POLÍTICA DE

SEGURANÇA DA INFORMAÇÃO

POLI-0001-01

MANTENHA APENAS UM: CONFIDENCIAL | RESTRITO | **USO INTERNO** | PÚBLICO

Obs. Este documento contou com a contribuição da Innocenti Advogados (consultora externa)

Controle de Versões

Data	Versão	Comentários	Autor
01.06.2021	1.0	Versão Inicial	Mariana M. Carregaro
13.01.2024	2.0	Revisão	Mariana M. Carregaro
13.01.2025	3.0	Revisão	Mariana M. Carregaro

Identificação e Classificação

Código do Documento	Tipo	Classificação
POLI-0001-01	Política	Restrito

Equipe e Responsáveis Envolvidos

Profissionais Envolvidos
Mariana M. Carregaro – Consultora Externa (Innocenti Advogados)
Lidiane P. dos Reis Barros – Encarregada

Documentos de Apoio ou Relacionados

Documentos de Apoio
Política de Incidente de Segurança (T.I.)
Política de Gestão de Risco (T.I.)
Política de Gestão de Continuidade do Negócio (T.I.)
Política de Backup e Restauração (T.I.)
Política de Mesa e Tela Limpa
Política de Senhas
Política de Notificação de Violação (T.I.)
Política de Auditoria Interna (T.I.)
Evidência e Controle das Vulnerabilidades Cibernéticas

Aprovação da Diretoria Responsável

Diretor Responsável	Ratificação	Data
Alexandre Gonçalves Duarte	APROVADO	13.01.2025

Sumário

1. Administrando e Organizando a Segurança 5
1.1. Descrição Geral 5
1.2. Responsável pela Segurança da Epeople 5
1.3. Modo de Operação da Epeople 6
1.4. Procedimento Administrativos 6
1.5. Relatando Incidentes de Segurança 7
1.6. Gerenciamento de Risco 8
1.7. Auditoria 8
2. Segurança Física 9
2.1 Ambientes de Segurança da Epeople 9
2.1.1 Ambiente de Segurança 9
2.1.2 Ambiente de Segurança Local 9
2.1.3. Ambiente de Segurança Eletrônica 10
2.2. Procedimentos de Verificação quando do Término da Hora de Trabalho 11
2.3 Controle de Equipamentos Informatizados da Epeople 11
3. Proteção Pessoal 11
3.1. Pessoas Autorizadas a participar do SIC 11
4. Segurança da Informação Física 12
4.1. Transferir Informação de/para usuários da Epeople 12
4.2. Armazenamento de Documentos Físicos 13
4.3. Ambiente de Armazenamento de Dados 13
4.4. Classificando e Etiquetando Documentos 14
4.5. Arquivando e Destruindo Documentos dentro da Epeople 17
5. Segurança da Informação Digital 17
5.1. Segurança de Hardware 17
5.2. Segurança de Software 18
5.3. Identificando Usuários 20
5.4. Autenticação de Usuários 20

5.5 Utilizando o Serviço de E-mail da Epeople 20
5.6. Utilizando o serviço de Internet 22
5.7. Acesso ao *Fileserver* 23
5.8. Backups 23
5.9. Erros (*Dropdowns* do Sistema) 24
5.10. Proteção Antivírus 24
5.11. Gestão Automática de Segurança e Auditoria 25
6. Gerenciamento de Configurações 25
7. Medidas de Planejamento para Emergências 27

1. Administrando e Organizando a Segurança

1.1. Descrição Geral

Na **Epeople** o responsável pela área de T.I. administra e organiza a segurança do ambiente tecnológico da **Epeople**, incluindo todo o conjunto de políticas e procedimentos operacionais.

1.2. Responsável pela Segurança da Epeople

Em razão da estrutura enxuta da **Epeople**, o responsável pela T.I. é suficiente para organizar, administrar e implementar todas as medidas de destinadas ao desempenho e bom funcionamento da **Epeople**.

As responsabilidades gerais deste responsável são:

- viabilizar a segurança de informações sigilosas armazenadas ou processadas pela área administrativa, comercial e de operações;
- inspecionar locais pertencentes a **Epeople** de um ponto de vista do ambiente de segurança global, local e eletrônico;
- realizar controles de segurança para testar a implementação de medidas de segurança na **Epeople**;
- avaliar os resultados dos testes de segurança realizados;
- elaborar procedimentos operacionais de segurança na **Epeople**;
- coordenar e regular a atividade interna no campo da proteção da informação em todos os departamentos dentro da **Epeople**;
- informar sobre possíveis ameaças, vulnerabilidades e riscos de segurança e propor medidas para prevenir, eliminar ou reduzir seus efeitos; e
- organizar atividades para treinar pessoal envolvido no processo de gerenciamento de informações dentro da **Epeople**.

