POLÍTICA DE SEGURANÇA DE INFORMAÇÃO

CLASSIFICAÇÃO: INTERNA

VERSÃO 1.1

ÚLTIMA REVISÃO: 01/06/2025

1. Introdução

1.1. Objetivo

Esta política tem como objetivo estabelecer as diretrizes e os requisitos para garantir a segurança da informação em nossa organização.

1.2. Escopo

Esta política se aplica a todos os funcionários, contratados, fornecedores e parceiros que lidam com as informações e ativos da organização.

2. Princípios de Segurança

2.1. Confidencialidade

Assegurar que as informações sejam acessadas apenas por pessoas autorizadas.

2.2. Integridade

Garantir a precisão e a consistência das informações e dos sistemas de informação.

2.3. Disponibilidade

Assegurar que os sistemas de informação e os recursos de TI estejam acessíveis quando necessário.

3. Gerenciamento de Acesso

3.1. Controle de Acesso

Implementar controles de acesso para garantir que apenas usuários autorizados possam acessar as informações e os sistemas.

3.2. Autenticação

Estabelecer processos de autenticação para verificar a identidade dos usuários que acessam os sistemas e informações.

3.3. Autorização

Garantir que os usuários autorizados tenham permissões apropriadas para acessar recursos e sistemas de informação.

4. Segurança Física e Ambiental

4.1. Proteção de instalações

Implementar medidas para proteger as instalações físicas onde os sistemas de informação e recursos de TI estão localizados.

4.2. Controle de acesso físico

Estabelecer medidas de controle de acesso para impedir o acesso não autorizado às áreas críticas.

4.3. Segurança ambiental

Implementar medidas para proteger os recursos de TI contra desastres naturais e outros riscos ambientais.

5. Segurança de Redes e Comunicações

5.1. Proteção de redes

Implementar controles para proteger as redes da organização contra ameaças externas e internas.

5.2. Monitoramento e detecção de intrusões

Estabelecer sistemas de monitoramento e detecção de intrusões para identificar e responder a incidentes de segurança.

6. Gestão de Incidentes de Segurança

6.1. Resposta a incidentes

Estabelecer um processo de resposta a incidentes para lidar com violações de segurança e minimizar seu impacto.

6.2. Relatórios de incidentes

Os funcionários devem relatar todos os incidentes de segurança imediatamente à equipe de segurança da informação.

7. Conscientização e Treinamento em Segurança

7.1. Programa de conscientização

Desenvolver e implementar um programa de conscientização sobre segurança para garantir que todos os funcionários compreendam suas responsabilidades e a importância da segurança da informação.

7.2. Treinamento em segurança

Fornecer treinamento em segurança regularmente para manter os funcionários atualizados sobre as melhores práticas e políticas de segurança.

8. Avaliação e Melhoria Contínua

8.1. Auditorias de segurança

Realizar auditorias de segurança periódicas para avaliar a eficácia das políticas e práticas de segurança e identificar áreas de melhoria.

8.2. Revisão de políticas e procedimentos

Revisar e atualizar as políticas e procedimentos de segurança regularmente, considerando as mudanças tecnológicas, as ameaças emergentes e as lições aprendidas com incidentes de segurança anteriores.

8.3. Análise de riscos

Realizar análises de risco para identificar e avaliar os riscos de segurança associados às informações e ativos da organização, e implementar medidas para mitigar esses riscos.

8.4. Medição de desempenho

Estabelecer métricas e indicadores-chave de desempenho (KPIs) para medir a eficácia dos programas de segurança e garantir que os objetivos de segurança sejam alcançados.

9. Conformidade Legal e Regulatória

9.1. Conformidade com leis e regulamentações

Garantir que as políticas e práticas de segurança estejam em conformidade com as leis e regulamentações aplicáveis, incluindo leis de privacidade e proteção de dados.

9.2. Gerenciamento de vulnerabilidades e patches

Implementar um processo para identificar, avaliar e corrigir vulnerabilidades de segurança nos sistemas e aplicativos, incluindo a aplicação regular de patches de segurança.

10. Responsabilidades

10.1. Direção

A direção da organização é responsável por estabelecer e apoiar as políticas de segurança da informação e garantir que os recursos adequados sejam alocados para a gestão da segurança.

10.2. Equipe de segurança da informação

A equipe de segurança da informação é responsável pela implementação, monitoramento e manutenção das políticas e práticas de segurança e pela resposta a incidentes de segurança.

