**PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS**

**INSTITUTO DE CIÊNCIAS EXATAS E INFORMÁTICA  
Bacharelado em Sistemas de Informação**

Alexandre Fernandes Abreu

Aline Souza Alves

Gabriel Henrique Martins Avelino

Higor Botelho Mendes

Leandro Felipe Gonçalves Barbosa

Thalita de Oliveira Farias

**GRUPO SWEETCRYSTAL**

**MANUFATURA**

Belo Horizonte

2024

**Alexandre Fernandes Abreu**

**Aline Souza Alves**

**Gabriel Henrique Martins Avelino**

**Higor Botelho Mendes**

**Leandro Felipe Gonçalves Barbosa**

**Thalita de Oliveira Farias**

**GRUPO SWEETCRYSTAL**

**MANUFATURA**

Trabalho apresentado como requisito parcial à aprovação na disciplina Projeto Estruturado de Redes de Computadores.

Professor: Alexandre Teixeira

Belo Horizonte

2024

**SUMÁRIO**

1. **TEMA3**
2. **RESPONSABILIDADE4**
3. **CRONOGRAMAS DE ATIVIDADE** **6**
4. **PLANEJAMENTO DOS RECURSOS DE REDE6**

**4.1** DIVISÃO FÍSICA DA REDE **7**

**4.2** PLANILHA DE MATERIAIS **7**

**4.3** DIVISÃO LÓGICA DA REDE 9

* 1. PLANILHA LINKS **13**

1. **IMPLEMENTAÇÃO DOS RECURSOS DA REDE**..................................................**13**

**5.1** IMPLEMENTAÇÃO SERVIDOR FÍSICO DA MATRIZ **13**

**5.1.1** INSTALAÇÃO E CONFIGURAÇÃO DO ACTIVE DIRECTORY (AD)**14**

**5.1.2** POLÍTICAS DE GRUPO APLICADAS**15**

**5.2** IMPLEMENTAÇÃO DE UM SERVIDOR NA NUVEM PARA A MATRIZ **16**

1. **GERENCIAMENTO DOS SERVIDORES NO ZABBIX21**

**6.1** GERENCIAMENTO DO SERVIDOR FÍSICO NO ZABBIX **21**

**6.2** GERENCIAMENTO DO SERVIDOR DA NUVEM ZABBIX **22**

**6.3** VISUALIZAÇÃO DO MONITORAMENTO DOS SERVIDORES NO ZABBIX **24**

1. **APLICAÇÃO BACK-END28**
2. **TEMA**

O projeto possui como proposta o desenvolvimento de uma rede que conecte todos os departamentos e setores de uma empresa manufatureira do setor de açúcar chamada Sweet Crystal que emprega cerca de 250 colaboradores.

A Sweet Crystal possui a seguinte estrutura:

* **Administração:** Responsável por coordenar e gerenciar, financeiros, físicos e tecnológicos em uma organização. Suas principais funções incluem, finanças, instalações, operações e sistemas de informação para garantir o funcionamento eficiente e o alcance dos objetivos da empresa.
* **Logística:** Responsável pelo processo de planejamento, implementação e controle eficiente do fluxo e armazenamento de bens, serviços e informações, desde o ponto de origem até o ponto de consumo, de forma a atender aos requisitos dos clientes. Envolve a gestão de transporte, armazenamento, inventário, embalagem e processamento de pedidos, visando maximizar a eficiência e minimizar os custos ao longo da cadeia de suprimentos.
* **Manufatura:** responsável por transformar as ideias em produtos reais que podem ser vendidos aos clientes. O setor de manufatura deve ser eficiente, produtivo, inovador e comprometido com a segurança e o meio ambiente.
* **Supply Chain:** refere-se ao conjunto de processos e atividades que envolvem a produção, distribuição e entrega de um produto ou serviço, desde a matéria-prima até o consumidor final. Isso inclui todos os estágios, desde a aquisição de matérias-primas, fabricação, armazenamento, transporte, até a venda e entrega do produto acabado. O objetivo da gestão da cadeia de suprimentos é otimizar esses processos para garantir a eficiência operacional, reduzir custos, melhorar a qualidade do produto e atender às demandas dos clientes de forma eficaz.
* **Setor de TI:** é responsável por garantir o bom funcionamento dos sistemas e infraestrutura tecnológica que suportam todas as operações da empresa.
* **Setor de Qualidade:** responsável por garantir que os produtos ou serviços de uma empresa atendam aos padrões e requisitos de qualidade estabelecidos. Suas principais responsabilidades incluem o desenvolvimento e implementação de políticas e procedimentos de controle de qualidade, realização de inspeções e testes de produtos, identificação e correção de defeitos ou não conformidades, além de monitorar e melhorar continuamente os processos para garantir a satisfação do cliente e a conformidade com regulamentos e padrões de qualidade. O setor de qualidade desempenha um papel crucial na garantia da reputação da empresa e na fidelização dos clientes.
* **Segurança:** é responsável por proteger os ativos da empresa contra diversas ameaças, como roubos, vandalismo e incêndios.
* **Recursos Humanos:** responsável pela gestão das relações entre a empresa e seus funcionários. Suas principais responsabilidades incluem recrutamento e seleção de pessoal, treinamento e desenvolvimento, administração de salários e benefícios, gestão de desempenho, resolução de conflitos, garantia do cumprimento das leis trabalhistas e promoção de um ambiente de trabalho saudável e produtivo. O RH desempenha um papel fundamental no desenvolvimento e na retenção de talentos, contribuindo para o sucesso e o crescimento sustentável da empresa.

