita na politica de mesa limpa.

7.1- TÉRMINIO OU MUDANÇA DO CONTRATO

7.2.1 - Devolução de Ativos/equipamentos

Na necessidade de devolução ou substituição do ativo/Equipamento, deve-se realizar previamente a eliminação das informações armazenadas, de forma que não seja possível a sua recuperação.

O Descarte da informação é feito segundo a politica de eliminação de dados.

7.2.2 - Acessos

Quando um colaborador é transferido entre departamentos, o Director que o transferiu deve certificar-se de que todos os direitos de acesso aos sistemas e outros controles de segurança ainda serão necessários na sua nova função e informar ao GTI qualquer com o conhecimento do DPB acerca da modificação necessária;

O Diretor deve enviar e-mail solicitando a remição dos acessos do colaborador à qualquer recurso a rede sistemas e aplicativos. Deve-se verificar a necessidade de troca de senhas de contas de uso comum ao departamento, evitando o acesso às informações.

Após a comunicação do responsável, solicitando a exclusão dos acessos do colaborador, os acessos são excluídos automaticamente por meio da atualização da base de dados do DPB, conforme rotina de processamento.

8. Controle de Acesso

É reservado o direito de desativar uma conta de usuário, por parte da equipe do GTI, caso verifique-se a ocorrência de Incidentes suspeitos de quebra de segurança nas contas dos colaboradores.

8.1- Solicitação de Registro de usuário/acesso

Todo colaborador poderá ter uma conta para acesso aos recursos da rede de computadores da Organização. Os acessos a demais sistemas devem ser informados pelo responsável da área no momento da solicitação da conta do colaborador. Para solicitação de criação de conta para novos colaboradors, os responsáveles devem proceder conforme descrito abaixo:

O Diretor de departamento a que o colaborador pertence deverá fazer uma solicitação de criação da conta, através do formulário Solicitação de Acessos, onde deverá informar os dados do colaborador, bem como os acessos para cada sistema que serão necessários.

O GTI retornará para o Diretor do departamento com as informações sobre a conta criada com o conhecimento do DPB.

8.2- MECANISMOS de Autenticação

O mais comum é o fornecimento de um nome de usuário e uma senha que seja apenas de seu conhecimento, entretanto, existem outros mecanismos de autenticação homologados. Cada um deles aplica-se a um conjunto de plataformas e/ou sistemas específicos

8.2.1- Gerenciamento de senha do usuário

As senhas são utilizadas por todos os sistemas e são consideradas necessárias como meio de autenticação. A eficiência das senhas depende do usuário, pois estes podem escolher senhas óbvias e fáceis de serem descobertas, ou ainda compartilha-las com outros colaboradores, não mantendo o sigilo necessário.

Regras Gerais

A concessão de senhas deve ser controlada, considerando:

- A senha deve ser redefinida pelo menos a cada 30 dias,

- As senhas devem ser bloqueadas após 3 a 5 tentativas sem sucesso, sendo que, o administrador da rede e o usuário devem ser notificados sobre estas tentativas.

- As responsabilidades do administrador do sistema incluem o cuidado na criação e alteração das senhas dos usuários, além da necessidade de manter atualizados os dados dos mesmos.

- As responsabilidades do usuário incluem, principalmente, os cuidados com a manutenção da segurança dos recursos, tais como sigilo da senha e o monitoramento de sua conta, evitando sua utilização indevida. As senhas são sigilosas, individuais e intransferíveis, não devendo ser divulgadas em nenhuma hipótese.

- Tudo que for executado com a senha de usuário da rede ou de outro sistema será de inteira responsabilidade do usuário.

As senhas são efetivas apenas quando usadas corretamente e sua escolha e uso requerem alguns cuidados como:

- Utilizar senha com pelo menos, oito caracteres;
- Misturar caracteres maiúsculos e minúsculos;
- Misturar números, letras e caracteres especiais;
- Incluir pelo menos, um caracter eespecial;

Utilize um método próprio para lembrar da senha, de modo que ela não precise ser escrita em nenhum local, em hipótese alguma;

- Não anotar a senha em papel ou em outros meios de registro de fácil acesso;
- Não utilizar o nome do usuário;
- Não utilizar o primeiro nome, o nome do meio ou o sobrenome;
- Não utilizar nomes de pessoas próximas, como da esposa(o), filhos ou amigos;
- Não utilizar senhas com repetição do mesmo dígito ou da mesma letra;

8.4- Acesso a Recursos

8.4.1- Normas e Procedimentos para a Gestão de Acessos a Recursos

A gestão do acesso a um recurso compreende as seguintes atividades:

- proteção;
- solicitação de permissão de acesso;
- aprovação ou negação da permissão de acesso;
- alteração no perfil de acesso;
- revisão com frequência mínima anual das permissões de acesso.

