# SEGURANÇA DA INFORMAÇÃO

Para reduzir o risco de ocorrências de falhas prejudicarem de algum modo a ACMTECH informática, as informações devem ser adequadamente utilizadas, armazenadas e protegidas. Sendo assim, as propriedades que devem ser preservadas para garantir a segurança das informações são as seguintes:

• Confidencialidade: garante que a informação estará disponível somente para as pessoas, entidades ou processos autorizados;

• Integridade: garante que a informação não pode ser alterada ou destruída sem a autorização adequada;

• Disponibilidade: possibilita que os recursos estejam sempre acessíveis, ao ser solicitado por uma entidade autorizada.

Desta forma, a ACMTECH informação a partir da adoção de uma boa estratégia, busca salvaguardar estes princípios em todos os aspectos, tanto tecnológico, humano, processual, jurídico ou negócio.

**Uso de E-mail**

O correio eletrônico é fundamental para funcionamento da empresa, pois permite a comunicações entre os vários departamentos da empresa e colaboradores internos facilitando o processo, também é monitorado pela equipe de T.I.

O uso do e-mail corporativo é responsabilidade do colaborador. As mensagens enviadas não podem conter:

* Conter linguagem ofensiva
* Trazer prejuízos a outras pessoas
* Conter conteúdos obscenos
* Vazar informações sigilosas da empresa

**Descarte de informações e mídia**

Para impedir que as informações sigilosas da empresa armazenadas nos equipamentos ou mídias sejam acessadas por agentes não autorizados, é importante que uma conduta do descarte correto de unidade de mídia e equipamentos seja seguida.

A eliminação segura acontece por meio da destruição ou deletar as informações que estão contidas nos equipamentos ou mídias, com o objetivo tornar as informações irrecuperáveis.

**Admissão e Demissão de colaboradores**

O Setor de departamento financeiro e pessoal deverá sempre informar ao setor de TI, a entrada e saída de colaboradores na empresa, o setor de TI ficará responsável pela criação de usuários e exclusão.

No caso de demissão, o colaborador deverá entregar todos os pertencentes da empresa, que ficou sobre sua responsabilidade durante o período trabalhado e ainda terá seus acessos excluídos do sistema, se ainda continuar tendo acessos as informações da empresa serão encaminhadas notificações ao departamento pessoal e financeiro solicitar a exclusão.

**Cópias de seguranças**

É imprescindível fazer a realização de backups diariamente na empresa para prevenir ataques de ransomwares e outros ataques cibernéticos, também proteger dados essenciais da empresa, por isso o setor de T.I criou um espaço de armazenamento que é protegido com senha, só é acessado quem possui a senha, a senha deve ter no mínimo 6 caracteres que é criada pelo usuário, esse espaço permite que os colaboradores possam fazer uploads de informações pessoais e corporativas que serão convertidos automaticamente em criptografia em servidores específicos da empresa.

**Controle contra Malware**

Todos os computadores corporativos da empresa vão ter antivírus instalado no processo de configuração. Setor de T.I fará a administração e o controle do antivírus, fazendo atualizações, manutenção e preventivas, o antivírus irá automaticamente fazer uma varredura diariamente garantindo que estejam livres e seguras de possíveis intrusos no sistema.