# Introdução

A **Política de Segurança da Informação das Indústrias Marrucci,** também denominada de **PSI** é um documento que visa orientar as ações, procedimentos e diretrizes para o uso dos ativos de Informação das Indústrias Marrucci.

A política deve ser seguida e praticada na sua integra, para garantir a proteção dos ativos de informação e a previsão de responsabilidade legal para todos os usuários, além de ser aplicada em todas as áreas da empresa.

# Objetivo

Esta Política é um conjunto de diretrizes que tem como objetivo conscientizar e orientar os clientes, fornecedores, parceiros e colaboradores da Marrucci para o uso seguro das Informações e Dados Pessoais, assegurando a observância aos princípios inerentes à Segurança da Informação, quais sejam:

1. **Confidencialidade:** Controle do acesso aos Dados Pessoais, conforme autorização e necessidade da empresa.
2. **Integridade:** Garantia da precisão e completude da informação, ou seja, salvaguarda da exatidão das informações e os dados pessoais.
3. **Disponibilidade:** Garantia de que as informações estejam acessíveis sempre que solicitadas por pessoas autorizadas.
4. **Autenticidade:** Garantia de que a pessoa ou sistema seja de fato quem ela diz ser.
5. **Não Repúdio:** Garantia da impossibilidade de negar a autoria de um evento.

## Abrangência

A **Política de Segurança da Informação** engloba a segurança e privacidade da informação, e as obrigações e deveres de cada um que venha a fazer uso dos recursos de tecnologia disponibilizados pela Marrucci, e principalmente no que diz respeito ao Tratamento de Dados Pessoais compartilhados pelos colaboradores, terceiros, prestadores de serviços, clientes e parceiros, definindo dessa forma responsabilidade Civil e Criminal por qualquer dano que venha a ser causado à empresa e/ou qualquer tipo de infração ou violação de leis e normas, uma vez que esta Política observará os princípios dispostos na Lei Geral de Proteção de Dados (Lei 13.709/2018), em especial:

1. **Boa-fé;**
2. **Finalidade:** realização do Tratamento de Dados Pessoais para propósitos legítimos, específicos, explícitos e informados ao Titular;
3. **Adequação:** compatibilidade do Tratamento com as finalidades informadas ao Titular;
4. **Necessidade:** limitação do Tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do Tratamento de dados;
5. **Livre acesso:** garantia, aos Titulares, de consulta facilitada e gratuita sobre a forma e a duração do Tratamento, bem como sobre a integralidade de seus Dados Pessoais. Sobre as consultas dos Titulares, consultar Política de Privacidade e Proteção de Dados Pessoais da Marrucci;
6. **Qualidade dos dados:** garantia, aos Titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu Tratamento;
7. **Transparência:** garantia, aos Titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do Tratamento, observados os segredos comercial e industrial;
8. **Segurança:** utilização de medidas técnicas e administrativas aptas a proteger os Dados Pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
9. **Prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do Tratamento de Dados Pessoais;
10. **Não discriminação:** impossibilidade de realização do Tratamento para fins discriminatórios ilícitos ou abusivos;
11. **Responsabilização e prestação de contas:** demonstração pela Marrucci, da adoção de medidas eficazes e capazes de assegurar a observância e o cumprimento das normas de proteção de Dados Pessoais e, inclusive, da eficácia dessas medidas.

## Legislação Aplicável

Correlacionam-se com a política, com as diretrizes e com as normas de Segurança da Informação as Leis abaixo relacionadas, mas não se limitando às mesmas:

1. Lei Federal 8159, de 08 de janeiro de 1991 (Dispõe sobre a Política Nacional de Arquivos Públicos e Privados);
2. Lei Federal 9610, de 19 de fevereiro de 1998 (Dispõe sobre o Direito Autoral);
3. Lei Federal 9279, de 14 de maio de 1996 (Dispõe sobre Marcas e Patentes);
4. Lei Federal 3129, de 14 de outubro de 1982 (Regula a Concessão de Patentes aos autores de invenção ou descoberta industrial);
5. Lei Federal 10406, de 10 de janeiro de 2002 (Institui o Código Civil);
6. Decreto-Lei 2848, de 7 de dezembro de 1940 (Institui o Código Penal);
7. Lei Federal 9983, de 14 de julho de 2000 (Altera o Decreto-Lei 2.848, de 7 de dezembro de 1940 - Código Penal e dá outras providencias);
8. Lei Federal 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD)

# Nomeações e Atribuições

Para ajudar a promover a cultura de Segurança da Informação, bem como zelar pelo cumprimento dos itens dispostos nessa PSI, atendendo também os dispositivos legais, a Diretoria das Indústrias Marrucci, na figura do sr. Cesare Augusto Marrucci, nomeou um **DPO**, que será o Encarregado dos Dados, e criou também o **Comitê de Segurança da Informação**.

## Encarregado de Dados (DPO)

As Indústrias Marrucci, na posição de “Controlador dos Dados”, nomeiam como Encarregado pelo Tratamento de Dados Pessoais (DPO), nos termos do art. 41, da Lei Geral de Proteção de Dados Pessoais (LGPD), o sr. **Filipe Augusto Pak Lucon**, Supervisor do Sistema de Gestão Integrado.