8.4.2- Proteção do Recurso

A proteção corresponde ao cadastramento do recurso com o respectivo perfil de acesso nas bases de dados do software de segurança do servidor em que o recurso está alocado.

São elegíveis para proteção lógica todos os recursos que armazenam ou processam informações de propriedade da Organização. O Responsável do Recurso é o responsável pela definição da proteção do recurso. Compete ao responsável avaliar os riscos inerentes ao acesso ao recurso sendo protegido e selecionar o nível de proteção adequado, em função desses riscos.

8.4.4- Solicitação de Permissão de Acesso ao Recurso

As solicitações de acesso a recursos para colaboradores ou prestadores de serviço são de responsabilidade dos solicitantes das suas respectivos áreas. Os userids genéricos devem ser requisitados pelos órgãos de TI responsáveis pelos processos associados às mesmas.

Deve ser considerado na permissão e/ou concessão de acessos o princípio do mínimo privilégio, ou seja, os usuários (ou processos) devem acessar apenas os recursos necessários para o desempenho de suas atividades.

8.4.5- Aprovação ou Negação da Permissão de Acesso

O responsável pela aprovação ou negação da permissão do acesso ao recurso é o responsável do recurso.

Esse processo é decorrente da solicitação de permissão de acesso.

Antes de permitir ou negar o acesso ao recurso, o responsável deve obter as informações necessárias para subsidiar sua decisão.

Essas informações incluem:

- o motivo da permissão de acesso solicitada;
- o tipo de permissão de acesso necessária;
- o nível de acesso necessário.

Recomenda-se o contato com o solicitante responsável pelo encaminhamento da solicitação.

O responsável deve selecionar o perfil que melhor representa o recurso cuja permissão de acesso foi solicitada.

8.4.6- Revisão Periódica das Permissões de Acesso ao Recurso

Compete ao responsável do recurso a revisão periódica das suas permissões de acesso.

A periodicidade dessa revisão é mensal e a mesma é feito em coloboração com os Diretores de cada unidade orgânica.

Na revisão, o responsável deve obedecer ao princípio de mínimos privilégios, ou seja, os usuários ou processos devem acessar apenas os recursos necessários para o desempenho de suas atividades.

Os casos de dúvidas com relação à composição de grupos de userids e a necessidade de permissão de acesso por usuários e processos que compõem o perfil de acesso ao recurso devem ser tratados diretamente com os solicitantes ou aprovadores responsáveis por esses usuários e processos.

Recomenda-se que o responsável mantenha registros dos processos de revisão efetuados, para efeito de controle e auditoria.

8.5-Arquivos e Banco de Dados

Não é permitido acesso direto a arquivos e banco de dados de produção. Para o acesso dos usuários, deve existir uma aplicação (ex. Web) que faça a conexão ao Banco de Dados.

8.5.1- Acesso Emergencial

No caso de exceção de acesso de analistas de sistemas a arquivos ou banco de dados de produção cuja propriedade seja de uma área de negócios, este acesso deve ser feito de forma temporária e com alçada de aprovação mínima de superintendente.

8.5.2- Utilização de Usuário Genérico

Os usuários têm ciência de que é proibida a utilização de Usuário Genérico para logon pessoal, e que estão sujeitos a penalidades previstas no caso de violação desta diretriz de segurança.

A conexão aos bancos de dados em produção deve ser realizada por meio de usuário sistêmico.

8.5.3- uso dos serviços de Rede

Esse tópico visa definir as normas de utilização da rede que abrange o LOGIN, a manutenção de arquivos no servidor e as tentativas não autorizadas de acesso. Estes itens serão abordados para todos os usuários dos sistemas e da rede de computadores da Organização.

Regras Gerais

- Não são permitidas tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta. Isso inclui acesso aos dados não disponíveis para o usuário, conectar-se a servidor ou conta cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes;

- Não são permitidas tentativas de interferir nos serviços de qualquer outro usuário, servidor ou rede. Isso inclui ataques e tentativas de provocar congestionamento em redes, tentativas deliberadas de sobrecarregar um servidor e tentativas de “invadir” um servidor;

- Materiais de natureza pornográfica e discrminatória não podem ser expostos, armazenados, distribuídos, editados ou gravados através do uso dos recursos computacionais da rede;

- A pasta partilhada ou similar, não deverá ser utilizada para armazenamento de arquivos que contenham assuntos sigilosos ou de natureza específica. Ela deve ser utilizada apenas para armazenar informações de interesse geral;

- Não são permitidas alterações das configurações de rede e inicialização das máquinas, bem como demais modificações que não sejam justificadas e efetuadas pelo GTI.