1. **RESPONSABILIDADES**

|  |  |  |
| --- | --- | --- |
| **Nome** | **Papel** | **Responsabilidade** |
| Alexandre | Pesquisador | Realizar levantamento de requisitos;  Definir objetivos e metas alinhados com as demandas de rede. |
| Aline | Redatora | Coordenar a elaboração do cronograma do projeto, definindo etapas e prazos para as atividades;  Coletar, organizar e documentar dados relevantes para o projeto, garantindo a disponibilidade de informações para subsidiar as atividades. |
| Gabriel | Prazo e controle de qualidade | Realizar a contextualização das demandas do projeto, compreendendo as necessidades e objetivos. |
| Higor | Desenvolvimento | Participar das reuniões periódicas de acompanhamento do projeto, compartilhando atualizações sobre o progresso das atividades e contribuindo com ideias e soluções para os desafios enfrentados;  Coordenar o Protótipo da rede no Simulador da Cisco Packet Tracer. |
| Leandro | Gestão de Recursos | Participar das reuniões periódicas de acompanhamento do projeto, compartilhando atualizações sobre o progresso das atividades e contribuindo com ideias e soluções para os desafios enfrentados;  Coordenar a planilha de Recursos e Redes. |
| Thalita | Líder do projeto | Coordenar as reuniões semanais de acompanhamento do projeto;  Realizar a distribuição de tarefas entre os membros da equipe. |

1. **CRONOGRAMA DE ATIVIDADES**

|  |  |  |
| --- | --- | --- |
| **Semana** | **Dias de Dedicação** | **Atividades** |
| Semana 1  06/02/2024 | Sete | Definição do tema e formação do grupo. |
| Semana 2  20/02/2024 | Cinco | Planejamento inicial da proposta; |
| Semana 3  26/02/2024 | Cinco | Construção da planilha de recursos de rede; |
| Semana 4  04/03/2024 | Cinco | Protótipo de rede - Cisco Packet Tracer; |
| Semana 5  11/03/2024 | Cinco | Revisão e entrega |