Com isso, qualquer evento adverso, confirmado ou sob suspeita, deverá ser informado ao DPO, tais como:

* + 1. Evento adverso confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores, bem como estruturas físicas e lógicas associadas, que comprometa a confidencialidade, a integridade e a disponibilidade do ambiente da organização;
		2. Vazamento de informações confidenciais (informações de clientes, colaboradores, fornecedores, informações estratégicas, outros);
		3. Tentativas interna ou externa de ganhar acesso não autorizado a sistemas, a dados ou até mesmo comprometer o ambiente da TI;
		4. Uso ou acesso não autorizado a um sistema;
		5. Compartilhamento de senhas;
		6. O Tratamento de dados pessoais indevidos por qualquer integrante da empresa.

## Comitê de Segurança da Informação – CSI

O Comitê de Segurança da Informação nomeado pela Diretoria das Indústrias Marrucci, é constituído pelos seguintes membros:

* Cesare Marrucci – Diretor Presidente
* Filipe Augusto Pak Lucon – DPO e Supervisor do Sistema de Gestão Integrado
* Antônio Bortoletto – Supervisor de Recursos Humanos
* Thiago Sampaio – Diretor Administrativo e Financeiro
* Wlamir Machado – Supervisor de TI
* José Roberto Bassinelo – Gerente Administrativo e Financeiro
* Ronaldo Arbex – Supervisor de Compras
* Manoel Santiago – Diretor Industrial
* Marcelo Rufini – Gerente Comercial (Hidráulica)
* Lourival Trevisan – Gerente Comercial (Fundição)

# Termos e Definições

Para os efeitos desta Política, aplicam-se os seguintes termos e definições:

* **Aceitação de risco:** Decisão de aceitar um risco;
* **Áreas críticas**: dependências da **MARRUCCI** ou de seus clientes onde esteja situado um ativo de informação relacionado a informações críticas para os negócios da Marrucci ou de seus clientes.
* **Ameaça:** Causa potencial de um incidente indesejado, que pode resultar em danos a um sistema ou organização;
* **Análise de riscos:** Uso sistemático de informações para identificar fontes e estimar o risco.;
* **Avaliação de riscos:** Processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;
* **Ação Corretiva:** Ação para eliminar a causa de uma não-conformidade identificada ou outra situação indesejável;
* **Ataque:** Tentativa que para destruir, expor, alterar, desabilitar, roubar ou obter acesso não autorizado ou fazer uso não autorizado de um ativo;
* **Ativo da informação:** Conhecimento ou dados que tem valor para a organização;
* **Autenticidade:** Propriedade que uma entidade é o que afirma ser;
* **CSI:** Comitê de Segurança da Informação – Grupo multidisciplinar que reúne representantes de diversas áreas da Marrucci, aprovado pela Diretoria, com o intuito de definir e apoiar estratégias necessárias à implantação e manutenção da PSI.
* **Comunicação de risco:** Troca ou compartilhamento de informações sobre riscos entre o tomador de decisões e outras partes interessadas;
* **Confiabilidade:** Propriedades de comportamento desejado consistente e os resultados;
* **Confidencialidade:** Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;
* **Controle:** Meios de gerenciamento de risco, incluindo políticas, procedimentos, guias, práticas ou estruturas organizacionais, que podem ser administrativas, técnica, de gestão ou de natureza legal;

Nota: Nesta Norma o termo “controle” é usado como um sinônimo de “medida”.

* **Controle de acesso:** Meios para assegurar que o acesso a ativos é autorizado e restrito com base nos requisitos de segurança e de negócios;
* **Critérios de risco:** Termos de referência pelo qual é avaliada a importância do risco;
* **Declaração de aplicabilidade:** Declaração documentada que descreve os objetivos de controle e controles que são pertinentes e aplicáveis ao SGSI da organização.

Nota: Os objetivos de controle e controles estão baseados nos resultados e conclusões dos processos de análise/avaliação de riscos e tratamento de risco, dos requisitos legais ou regulamentares, obrigações contratuais e os requisitos de negócio da organização para a segurança da informação.

* **Disponibilidade:** Propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada;
* **DPO:** Data Protection Officer ou Encarregado dos Dados, é quem deve garantir, de forma independente, que a organização siga as leis que protegem os dados pessoais dos indivíduos;
* **Evento de segurança da informação:** Uma ocorrência identificada de um estado de sistema, serviço ou rede, indicando uma possível violação da Política de Segurança da Informação e Privacidade ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.
* **Gestão de riscos:** Atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos.;
* **Informações críticas para os negócios das Indústrias Marrucci:** Toda informação que, se for alvo de acesso, modificação, destruição ou divulgação não autorizada, resultará em perdas operacionais ou financeiras à **Marrucci** ou seus clientes. Exemplo: dados dos clientes, fontes de sistema, regras de negócios, informações estratégias ou de negócio de clientes obtida em reuniões, planejamento estratégico da **Marrucci**, prospecções, informações estratégicas da **Marrucci**;
* **Impacto:** Mudança adversa ao nível dos objetivos de negócios alcançado;
* **Incidente de segurança da informação:** Um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;
* **Integridade:** Propriedade de salvaguarda da exatidão e completeza dos ativos;
* **LGPD:** Lei Geral de Proteção de Dados;
* **Mitigação:** Limitação das consequências negativas de um determinado evento;
* **Não-repúdio:** Capacidade de provar a ocorrência de um evento alegado ou de ação e de suas entidades de origem, a fim de resolver disputas sobre a ocorrência ou não ocorrência de evento ou ação e envolvimento de entidades no evento;
* **PSI:** Política de Segurança da Informação.
* **Risco:** Combinação da probabilidade de um evento e suas consequências;
* **Risco de segurança da Informação:** Potencial que uma ameaça irá explorar uma vulnerabilidade de um ativo ou grupo de ativos e, assim, causar danos à organização;
* **Risco residual:** Risco remanescente após o tratamento de riscos;
* **Segurança da informação:** Preservação da confidencialidade, integridade e disponibilidade da informação;

Nota: adicionalmente, outras propriedades, tais como a autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.