8.6- Estações de Trabalho

Cada estação de trabalho possui códigos internos os quais permitem que ela seja identificada na rede. Sendo assim, tudo que for executado na estação de trabalho será de responsabilidade do

usuário. Por isso, sempre que sair de frente da estação de trabalho, o usuário deverá ter certeza que efetuou o logoff ou bloqueou a estação de trabalho.

Os equipamentos são recursos da Organização e, como tais, devem ser utilizados de acordo com as diretrizes descritas nas Políticas de Segurança da Informação.

Regras Gerais

- as estações de trabalho devem ser utilizadas exclusivamente para realização de atividades profissionais da Organização;

- as informações corporativas devem ser armazenadas em servidores de arquivos, onde existam processos consolidados e direcionados a sua integridade, disponibilidade e confidencialidade;

- a senha é pessoal e intransferível, não sendo permitido o seu compartilhamento;

- todas as estações de trabalho devem estar associadas a um domínio válido pela Organização para garantir que as políticas de segurança sejam aplicadas;

- todas as estações de trabalho devem possuir software antivírus instalado, atualizado e ativo;

- todas as estações de trabalho devem possuir somente softwares e aplicativos homologados);

- todas as estações de trabalho devem ser desligadas ao final do expediente. Caso não seja desligada, há um sistema que desligará automaticamente o equipamento. Exceções devem ser justificadas;

- utilizar a proteção de tela corporativa definida pela Organização;

- não é permitida a conexão e/ou sincronização de equipamentos particulares na rede da Organização;

- não é permitida a alteração física nos componentes dos microcomputadores tais como memória, discos etc.;

- a instalação de qualquer software de segurança deve ser analisada e autorizada pelo GTI.

As ferramentas que violam direitos autorais, como, por exemplo, cracks e keygens (geradores de licenças), não são autorizados.

- não é permitida a instalação de softwares não homologados pela instituição.

- todos os notebooks devem ser equipados com cabos de aço de segurança, presos às mesas e o disco rígido deve estar criptografado.

- os desktops devem ser dotados de cadeados para proteção contra o furto de placas de memória e discos rígidos.

- deve haver um processo de eliminação de dados dos desktops e notebooks quando da substituição, descarte ou cessão desses equipamentos, para evitar a recuperação de dados críticos por terceiros.

8.6.1- Política de mesa limpa

A política de mesa limpa deve ser considerada para todos os departamentos e seguida por todos os colaboradors/colaboradores, de forma a garantir que papéis e mídias removíveis não fiquem

expostas ao acesso não autorizado.

Regras Gerais

- Os papéis ou mídias de computador não devem ser deixados sobre as mesas, quando não estiverem sendo usados. Devem ser guardados de maneira adequada, de preferência em gavetas ou armários trancados;

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

- Sempre que o computador não estiver em uso, não se deve deixar nenhum arquivo aberto, de modo que as informações possam ser visualizadas por outras pessoas que estiverem no local;

- Agendas, livros ou qualquer outro material que possa conter informações sobre a empresa ou informações particulares devem sempre ser guardadas em locais fechados, evitando o acesso de outras pessoas que não as responsáveis pela informação.

- 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 colaboradors/colaboradores não autorizados.

8.7- Comunicação Móvel

O uso de dispositivos móveis dentro de áreas críticas deve ser restringido, havendo a necessidade de controle e monitoração dessa atividade.

Os dispositivos móveis de propriedade da organização devem possuir mecanismos de criptografia de dados (recebidos e enviados), devendo também permitir a configuração de senha de acesso.

8.7.1- Equipamentos Particulares

Não é permitida conexão ou sincronização de qualquer equipamento particular na rede da organização.

Os equipamentos particulares não devem ser utilizados para armazenamento de informações da Organização.

As violações a esta Política estão sujeitas a sanções disciplinares

8.8– Trabalho remoto

Deverá existir um processo de aprovação de utilização com alçada de aprovação superior para utilização de acesso remoto onde deve ser estipulado um período de concessão do acesso (este período não pode ser permanente), bem como o nível de acesso que este usuário possuirá.

8.7.1- Normas para Utilização de Acesso Remoto

O acesso remoto pode ser utilizado por colaboradores colaboradors e colaboradores terceiros em atividades de suporte técnico. Essa situação possui norma específica de utilização.