DEMAIS MEMBROS da **Epeople** e usuários, cujas principais responsabilidade são:

Classificação do Documento: Restrito

- participar de treinamentos organizados;
- conhecer e atender aos procedimentos e regras de segurança aprovados para estações de trabalho e suas normas de aplicação para a **Epeople**;
- conhecer e atender aos procedimentos e regras de segurança aprovados para os postos de trabalho e suas normas de aplicação para os departamentos dos quais fazem parte;
- conhecer e cumprir as disposições dos procedimentos implementados para a segurança dos dados pessoais;
- classificar e gerenciar corretamente as informações recebidas de acordo com as condições de segurança;
- assinar o "Termo de Responsabilidade"; e
- comunicar imediatamente qualquer violação ou incidente relacionado à segurança dos sistemas da **Epeople**, bem como quaisquer outros problemas significativos do ponto de vista de segurança do sistema utilizado pela **Epeople**.

1.3. Modo de Operação da Epeople

O modo de operação da **Epeople** é considerado de "HIGH LEVEL", isto é, TODAS as pessoas com direito de acesso ao sistema da **Epeople** estão autorizadas para o mais alto nível de classificação das informações armazenadas, tratadas ou transmitidas ao sistema e acesso à informação e, é diferenciada, de acordo com o princípio da "necessidade de saber".

1.4. Procedimento Administrativos

A desconexão do acesso ao sistema do Office 365 da **Epeople** pode ser o resultado de uma decisão do responsável de T.I., enviando previamente uma notificação a esse respeito para sócia fundadora, quando:

- Não respeitar as medidas aprovadas na documentação de segurança;
- A ocorrência com novos riscos de segurança de nível inaceitável;
- Não cumprir as medidas aprovadas através da documentação de segurança;

- A ocorrência de um incidente de segurança e o não cumprimento de procedimentos relativos ao endereçamento de incidentes de segurança; e
- Reorganizando a localização ou o sistema.

1.5. Relatando Incidentes de Segurança

Os incidentes de segurança podem ser classificados da seguinte forma:

a) Incidentes Maiores – esses incidentes são referentes a qualquer um dos casos abaixo:

- Desenvolvimento ou possíveis ações de sabotagem;
- Violações de regras de segurança com o resultado de comprometer informações confidenciais;
- Descobrir vulnerabilidades significativas no sistema da **Epeople**, sistemas de detecção de intrusão, sistemas de detecção e extinção de incêndios ou quaisquer outros sistemas físicos ou eletrônicos;
- Incidentes significativos causados por software mal-intencionado que podem afetar outros sistema ou que possam ativar outros tipos ou versões desconhecidas de softwares mal-intencionados;
- Incidentes envolvendo ações criminosas no TI; e
- Incidentes causados por catástrofes naturais, acidentais ou causados por negligência da equipe, que afetam a segurança, equipe e / ou ativos da **Epeople**.

b) Incidentes Regulares – esses incidentes podem ser relacionados a qualquer dos casos abaixo:

- Incidentes isolados causados por software mal-intencionado conhecido; e
- Violações de regras de segurança que não fazem parte da categoria de incidentes principais;

No caso de descoberta da ocorrência de incidentes maiores as seguintes medidas devem ser tomadas:

Classificação do Documento: Restrito

a) a pessoa que descobriu a falha tem de reportar imediatamente ao responsável de T.I.;
b) o responsável de T.I. comunica o incidente à sócia fundadora da **Epeople**, que determina a imediata pesquisa para determinar a falha ocorrida; e
c) assim que as causas do incidente tenham sido determinadas, o responsável de T.I. encaminha, o quanto antes, o formulário preenchido com medidas tomadas para remediar o incidente e / ou que deve ser implementado para o gerenciamento da **Epeople**.

1.6. Gerenciamento de Risco

O responsável de T.I. da **Epeople** tem a função de verificar cada local dentro da **Epeople**, pelo menos, uma vez por ano, bem como a qualquer momento, ao ser notificado de modificações infligidas em condições existentes.

