BRUNO PERDIGÃO SANTOS

DARLAN STORTO

DIEGO GONCALVES DE JESUS

DIOGO DE SOUZA BARBOSA

FERNANDA COELHO DA SILVA

PLATAFORMA DE BOTÂNICA E PAISAGISMO:
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Documentação apresentada como requisito parcial para obtenção de menção na disciplina de Desenvolvimento do Trabalho de Conclusão de Curso do Curso Técnico de Desenvolvimento de Sistemas da ETEC Centro Paula Souza.

Docente: Julius Cesar José Capellini

São Paulo

2022

SUMÁRIO

1. OBJETIVOS

Nosso dever é garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das informações necessárias para a realização dos negócios da organização.

2. ABRANGÊNCIA

Se aplica a todos os administradores, funcionários, estagiários, prestadores de serviços, sistemas e serviços, incluindo trabalhos executados externamente ou terceirizados, que utilizem o ambiente de processamento, ou com acesso a informações que pertençam a nossa organização.

Todo e qualquer funcionário que estiver fazendo uso de recursos computacionais da empresa tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática ao qual utilizar.

3. PILARES DA SEGURANÇA DA INFORMAÇÃO

A segurança da informação é aqui caracterizada pela preservação dos seguintes conceitos:

(a) **Confidencialidade**: Garante que a informação seja acessível somente pelas pessoas autorizadas, pelo período necessário;

(b) Disponibilidade: Garante que a informação esteja disponível para as pessoas autorizadas sempre que se faça necessário;

(c) Integridade: Garante que a informação esteja completa e íntegra e que não tenha sido modificada ou destruída de maneira não autorizada ou acidental durante o seu ciclo de vida.

4. DEFINIÇÕES GERAIS

(a) Informação: resultado do processamento e organização de dados (eletrônicos ou físicos) ou registros de um sistema, podendo ser de autoria da organização ou de terceiros com a devida permissão.

(b) Ativos de Informação: conjunto de informações, armazenado de modo que possa ser identificado e reconhecido como valioso para a empresa.

(c) Sistemas de informação: de maneira geral, são sistemas computacionais utilizados pela empresa para suportar suas operações.

(d) Segregação de funções: consiste na separação entre as funções de autorização, aprovação de operações, execução, controle e contabilização, de tal maneira que nenhum funcionário, estagiário ou prestador de serviço detenha poderes e atribuições em desacordo com este princípio.

5. CLASSIFICAÇÃO DA INFORMAÇÃO

As informações geradas com as atividades da empresa deverão ser separadas com os seguintes níveis de confidencialidade:

(a) **Pública:** Essas informações serão de acesso público, onde qualquer usuário poderá ter acesso. Exemplo: Informações gerais sobre plantas.

(b) **Sob pagamento:** Essas informações só poderão ser vistas pelo público assinante. São informações mais completas sob domínio da empresa. Exemplo: Informações sobre doenças e pragas.

(c) **Interna:** Informações que serão de acesso apenas dos funcionários da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da empresa. Exemplo: Boletins semanais.

(d) **Confidencial:** Toda informação que pode ser acessada por usuários específicos, com validação e autorização da organização. A divulgação dessa informação pode causar um impacto negativo aos negócios da organização ou

aos parceiros de negócios (sendo esse impacto financeiro, de imagem ou operacional). Exemplo: Documentos sobre acordos comerciais.

(e) **Restrita:** Toda informação que só será permitido o acesso por usuários da organização explicitamente selecionados pelo nome ou área de atuação. A divulgação dessas informações pode causar sérios impactos aos negócios da organização. Exemplo: Informações sobre funcionários como folha de pagamento, são restritos ao setor de RH.

6. RESPONSABILIDADES

De forma geral, cabe a todos os administradores, funcionários, estagiários e prestadores de serviços:

- Cumprir fielmente a Política de Segurança da Informação e as regras aqui apresentadas;
- Proteger as informações da organização contra acessos, modificação, destruição ou divulgação não autorizados;
- Assegurar que os recursos tecnológicos, as informações e sistemas à sua disposição sejam utilizados apenas para os meios aprovados segundo este documento;
- Cumprir as leis e as normas que regulamentam a propriedade intelectual;
- Não discutir assuntos confidenciais de trabalho em locais públicos ou em áreas expostas (aviões, transporte rodoviário, restaurantes, encontros sociais etc.), incluindo a emissão de comentários e opiniões em blogs e/ou redes sociais, bem como não compartilhar informações confidenciais da organização, de qualquer tipo;
- Comunicar imediatamente ao seu superior qualquer descumprimento ou violação desta Política e/ou de suas Normas e Procedimentos.