8.7.1.1- Utilização do Acesso Remoto pelos Colaboradores Colaboradors e Colaboradores Terceiros

8.7.1.1A- Solicitação de Cadastramento de Acesso Remoto
Deve ser realizada via sistema WEB por usuário solicitante. A alçada para aprovação é de diretor, superintendente e gerente que aprova a solicitação eletronicamente no sistema WEB e manualmente para colaboradors ou colaboradores terceiros que não possuem acesso ao sistema WEB utilizando o Termo de Solicitação e de Responsabilidade para Acesso Remoto. Após o acesso ser aprovado, o colaborador ou colaborador terceiro receberá um e-mail com as instruções de instalação.
O Termo de Recebimento para Acesso Remoto deverá ser assinado e encaminhado para GTI, para confirmação de recebimento e inicialização do para sua utilização em caso de cadastro manual.

9. Conscientização da Segurança

Materiais destinados a aumentar a compreensão e a consciência dos colaboradores da Organização sobre a importância da segurança da informação, serão rotineiramente divulgados. Estes materiais irão enfatizar a importância dos procedimentos de segurança da informação, especialmente no que tange à informação eletrônica protegida.

10. Informações de Controle

Vigência:01.01.2024 a 31.12.2025

Versão: 1.0

Aprovado por:

Diretor do Gabinete de Tecnologia de informação - CISO

Security Officer

Superintendente de Segurança da Informação

Responsável do Comitê de Segurança da Informação

ANEXO I – TERMO DE COMPROMISSO

TERMO DE COMPROMISSO

Identificação do Colaborador	
NOME	
BI	

DIREÇÃO	
CATEGORIA	

Comprometo-me a:

1. Executar minhas tarefas de forma a cumprir com as orientações da Política de Segurança e com as Normas e Padrões vigentes.

2. Utilizar adequadamente os equipamentos da Organização, evitando acessos indevidos aos ambientes computacionais aos quais estarei habilitado, que possam comprometer a segurança das informações.

3. Não revelar fora do âmbito profissional, fato ou informações de qualquer natureza que tenha conhecimento devido a minhas atribuições, salvo em decorrência de decisão competente do superior hierárquico.

4. Acessar as informações somente por necessidade de serviço e por determinação expressa do superior hierárquico.

5. Manter cautela quando a exibição de informações sigilosas e confidenciais, em tela, impressoras ou outros meios eletrônicos.

6. Não me ausentar do local de trabalho sem encerrar a sessão de uso do computador ou sistema, evitando assim o acesso por pessoas não autorizadas.

7. Observar rigorosamente os procedimentos de segurança estabelecidos quanto à confidencialidade de minha senha, através dos quais posso efetuar operações a mim designadas nos recursos computacionais que acesso, procedendo a:

A. Substituir a senha inicial gerada pelo sistema, por outra secreta, pessoal e intransferível;

B. Não divulgar a minha senha a outras pessoas;

C. Nunca escrever a minha senha, sempre memorizá-la;

D. De maneira alguma ou sobre qualquer pretexto, procurar descobrir as senhas de outras pessoas;

E. Somente utilizar o meu acesso para os fins designados e para os quais estiver devidamente autorizado, em razão de minhas funções;

F. Responder em todas as instâncias, pelas conseqüências das ações ou omissões de minha parte que possam por em risco ou comprometer a exclusividade de conhecimento da minha senha ou das transações a que tenho acesso;

G. Reportar imediatamente ao superior imediato ou ao Administrador de Segurança em caso de violação, acidental ou não, da minha senha, e providenciar a sua substituição.

H. Solicitar o cancelamento de meus usuário/senhas quando não for mais de minha utilização.

I. Solicitar o cancelamento de usuários/senhas solicitados para funcionários/terceiros sob minha responsabilidade, quando do seu desligamento ou término do serviço que originou a respectiva solicitação.

DS DS DS

Declaro estar ciente das determinações acima, compreendendo que quaisquer descumprimentos dessas regras podem implicar na aplicação dos sansões disciplinares cabíveis.

Maputo _____ de _____ de _____.

_____.

Assinatura do Colaborador

Histórico do documento

Revisão Nº	Páginas revistas	Alterações efectuadas	Data	Validação		
				Elabobrou	Aprovação (CE)	Assinaturas
1	Não aplicável	1ª Edição	29.11.2024	GTI	Ruben Chivale Olivio Melembe Nasma Omar	DocuSigned by: BB56AA22FCF9481... DocuSigned by: B9A331054376452... DocuSigned by: 7A41BCF05F2F42F...