* **Sistema de Gestão Integrado (SGI):** Estrutura de políticas, procedimentos, guias e recursos associados, para atingir os objetivos da organização;
* **Tratamento do risco:** Processo de seleção e implementação de medidas para modificar um risco.;
* **Vulnerabilidade:** Fraqueza de um ativo ou controle que pode ser explorada por uma ameaça.

# Aplicações da PSI

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores e aos seus parceiros de negócio em atendimento aos requisitos do Sistema de Gestão Integrado, e se aplicam à informação, em qualquer meio ou suporte, ou seja, esta política se aplica não apenas para os dados que estão armazenados no meio tecnológico (computadores, e-mails, redes ou sistemas), ela engloba também, as informações e dados no meio físico, impressos ou salvos em mídias digitais.

Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

É também obrigação de cada colaborador se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da supervisão de TI sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de dados e informações.

Este documento estará disponível para acesso de todos os colaboradores no diretório SGI podendo ser acessado a qualquer momento para consulta.

# Princípios da PSI

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela Marrucci pertence à referida organização.

As exceções devem ser explícitas e formalizadas em contrato entre as partes.

## Classificação da Informação

As informações, sejam elas físicas ou eletrônicas que são produzidas ou que circulam pelas Indústrias Marrucci, por padrão são classificadas como confidenciais, exceto, por definição interna ou legislação que obrigue o contrário.

Cabe ao colaborador **autor** da Informação definir os acessos, níveis de permissão e formas de proteção quando se tratar de uma Informação **restrita**, **confidencial** ou de **uso interno**.

Será considerado como autor da informação o colaborador que primeiro produzir, criar ou manipular a informação/documento dentro do ambiente das Indústrias Marrucci.

Todo colaborador, direto ou indireto, deve zelar pela manutenção dos níveis de confidencialidade adequados, e tornar a classificação explícita sempre que possível, e deve estar ciente de que se deve apenas ter ou solicitar acesso à informação estritamente necessária para execução de suas atividades.

Os níveis das classificações são identificados como:

* **Confidencial**: todas as informações classificadas como “**confidenciais”** deverão ser mantidas em arquivos físicos ou eletrônicos com níveis de segurança compatíveis com a relevância da informação, tais como cofres, armários/gavetas com chaves, diretórios com acesso restrito.

A transmissão de arquivos confidenciais só deverá ser feita utilizando meios de transmissão seguras, e após a inclusão de mecanismos de segurança (senha ou criptografia) para as partes previamente autorizadas.

* **Restrita:** todas as informações classificadas como **“restrita”,** são sigilosas, e/ou estratégicas e somente poderão ser acessadas dentro das Indústrias Marrucci, não devendo ser compartilhadas com pessoas fora da empresa.

Normalmente são Informações de uma determinada área que não devem ser acessadas por outros setores, como por exemplo os documentos do setor de RH ou departamento financeiro da empresa.

**Uso Interno:** todas as informações classificadas como **“uso interno”** não poderão ser encaminhadas, divulgadas ou publicadas em quaisquer meios para terceiros não autorizados, devendo a sua disponibilização ser restrita ao ambiente de trabalho das Indústrias Marrucci, e limitado aos colaboradores ou terceiros que realmente necessitem ter acesso a tais Informações.

* **Pública:** todas as informações classificadas como **“uso interno”** são de conhecimento público e estão disponibilizadas para Clientes, Colaboradores e Público em Geral através da Internet, ou veiculadas em documentos publicados em jornais, revistas, folders, redes sociais, panfletos, avisos ou palestras autorizadas.

Dessa forma. são informações que não necessitam de proteção sofisticada contra vazamento de dados.

# Requisitos da PSI

Para que essa Política de Segurança da Informação seja aplicada e atendida, alguns pontos são mandatórios:

1. Para a uniformidade da informação, a PSI deverá ser comunicada a todos os colaboradores das Indústrias Marrucci a fim de que a política seja cumprida dentro e fora da empresa.
2. Deverá existir um comitê multidisciplinar, responsável pela gestão da segurança da informação, doravante designado como **Comitê de Segurança da Informação.**
3. A PSI deverá ser revista e atualizada periodicamente, sempre que algum fato relevante ou evento motive sua revisão, conforme análise e decisão do Comitê de Segurança da Informação.
4. Deverá constar em todos os contratos das Indústrias Marrucci, o Acordo de Confidencialidade ou Cláusula de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela empresa.
5. A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores. Todos os colaboradores devem ser orientados sobre a PSI – Política de Segurança da Informação da Marrucci, procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Eles devem assinar um termo de responsabilidade.
6. Nos casos específicos de terceiros e prestadores de serviços, essa responsabilidade cabe ao gestor da área contratante, onde fica definido que ele tem a obrigatoriedade de passar os termos da PSI para o contratado.
7. Todo incidente que afete a segurança da informação deverá ser comunicado ao DPO, que se julgado necessário, acionará o departamento de TI para análise, e em casos mais graves deverá comunicar ao CSI para que sejam adotadas as devidas ações.
8. Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.
9. Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.
10. Deverão ser criados e instituídos controles apropriados, logs de auditoria ou registros de atividades, em todos os pontos e sistemas em que a empresa julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, laptops, nos acessos à internet, no correio eletrônico, nos sistemas comerciais e financeiros desenvolvidos pela Marrucci ou por terceiros.
11. Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e/ou homologação.
12. As Indústrias Marrucci se isentam de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.
13. Esta PSI será implementada na Marrucci por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço.
14. O não cumprimento dos requisitos previstos nesta PSI e das Normas de Segurança da Informação acarretará violação às regras internas da empresa e sujeitará o usuário às medidas administrativas e legais cabíveis.