Após finalizar as inspeções de verificação, o responsável de T.I. da **Epeople** elabora um novo relatório de análise de risco e determina quais medidas são necessárias para minimizar riscos e evitar vulnerabilidades reconhecidas.

1.7. Auditoria

Auditoria refere-se às atividades realizadas para monitorar eventos relacionados à segurança da informação dentro da **Epeople**.

Os registros de auditoria do sistema são consultados pelo responsável de T.I., a fim de identificar possíveis tentativas fracassadas de acesso ao sistema da **Epeople**.

2. Segurança Física

2.1 Ambientes de Segurança da Epeople

2.1.1 Ambiente de Segurança

Para a **Epeople**, o ambiente de segurança consiste na proximidade de outros departamentos onde a **Epeople** realiza sua atividade.

Assegurar a segurança do ambiente é de responsabilidade de todos os profissionais da **Epeople**, a fim de proibir o acesso não autorizado de terceiros em locais onde a presença não é necessária e, inclui as seguintes medidas:

- Barreira física protegendo os limites do escritório;
- Controle de acesso (eletrônico, eletromecânico ou por outros meios); e
- Luzes de CCTV e segurança.

Para que as pessoas tenham acesso ao interior da **Epeople**, elas devem ser identificadas; os visitantes são identificados e seus dados de identificação são registrados nos registros de controle de acesso; eles são acompanhados durante toda a visita e sua atividade ocorre na presença do pessoal da organização.

2.1.2 Ambiente de Segurança Local

O ambiente de segurança local consiste nas salas onde a **Epeople** desempenha sua atividade.

A área onde os equipamentos pertencentes a **Epeople** estão instalados deve ser classificada como sendo pelo menos no nível de "**área administrativa**".

Classificação do Documento: Restrito

O acesso a salas projetadas para equipamentos conectados à rede da **Epeople** é limitado e permitido apenas para profissionais que executam atividades nessa área.

As estações de trabalho são colocadas de modo a:

- Impedir a visualização não autorizada de informações colocando o monitor contra as portas de acesso na área de informações classificadas; e
- Impedir a colocação perto de possíveis fontes de inundação.

2.1.3. Ambiente de Segurança Eletrônica

O ambiente de segurança eletrônica é definido por limites de segurança significativos no contexto eletrônico ou de processamento.

Cada estação de trabalho tem opções para realizar gravações de auditoria e login ativas.

A rede da **Epeople** é protegida usando as seguintes tecnologias e equipamentos:

a) Tecnologias do tipo SSL / TLS;
b) Tecnologias de tipo de inspeção de estado - o acesso aos servidores de distribuição é filtrado usando um firewall; e
c) Tecnologias do tipo antivírus - o servidor de correio tem um servidor antivírus integrado, que verifica todas as mensagens, tanto as recebidas como as enviadas.

Medidas e mecanismos de proteção são implementados para a segurança dos servidores, visando:

- Controle de acesso usando um nome de usuário e uma senha com pelo menos 8 caracteres;
- Impossibilidade para usuários do sistema com direitos limitados de acesso por meio da desativação de contas de shell no servidor;
- Proteção antivírus atualizada automaticamente; e

- Fornecer disponibilidade de todas as funções e serviços configurando máquinas em regime 1 + 1.

2.2. Procedimentos de Verificação quando do Término da Hora de Trabalho

Os usuários da **Epeople** são obrigados a encerrar a sessão de trabalho usando "Log off" ou "Suspender" a cada vez que sais da estação de trabalho.

2.3 Controle de Equipamentos Informatizados da Epeople

O responsável de T.I. elabora e mantém uma lista de equipamentos aprovados para uso dos colaboradores.

A lista de equipamentos contém o nome do equipamento, o tipo e a série.

É proibido trazer ou usar equipamentos ou dispositivos que permitam armazenar ou enviar dados eletrônicos na área onde as informações classificadas são gerenciadas, exceto aquelas aprovadas pela sócia fundadora.

3. Proteção Pessoal

3.1. Pessoas Autorizadas a participar do SIC

A aprovação do acesso às informações classificadas é obtida de acordo com os procedimentos internos da organização.

A "necessidade de saber", para informação classificada, é estabelecida pela sócia fundadora da

Epeople por meio de decisão interna.

Cada usuário com direito de acesso possui uma conta pessoal que pode ser acessada com base no nome de usuário e senha (que deve ser pessoal e intransferível).