10.3. Funcionários

Todos os funcionários são responsáveis por seguir as políticas e práticas de segurança estabelecidas e por relatar qualquer incidente de segurança ou preocupações relacionadas à segurança da informação.

1. Introdução

1.1. Objetivo

Esta política tem como objetivo estabelecer as diretrizes e os requisitos para garantir a segurança da informação na BeautyCorp, protegendo os dados corporativos, sistemas de TI e infraestrutura contra ameaças internas e externas. Além disso, busca-se assegurar a conformidade com regulamentações aplicáveis e a continuidade dos negócios.

1.2. Escopo

Esta política se aplica a:

- Todos os funcionários (efetivos, temporários e estagiários);

- Terceirizados, fornecedores e parceiros que acessem sistemas ou dados da BeautyCorp;

- Todos os ativos de informação, incluindo hardware, software, redes, dados físicos e digitais;

- Todas as unidades da empresa (Matriz em Contagem, escritório em Belo Horizonte e filiais em Montes Claros, Juiz de Fora e Uberlândia).

2. Princípios e Compromissos de Segurança da Informação

A **BeautyCorp**, enquanto líder inovadora no setor de manufatura de cosméticos, estabelece a Segurança da Informação como um **imperativo estratégico e responsabilidade corporativa fundamental**. A alta administração da BeautyCorp, em alinhamento com sua Missão e Visão de sustentabilidade e excelência, compromete-se a assegurar a proteção contínua e robusta de todos os ativos informacionais e de Tecnologia Operacional (TO), fundamentada nos seguintes princípios:

2.1. Confidencialidade

A Confidencialidade é o **atributo essencial** que garante que as informações classificadas como proprietárias, sensíveis ou confidenciais da BeautyCorp sejam **acessadas, processadas, armazenadas, transmitidas e divulgadas exclusivamente por indivíduos, processos ou sistemas expressamente autorizados**, com base no princípio do **mínimo privilégio (least privilege)** e na **necessidade de conhecimento (need-to-know)**.

- **Propriedade Intelectual (IP):** Fórmulas de produtos (incluindo composições, excipientes, aditivos), metodologias de P&D, dados de testes de eficácia e segurança, patentes e segredos comerciais.
- **Dados de Clientes e Mercado:** Informações de CRM, histórico de pedidos, estratégias de precificação e inteligência de mercado, que, se comprometidos, impactam diretamente a competitividade.
- **Informações de Produção e Cadeia de Suprimentos:** Especificações de insumos, dados de fornecedores estratégicos, otimização de linhas de produção, volumes de produção e rotas de distribuição.
- **Credenciais e Acessos Privilegiados:** Chaves criptográficas, credenciais de sistemas de automação industrial (SCADA, MES), e privilégios administrativos em sistemas ERP, WMS e APIs.
- **Centro Educacional para Funcionários:** Cursos de informática, atividades administrativas, matrículas, informações dos funcionários.

A violação da confidencialidade impacta diretamente a competitividade, a conformidade regulatória (ex: LGPD para dados de clientes) e a reputação da marca. A **alta administração é responsável por fomentar uma cultura de confidencialidade**, e os gerentes de cada departamento são encarregados de garantir a aplicação rigorosa dos controles de acesso e a conscientização de suas equipes sobre a importância da proteção da informação.

2.2. Integridade

A Integridade é o **atributo crítico** que assegura a **precisão, completude, consistência, autenticidade e validade não-repudiável** dos dados e da funcionalidade dos sistemas de informação e controle operacional (TO) da BeautyCorp, desde a entrada até o armazenamento e o processamento, através de todo o seu ciclo de vida.

- **Processos de Manufatura:** Assegurar que as instruções de produção, receitas (batch records), parâmetros de controle de qualidade e dados de máquinas sejam inalterados e reflitam a realidade para evitar desvios na produção ou produtos fora de especificação.
- **Qualidade e Conformidade Regulatória:** Manter a imutabilidade e a rastreabilidade dos dados de conformidade (ex: GMP, ISO), registros de auditoria e validação de processos para garantir a qualidade do produto final e evitar sanções regulatórias.
- **Consistência de Dados Transacionais:** Garantir que transações financeiras, dados de inventário, ordens de compra e venda nos sistemas ERP e WMS sejam precisas e não adulteradas.
- **Integridade do Código e Configurações:** Proteger o código-fonte da API, dos sistemas de controle e as configurações de equipamentos industriais contra alterações não autorizadas que possam introduzir vulnerabilidades ou interrupções.