# Deveres e Responsabilidades

## Dos Colaboradores em Geral

1. Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da organização.
2. Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar à Marrucci e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referida.
3. É de responsabilidade de cada colaborador tomar conhecimento, e cumprir a presente política, e em caso de dúvida, buscar orientação.
4. Fiscalizar e orientar os parceiros e clientes da Marrucci no que se refere as diretrizes dessa política, e comunicar imediatamente o CSI quando do descumprimento ou violação desta política.

## Dos Colaboradores em Regime de Exceção (Temporários)

1. Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pelo Comitê de Segurança da Informação.
2. A concessão poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

## Dos Gestores de Pessoas e/ou Processos

1. Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.
2. Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI da Marrucci.
3. Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da empresa.
4. Antes de conceder acesso às informações da organização, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.
5. Definir dentre os colaboradores de sua área, no mínimo um usuário chave (key user) para servir como replicadores da PSI perante os demais colaboradores.
6. Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

## Dos Fornecedores e Parceiros

1. Deverão estar cientes e comprometidos com as Políticas da empresa no que diz respeito à Segurança da Informação “PSI” e Tratamento de Dados Pessoais;
2. Os contratos celebrados com os fornecedores e parceiros deverão conter cláusulas relacionadas às diretrizes de segurança da informação e a Lei Geral de Proteção de Dados Pessoais (LGPD) que devem ser conduzidas por eles internamente visando viabilizar a relação jurídica contratual.
3. Justifica-se a rescisão contratual, bem como a não celebração de contrato com empresas prestadoras ou parceiras que não estejam se adequando à Lei geral de Proteção de Dados - LGPD.

## Dos Custodiantes da Informação

### Do Encarregado da Informação (DPO)

1. Receber as reclamações e comunicações, analisá-las, prestar esclarecimentos e adotar as devidas providências;
2. Liderar a equipe do Comitê de Segurança da Informação;
3. Receber comunicações da autoridade nacional e adotar providências;
4. Orientar os colaboradores e os contratados a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
5. Mediante solicitação, assessorar o Controlador na realização de avaliação de impacto à proteção de dados e suas implementações, nos termos da Lei Geral de Proteção de Dados Pessoais (LGPD);
6. Atuar como ponto de contato da Autoridade Nacional de Proteção de Dados em questões relacionadas com o tratamento de dados pessoais, incluindo consultas prévias sobre a avaliação de impacto à proteção de dados nos termos da Lei Geral de Proteção de Dados Pessoais (LGPD), quando apropriado, assessorando em todas as outras questões;
7. Atuar como ponto de contato para o exercício dos direitos dos titulares de dados nos termos da Lei Geral de Proteção de Dados Pessoais (LGPD) e processar suas consultas relacionadas às atividades de tratamento de dados.

### Do Comitê de Segurança da Informação

1. Propor investimentos relacionados à segurança da informação com o objetivo de reduzir mais os riscos;
2. Propor alterações nas versões da PSI, a inclusão, eliminação ou mudança de normas complementares;
3. Avaliar os incidentes de segurança e propor ações corretivas;
4. Definir as medidas cabíveis nos casos de descumprimento da PSI e/ou das Normas de Segurança da Informação complementares.

### Da Área de Tecnologia da Informação

1. Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.
2. Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes, os quais são categorizados por tipos de problemas em uma SLA (Service Level Agreement).
3. Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI, e em sua versão corporativa, pelas Normas de Segurança da Informação complementares.
4. Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.
5. Segregar as funções administrativas e operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.
6. Garantir segurança especial para sistemas com acesso público, incluindo o ambiente externo, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação (Lei N° 12.965/14).
7. Gerar e manter as logs para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes.
8. Para os logs geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.
9. Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a Marrucci.
10. Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.
11. O gestor da informação deve ser previamente informado sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo custodiante.
12. Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.
13. Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.
14. Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:
* **Os usuários** (logins) individuais de empregado serão de responsabilidade do próprio colaborador.
* **Os usuários** (logins) de departamentos serão de responsabilidade do gestor da área.
* **Os usuários** (logins) de terceiros serão de responsabilidade do gestor da área contratante.
1. Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.
2. Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.
3. Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, exigindo o seu cumprimento dentro da empresa.
4. Realizar auditorias periódicas de configurações técnicas e análise de riscos.
5. Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.
6. Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.
7. Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro, utilizando-se do horário oficial de Brasília, e criar e manter mecanismos que proíbam a alteração desta data e horário.
8. Monitorar o ambiente de TI, gerando indicadores e históricos de:
* Uso da capacidade instalada da rede e dos equipamentos;
* Tempo de resposta no acesso à internet e aos sistemas críticos da Marrucci;
* Períodos de indisponibilidade no acesso à internet e aos sistemas críticos da Marrucci;
* Incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);
* Atividade de todos os colaboradores durante os acessos às redes internas e externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);