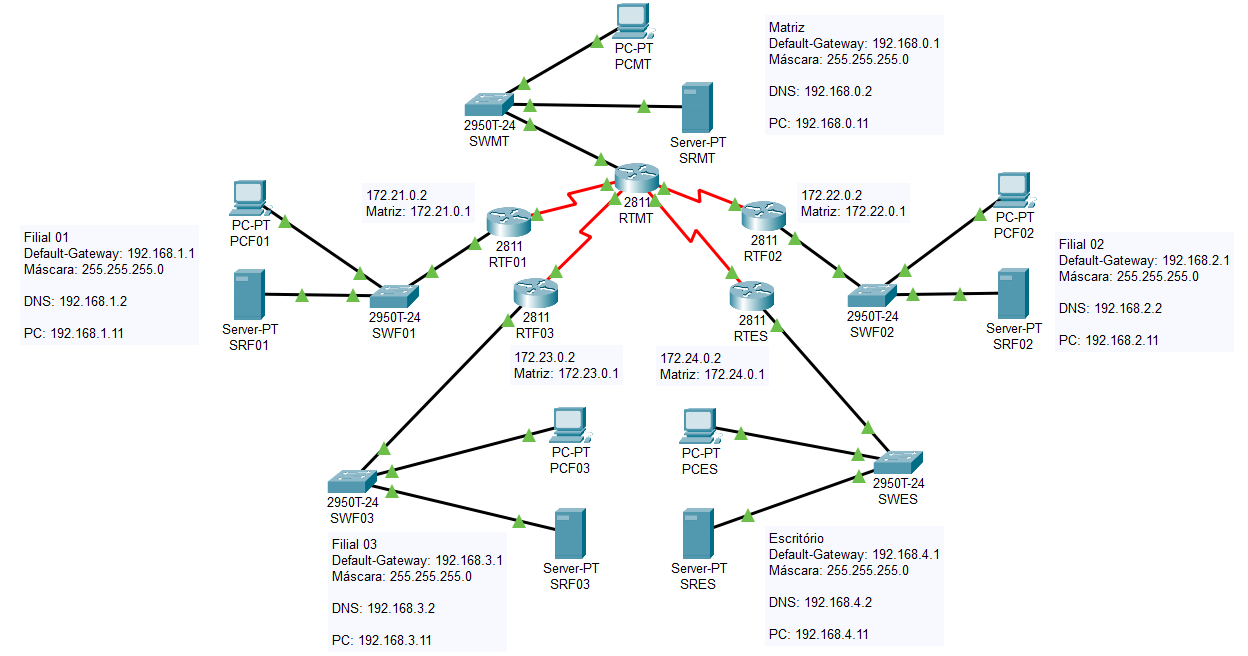
1. **PLANEJAMENTO DOS RECURSOS DE REDE**

A estrutura física da empresa está dividida da seguinte forma: A Matriz está situada no município de Unaí, sendo o escritório em Belo Horizonte. As filiais estão localizadas nos municípios Santa Fé de Minas e Paracatu, em Minas Gerais; e em Buritis, no Espírito Santo.

Os departamentos estão divididos na forma que segue:

* **Matriz**
  + Administração;
  + Logística;
  + Manufatura;
  + Supply Chain;
  + Setor de TI;
  + Setor de Qualidade;
  + Segurança;
* **Escritório**
  + Administração;
  + Recursos Humanos.
* **Filiais**
  + Logística;
  + Manufatura.
  1. **DIVISÁO FÍSICA DA REDE**

Considerando as necessidades da empresa objeto deste projeto, a divisão física da rede foi configurada conforme o modelo apresentado abaixo:



Fonte: Cisco Packet Tracer

* 1. **PLANILHA DE MATERIAIS**

A seguir, cada tabela apresenta os equipamentos que irão equipar a matriz, o escritório e as filiais. Conforme é possível observar, o valor total de investimento demandado para implementação do sistema de rede na matriz é de R$ 355.370,64.

****

Interface gráfica do usuário, Tabela

Descrição gerada automaticamente

Tabela

Descrição gerada automaticamente

Interface gráfica do usuário, Tabela

Descrição gerada automaticamente

Interface gráfica do usuário, Aplicativo, Tabela

Descrição gerada automaticamente

* 1. **DIVISÃO LÓGICA DA REDE**

|  |  |  |
| --- | --- | --- |
| **Dispositivos** | **Nome** | **Portas/Endereçamento** |
| Router | RTMT |  |
| Router | RTF01 |  |
| Router | RTF02 |  |
| Router | RTF03 |  |
| Router | RTES |  |
| Switch | SWMT |  |
| Switch | SWF01 |  |
| Switch | SWF02 |  |
| Switch | SWF03 |  |
| Switch | SWES |  |
| Server | SRMT |  |
| Server | SRF01 |  |
| Server | SRF02 |  |
| Server | SRF03 |  |
| Server | SRFES |  |
| PC | PCMT |  |
| PC | PCF01 |  |
| PC | PCF02 |  |
| PC | PCF03 |  |
| PC | PCES |  |

* 1. **PLANILHA LINKS**

Conforme é possível observar, a tabela abaixo apresenta o número de computadores em cada filial, na matriz e no escritório e os valores correspondem a utilização de estrutura de rede.

Tabela

Descrição gerada automaticamente

1. **IMPLEMENTAÇÃO DOS RECURSOS DA REDE**
   1. **IMPLEMENTAÇÃO SERVIDOR FÍSICO DA MATRIZ**

O servidor local implementado em via VM Virtual Box da Oracle apresenta as seguintes configurações:

* **Sistema Operacional:** Windows Server 2012 R2 64 bits;
* **CPU:** AMD Ryzen 5 3500U with Radeon Vega Mobile Gfx 2.10 GHz;
* **Memória RAM:** 2GB;
* **Nome do servidor:** sweetcrystal.minasgerais.net;
* **Domínio:** minasgerais.net

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

Especificações do servidor local (Windows 2012).