Em um ambiente de manufatura, a integridade é vital para a **precisão das receitas de produção**, a **confiabilidade dos dados de controle de qualidade**, a **rastreabilidade da cadeia de suprimentos** e a **segurança dos sistemas de automação industrial (SCADA/MES)**. Alterações não autorizadas ou acidentais em fórmulas, parâmetros de máquinas ou dados de inventário podem resultar em produtos defeituosos, prejuízos financeiros significativos, danos à saúde dos consumidores e graves implicações regulatórias. A **Diretoria de Operações e a Gerência de TI/TO são conjuntamente responsáveis por implementar e auditar os controles técnicos** (como validação de entrada, controle de versão, logs de auditoria e backup/restauração) que sustentam a integridade dos processos e dados críticos da produção.

2.3. Disponibilidade

A Disponibilidade é o atributo que assegura que os **sistemas de informação, recursos de Tecnologia da Informação (TI) e Tecnologia Operacional (TO), e os dados da BeautyCorp estejam acessíveis e operacionais para usuários e processos autorizados no momento e no local necessários**, garantindo a continuidade das operações de manufatura e distribuição. Este princípio é vital para:

- **Operações de Produção:** Manter a operabilidade contínua dos sistemas SCADA, MES, automação de linha e robótica para evitar paradas na produção e garantir a entrega de produtos.
- **Cadeia de Suprimentos:** Assegurar o acesso ininterrupto a sistemas de gestão de inventário, transporte e distribuição para otimizar o fluxo de matérias-primas e produtos acabados.
- **Comunicação e Colaboração:** Garantir a funcionalidade das plataformas de comunicação, e-mail e sistemas colaborativos para a coordenação eficiente entre equipes de P&D, produção, vendas e logística.
- **Serviços de TI Essenciais:** Prover acesso contínuo a ERP, sistemas de RH, e-commerce e infraestrutura de rede para suportar todas as funções de negócio.

A continuidade das operações de manufatura de cosméticos está intrinsecamente ligada à disponibilidade de sistemas como ERP, WMS, e especialmente os sistemas de chão de fábrica. Interrupções podem levar a paradas na produção, atrasos na distribuição, perda de vendas e impacto na capacidade de inovar e entregar produtos. A **Diretoria Executiva da BeautyCorp endossa a alocação de recursos para infraestrutura resiliente** (alta disponibilidade, redundância, planos de contingência) e a **equipe de TI/TO é encarregada de desenvolver,**

implementar e testar regularmente planos de continuidade de negócios (BCP) e recuperação de desastres (DRP), com a definição clara de RTO (Recovery Time Objective) e RPO (Recovery Point Objective) para os serviços críticos.

3. Gerenciamento de Acesso

O Gerenciamento de Acesso na BeautyCorp é um componente crítico da estratégia de segurança da informação, projetado para proteger ativos informacionais e operacionais, desde fórmulas de produtos até sistemas de manufatura e dados de clientes, garantindo que o acesso seja concedido de forma precisa e restrita ao mínimo privilégio necessário. Esta política aplica-se a todos os funcionários, colaboradores, terceiros e sistemas que interagem com os ambientes de Tecnologia da Informação (TI) e Tecnologia Operacional (TO) da Matriz em Contagem-MG, bem como das filiais em Belo Horizonte-MG, Montes Claros-MG, Juiz de Fora-MG e Uberlândia-MG (incluindo o Centro Educacional).

3.1. Controle de Acesso

A BeautyCorp implementará controles de acesso abrangentes para garantir que apenas indivíduos, processos e sistemas devidamente autorizados possam acessar informações e recursos.

- **Princípio do Mínimo Privilégio (Least Privilege):** O acesso a sistemas, informações e recursos de rede será concedido com base na estrita necessidade de conhecimento ("Need-to-know") e necessidade de uso ("Need-to-use"), minimizando as permissões concedidas a cada usuário ou sistema.
- **Segregação de Funções (Separation of Duties):** Funções críticas de segurança ou que, se combinadas, poderiam resultar em fraude ou erro significativo, serão segregadas entre diferentes indivíduos para evitar conflitos de interesse e mitigar riscos.
- **Gerenciamento do Ciclo de Vida do Acesso:** O acesso será gerenciado desde a requisição inicial, passando pela aprovação, concessão, revisão periódica até a revogação em caso de mudança de função ou desligamento. Todos os acessos serão formalmente documentados.
- **Acesso Lógico:** Controles serão aplicados a sistemas operacionais, aplicações (incluindo a API .NET 8 e sistemas ERP/MES/WMS), bancos de dados e redes. Isso inclui o gerenciamento de usuários locais e de domínio, grupos de segurança e permissões em sistemas de arquivos e diretórios compartilhados.
- **Acesso Físico:** Controles físicos serão implementados para proteger data centers, servidores, equipamentos de rede, áreas de produção e outros locais com ativos de informação críticos em todas as unidades da BeautyCorp.