### Da Área de Segurança da Informação

1. Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.
2. Propor e apoiar iniciativas que visem à segurança dos ativos de informação da Marrucci.
3. Publicar e promover as versões da PSI e as Normas de Segurança da Informação aprovadas pelo Comitê de Segurança da Informação.
4. Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio das Indústrias Marrucci, mediante treinamentos e informativos.
5. Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.
6. Analisar criticamente incidentes em conjunto com o Comitê de Segurança da Informação.
7. Apresentar as atas e os resumos das reuniões do Comitê de Segurança da Informação, destacando os assuntos que exijam intervenção do próprio comitê ou de outros membros da diretoria.
8. Manter comunicação efetiva com o Comitê de Segurança da Informação sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar a Marrucci.
9. Buscar alinhamento com as diretrizes corporativas da organização e com as legislações brasileiras, em especial o Marco Civil da internet e a LGPD.

## Do Monitoramento e da Auditoria do Ambiente

Para garantir as regras mencionadas nessa PSI, a Marrucci poderá:

1. Definir as medidas cabíveis nos casos de descumprimento da PSI e/ou das Normas de Segurança da Informação complementares.
2. Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede, onde a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
3. Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Comitê de Segurança da Informação;
4. Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
5. Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

## Do uso do E-mail / Correio Eletrônico

* 1. O uso do correio eletrônico da Marrucci é para fins corporativos e relacionados às atividades do colaborador/usuário dentro da organização. A utilização desse serviço para fins pessoais é proibida.
	2. As Informações contidas nas mensagens eletrônicas são de propriedade das Indústrias Marrucci, podendo ser monitoradas a qualquer tempo sem aviso ou notificação prévia para fins de auditoria de conformidade às normas internas, regulamentações ou boas práticas aplicadas ao negócio.
	3. É expressamente proibido o envio de informações classificadas como **“uso interno”** e “**confidencial”** para endereços de e-mail de outros domínios além do @marrucci.com.br, exceto para terceiros (clientes ou fornecedores) diretamente envolvidos no assunto da mensagem.
	4. É vedado aos colaboradores o uso do correio eletrônico da Marrucci para enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da organização;
	5. Não é permitido enviar mensagens por correio eletrônico pelo endereço de outro departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
	6. É proibido enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a Marrucci vulneráveis a ações civis ou criminais;
	7. Não é permitido divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
	8. É proibido falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
	9. É proibido apagar mensagens pertinentes de correio eletrônico quando a Marrucci estiver sujeita a algum tipo de investigação;
	10. É proibido produzir, transmitir ou divulgar mensagem que contenham:
		+ - qualquer ato, ou forneça orientação que conflite ou contrarie os interesses da Marrucci;
			- ameaças eletrônicas, como: spam, mail bomb (mass mailing), vírus de computador, etc;
			- arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
			- vise obter acesso ou conceber acesso não autorizado a outro computador, servidor ou rede;
			- vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
			- vise burlar qualquer sistema de segurança;
			- vise vigiar secretamente ou assediar outro usuário;
			- vise acessar informações confidenciais sem explícita autorização do proprietário;
			- vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
			- inclua imagens criptografadas ou de qualquer forma mascaradas;
			- anexo(s) superior(es) a 30 MB para envio (interno e internet) e 30 MB para recebimento (internet);
			- tenha conteúdo considerado impróprio, obsceno ou ilegal;
			- caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
			- palavras de baixo calão;
			- perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
			- fins políticos locais ou do país (propaganda política);
			- inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.
	11. É terminantemente proibido a alteração de qualquer informação contida na assinatura de e-mail, e todas as mensagens deverão sempre incluir a assinatura padrão, definido pela Marrucci.

A assinatura deve obedecer ao seguinte layout:

|  |
| --- |
|  |

## Do acesso e uso da Internet

1. As Indústrias Marrucci poderão permitir o acesso à Internet e a navegação em sites de conteúdo, sempre de acordo com a política de Segurança da Informação e bloqueios de sites classificados como inseguros ou não confiáveis.
2. O uso da internet deve ser feito com comportamento eminentemente ético e profissional.
3. É explicitamente proibido a transferência de arquivos por meio de quaisquer protocolos, aplicativo ou ferramenta que não forem previamente e explicitamente aprovados pela área de Segurança da Informação das Indústrias Marrucci.
4. Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, as Indústrias Marrucci, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos.
5. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da empresa, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Tecnologia da Informação.
6. A internet disponibilizada pela empresa aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos.
7. Como é do interesse da Marrucci que seus colaboradores estejam bem-informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.
8. Somente os colaboradores que estão devidamente autorizados a falar em nome das Indústrias Marrucci para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.
9. Apenas os colaboradores autorizados pela empresa poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais ([LEI Nº 12.853/2013](http://legislacao.planalto.gov.br/legisla/legislacao.nsf/Viw_Identificacao/lei%2012.853-2013?OpenDocument)).
10. É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.
11. Os colaboradores com acesso à internet poderão fazer o download (baixar) somente de arquivos ligados diretamente às suas atividades na Marrucci.
12. O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pelo departamento de TI.
13. Os colaboradores não poderão em hipótese alguma utilizar os recursos da Marrucci para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.
14. O download e a utilização de qualquer tipo de programas poderão ser realizados único e exclusivamente pelo departamento de TI, passando anteriormente por uma avaliação de segurança e de validação de licenciamento, onde se for constatado de que não é gratuito, o mesmo não deverá ser instalado antes de uma compra legalizada das licenças de uso.
15. Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.
16. Colaboradores com acesso à internet não poderão efetuar upload (enviar), cópias em CD, DVD, HD externos, pendrives, ou qualquer outro dispositivo de qualquer software licenciado à Marrucci ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.
17. Os colaboradores não poderão utilizar os recursos da Marrucci para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.
18. O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) é proibido. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos. Porém, os serviços de comunicação instantânea (Teams, Skype for business, Gotomeeting, webex e afins) serão inicialmente disponibilizados aos usuários e poderão ser bloqueados caso o gestor requisite formalmente à Supervisão de TI.
19. Não é permitido acesso a sites de proxy (sites que redirecionem os acessos para acessar páginas proibidas pela empresa).