6.1 DEVER DOS INTEGRANTES DA ORGANIZAÇÃO

Considerar a informação como sendo um ativo da empresa, um dos recursos críticos para a realização do negócio, que possui grande valor e deve sempre ser tratada profissionalmente.

É de responsabilidade do Gerente/Supervisor de cada área classificar a informação (relatórios, documentos, modelos, procedimentos, planilhas) gerada por sua área de acordo com o nível de confidencialidade estabelecido neste documento.

6.2 BOAS PRÁTICAS

- Bloquear o acesso ao computador sempre que sair da sua mesa de trabalho, mesmo que por alguns minutos;
- Manter mesas organizadas e documentos com informações confidenciais trancados, quando não os estiver utilizando.

7. SEGURANÇA FÍSICA

A norma deve definir os requisitos mínimos de segurança física que os ambientes considerados críticos na empresa, onde há informações sigilosas, devem possuir para assegurar a proteção de seus ativos contra fatores que possam causar interrupção das atividades, alteração ou vazamento das informações e consequente prejuízo financeiro.

- Todas as áreas classificadas como críticas devem estar protegidas por controles físicos apropriados;
- Esses controles devem ser proporcionais à criticidade dos equipamentos, dos sistemas e das informações mantidas e manuseadas nestas áreas.
- As áreas classificadas como críticas devem estar devidamente protegidas por acesso não autorizado, dano ou interferência.

- Todo o indivíduo ao ingressar nas instalações da empresa deverá usar crachá de identificação.
- Pessoas externas à companhia deverão ser identificadas na recepção e o seu ingresso nas instalações da empresa será realizado mediante autorização e acompanhamento do empregado da companhia.
- Todo o equipamento que ingressar ou sair da empresa, deverá estar acompanhado da respectiva nota fiscal e autorização do setor de patrimônio.
- Os prestadores de serviços da empresa são responsáveis pelas ações ou prejuízos causados por seus empregados ao patrimônio da empresa, bem como deverão garantir a manutenção da confidencialidade das informações acessadas.
- Documentos ou papéis contendo informações confidenciais, quando não mais necessários, devem ser triturados ou destruídos de forma a impossibilitar leitura.
- Mídias do tipo somente leitura (discos CD-ROM, CD-R, DVD, etc.) contendo informações confidenciais, quando não mais necessárias, devem ser quebradas ou destruídas de forma a impedir seu uso indevido.
- Mídias regraváveis (drives HD ou SSD, pen drives, cartões SD, fitas, discos CD ou DVD do tipo RW, ou assemelhados) contendo informações confidenciais, quando não mais necessárias, devem ser zeradas com o procedimento seguro adequado indicado pela equipe de Segurança da Informação antes de seu reuso ou descarte.
- A entrega de documentos com informações confidenciais pode ocorrer apenas com registro e a garantia de identificação de quem recebe e mediante prévia assinatura de termo de confidencialidade.
- Os equipamentos e seus componentes internos serão inventariados periodicamente e somente funcionários autorizados podem fazer remanejo de equipamentos e peças.

7.1 CONTROLE DE ACESSO FÍSICO

As credenciais ou crachás são identificadores internos e externos para uso pessoal que devem estar atualizadas e legíveis.

- Credenciais, identificações e senhas de acesso devem ser individuais e mantidas em sigilo, não devem ser transferidas ou compartilhadas.
- Cada funcionário deve trocar periodicamente suas senhas e é de sua responsabilidade escolher senhas robustas, complexas e longas.
- As senhas devem ser únicas, não devem ser usadas senhas idênticas ou semelhantes para identificação em sistemas, sites ou serviços não gerenciados pela empresa, sejam de natureza pessoal ou não.

7.2 CONTROLE DE ACESSO ÀS INFORMAÇÕES

No controle de acesso às informações deve definir os requisitos necessários para que o usuário da informação obtenha acesso ao ambiente de tecnologia da empresa.

- O acesso a todos os sistemas e informações da empresa deve ser concedido de acordo com as necessidades da função do usuário para a execução de suas atividades;
- O responsável pelos sistemas ou da informação é o responsável pela concessão de acesso a todos os recursos que estejam sob sua responsabilidade. Os acessos concedidos deverão ser periodicamente revisados;
- Os usuários devem se restringir às informações e ambientes aos quais estão autorizados, devendo acessá-los somente se houver a necessidade para desempenho de suas atividades profissionais.

8. DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

Este item enumera os requisitos de segurança para desenvolvimento, manutenção e parametrização de sistemas.

- Todos os sistemas desenvolvidos pela empresa ou por empresas contratadas por esta, deverão atender aos requisitos de segurança definidos pela Norma de Segurança da Informação.
- É responsabilidade de todos os usuários de informações auxiliar na manutenção dos requisitos de segurança e nos regulamentos ditados por lei.
- A empresa deve estar em conformidade com todas as regras e regulamentos instituídos por lei. Isto inclui qualquer lei civil ou criminal, estatutos ou obrigações contratuais feitas envolvendo a empresa.

9. DIRETRIZES SOBRE DADOS PESSOAIS DE FUNCIONÁRIOS

Esta organização se compromete em não acumular ou manter intencionalmente dados pessoais de funcionários além daqueles relevantes na condução do seu negócio. Todos os dados pessoais dos funcionários serão considerados confidenciais.

Os dados pessoais de funcionários sob a responsabilidade desta organização não serão usados para fins diferentes daqueles para os quais foram coletados, sendo geridos segundo a Lei Geral de Proteção de Dados (LGPD)

Dados pessoais de funcionários não serão transferidos para terceiros, exceto quando exigido pelo nosso negócio, e desde que tais terceiros mantenham a confidencialidade dos referidos dados.

10. ADMISSÃO/DEMISSÃO DE ADMINISTRADORES

O setor de RH deverá informar a equipe de segurança da informação da organização toda e qualquer movimentação de temporários e/ou estagiários, e admissões e/ou demissões de funcionários, para que os mesmos possam ser cadastrados ou descadastrados nos sistemas da empresa.

O RH deverá questionar ao setor responsável pela contratação quais sistemas e repositórios de arquivos de trabalho o novo colaborador deverá ter direito de acesso, e quais sistemas um antigo colaborador tinha direito de acesso.

11. CONCESSÃO E REVOGAÇÃO DE ACESSOS

Se houver necessidade de concessão ou revogação de acessos à alguma informação confidencial, o setor solicitante comunicará o administrador da área, para que avalie o pedido, e assim, prossiga com o pedido.

12. POLÍTICA DE SENHAS

Obrigatórios senhas com no mínimo 8 caracteres, contendo ao menos: letras maiúsculas, minúsculas e números. Se e somente se o usuário for desligado dos serviços da empresa, seus acessos e senhas serão deletados no mesmo dia.

13. ARQUIVOS DE TRABALHO

Os arquivos considerados essenciais para a progressão da empresa, serão mantidos sob controle de um administrador específico. São exemplos de arquivos de trabalho:

(a) Planilha de faturamento;

(b) Notas fiscais;

(c) Propostas comerciais;

(d) Banco de dados com informações dos clientes.

14. ARQUIVOS INDIVIDUAIS

São considerados arquivos individuais aqueles criados, copiados ou desenvolvidos pelos administradores, que não sejam parte integrante do produto entregável pelo seu trabalho, seja ele interno ou para clientes. Não é permitido aos administradores o uso ou armazenamento dos tipos de arquivos abaixo relacionados em suas estações de trabalho:

(a) Músicas, filmes, séries, programas de TV;

(b) Vídeos não relacionados à atividade profissional;

(c) Conteúdo pornográfico.

15. COMPARTILHAMENTO DE PASTAS E DADOS

O compartilhamento de pastas e arquivos de trabalho cujo conteúdo seja classificado como sendo de informação confidencial ou restrita é proibido através dos exemplos seguintes:

- Comunicador de mensagens instantâneas;
- Compartilhamento de pastas do Windows;
- Bluetooth;
- Cópia via pen drive ou qualquer outro dispositivo removível;
- Driver virtual (com exceção google drive).

Havendo necessidade de se realizar o compartilhamento de dados entre administradores, deve-se utilizar o sistema google drive, com o login e senha da empresa. Para obter o login e a senha, o administrador deverá entrar em contato com o administrador responsável por tal.

16. CÓPIAS DE SEGURANÇA, RECUPERAÇÃO E INTEGRIDADE DOS SISTEMAS E DE SEUS BANCOS DE DADOS

Tendo em vista que a empresa será composta por administrador, funcionários e prestadores de serviços, foi definido que será de inteira responsabilidade do administrador, realizar a cópia de segurança dos sistemas, repositórios de arquivos de trabalho, bancos de dados e configurações dos equipamentos e servidores de rede, desta forma, atribuindo ao administrador o controle total do acesso.