3.2. Autenticação

A BeautyCorp estabelecerá processos rigorosos de autenticação para verificar a identidade de usuários, dispositivos e processos que buscam acessar seus sistemas e informações.

- **Autenticação Forte:** Será priorizada a implementação de métodos de autenticação que ofereçam alta garantia de identidade.
- **Senhas:** Senhas devem aderir a uma política de complexidade (comprimento mínimo, combinação de caracteres), história e expiração. O armazenamento de senhas será realizado exclusivamente por meio de algoritmos criptográficos robustos de hash (ex: BCrypt, Argon2) com salting, e nunca em texto plano.
- **Autenticação Baseada em Token (para APIs e Aplicações Web):** Para a API .NET 8 e outras interfaces de programação, será empregada autenticação baseada em tokens (ex: JWT - JSON Web Tokens). Os tokens devem possuir tempo de vida limitado, serem gerados com algoritmos de assinatura criptográfica forte e chaves secretas devidamente protegidas, e sua validação rigorosa (incluindo assinatura e claims) será mandatória em cada requisição protegida.
- **Autenticação Multifator (MFA/2FA):** A implementação de MFA será obrigatória para acesso a sistemas críticos (ex: ambientes de produção, acesso remoto privilegiado, ERP, sistemas de controle industrial) é

fortemente recomendada para todos os demais acessos, elevando a segurança contra comprometimento de credenciais.
- **Gerenciamento de Credenciais:** As credenciais de acesso, incluindo senhas, chaves de API e certificados digitais, serão geridas de forma segura, com políticas para criação, armazenamento, uso, rotação e revogação. Credenciais de serviço e de sistemas automatizados serão gerenciadas separadamente e protegidas.
- **Bloqueio de Contas:** Mecanismos de bloqueio de contas ou atraso de tentativas de login serão implementados para mitigar ataques de força bruta ou preenchimento de credenciais.

3.3. Autorização

A BeautyCorp assegurará que, uma vez autenticada a identidade de um usuário ou sistema, suas permissões de acesso aos recursos e sistemas de informação sejam apropriadas e devidamente controladas.

- **Modelo de Autorização:** Será adotado um modelo de autorização formal (ex: Role-Based Access Control - RBAC, ou Attribute-Based Access Control - ABAC), onde as permissões são atribuídas a papeis ou atributos, e não diretamente a usuários individuais.
- **Matriz de Permissões:** Será mantida e periodicamente revisada uma matriz clara de permissões, detalhando quais papeis têm acesso a quais sistemas e quais operações podem realizar (Criar, Ler, Atualizar, Deletar - CRUD) em cada recurso.
- **Autorização em Nível de Aplicação e Dados:** As verificações de autorização serão implementadas no nível da aplicação (backend da API .NET 8, lógica de negócios dos sistemas), e não apenas no frontend, garantindo que mesmo requisições diretas à API sejam devidamente autorizadas. Para acesso a dados específicos, a autorização considerará o nível de objeto (ex: um usuário só pode acessar seus próprios registros de `viagem` ou `cliente` na API de Logística).
- **Revisões de Acesso:** Auditorias e revisões periódicas das permissões de acesso serão realizadas para garantir que estas permaneçam alinhadas às necessidades de negócio e aos princípios de menor privilégio. Quaisquer acessos desnecessários ou excessivos serão prontamente revogados.
- **Segurança no Centro Educacional:** Para os 30 computadores do Centro Educacional em Uberlândia-MG, serão implementados perfis de usuário restritos, sem privilégios administrativos, e com acesso limitado à internet e a recursos da rede corporativa, segregando-os do ambiente de produção e administrativo da BeautyCorp.

4. Segurança Física e Ambiental

Este plano garante que a infraestrutura de rede da BeautyCorp esteja protegida contra ameaças físicas e ambientais, alinhando-se às necessidades de cada unidade (Matriz, Filiais e Centro Educacional).

4.1. Proteção de Instalações

Objetivo: Garantir a segurança física dos servidores, equipamentos de rede e infraestrutura crítica da BeautyCorp.