## Do uso dos Ativos de TI

Entende-se como Ativo de TI todo e qualquer equipamento e/ou dispositivo tecnológico disponibilizado pela Marrucci para uso nas atribuições das funções e como ferramenta de trabalho dos colaboradores e o uso dessas ferramentas está sujeito as regras aqui definidas:

1. Os ativos de TI disponibilizados são de propriedade da Marrucci, e são geridos pelo departamento de TI que possui total autoridade sobre a utilização destes, e os faz da forma que melhor atenda às necessidades da empresa.
2. É responsabilidade de cada usuário utilizar os ativos de TI com zelo, e manuseá-los corretamente para as atividades de interesse da empresa, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.
3. Sempre que um colaborador for desligado da empresa, os ativos que estavam atribuídos a ele, devem ser retornados para o departamento de TI, sendo posteriormente disponibilizado para qualquer outro departamento da empresa.
4. É expressamente proibido o uso de qualquer ativo de TI bem como quaisquer meios de comunicação corporativas para uso pessoal e/ou prática de qualquer ato ilícito, sob pena de responsabilização civil ou até criminal, sendo que nesses casos a Marrucci cooperará ativamente com as autoridades competentes.
5. O colaborador é responsável pelos ativos de TI da Marrucci, bem como pelas Informações que inserir em tais ativos.
6. Não é permitido por qualquer colaborador a tentativa de alteração de parâmetros de segurança previamente configurados ou definidos sem o devido credenciamento e autorização para tal. Caso isso venha a acontecer, isso será julgado inadequado e os riscos relacionados serão informados ao colaborador e ao respectivo gestor.
7. É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um Colaborador/Estagiário ou da Supervisão de TI da Marrucci, ou de quem este determinar. As gerências que necessitarem fazer testes deverão solicitá-los previamente à Supervisão de TI.

### Do Uso dos Computadores/Laptops

1. Não é permitido alterar o plano de fundo e a proteção de tela previamente configurados nos computadores da Marrucci.
2. Todos os computadores deverão ter senha de Bios para restringir o acesso de colaboradores não autorizados.
3. Os colaboradores devem informar ao departamento de TI qualquer identificação de dispositivo estranho conectado ou não ao seu computador;
4. É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos;
5. Todos os recursos tecnológicos adquiridos pela Marrucci devem ter imediatamente suas senhas padrões (default) alteradas;
6. Sempre que se encerrar o expediente de trabalho, o usuário deve desligar o computador;
7. Atendendo o disposto na **“Política de Tela e Mesa Limpa”**, após 5 minutos de inatividade, o computador deverá entrar em descanso de tela, bloqueando a estação de trabalho.
8. Independente do bloqueio de tela automático, é de responsabilidade do usuário que sempre que se ausentar de sua estação de trabalho, que faça o bloqueio do computador para evitar acessos indevidos.
9. Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar imediatamente o departamento de TI.

### Do uso das Impressoras

1. Não é permitido a impressão de documentos que infrinjam direitos autorais.
2. Todo e qualquer uso pessoal, ou que fuja das rotinas de trabalho, como trabalhos de faculdade, textos e/ou imagens com o intuito de fazer brincadeiras ou qualquer atividade que promova a desordem e improdutividade dos colaboradores é vetada e passível de punição.
3. É recomendável sempre a revisão do conteúdo a ser impresso antes de enviar a impressão, para assim, evitar erros e desperdício com impressões indevidas;
4. Em caso de impressão errada ou com falha, deixe a folha como rascunho para ser reutilizada, desde que o conteúdo não seja restrito e/ou confidencial;

### Do uso de Arquivos e Documentos

1. Arquivos pessoais e/ou não pertinentes aos negócios da Marrucci (fotos, músicas, vídeos etc.), não deverão ser copiados/movidos para os drives de rede/SharePoint, pois podem sobrecarregar o armazenamento e os backups.

Caso identificada a existência desses arquivos, eles deverão ser excluídos definitivamente sem comunicação prévia ao usuário.