Os portais de acesso remoto ao sistema da **Epeople** devem ser acessados apenas por usuários autorizados com base em uma conta de usuário, criada pelo responsável de TI e uma senha estabelecida pelo usuário após a criação da conta.

Principais obrigações dos usuários:

- Conhecer e cumprir os procedimentos operacionais e regulamentos de segurança aprovados para estações de trabalho, dependendo do nível de acesso aprovado;
- Conhecer a as Políticas da **Epeople**;
- Gerenciar, em condições de segurança, as informações recebidas; e
- Notificar imediatamente o responsável do T.I. sobre qualquer violação ou incidente relativo à segurança do sistema que encontrar ou quaisquer outros problemas significativos do ponto de vista de segurança da **Epeople**.

4. Segurança da Informação Física

4.1. Transferir Informação de/para usuários da Epeople

As informações recebidas pelos usuários da **Epeople** são salvas no Onedrive e/ou pasta de Sharepoint específica, especialmente para cumprir com a "Política de backup".

A informação classificada é armazenada dentro de uma área especial, creditada pela organização de acordo com os regulamentos de proteção interna das informações classificadas.

A distribuição das informações classificadas é feita de acordo com a "necessidade de saber" com

base em uma autorização de acesso específica.

É proibido excluir mensagens classificadas ou documentos do sistema sem a aprovação prévia do responsável de T.I.

Periodicamente, os documentos podem ser salvos em ambientes de armazenamento, rotulados e armazenados dentro do compartimento de evidência de documentos classificados.

É proibido transmitir informações de fomento industrial e segredos comerciais, além de outros dados de operação da **Epeople**, para pessoas não autorizadas, ou através de sistemas que não sejam certificados no mesmo nível de classificação das informações.

Informações de fomento industrial e segredos comerciais devem ser redigidos de forma sigilosa e, ter o nível de confidencialidade dos documentos devidamente classificados e protegidos.

4.2. Armazenamento de Documentos Físicos

Os documentos da **Epeople** são armazenados em armários encontrados dentro das salas onde o pessoal da **Epeople** executa sua atividade diária.

Os documentos classificados são armazenados em recipientes de segurança encontrados em uma sala autorizada pela organização da **Epeople**.

4.3. Ambiente de Armazenamento de Dados

Os ambientes de armazenamento das informações, usados para salvar ou transferir informações classificadas, devem estar registrados nos ambientes de armazenamento, mantidos em um local autorizado.

Os ambientes de armazenamento incluem tags / etiquetas especiais que contêm o número de registro e o nível de classificação.

Os ambientes de armazenamento são assumidos pelos usuários com base na assinatura do registro de evidências. Ambientes de armazenamento dedicados para informações classificadas não podem ser usados para armazenar outras informações.

4.4. Classificando e Etiquetando Documentos

Os documentos impressos devem ser classificados e etiquetados de acordo com o nível de confidencialidade. Lembrando que, somente as pessoas autorizadas aos documentos classificados é que podem ter acesso aos mesmos.

Dentro da **Epeople**, os seguintes tipos de informação são processados, armazenados e transmitidos:

CATEGORIA DE CONFIDENCIALIDADE	CLASSE DE CONFIDENCIALIDADE	NÍVEL DE CONFIDENCIALIDADE
INFORMAÇÃO NÃO CLASSIFICADA	PÚBLICO	NÃO CONFIDENCIAL
INFORMAÇÃO INTERNA	PRIVADO	INTERNA
INFORMAÇÃO CLASSIFICADA	RESTRITA	RESTRITA
	CONFIDENCIAL	CONFIDENCIAL

Categoria – **INFORMAÇÃO NÃO CLASSIFICADA**

Classe – **DOCUMENTOS PÚBLICOS**:

NÃO CONFIDENCIAL

- Informações acessíveis a qualquer usuário de e para a **Epeople**.
- Marcação de dados e evidência: não requer qualquer marcação ou evidência especial; são documentos, dados ou informações obtidas de fontes públicas.
- Autorização: o acesso não deve ser autorizado.
- Divulgação: não é confidencial.

Categoria – **INFORMAÇÃO INTERNA**

Classe – **DOCUMENTOS PRIVADOS**:

*INTERNO(código de cor – Modelo: Vermelho, Amarelo, Azul _ as cores de classificação podem ser alteradas de acordo com o interesse da **Epeople**)*

- Tais informações, por sua importância, são acessíveis apenas a um número restrito de pessoas autorizadas, que não devem ser tornadas públicas e que podem ser utilizadas dentro da **Epeople** pelos funcionários; Tais informações podem ser distribuídas aos parceiros da **Epeople** após a conclusão de acordos de confidencialidade com eles.