Medidas Implementadas:

- Câmeras de segurança com gravação em nuvem em todas as salas de servidores (Matriz e Filiais).

- Sensores de movimento e alarmes contra intrusão.

- Acesso Restrito:

- Salas de servidores trancadas com fechaduras eletrônicas e controle por biometria/cartão de proximidade.

- Registro de acesso logado para auditoria (ex.: quem entrou/saiu e horário).

- Proteção contra Roubo/Vandalismo:

  - Racks e servidores fixados com travas físicas.

  - Equipamentos de rede em ambientes sem identificação visível (evitar alvo de furtos).

4.2. Controle de Acesso Físico

Objetivo: Impedir acesso não autorizado a áreas críticas (salas de TI, CPD, racks).

Medidas Implementadas:

- Matriz (Contagem) e Filiais:

  - Catracas ou portas com leitor de cartão RFID para acesso às áreas de TI.

  - Credenciais hierárquicas:

    - Nível 1 (TI): Acesso total às salas de servidores.

    - Nível 2 (Funcionários): Acesso restrito a áreas comuns.

    - Visitantes: Acompanhados por um funcionário autorizado.

  - Procedimento de Visitantes:

    - Cadastro prévio com documento de identificação.

    - Crachá temporário com limite de horário.

4.3. Segurança Ambiental

Objetivo: Proteger a infraestrutura contra desastres naturais e falhas ambientais.

Medidas Implementadas:

- Controle de Temperatura e Umidade:

  - Sistemas de refrigeração redundantes (ar-condicionado industrial) nas salas de servidores.

  - Sensores de temperatura e umidade conectados ao Zabbix para alertas em tempo real.

- Proteção contra Energia Instável:

  - No-breaks (UPS) para servidores críticos (autonomia mínima de 2 horas).

  - Geradores a diesel para manter operação durante quedas prolongadas.

- Prevenção contra Incêndios e Enchentes:

  - Extintores de gases inertes (não danificam equipamentos) em salas de TI.

  - Sensores de fumaça e água com alarme integrado.

  - Drenagem elevada para evitar alagamentos (principalmente em Montes Claros e Juiz de Fora, cidades com histórico de chuvas intensas).

Integração com a Infraestrutura Existente

- Monitoramento Centralizado:

  - Alertas do Zabbix para falhas ambientais (ex.: temperatura alta, umidade crítica).

  - Câmeras e sensores integrados a um sistema de gestão de segurança (ex.: Milestone XProtect).

- Plano de Contingência Físico:

- Backup georreferenciado dos dados em filiais distintas (ex.: servidor em Uberlândia armazena cópia dos dados da Matriz).

Responsáveis pela Implementação:

- TI da BeautyCorp (equipe interna) + parceiros especializados em segurança física (ex.: Tyco Security).

- Custo Estimado: R$ 120.000 (investimento inicial em equipamentos e sistemas).

Resultados Esperados:

- Redução de 99% em incidentes por falhas físicas/ambientais no primeiro ano.

- Compliance com normas de segurança (ex.: ISO 27001, PCI DSS).

5. Segurança de Redes e Comunicação

5.1. Proteção de redes

A organização deve implementar firewalls, sistemas de prevenção de intrusões (IPS) e segmentação de redes para proteger os dados contra acessos não autorizados. Todo tráfego de rede deve ser filtrado e monitorado, especialmente aquele que transita entre a rede corporativa e a internet. A rede deve ser configurada para minimizar pontos únicos de falha, e os equipamentos de rede devem estar atualizados com os patches de segurança. A segurança de redes deve incluir medidas específicas para proteger sistemas de controle industrial e equipamentos de automação usados na produção dos cosméticos.

5.2. Monitoramento e detecção de intrusões

Devem ser implementados sistemas de detecção e resposta a intrusões (IDS/EDR) para monitoramento contínuo de redes e terminais, com alertas automatizados em caso de atividades suspeitas. Logs de acesso e eventos devem ser mantidos e analisados regularmente. A detecção precoce de invasões é essencial para proteger dados de formulações, propriedade intelectual e informações pessoais de clientes e fornecedores. A equipe de TI deve garantir que os alertas sejam correlacionados e investigados dentro de prazos definidos.