1. Documentos imprescindíveis para as atividades dos colaboradores da Marrucci deverão ser salvos nos drives e pastas pré-estabelecidas no SharePoint, pois é mantido diariamente e regularmente rotinas de backup e cópias de segurança, podendo assim, ser facilmente recuperado algum arquivo ou documento, em casos de falha ou exclusão acidental.
2. Todas as pastas do SharePoint possuem limitação de acesso mediante permissões específicas. Apenas os supervisores de cada área podem permitir o acesso a estes diretórios.
3. Arquivos e documentos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão qualquer tipo de backup ou cópia de segurança e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade única do próprio usuário. O departamento de TI da Marrucci se isenta de qualquer culpa em caso de perda de arquivos e documentos salvos localmente no computador.
4. Fica proibido que os usuários coloquem senhas nos arquivos da Marrucci. Toda e qualquer necessidade de restrição e/ou limitação de acesso deve ser feito por meio das pastas já previamente configuradas para essa finalidade.
5. A liberação de acesso às pastas da rede deve ser autorizada única e exclusivamente pelo supervisor da área afim, onde deve explicitar via abertura de chamado, o nível de acesso ao diretório, se é permitido leitura e/ou escrita.
6. Não é permitido a liberação de acesso a pastas por qualquer outro colaborador que não seja o supervisor da área, e o Departamento de TI não está autorizado a liberar o acesso sem a solicitação formal da supervisão.

## Do uso de dispositivos de identificação e senhas

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário.

Essa norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

1. É proibido o uso dos dispositivos e/ou senhas de identificação de outra pessoa, pois constitui crime tipificado no Código Penal Brasileiro (Art. 307 - Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem: Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave.).
2. Todos os dispositivos de identificação utilizados na Marrucci, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.
3. O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).
4. Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em hipótese nenhuma.
5. Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante a Marrucci e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.
6. É proibido o compartilhamento de login para funções de administração de sistemas.
7. O Departamento de Recursos Humanos da Marrucci é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores.
8. O departamento de TI responde pela criação da identidade lógica dos colaboradores na empresa, nos termos do Procedimento para Gerenciamento de Contas de Grupos e Usuários.
9. Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.
10. Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 6 (seis) caracteres alfanuméricos (letras e números), utilizando caracteres especiais (@ ! # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo).
11. Os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 8 (oito) caracteres, alfanumérica (letras e números), utilizando caracteres especiais (@ ! # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.
12. É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados. As senhas são pessoais e intransferíveis, sendo de total responsabilidade de cada usuário sua salvaguarda e alteração sempre que julgar necessário, salvo exceção para os logins compartilhados, onde esta responsabilidade fica dividida entre os que fizerem uso desse acesso, e somente a eles.
13. As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.
14. Após 3 (três) tentativas incorretas de acesso, a conta do usuário será bloqueada por 15 minutos. Após decorrido esse tempo, o usuário é desbloqueado automaticamente, sendo possível tentar novamente o acesso com a senha.
15. O processo para a renovação de senha ocorre a cada 180 dias, onde decorrido esse tempo o usuário é obrigado a alterar sua senha, e a nova deve obedecer aos mesmos critérios de segurança e complexidade, além de ter que ser diferente das últimas 3 senhas utilizadas.
16. Independente da validade da senha, a qualquer momento os próprios usuários podem fazer a alteração da sua senha, e devem ser orientados a fazê-lo sempre que suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.
17. Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum colaborador for demitido ou solicitar demissão, ou de alguma forma se tornar inapto a continuar exercendo suas atividades na empresa, o Departamento de Recursos Humanos deverá imediatamente comunicar tal fato ao Departamento de Tecnologia da Informação, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.
18. Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer ao TI para efetuar a troca.

## Do Local de Trabalho

1. Todos os colaboradores deverão obedecer às regras de limpeza e organização do ambiente de trabalho a fim de não expor desnecessariamente Informações classificadas;
2. Os documentos impressos e anotações que precisem estar em um papel (impresso ou anotações) devem permanecer nas mesas em caráter temporário devendo ser recolhidos em compartimentos fechados disponíveis em seu departamento ou qualquer dependência da empresa que forneça segurança e proteção a esses materiais.
3. Toda Informação que permanecer nas mesas poderá e deverá ser destruída pelo colaborador responsável ou por qualquer outro colaborador que assim o quiser fazê-lo exercitando as boas práticas de proteção de Informações das Indústrias Marrucci.

## Do acesso físico

1. O acesso de visitantes às dependências das Indústrias Marrucci, não poderão ser feitos por pessoas desacompanhadas. O anfitrião do visitante deverá acompanhá-lo, desde a chegada na portaria da Marrucci, até o local onde este visitará.
2. É proibido ao visitante ou terceiro, filmar ou fotografar os equipamentos e/ou estrutura sem a devida autorização da Supervisão responsável.
3. As chaves de acesso às salas da empresa serão disponibilizadas somente após a assinatura da folha de controle disponibilizada na portaria.
4. As chaves da empresa e de acesso a departamentos devem ser guardadas de maneira segura e não devem ser emprestadas a terceiros e colegas de outros setores;
5. A perda ou extravio de qualquer chave deve ser comunicada imediatamente ao RH;
6. O acesso ao departamento de TI e principalmente ao Datacenter deve ser feito somente acompanhado por um colaborador da TI, e o local deverá permanecer sempre fechado com chave.
7. No caso de desligamento de empregados ou colaboradores que possuam chaves de acesso, imediatamente deverá ser retirado a cópia da chave do mesmo.

# Engenharia Social

**Engenharia social** é o termo utilizado para descrever método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou dados da empresa.