17. POLÍTICA DE BACKUP

(a) Dados a serem armazenados e estilo de backups:

Completo/ Incremental:

- Dados novos e/ou atualizados de plantas inseridas na aplicação.

- Dados novos e/ou atualizados de pragas e doenças inseridas na aplicação.

- Dados atualizados de antigos usuários.

- Dados cadastrais de novos usuários.

- Dados de plantas pessoais cadastradas pelos usuários.

- Perguntas novas e/ou atualizadas do FAQ.

Diferencial:

- Dados novos e/ou atualizados de produtos (incluindo pedidos e relacionados).

- Dados de funcionários e tudo que abrange o mesmo (Área de atuação, salário, ativo ou demitido, etc.)

(b) Tempo de realização de cada backup: Serão feitos backups mensalmente.

(c) Local de armazenamento e autorização de acesso: Os Backups serão armazenados na nuvem e em SSD físico, onde o mesmo será guardado com nível de segurança máxima. Somente a equipe de segurança digital terá acesso, ou será autorizada a realizar e guardar os backups.

18. USO DA INTERNET

Visando garantir que o uso do espaço destinado para os funcionários trabalharem será respeitado seguindo as normas éticas e trabalhistas, o administrador terá a atribuição de monitorar o uso da internet, através de mecanismos facilitadores, como softwares ou aplicativos, que ajudem nessa função. O uso da Internet será monitorado pelo administrador, através do uso de sistema de registro de navegação que informa qual usuário está conectado, o tempo que usou a Internet e qual página acessou.

Priorizando o bom relacionamento interpessoal entre os funcionários da empresa, conforto e bem estar, será evitado e bloqueado o uso exagerado de redes sociais, sites externos, uso da internet fora do contexto original da empresa, a fim de tornar os funcionários mais comprometidos e concentrados nas atribuições no qual foram eleitos. Será de inteira responsabilidade do administrador definir as permissões dos funcionários que terão acesso.

Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros.

- Visualização e transferência de arquivos (downloads);
- Estações de rádio (*);

- De conteúdo pornográfico ou relacionados a sexo;
- De jogos on-line;
- Que defendam atividades ilegais;
- Que menosprezem, depreciem ou incitem o preconceito a determinadas classes;

Ficando ciente que todo e qualquer acesso às redes sociais que não seja relacionado com a área de interesse da empresa não é permitido e, sendo assim, passível de punição.

19. USO DO CORREIO ELETRÔNICO (“E-MAIL”)

Será disponibilizado um e-mail comercial para uso individual dos funcionários, devendo a cargo de cada funcionário a responsabilidade individual do uso do mesmo.

O e-mail tem a finalidade de ser um facilitador na comunicação interna e externa quando necessário, possibilitando fluidez no trabalho e dinamismo na realização dos negócios da empresa, devendo a todos os funcionários manter um padrão na escrita, linguagem profissional, organizada e não devem comprometer a imagem da empresa, não podem ser contrárias à legislação vigente e nem aos princípios éticos estabelecidos pela empresa.

É dever de cada funcionário usar o correio eletrônico com responsabilidade e integridade, ficando cientes que o uso inadequado do mesmo poderá acarretar medidas cabíveis. Não é permitido o cadastro de contatos pessoais nos sistemas de mensagens instantâneas (ao utilizar a conta profissional); e nem a utilização de contas pessoais. É terminantemente proibido o envio de mensagens que:

- Contenham declarações difamatórias e linguagem ofensiva;
- Possam trazer prejuízos a outras pessoas;

- Sejam hostis;
- Sejam relativas a “correntes”, de conteúdos pornográficos ou equivalentes;
- Possam prejudicar a imagem da empresa e/ou de outras empresas;

Não será permitido o uso de e-mail gratuitos (Gmail, Yahoo!, Hotmail, etc.), nos computadores da empresa. O administrador poderá, mediante análise comprobatória, visando evitar a entrada de vírus nos computadores da empresa, bloquear o recebimento de e-mails provenientes de e-mails gratuitos.