6. Gestão de Incidentes de Segurança

6.1. Resposta a incidentes

Deve haver um plano formal de resposta a incidentes de segurança da informação, que inclua a identificação, contenção, erradicação, recuperação e análise pós-incidente. Esse plano deve abranger desde vazamentos de dados até interrupções em sistemas de produção automatizados. Equipes responsáveis devem ser previamente treinadas e prontas para atuação rápida, com linhas claras de comunicação e escalonamento. A continuidade dos negócios e a integridade da produção devem ser priorizadas.

6.2. Relatórios de incidentes

Todos os colaboradores têm a obrigação de relatar imediatamente qualquer suspeita ou ocorrência de incidente de segurança, como acessos não autorizados, e-mails de phishing ou uso indevido de sistemas. Os relatórios devem ser encaminhados diretamente à equipe de segurança da informação ou por meio de canais oficiais previamente estabelecidos (e.g., e-mail, sistema interno ou hotline). O não reporte de incidentes pode representar riscos operacionais e legais graves à empresa, e será tratado conforme a política disciplinar.

7. Conscientização e Treinamento em Segurança

7.1. Programa de conscientização

A empresa deve manter um programa contínuo de conscientização sobre segurança da informação, adaptado aos diferentes perfis de funcionários (administrativo, produção, P&D, vendas etc.). O programa deve incluir conteúdos sobre ameaças comuns (e.g., engenharia social, vazamentos de dados), o uso seguro de e-mails e senhas, além de instruções específicas para proteção da propriedade intelectual de fórmulas e procedimentos de produção de cosméticos.

7.2. Treinamento em segurança

Treinamentos obrigatórios devem ser realizados ao menos uma vez por ano, com reciclagens sempre que houver atualizações relevantes nas políticas ou quando um novo risco for identificado. Novos colaboradores devem receber treinamento de segurança como parte do processo de integração. Simulações de incidentes, como campanhas de phishing internas, podem ser utilizadas para reforçar a aprendizagem e testar a eficácia dos treinamentos. A participação nos treinamentos será registrada e auditada periodicamente.

8. Avaliação e Melhoria Contínua

A BeautyCorp reconhece que a segurança da informação é um processo dinâmico e contínuo, e não um estado estático. A evolução das ameaças cibernéticas, as inovações tecnológicas (incluindo o desenvolvimento de APIs .NET 8 e a infraestrutura AWS) e as mudanças nos requisitos de negócio e regulatórios exigem uma abordagem proativa e interativa para a gestão da segurança. Esta seção define os mecanismos para avaliar, aprimorar e manter a eficácia do programa de segurança da informação da BeautyCorp em todas as suas unidades (Matriz em Contagem-MG, Filiais em Belo Horizonte-MG, Montes Claros-MG, Juiz de Fora-MG e Centro Educacional em Uberlândia-MG).

8.1. Auditorias de segurança

A BeautyCorp realizará auditorias de segurança periódicas, planejadas e independentes, para avaliar a conformidade e a eficácia das políticas, procedimentos e controles de segurança implementados.

- **Escopo e Frequência:** As auditorias abrangerão sistemas de TI e TO (incluindo a API .NET 8, ERP, MES, sistemas SCADA), infraestrutura de rede (matriz e filiais), conformidade com padrões internos e regulatórios (ex: LGPD, certificações de qualidade). A frequência será determinada pela criticidade dos sistemas e riscos associados, com auditorias externas sendo realizadas anualmente e auditorias internas com maior frequência.
- **Resultados e Relato:** Os resultados das auditorias, incluindo não-conformidades, vulnerabilidades identificadas e áreas de melhoria, serão documentados em relatórios formais. Estes relatórios serão apresentados à **alta administração, ao Comitê de Segurança da Informação e aos gerentes de departamento relevantes**, para assegurar a visibilidade e o comprometimento com a remediação.
- **Ação Corretiva:** Planos de ação corretiva serão desenvolvidos e implementados em resposta às descobertas da auditoria, com prazos e responsabilidades claramente definidos. A eficácia das ações corretivas será monitorada e verificada em auditorias subsequentes.

8.2. Revisão de Políticas e Procedimentos

As políticas e procedimentos de segurança da informação da BeautyCorp não são documentos estáticos; eles serão revisados e atualizados regularmente para garantir sua relevância, eficácia e alinhamento com as melhores práticas de segurança e as necessidades do negócio.