Fonte: autoria própria

As credenciais de acesso são as seguintes:

* **Usuário:** admin
* **Senha:** 123456
  + 1. **INSTALAÇÃO E CONFIGURAÇÃO DO DHCP**

Foi ativado o recurso do *Active Directory* e configurado para o domínio minasgerais.net, onde foram criadas as estruturas organizacionais.

As estruturas organizacionais foram criadas contemplando a Matriz, no município mineiro de Unaí, o escritório em Belo Horizonte, e as filiais nos municípios de Santa Fé de Minas; Paracatu; e Buriti, no Espírito Santo. Além disso, foram criados usuários dentro do domínio.

Interface gráfica do usuário, Aplicativo, Word

Descrição gerada automaticamente

Usuários Ativos.

Fonte: autoria própria.

* + 1. **POLÍTICAS DE GRUPO APLICADAS**

Foram implementadas as seguintes políticas:

* Ir para a área de trabalho, e não para a tela inicial, quando entrar;
* Remover ícone do controle de volume;
* Proibir acesso ao Painel de Controle e às configurações do PC.

A imagem a seguir apresenta a política implementada em relação aos usuários do escritório localizado em Belo Horizonte; contudo, é importante ressaltar que a mesma política foi implementada para usuários das demais unidades que compõe a unidade organizacional da empresa.

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

Políticas de Grupo Aplicadas aos Usuários do Escritório em Belo Horizonte.

Fonte: autoria própria.

* 1. **IMPLEMENTAÇÃO DE UM SERVIDOR NA NUVEM PARA MATRIZ**

Para criação de servidor na AWS, com o propósito de atender às necessidades da matriz, foi criada rede virtual (VPC) visando a configuração dos recursos da rede. Esta foi chamada de sweet-crystal com duas sub-redes públicas e duas privadas.

Tela de computador com jogo

Descrição gerada automaticamente

VPCs na AWS.

Fonte: AWS

Tela de computador com jogo

Descrição gerada automaticamente

Sub-redes na AWS.

Fonte: AWS

Em relação à configuração do grupo de segurança, neste caso, denominado *G7sec*, foram criadas duas regras: A primeira constitui em permissão de acesso de qualquer IPV4 via RDP e, a segunda, permissão de acesso de qualquer IPV4 via navegador web utilizando protocolo HTTP.

Interface gráfica do usuário

Descrição gerada automaticamente

Grupo de Segurança.

Fonte: AWS

Tela de vídeo game

Descrição gerada automaticamente

Regras de Entrada do Grupo de Segurança.

Fonte: AWS

Em seguida, foi criado uma instância EC2, utilizando-se o sistema operacional Windows Server 2016, sendo o tipo de instância definido como t2.micro. A referida instância encontra-se dentro da VPC sweet-crystal e do grupo de segurança *G7sec*.

Tela de computador

Descrição gerada automaticamente

Instância do Servidor Web

Fonte: AWS

Após instalar o servidor web da Microsoft, o IIS; acessa-se o servidor criado via RDP. Conforme é possível observar nas imagens abaixo, o servidor foi acessado no IP público 44.200.202.27. É importante destacar, no entanto, que outro IP será atribuído pela AWS em acesso futuro; tratando-se de comportamento comum da referida plataforma de nuvem.

Interface gráfica do usuário

Descrição gerada automaticamente

Acesso via RDP ao servidor

Fonte: autoria própria.

Interface gráfica do usuário

Descrição gerada automaticamente

Servidor IIS disponível no servidor.

Fonte: autoria própria.

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

Acesso à página do servidor web pelo navegador.

Fonte: autoria própria.

1. **GERENCIAMETNO DOS SERVIDORES NO ZABBIX**
   1. **GERENCIAMENTO DO SERVIDOR FÍSICO NO ZABBIX**

Para realização do gerenciamento do servidor físico na rede, utilizou-se a plataforma Zabbix – ferramenta de monitoramento de rede que permite verificar a disponibilidade e o desempenho de servidores e dispositivos de rede.

Além da referida ferramenta, optou-se pelo protocolo SNMP – *Simple Network Managment Protocol* – uma vez que se trata de padrão quando o objetivo é o monitoramento de dispositivos de rede conectados por IP.

O serviço do protocolo SNMP foi instalado no servidor local, conforme apresentado na imagem abaixo, com duas *community strings: private* (que permite ler e escrever) e *public* (que permite apenas ler). Essas *strings* servem como senhas de acesso para a comunicação do servidor com o software Zabbix.

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Servidor de SNMP no servidor local.

Fonte: autoria própria.