- Marcação de dados e evidência: marcadas como INTERNOS ou não, estes documentos, dados ou informações processadas, armazenados ou manuseados dentro da **Epeople**, serão considerados restritos aos funcionários e deverão ser comprovados de acordo com o regimento interno.

- Autorização: Somente funcionários da **Epeople** têm acesso a tais documentos de acordo com o princípio de "necessidade de saber".

- Disseminação: Sua divulgação deve ser evidenciada nos registros internos (Registro de entrada / saída).

- Esta categoria inclui, mas não se limita aos seguintes tipos de informação:

  - Informações de contato dos funcionários;
  - Políticas da companhia, procedimentos e regulações;
  - Comunicações internas e específicas para a **Epeople**; e
  - Informações relativas à lista de fornecedores da **Epeople**.

Categoria – **INFORMAÇÃO CLASSIFICADA**

Classe - Restrita *(Código de cor: fica a critério da **Epeople**)*

- Marcação de dados e evidência: exige uma marcação especial e evidência de acordo com os regulamentos de proteção interna para informações classificadas.

- Autorização: Todos os funcionários da **Epeople** que executam sua atividade dentro de projetos determinados devem ter acesso às autorizações para informação RESTRITA. As autorizações para acessar a informação RESTRITA são obtidas de acordo com as especificações definidas pela **Epeople**.

- Disseminação: A disseminação da informação RESTRITA deve ser evidenciada no Registro de Evidência de Informação Restritas.

classe – DOCUMENTOS **CONFIDENCIAIS:**

*CONFIDENCIAL (Código de cor: fica a critério da **Epeople**)*

- Marcação de dados e evidência: exige uma marcação especial e evidência de acordo com os regulamentos de proteção interna para informações classificadas.

- Autorização: Todos os funcionários da Epeople que executam sua atividade dentro de projetos determinado devem ter autorizações de acesso às informações **CONFIDENCIAIS**. As autorizações de acesso à INFORMAÇÕES CONFIDENCIAIS são obtidas pela gerência, de acordo com os procedimentos internos específicos.

- Divulgação: Sua disseminação deve ser evidenciada no Registro de Evidência de Informação sobre INFORMAÇÕES CONFIDENCIAIS.

- Esta categoria inclui, mas não se limita aos seguintes tipos de informação:

- Arquivo pessoal dos funcionários, organograma e folha de pagamento;
- Dados sobre clientes da Epeople;

- Planos de desenvolvimento;
- Dados financeiros ainda não publicados; e
- Planos de negócio da Epeople.

4.5. Arquivando e Destruindo Documentos dentro da Epeople

O arquivamento de documentos classificados é feito de acordo com as regulamentações nacionais relativas à proteção de informações.

Se for necessário substituir o HD que foi utilizado para informação classificada, este deve ser destruído e / ou eliminado utilizando um produto certificado, e a operação é executada, com a aprovação da **Epeople**.

As operações relativas à destruição dos ambientes de armazenamento são registradas em um relatório de destruição, aprovado pelo responsável de T.I., no qual é apresentado o método de destruição, quem executou as operações e a data das operações.

O relatório de destruição é armazenado de acordo com os regulamentos internos relativos à proteção da informação.

5. Segurança da Informação Digital

5.1. Segurança de Hardware

Usuários autorizados da **Epeople** são obrigados a conhecer e cumprir os procedimentos de trabalho e equipamentos eletrônicos.

O departamento de TI é responsável por uma instalação, manutenção e modificação corretas das configurações dos componentes de hardware.

Classificação do Documento: Restrito

Os equipamentos de hardware nos quais as informações classificadas são armazenadas e marcadas com as mensagens de aviso no nível máximo de classificação das informações circuladas.

A manutenção / reparação de equipamentos é feita pelo pessoal autorizado dentro do departamento de TI ou de empresas de manutenção.

A fim de evitar a possibilidade de recuperar determinadas informações classificadas das restantes memórias do equipamento, estas devem ser excluídas da seguinte forma:

- Memórias são removidas do equipamento;
- São instalados em um equipamento similar para processamento de informações sigilosas e não conectados a outros sistemas;
- Várias aplicações são lançadas em execução e dados não classificados são usados para processamento no equipamento que executa as memórias;
- O equipamento é reiniciado, repetindo as operações anteriores por pelo menos três ciclos; e
- O equipamento está parado e as memórias são retiradas e reinseridas dentro do equipamento básico.