- **Periodicidade:** Uma revisão formal e abrangente de toda a PSI e dos procedimentos de segurança associados será realizada, no mínimo, anualmente ou sempre que ocorrerem eventos significativos, tais como:

- Mudanças na arquitetura de TI ou TO (ex: implementação de novas tecnologias como a API em .NET 8, expansão de infraestrutura em nuvem na AWS).
- Surgimento de novas ameaças cibernéticas e vulnerabilidades críticas.
- Alterações na legislação ou regulamentação aplicável ao setor de cosméticos ou à proteção de dados.
- Incidentes de segurança relevantes que revelam falhas nos controles existentes.
- Alterações organizacionais ou de processos de negócio.
- **Responsabilidade:** A **Diretoria de Segurança da Informação (ou equivalente)**, em colaboração com os gerentes de TI/TO, jurídico, RH e as lideranças de negócio, será responsável por coordenar o processo de revisão e garantir que as atualizações sejam comunicadas efetivamente a todas as partes interessadas.

8.3. Análise de Riscos

A BeautyCorp implementará um processo contínuo e estruturado de análise de riscos para identificar, avaliar e mitigar ameaças à confidencialidade, integridade e disponibilidade de suas informações e ativos.

- **Metodologia:** Será utilizada uma metodologia de análise de risco reconhecida (ex: NIST CSF, ISO 27005) para identificar os ativos críticos (informações, sistemas de produção, API, dados de clientes), as ameaças potenciais (cibernéticas, físicas, ambientais), as vulnerabilidades (conforme identificado na Análise de Vulnerabilidade inicial), e o impacto potencial em caso de exploração.
- **Frequência:** A análise de riscos será realizada periodicamente (ex: anualmente) e sempre que houver mudanças significativas no ambiente de negócio, tecnologia ou ameaças.
- **Gerenciamento de Riscos:** Os riscos identificados serão priorizados com base em sua probabilidade e impacto. Planos de tratamento de riscos (mitigação, transferência, aceitação ou evitação) serão desenvolvidos, com a implementação de controles de segurança adequados. A **alta administração e o Comitê de Segurança da Informação são os responsáveis finais pela aceitação dos níveis de risco residual**.

8.4. Medição de Desempenho

A BeautyCorp estabelecerá métricas e Indicadores-Chave de Desempenho (KPIs) para monitorar e medir a eficácia de seu programa de segurança da informação, assegurando que os objetivos de segurança sejam atingidos e que a empresa esteja continuamente aprimorando sua postura de segurança.

- **KPIs Relevantes:** Os KPIs incluirão, mas não se limitarão a:
- Número e severidade de vulnerabilidades identificadas e remediadas (relacionado à Análise de Vulnerabilidade da API).
- Tempo médio para detecção (MTTD) e tempo médio para resposta (MTTR) a incidentes de segurança.
- Percentual de conformidade com políticas de segurança (ex: uso de senhas fortes, aplicação de patches).
- Taxa de sucesso em testes de phishing e treinamento de conscientização.
- Disponibilidade dos sistemas críticos (SLA).
- Métricas de utilização de recursos de segurança (ex: WAF, soluções de DLP).
- **Relato e Ação:** Os resultados dos KPIs serão coletados, analisados e apresentados regularmente à **alta administração e ao Comitê de Segurança da Informação**. Desempenhos abaixo do esperado dispararão ações corretivas e ajustes no plano de segurança, impulsionando a melhoria contínua e a otimização dos investimentos em segurança.

9. Conformidade Legal e Regulatória

9.1. Conformidade com leis e regulamentações

A empresa deve garantir que todas as políticas, processos e práticas de segurança da informação estejam em total conformidade com a legislação vigente, incluindo:

- Lei Geral de Proteção de Dados (LGPD) no Brasil.
- Normas da ANVISA, quando aplicável à manipulação, produção e rotulagem de cosméticos, especialmente no que diz respeito ao armazenamento e sigilo de informações sobre ingredientes, testes e rastreabilidade.
- Requisitos de conformidade com auditorias internas e externas (ex: ISO 22716 - Boas Práticas de Fabricação de Cosméticos, e ISO/IEC 27001 - Gestão de Segurança da Informação, se adotadas).
- Todos os contratos com terceiros e fornecedores devem incluir cláusulas específicas de proteção de dados e segurança da informação. A não conformidade pode acarretar sanções legais, reputacionais e financeiras, devendo ser continuamente monitorada e auditada.