Com a definição das *communities* no servidor local, deu-se início a etapa de configuração do host no Zabbix. Para isso foi preciso informar alguns dados na plataforma de monitoramento como o nome do host, o protocolo usado, seu IP, a porta, seu template e seu host group.

Esses dados foram essenciais para o Zabbix conseguir localizar e solicitar informações do host a ser monitorado. As regras de firewall no servidor local foram verificadas para que a porta 161 não impedisse a comunicação do Zabbix. Porém, não tivemos nenhum problema nessa fase.

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

Adição do servidor local na plataforma Zabbix.

Fonte: autoria própria.

* 1. **GERENCIAMENTO DO SERVIDOR DA NUVEM NO ZABBIX**

Os mesmos procedimentos para configuração do servidor local foram aplicados ao servidor AWS na nuvem na configuração do SNMP; execução do serviço SNMP e definição da *Community* sweetcrystal.

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

Serviço SNMP no servidor da nuvem.

Fonte: autoria própria

A configuração do servidor localizado em nuvem no Zabbix seguiu os mesmos critérios em relação ao preenchimento das suas informações na plataforma, conforme imagem abaixo.

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

Adição de servidor da nuvem no Zabbix.

Fonte: autoria própria.

O único procedimento adicional necessário na configuração do servidor da nuvem foi a abertura de portas referentes aos protocolos SNMP e ICMP no grupo de segurança criado na AWS; caso contrário o Zabbix não conseguiria se comunicar com o servidor na nuvem.

Tela de computador com jogo

Descrição gerada automaticamente

Regras de entrada e saída no grupo de segurança na nuvem.

Fonte: autoria própria.

* 1. **VISUALIZAÇÃO DO MONITORAMENTO DOS SERVIDOS NO ZABBIX**

Uma vez configurado o servidor local e o servidor na nuvem, o monitoramento de ambos os servidores passou a ser feito pelo Zabbix. Observamos na ferramenta que as comunicações com os hosts ocorriam sem problemas, conforme as imagens abaixo.

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

Visualização dos hosts adicionados para monitoramento via Zabbix.

Fonte: autoria própria.

No momento da realização do monitoramento dos servidores via Zabbix, foi possível observar – conforme visualiza-se nas imagens abaixo – que a referida ferramenta acusou que o tempo de resposta do *ping* no servidor da AWS estava acima daquilo que é considerável aceitável.

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

Monitoramento dos hosts via Zabbix.

Fonte: autoria própria

Este aviso pode significar latência alta na rede, o que pode ser causado por congestionamento de rede, problemas relativos ao roteamento, ou falhas em dispositivos de rede.

Interface gráfica do usuário, Aplicativo, Word

Descrição gerada automaticamente

Monitoramento de problema de alta latência no servidor AWS na nuvem.

Fonte: autoria própria.

Gráfico

Descrição gerada automaticamente

Monitoramento do tráfego de rede do servidor AWS em nuvem.

Fonte: autoria própria.

Gráfico

Descrição gerada automaticamente

Monitoramento do tráfego de rede do servidor local.

Fonte: autoria própria.

Por fim, o Zabbix permite a construção de mapa representativo da infraestrutura da rede objeto de monitoramento, destacando-se a integração entre o servidor local e o servidor AWS na nuvem, conforme visualiza-se na imagem abaixo.

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

Mapa da rede da infraestrutura monitorada via Zabbix.

Fonte: autoria própria.

1. **APLICAÇÃO BACK-END**

Acessando o endereço www.sweetcrystal.tech, o cliente terá acesso ao site da aplicação onde encontrará link que o direciona à tela de login/cadastro do usuário, conforme verifica-se abaixo.

Interface gráfica do usuário, Aplicativo, PowerPoint

Descrição gerada automaticamente

Página Principal - Home

Acessando a tela de login, o cliente cadastrado deverá entrar com o nome de usuário e senhas registrados na ocasião do cadastro.

Interface gráfica do usuário, Site

Descrição gerada automaticamente

Tela de login

Caso não tenha registro, existe link que direciona à tela onde o cliente poderá se registrar.

Uma vez logado no sistema, o cliente visualizará aqueles produtos mais acessados, facilitando, assim, a manipulação de informações referentes aos mesmos.

Interface gráfica do usuário, Aplicativo, Tabela

Descrição gerada automaticamente

Tela de Produtos mais acessados

A aba movimentações leva à tela que apresenta o registro de todos os produtos cadastrados, permitindo ao cliente editar suas informações, excluí-los e cadastrar novos produtos.

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

Tela de Movimentações

Por fim, o cliente possui acesso à tela de relatório, em que poderá visualizar o registro de todas as entradas e saídas de produtos no estoque da empresa, permitindo controle eficiente de produtos.