20. USO DE EQUIPAMENTOS DE PROPRIEDADE DA EMPRESA

Em decorrência da COVID, alguns funcionários serão autorizados a trabalhar remotamente (home office), sendo disponibilizado para os mesmos equipamentos (desktop, notebook, celular ou tablet) de propriedade da empresa para mantê-los produtivos e em comunicação com a equipe, devendo estar cientes de que:

- Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo a realização de atividades profissionais;
- A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário;
- É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo;
- O usuário não deve alterar a configuração do equipamento recebido;
- O usuário não deve instalar ou remover nenhum programa do equipamento recebido. Também não deve alterar a configuração de nenhum programa previamente instalado.

20.1 FORA DO TRABALHO

- Mantenha o equipamento sempre com você;
- Atenção em hall de hotéis, aeroportos, aviões, táxi e etc.;
- Quando transportar o equipamento em automóvel utilize sempre o porta-malas ou lugar não visível;
- Atenção ao transportar o equipamento na rua.

20.2 EM CASO DE FURTO

- Registre a ocorrência em uma delegacia de polícia;
- Comunique o fato o mais rápido possível ao seu superior imediato e ao administrador da empresa;
- Envie uma cópia do boletim de ocorrência para o RH.

21. RESPONSABILIDADES DOS GERENTES/SUPERVISORES

O administrador é responsável por definir os direitos de acesso de seus subordinados aos sistemas e informações da empresa, cabendo a eles verificarem se os mesmos estão acessando exatamente os sistemas e as áreas de dados compatíveis com as suas respectivas funções, usando e conservando adequadamente os equipamentos, e mantendo cópias de segurança de seus arquivos individuais.

O administrador ditará as regras que devem ser seguidas pelos demais funcionários em relação ao que deve ser acessado:

- Que tipo de informação o usuário pode acessar;
- Quem está autorizado a acessar determinado sistema e/ou informação;
- Quem acessou determinada sistema e informação;

- Quem autorizou o usuário a ter permissão de acesso à determinado sistema ou informação;
- Que informação ou sistema determinado usuário acessou;
- Quem tentou acessar qualquer sistema ou informação sem estar autorizado.

22. SISTEMA DE TELECOMUNICAÇÕES

É concedido aos funcionários acesso às formas de comunicação aos funcionários, internamente e externamente, a fim de facilitar o dia a dia do funcionário, no que se refere à comunicados, avisos importantes, uso pessoal, mas com moderação.

23. VIOLAÇÃO DA POLÍTICA DE SEGURANÇA

É qualquer ato que:

- Exponha a empresa a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados ou de informações ou ainda da perda de equipamento;
- Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos;
- Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

24. PENALIDADES

O não cumprimento desta Política de Segurança da Informação implica em falta grave e poderá resultar nas seguintes ações: advertência formal,

suspensão da conta, rescisão do contrato de trabalho, outra ação disciplinar e/ou processo civil ou criminal.

25. TERMO DE RESPONSABILIDADE

Termo de Responsabilidade

Eu, _____

portador do CPF n° _____, no exercício da função de _____, responsabilizo-me pela leitura das diretrizes presentes no documento de **Política de Segurança da Informação** disponibilizado pela empresa Mais Que Plantas e declaro estar ciente dos meus direitos e deveres como funcionário em relação a proteção dos equipamentos, dados sensíveis e/ou de propriedade intelectual da empresa a qual terei acesso.

Assim, declaro:

Comprometer-se a manter sigilo não utilizando tais informações confidenciais em proveito próprio ou alheio.

I) Utilizar tais informações apenas para o bom e fiel propósito de atingir os objetivos da empresa;

II) Manter a confidencialidade das Informações Confidenciais e divulgá-las apenas aos funcionários que precisam saber;

III) Proteger as Informações Confidenciais divulgadas a você, usando o mesmo nível de cuidado com que você protegeria suas próprias Informações Confidenciais;

IV) Manter procedimentos administrativos adequados para evitar a perda ou extravio de quaisquer documentos ou informações confidenciais,

devendo comunicar imediatamente à empresa eventos dessa natureza, o que não exime sua responsabilidade.

Não configuram informações confidenciais aquelas:

V) Já disponíveis ao público em geral sem culpa do funcionário;

VI) Que já eram do conhecimento do funcionário antes de sua do ingresso na empresa e que não foram adquiridas direta ou indiretamente da empresa;

VII) Que não são mais tratadas como confidenciais pela empresa.

Declaro que li o documento de **Política de Segurança da Informação** e o **Termo de Responsabilidade** da empresa Mais que Plantas e estou ciente dos meus deveres como funcionário em relação a proteção dos equipamentos, dados sensíveis ou de propriedade intelectual da empresa a qual terei acesso.

São Paulo – SP, ___/___/_____

_____

Assinatura