5.2. Segurança de Software

As aplicações de computador aprovadas a serem instaladas em todos os terminais conectados à rede da **Epeople** são:

- sistemas Operacionais Windows;
- servidor de e-mail e sistema do Office 365;
- suíte de aplicativos MSOffice;
- Adobe acrobat reader; e
- antivírus de software Kaspersky.

O software instalado é licenciado e assegurado pelo resposnável de TI.

É proibido instalar outras categorias de software, exceto as aprovadas e instaladas pelo responsável de TI.

As sessões dos terminais são bloqueadas após 5 minutos de inatividade e podem ser desbloqueadas com a inserção da senha.

O sistema operacional é atualizado com as melhorias necessárias em relação à segurança (hot-fixes, patch-es, service-packs) apenas pelo responsável de TI.

Firewalls são implementados com base nos princípios de privilégios minimalistas e mínimos, sendo assim configurado:

- Registra todos os aplicativos bloqueados pela política de segurança;
- Recusa o tráfego de saída que não pode ser gerado por endereços internos;
- Recusa todo o tráfego gerado por endereços de origem inválidos;
- Recusa o tráfego de fontes externas que possam ser geradas por endereços internos;
- Remonta os fragmentos em pacotes completos antes de aplicar a política de segurança do firewall.

Para prevenir e detectar intrusões ou outros ataques cibernéticos ao seu endereço, a **Epeople** se beneficia de serviços específicos da ferramente de antivírus. Os eventos dentro da rede da **Epeople** são registrados e armazenados por um período de 6 meses.

Nos servidores Exchange, todas as mensagens são verificadas com vários mecanismos antivírus / antispyware / antispam licenciados.

5.3. Identificando Usuários

Todas as pessoas com acesso à **Epeople** são identificáveis e autorizadas. Os endereços de e-mail são criados no servidor de e-mail do Office 365 da **Epeople**, correspondente a cada usuário.

Cada usuário com direitos de acesso ao terminal interno da **Epeople** possui uma conta pessoal no computador conectado ao sistema atribuído por um nome de usuário e senha.

Apenas o responsável de TI pode estabelecer e configurar as contas dos usuários autorizados.

Somente sócia fundadora e o responsável de T.I. têm acesso à conta de administrador.

5.4. Autenticação de Usuários

Senhas de usuários preenchem as seguintes condições:

- São trocadas a cada 3 meses;
- Letras maiúsculas e minúsculas devem ser usadas, números, caracteres especiais que são aceitos pelo mecanismo de autenticação;
- O comprimento das senhas deve ser de pelo menos 8 caracteres;
- Eles não têm significado ou identidade lógica; e
- Ao alterar a senha, uma senha diferente das 5 anteriores deve ser escolhida (histórico de senhas -5).

É proibido escrever a senha ou transmiti-la a outras pessoas.

Estações de trabalho conectadas à rede da **Epeople** são configuradas para ativar a proteção de tela após 5 minutos de inatividade e inserindo a senha.

5.5 Utilizando o Serviço de E-mail da Epeople

O serviço de correio eletrônico (e-mail) da **Epeople** deve melhorar os serviços para os clientes desta, por meio de uma melhor comunicação interna e externa e, ao mesmo tempo, reduzir o uso de spam e outros programas maliciosos. Os colaboradores que usam o sistema de correio eletrônico da **Epeople** devem aderir às seguintes políticas e procedimentos:

a) Devem ser utilizados apenas para uso da **Epeople**;
b) Todas as informações criadas, enviadas ou recebidas através deste serviço, incluindo todas as mensagens de e-mail e arquivos eletrônicos, são de propriedade da **Epeople**;
c) Os usuários devem garantir que o endereço de e-mail correto do destinatário seja escrito dentro da caixa Para...;
d) Qualquer mensagem de arquivo transmitida por e-mail deve incluir o nome do colaborador;
e) O uso de outras contas de e-mail pessoais é proibido sem a aprovação prévia da sócia fundadora;
f) As informações confidenciais não devem ser transmitidas por e-mail sem serem sinalizadas como tal;
g) As mensagens de e-mail devem conter uma linguagem apropriada e profissional - é proibido distribuir mensagens racistas e preconceituosas que possam discriminar, incluir elementos pornográficos, obscenas ou com outras ofensas;
h) É proibido o uso do sistema de e-mail da **Epeople** para fins pessoais ou outros fins que não sejam negócios sem o acordo prévio da organização;
i) É proibido transmitir pontos de vista pessoais sobre eventos sociais, políticos, religiosos ou outros eventos que não estejam relacionados com o negócio da **Epeople**; e
j) É proibido transmitir, via e-mail, materiais comerciais ou publicitários que não tenham sido solicitados pela **Epeople**.