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

Tela Relatório

**ANEXO I**

**Política de Segurança da Informação**

Junho de 2024

|  |  |
| --- | --- |
| Tipo de Documento: **Política** | |
| Data de Aprovação: **16/06/2024** | Revisão: **Anual** |
| Data de Efetivação: **16/06/2024** | Código do Documento: **PSI-001-2024** |

1. **OBJETIVO**

O objetivo da referida Política de Segurança da Informação é estabelecer as diretrizes e procedimentos visando a proteção da informação e processos de negócio, incluindo sua matriz e suas filiais. A política se aplica aos Colaboradores (Funcionários, Estagiários e aos Prestadores de Serviços (Terceiros)) e todos aqueles que acessem ou façam uso dos sistemas de informação da SWEETYCRYSTAL.

1. **ABRANGÊNCIA**

Esta política é um normativo interno, com valor jurídico e aplicabilidade irrestrita e imediata a todos colaboradores, bem como, a todos que acessem a rede corporativa, serviços e sistemas de informações.

1. **PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO**

A política de segurança da informação da SWEETYCRYSTAL é baseada nos seguintes princípios:

1. **CONFIDENCIALIDADE:** permite que apenas pessoas legitimamente autorizadas acessem dados e informações;
2. **INTEGRIDADE:** garante que todas as características da mensagem original sejam mantidas durante qualquer operação, entre a sua origem e destino.
3. **DISPONIBILIDADE:** permite que usuários autorizados tenham acesso a informações de seus interesses sempre que necessário, para o seu uso legítimo.
4. **AUTENTICIDADE:** permite garantir que o emissor de determinada informação seja realmente quem alega ser, assegurando que a mensagem é realmente proveniente da fonte declarada.
5. **SEGURANÇA É RESPONSABILIDADE DE TODOS**

Todo Colaborador é responsável pela guarda e segurança das informações que produz ou custodia. Como também, possui a obrigação de contribuir de forma contínua na proteção de dados, informações e dos processos de negócio.

1. **DIRETRIZES**
   1. **CLASSIFICAÇÃO DA INFORMAÇÃO**

É dever de cada colaborador classificar cada informação no momento que ela for gerada, como pública, interna ou confidencial, para garantir que as informações sejam devidamente protegidas e garantir a confidencialidade.

* + - 1. Informação **PÚBLICA**: é a informação que pode ser acessada por qualquer pessoa, sem restrições. É de livre circulação e não gera danos à empresa ou colaboradores caso seja divulgada.
      2. Informação **INTERNA**: é a informação que não pode ser divulgada para pessoas fora da empresa, mas que, caso isso aconteça, não causará grandes prejuízos. A preocupação principal nesse nível está relacionada à integridade da informação.
      3. Informação **CONFIDENCIAL**: é a informação que, se divulgada interna ou externamente, tem potencial para trazer grandes prejuízos financeiros ou à imagem da empresa. É o nível mais alto de confidencialidade e deve ser protegida por medidas rigorosas de segurança.
    1. **ROTULAGEM DAS INFORMAÇÕES**: quando as informações não forem públicas, estas precisam ser rotuladas no momento que foram geradas, armazenadas e/ou disponibilizadas.
    2. Para as informações geradas e mantidas em ambientes lógicos, utilizar documentação específica para definir o nível de classificação da informação.
    3. O acesso e o compartilhamento de informações devem respeitar o sigilo profissional e contratual.
    4. Havendo dúvidas sobre a classificação da informação, a classifique como interna, para preservar as informações da empresa.
  1. **CONTROLE DE ACESSO**

Todos os colaboradores possuem uma credencial de acesso, esta credencial é pessoal e intransferível, é vedado o seu empréstimo ou compartilhamento. Para ter acesso a Rede Corporativa, aos sistemas de informação e aos demais serviços, o colaborador deve utilizar a sua credencial de acesso.

Todos os acessos, seja as informações, sistemas ou instalações físicas da empresa devem ser monitorados. Desta forma, o colaborador terá acesso apenas as atividades e informações necessárias para o exercício das suas atividades.

A concessão de acessos precisa obedecer aos critérios de menor privilégio, onde os colaboradores terão acessos as informações e recursos necessários para o exercício das atividades laborais. Todos os acessos precisam assegurar a irretratabilidade e a rastreabilidade da solicitação.

* 1. **INTERNET**

Os recursos de conectividade são concedidos para atender as finalidades da empresa. Portanto, os colaboradores devem fazer uso da internet observando as leis em vigor. Vale ressaltar, que caso ocorra o uso ilegal ou indevido deste recurso, o colaborador será responsabilizado pelo descumprimento.