## Técnicas mais utilizadas

* + 1. **Ligação Telefônica**: simula-se uma pesquisa ou uma atualização cadastral, e faz-se perguntas acerca da estrutura da empresa, número de funcionários dentre outras informações que se realmente fosse da empresa que estes alegam ser, saberiam;
		2. **E-mails** **e Pishing**: Promoções, links, cadastros, notícias falsas, alertas de inadimplência ou da justiça, atualizações cadastrais do banco, dentre outros. Geralmente contém um link que redireciona para uma página falsa com o intuito de colher as informações pessoais e/ ou senhas. Pode ser de remetente desconhecido ou as vezes de um conhecido caso este já esteja infectado por algum vírus;
		3. **Abordagem pessoal**: Pessoas se fazendo passar por consultor, fornecedor, conhecido de alguém da direção, prestador de serviço, agente fiscal, ou qualquer outra pessoa com o intuito de conseguir entrar na empresa e realizar as abordagens necessárias para colher informações;
		4. **Análise de Lixo**: O lixo é uma das fontes mais ricas de informações, visto que através de papéis coletados no lixo pode-se conseguir nome de funcionários, telefone, e-mail, senhas, contato de clientes, fornecedores, transações efetuadas, entre outros.

## Prevenção

Para evitar esses problemas, as seguintes medidas se fazem necessárias para diminuir a vulnerabilidade da empresa a esse tipo de ataque:

* + 1. Nenhum funcionário está autorizado a responder qualquer tipo de pesquisa ou questionário por telefone, todo questionário deve ser enviado por e-mail, onde deverá ser analisado pela Supervisão da área;
		2. Não descartar integralmente no lixo papéis contendo informações de funcionários, contato de clientes, fornecedores, transações entre outros, estes devem ser fragmentados para serem descartados;
		3. Fica proibido a divulgação de todo e qualquer tipo de informação e/ou fotos das Indústrias Marrucci em redes sociais e qualquer tipo de site da internet sem o devido aval da Supervisão;
		4. Fica proibido a divulgação de qualquer informação referente a TI, seja sobre estrutura, funcionários, equipamentos etc., para visitantes, sejam eles terceiros, prestadores de serviços ou de qualquer outra natureza;
		5. Não é permitido abrir e-mail de remetente desconhecido e de forma alguma clicar em links que possam direcionar para páginas inseguras;
		6. Não é permitido liberar acesso remoto para qualquer pessoa e/ou empresa. Salvo exceção quando este for de ciência da TI e ainda assim necessitando da anuência ao termo de confidencialidade;
		7. Não é permitido realizar doações, cadastros em programas de voluntariados e responder qualquer questionário do tipo para essa finalidade para evitar alimentar banco de dados alheios com informações pessoais que possam ser usadas em futuros ataques;

# Penalidades

A violação desta Política poderá acarretar sanções administrativas e/ou legais, sem prejuízo da

rescisão do contrato de trabalho e/ou qualquer outro contrato de relacionamento de prestação de serviço entre o colaborador, associado, consultor e/ou sócio, assim como qualquer entidade com relação contratual direta ou indireta com as Indústrias Marrucci.

Situações que podem ocasionar sanções incluem, mas não se limitam, a:

1. O descumprimento confirmado de qualquer disposição desta política “PSI” poderá acarretar a imposição de sanção ao colaborador que incorrer no descumprimento;
2. O procedimento de apuração será conduzido pelo encarregado de dados, deferido espaço de justificativa da conduta pelo colaborador em suspeita de desvio;
3. As sanções, de maneira proporcional, poderão ser: advertência verbal, na reincidência, advertência por escrito, suspensão e demissão;
4. A advertência verbal será aplicada na hipótese de descumprimento cometido por colaborador primário ou na ocorrência de desvio leve e que não tenha implicado em vazamento de dados sensíveis;
5. A advertência por escrito será aplicada na hipótese de reincidência de colaborador em conduta que já tenha ciência desta política “PSI” e que não tenha implicado em vazamento de dados sensíveis.
6. A suspensão será aplicada na hipótese de recorrente reincidência para casos mais graves e que não tenham implicado em vazamento de dados;
7. A demissão por justa causa poderá ser aplicada na reincidência de desvios de conduta que tenham implicado em vazamento de dados.
8. A demissão será aplicada para o colaborador que incidir em conduta que implique em vazamento de dados ou que torne inviável a entrega de comunicação a contento ao titular de dados ou a Autoridade Nacional de Proteção de Dados.
9. Será extremamente importante que toda a advertência escrita seja formalizada, visto que em caso de uma demissão, poderá fundamentar a decisão do empregador. Em alguns casos ela pode configurar até como prova da má conduta do colaborador em uma possível ação judicial.

# Das Disposições Finais

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna das Indústrias Marrucci, ou seja, qualquer incidente de segurança subtende-se como ação deliberada de um indivíduo contra a ética e os bons costumes regidos e preconizados pela organização.

A presente Política passa a valer a partir da data de sua aprovação e publicação, sendo válida por prazo indeterminado.

Todos os colaboradores tiveram acesso e participaram de treinamento no que diz respeito às rotinas desta Política de Segurança da Informação, não podendo justificar seu descumprimento ao argumento de falta de ciência de seu conteúdo.

Treinamentos periódicos podem ser realizados visando fortalecer as premissas desta Política, aos qual todos os colaboradores estão obrigados a participar.

# IDENTIFICAÇÃO DAS ALTERAÇÕES

|  |  |  |
| --- | --- | --- |
| **REVISÃO** | **DATA** | **RESUMO DA ALTERAÇÃO** |
| 00 | 10/03/2023 |  Elaboração inicial do documento. |