5.6. Utilizando o serviço de Internet

O responsável de TI autoriza e aprova as conexões de Internet usadas dentro da **Epeople** e cuida das operações relacionadas à proteção das conexões de acesso à Internet por meio das operações de firewall atuais.

Todos os usuários da **Epeople** que têm acesso à Internet devem cumprir as disposições expressas nas políticas de segurança de TI e agir em conformidade.

Qualquer outra conexão adicional deve ser autorizada e aprovada pelo departamento de TI. Essas conexões auxiliares podem ser, mas não limitadas a:

a) Modems de dados ou qualquer outro dispositivo de comunicação que permita conexão à internet ou a outras redes;
b) Acesso a rede sem fio;
c) O uso da internet deve ser feito seguindo os seguintes aspectos:
   - Todos os funcionários devem usar o acesso à internet para fins profissionais e para a atividade atual;
   - Todos os colaboradores devem utilizar o acesso à Internet em conformidade com as disposições legais em vigor;
   - O uso da conexão de internet pelos usuários é monitorado e registrado;
d) A **Epeople** não possui nenhum controle sobre as informações acessadas pelos usuários na Internet e sobre seu conteúdo, assim, a **Epeople** não assume qualquer responsabilidade sobre as informações acessadas por seus usuários e seu conteúdo;
e) Qualquer software ou arquivos baixados através da internet através da rede da **Epeople**, tornam-se propriedade DESTA; qualquer elemento baixado deve ser usado pelos funcionários em conformidade com os direitos de licenciamento e uso aferentes;
f) A **Epeople** se reserva o direito de bloquear, temporária ou permanentemente, o acesso a determinados sites, serviços ou até mesmo suspender a conexão com a internet;
g) Qualquer arquivo baixado da internet, antes de ser aberto deve ser escaneado com o software de proteção antivírus da **Epeople**;

Classificação do Documento: Restrito

h) O uso da internet da **Epeople** é proibido nos seguintes casos:

- Acesso, upload, download ou distribuição de material pornográfico ou com conteúdo sexual;
- Violação de regras vigentes;
- Vandalizar ou destruir a propriedade individual ou organizacional;
- Invadir o direito privado de outro;
- Violar os direitos de uso ou o uso dos direitos autorais sem qualquer permissão;
- Usá-los para ganhos financeiros ou comerciais;
- Degradar ou interromper o desempenho geral da rede; e
- Introdução dentro da rede da **Epeople**, se houver algum formulário de software ou outros materiais de malware.

5.7. Acesso ao *Fileserver*

O acesso ao *FileServer* é feito com base no princípio de "necessidade de saber", incluindo pastas criadas para cada departamento que podem ser acessadas apenas pelas pessoas dentro do departamento, de acordo com os direitos de acesso concedidos pelo gerente do respectivo departamento, exceto para a **pasta pública**, que inclui informações de interesse geral, disponíveis para todos os funcionários.

5.8. Backups

Backups de documentos públicos ou privados (não classificados ou classificados) são feitos de acordo com a política de backup dos usuários.

Para realizar a estratégia de backup da **Epeople**, os seguintes aspectos foram considerados:

- Onde os ambientes de backup devem ser armazenados;
- Quais dados devem ser armazenados em backup;
- Com que frequência o backup deve ser executado;

- Com que rapidez os ambientes de backup podem ser acessados quando ocorre um evento indesejado;
- Quem está autorizado a ter acesso a ambientes de backup;
- Onde os ambientes de backup devem ser entregues;
- Quem deve restaurar os dados dos ambientes de backup;
- Qual é o esquema principal para marcar ambientes de backup;
- Por quanto tempo os ambientes de backup serão armazenados;
- Quando os ambientes de backup são armazenados no local de backup; e
- Quais medidas são tomadas para sua segurança.

5.9. Erros (*Dropdowns* do Sistema)

Se determinados defeitos forem detectados nos servidores, estações de trabalho independentes ou conectados à rede da **Epeople**, somente o responsável de TI tomará medidas para substituí-los e restabelecer a conexão com o sistema.