* 1. **E-MAIL**

A utilização do e-mail (correio eletrônico) deve respeitar as diretrizes e normas de segurança da informação, bem como devem atender aos fins institucionais, respeitando as regras de direitos autorais, licenciamento de software, direitos de propriedade e privacidade.

* 1. **DISPOSITIVOS INSTITUCIONAIS**

A utilização dos dispositivos da empresa ou mantidos por ela, é restrito aos colaboradores e as pessoas autorizadas pela instituição. Quantos aos dispositivos móveis, eles devem conter o menor número de informações, para que não comprometa a proteção de dados e informações.

Em casos de perdas, furtos ou roubos de dispositivos institucionais de contenham informações da empresa, o colaborador deve registrar um B.O. (Boletim de Ocorrência), e entregar cópia a equipe de segurança patrimonial e ao seu gestor.

* 1. **ARMAZENAMENTO DE INFORMAÇÕES**

Todos os colaboradores devem armazenar as informações em locais apropriados e destinados a esse fim. Quanto as informações digitais devem ser mantidas nos servidores na rede corporativa. Já, as informações físicas, devem ser guardadas nos armários trancados e locais apropriados.

De acordo com a Lei Geral de Proteção de Dados – LGPD, as informações devem ser mantidas pelo período necessário. E, estas podem ser removidas por solicitação.

* 1. **REPOSITÓRIOS DIGITAIS**

Os repositórios digitais da empresa são ferramentas importantes para o armazenamento, compartilhamento e disseminação de informações. É importante usá-los de forma responsável e de acordo com as regras estabelecidas, para garantir a segurança e a confidencialidade das informações.

* 1. **MÍDIAS SOCIAIS**

O acesso as mídias socias são restritos aos setores de Comunicação e Marketing, para exercício das atividades institucionais. O colaborador que utilize as mídias para fins distintos, responderá por suas ações ou omissões que resulte de sua conduta.

* 1. **VISIBILIDADE DAS INFORMAÇÕES NO AMBIENTE DE TRABALHO**

As informações imprensas e digitais não devem ser deixadas expostas, a vista de todos. Todo o documento impresso e que não possuir mais utilidade, deve ser destruído.

Ao deixar o computador, cabe ao colaborador realizar o bloqueio de sua estação de trabalho, para proteção das informações contidas no equipamento.

* 1. **ÁUDIOS, VÍDEOS E FOTOS**

Não é permitido fotografar, gravar, filmar, publicar ou compartilhar imagens da empresa, sem a devida autorização e que não sejam para fins institucionais.

* 1. **APLICATIVOS DE COMUNICAÇÃO**

O uso de aplicações de chamada de vídeo para comunicação interna e externa, deve ser feito de acordo com as políticas da empresa. A aplicação de chamada de vídeo deve ser usada apenas para fins corporativos legítimos.

* 1. **MONITORAMENTO**

A empresa realiza o registro e armazenamento de atividades (logs) e monitoram seus ambientes físicos e lógicos. Os dados resultantes do monitoramento são utilizados para fins internos e legais, além de corroborar para proteção e futuras investigações de autoridades.

* 1. **SOFTWARE DE ANTIVÍRUS**

Todos os desktops e notebooks da empresa devem possuir antivírus instalados e atualizados. Os softwares devem ser configurados para realizar as varreduras regulares em busca de malware.

Todos os computadores da Empresa devem ter software antivírus instalado e atualizado. O software antivírus deve ser configurado para realizar varreduras regulares em busca de malware.

* 1. **ENCERRAMENTO DOS CONTRATOS DE TRABALHO E DE PRESTAÇÃO DE SERVIÇOS**

Em casos de rescisão contratual ou término contratual, a equipe central de gestão de acessos deve desativar todos os acessos à rede corporativa, bem como aos sistemas da empresa. A equipe de segurança patrimonial será responsável inativação das suas credenciais de acessos físicos.

* 1. **SEGURANÇA DA INFORMAÇÃO**

A empresa deve estar comprometida com o dever de orientar os seus colaboradores e todos que acessam a rede corporativa e os recursos de tecnologia da informação sobre o seu uso seguro.

1. **CONSCIENTIZAÇÃO E TREINAMENTO DE CYBERSEGURANÇA**

O objetivo de um programa de treinamento e conscientização sobre a segurança é educar os Colaboradores e os Prestadores de Serviços da SWEETYCRYSTAL, sobre como interagir com os dados e ativos corporativos de maneira segura.