9.2. Gerenciamento de vulnerabilidades e patches

Deve ser implementado um processo sistemático de gerenciamento de vulnerabilidades, incluindo:

- Varreduras periódicas em sistemas internos e expostos à internet (e.g., sistemas ERP, dispositivos IoT usados na produção, websites e aplicações de e-commerce).
- Classificação e priorização de vulnerabilidades com base em criticidade (ex: CVSS score) e risco ao negócio.
- Aplicação regular e tempestiva de patches de segurança em sistemas operacionais, aplicativos comerciais, softwares de controle de produção e sistemas embarcados.
- Definição de prazos máximos para correção com base na gravidade da vulnerabilidade (por exemplo, falhas críticas devem ser corrigidas em até 72 horas).
- Testes em ambientes controlados antes da aplicação de atualizações em sistemas produtivos, para evitar interrupções nas linhas de fabricação.
- É responsabilidade da equipe de TI manter registros dessas atividades, com evidências e relatórios de conformidade.

10. Responsabilidades

10.1. Direção

A direção da organização é responsável por estabelecer e apoiar as políticas de segurança da informação e garantir que os recursos adequados sejam alocados para a gestão da segurança.

10.2. Equipe de segurança da informação

A equipe de segurança da informação é responsável pela implementação, monitoramento e manutenção das políticas e práticas de segurança e pela resposta a incidentes de segurança.

10.3. Funcionários

Todos os funcionários são responsáveis por seguir as políticas e práticas de segurança estabelecidas e por relatar qualquer incidente de segurança ou preocupações relacionadas à segurança da informação.

11. Glossário

- **API (.NET 8):** Interface de Programação de Aplicações desenvolvida com a tecnologia .NET 8, que permite a comunicação entre diferentes sistemas de software.
- **Autenticação Multifator (MFA/2FA):** Processo de verificação da identidade de um usuário que requer duas ou mais formas de prova, como senha e código de verificação enviado ao celular.
- **BCP (Business Continuity Plan):** Plano de Continuidade de Negócios, um conjunto de procedimentos para garantir que as operações críticas continuem durante e após um desastre.
- **Criptografia:** Processo de codificar informações para torná-las ilegíveis para quem não possui a chave de decodificação.
- **DRP (Disaster Recovery Plan):** Plano de Recuperação de Desastres, um conjunto de procedimentos para restaurar sistemas e dados após um desastre.
- **ERP (Enterprise Resource Planning):** Sistema de Planejamento de Recursos Empresariais, um software que integra e gerencia processos de negócios essenciais.
- **Firewall:** Dispositivo de segurança de rede que monitora e controla o tráfego de entrada e saída, bloqueando ou permitindo o tráfego com base em regras de segurança definidas.
- **IDS/EDR (Intrusion Detection System/Endpoint Detection and Response):** Sistemas que monitoram redes e dispositivos para atividades suspeitas e respondem a incidentes de segurança.
- **IPS (Intrusion Prevention System):** Sistema de Prevenção de Intrusões, que detecta e bloqueia automaticamente tentativas de exploração de vulnerabilidades.
- **LGPD (Lei Geral de Proteção de Dados):** Legislação brasileira que estabelece regras para a coleta, uso, tratamento e compartilhamento de dados pessoais.
- **MTTD (Mean Time To Detect):** Tempo médio para detectar um incidente de segurança.
- **MTTR (Mean Time To Respond):** Tempo médio para responder e resolver um incidente de segurança.
- **Patch:** Atualização de software que corrige vulnerabilidades ou falhas de segurança.
- **RBAC (Role-Based Access Control):** Controle de Acesso Baseado em Funções, onde permissões são atribuídas a funções específicas e não a usuários individuais.
- **RPO (Recovery Point Objective):** Ponto Objetivo de Recuperação, a quantidade máxima de dados que podem ser perdidos durante um incidente.
- **RTO (Recovery Time Objective):** Tempo Objetivo de Recuperação, o tempo máximo aceitável para restaurar um sistema ou serviço após um incidente.
- **SCADA (Supervisory Control and Data Acquisition):** Sistema de Controle Supervisório e Aquisição de Dados, usado para monitorar e controlar processos industriais.
- **SLA (Service Level Agreement):** Acordo de Nível de Serviço, um contrato entre um provedor de serviços e um cliente que define o nível de serviço esperado.
- **TO (Tecnologia Operacional):** Refere-se aos sistemas de hardware e software que monitoram e controlam equipamentos e processos industriais.

- **WAF (Web Application Firewall):** Firewall de Aplicações Web, que protege aplicações web de ataques, filtrando e monitorando o tráfego HTTP.
- **WMS (Warehouse Management System):** Sistema de Gerenciamento de Armazém, um software que gerencia e otimiza operações de armazém.