5.10. Proteção Antivírus

Todas as estações de trabalho e servidores dentro da infraestrutura de TI da **Epeople**, independentes ou conectados à rede da **Epeople**, máquinas físicas ou virtuais, usam o programa antivírus aprovado pelo responsável de T.I., que cumpre as seguintes regras:

a) O programa antivírus NÃO deve ser desativado de forma alguma, exceções devem ser aprovadas pela sócia fundadora;
b) A instalação, configuração, modificação ou exclusão dos programas antivírus é feita pelo responsável de T.I.;
c) A configuração do programa antivírus não deve ser modificada de forma a restabelecer a eficiência do programa;
d) A frequência das atualizações automatizadas do programa é agendada pelo responsável de TI e não deve ser modificada de forma alguma; e

Classificação do Documento: Restrito

e) Qualquer notificação do programa antivírus de uma estação de trabalho ou servidor deve ser imediatamente notificada ao responsável de TI pelo usuário que a reportar.

5.11. Gestão Automática de Segurança e Auditoria

O responsável de T.I. é obrigado a ativar o sistema de auditoria automatizado dos sistemas operacionais dos terminais e configurá-los para registro de periódicos.

Registros de auditoria dos sistemas devem ser registrados mensalmente, ou em qualquer momento necessário, pelo responsável de T.I., a fim de determinar tentativas de acesso ao sistema sem sucesso e são armazenadas por pelo menos 6 meses.

6. Gerenciamento de Configurações

O gerenciamento da configuração do SIC da **Epeople** é feito pelo departamento de TI, com o envolvimento do ASO e consiste em identificar, controlar, evidenciar e auditar todas as modificações dentro da configuração de hardware e software do SIC.

O administrador de segurança de cada local é responsável pela configuração de hardware e software dos equipamentos instalados na área de responsabilidade.

Se for necessário modificar a configuração do local de submissão dos equipamentos, o administrador de segurança local notificará imediatamente o gerente do ASO e / ou o gerente do departamento de TI.

O gerenciamento da configuração SIC da **Epeople** inclui a implementação de várias medidas de segurança:

Classificação do Documento: Restrito

- Durante todo o ciclo de vida do sistema, modificações de configuração de hardware e software são realizadas por especialistas do departamento de TI, após notificar o ASO e a aprovação prévia da gerência da organização;
- O administrador de segurança e o administrador do sistema possuem uma cópia do inventário completo dos equipamentos SIC encontrados em sua responsabilidade, da mesma forma um esquema detalhado da configuração de hardware e software;
- Qualquer modificação na configuração de hardware e software dos equipamentos do sistema deve ser registrada pelo administrador de segurança e / ou sistema dentro dos arquivos de equipamentos; e
- Todos os equipamentos do sistema devem ser marcados adequadamente (aferente a um sistema e o nível de classificação, por caso).

O administrador de segurança e o administrador do sistema devem executar, pelo menos, um controle anual da configuração de hardware e software, atividade registrada no "registro de eventos".

O gerenciador do ASO pode organizar controles não programados da configuração de hardware e software do sistema para verificar se outros recursos são usados, além dos aprovados, ou outras versões de software modificadas.

É proibido realizar quaisquer modificações na configuração de hardware ou software das estações de trabalho utilizadas para o cumprimento de tarefas de trabalho.

A descoberta de métodos ou suspeitas relativas à modificação da configuração de hardware ou software das estações de trabalho deve ser confirmada pela autoridade de segurança local, que deve notificar o administrador de segurança e / ou o gerente do ASO para verificar a configuração do sistema em regime de emergência.

Qualquer modificação importante da configuração ou localização do estabelecimento dos equipamentos do sistema deve determinar a modificação apropriada da documentação de segurança.

Classificação do Documento: Restrito

7. Medidas de Planejamento para Emergências

O plano de medidas para continuar a atividade e recuperação de desastres (PCA-RD) estabelece os procedimentos para restaurar operações, recursos e serviços específicos da **Epeople**, em situações especiais que resultam na desativação de locais / departamentos de dentro da **Epeople**.

O PCA-RD para os locais / departamentos dentro da **Epeople** se aplicam a recursos e serviços de TI que devem ser restabelecidos em emergências e são aplicados a cargos, operações e recursos de segurança para restabelecer sua condição operacional.