Os treinamentos de Cibersegurança, compõe a lista de treinamentos obrigatório, sendo necessário à sua realização no momento da contratação. A depender da área, a renovação do curso deve ser semestral ou anual.

É necessário o engajamento das áreas para temas sensíveis como a engenharia social, MFA (duplo fator de autenticação), *phishing*, dentre outros.

1. **PAPÉIS E RESPONSABILIDADES**

A gestão da aplicação das políticas de Segurança da Informação é um procedimento crucial para garantir a proteção dos dados e ativos da empresa. Esta atividade exige a compreensão e colaboração de diferentes níveis hierárquicos. É papel de cada um dos atores abaixo:

1. **ALTA ADMINISTRAÇÃO – PRESIDÊNCIA E DIRETORIA:** os gestores e líderes de alta escalão deve demonstrar compromisso com a aplicação das normas, bem como devem promover e alocar recursos necessários para a promoção de uma cultura de segurança da informação na empresa.

Definir as diretrizes gerais da política de segurança da informação, como também estar alinhados com os objetivos estratégicos da empresa e os requisitos legais, é uma das principais atividades da alta gestão.

1. **GESTÃO DE SEGURANÇA DA INFORMAÇÃO:** é a equipe responsável pela implementação e manutenção da política de segurança da informação, incluindo a criação de procedimentos, controles e medidas de segurança.

Como também, é a equipe responsável pelo monitoramento e avaliação dos pontos de melhoria e gerenciamento dos riscos. O treinamento e conscientização dos colaboradores é de suma importância para a proteção dos dados e informação.

Na ocorrência de incidentes ou necessidade de investigação para resposta a incidentes de segurança da informação, deve tomando as medidas cabíveis para minimizar os dados e restaurar o normal funcionamento dos sistemas.

1. **GESTORES E LÍDERES DE ÁREA:** são responsáveis por implementar a política de segurança da informação em suas respectivas áreas, garantindo que seus colaboradores estejam cientes das políticas e procedimentos e que os controles de segurança estejam em vigor. Devem realizar treinamentos, como também, incentivar que as equipes realizem os treinamentos necessários. Na ocorrência de incidentes e violação devem reportar a equipe de segurança da informação.
2. **COLABORADORES:** todos os colaboradores devem cumprir a política de segurança da informação e os procedimentos de segurança estabelecidos pela organização. Os colaboradores devem utilizar os sistemas e recursos da organização de forma segura, seguindo as políticas e procedimentos de segurança estabelecidos.
3. **DISPOSIÇÕES FINAIS**
   1. **APLICAÇÃO**

O Colaborador que não cumprir as diretrizes e as normas internas está sujeito aos processos disciplinares da empresa. Quanto aos Prestadores de Serviços e Fornecedores estão sujeitos à aplicação de sanções cíveis, penais e administrativas.

* 1. **REVISÃO E ATUALIZAÇÃO**

A política deve ser revisada e atualizada anualmente ou quando houver necessidade, para refletir as mudanças dos processos de negócios e as novas ameaças à segurança da informação.

* 1. **CANAIS DE DENÚNCIA**

Para garantir o disposto neste código e a preservação dos recursos de tecnologia e informação, a empresa disponibiliza canais para denúncias de atividades incompatíveis com o disposto nas políticas e normas da empresa. Todas as denúncias podem ser feitas através do e-mail: [segdainformacao@sweetcrystal.com.br](mailto:segdainformacao@sweetcrystal.com.br) ou pelo telefone (31) 4321-0987.

1. **DOCUMENTOS DE REFERÊNCIA**

O presente documento será complementado pelos Procedimentos, Códigos e Normas de Segurança da Informação da SWEETYCRYSTAL e está de acordo com os seguintes documentos:

* **ABNT NBR ISO/IEC 27001:2013** – Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos;
* **ABNT NBR ISO/IEC 27002:2013** – Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação;
* **ABNT NBR ISO/IEC 27014:2013** – Tecnologia da informação — Técnicas de segurança — Governança de segurança da informação;
* **Norma ISO/IEC 27005:2011** – Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação;

**ANEXO II**

**Cartilha de Segurança da Informação**

Junho de 2024

Texto, chat ou mensagem de texto

Descrição gerada automaticamente

Texto, chat ou mensagem de texto

Descrição gerada automaticamente

**APÊNDICE**

**Incidente de Segurança da Informação:** qualquer evento que possa comprometer a confidencialidade, integridade ou disponibilidade da informação da empresa.

**Informação:** qualquer dado ou conjunto de dados que tenha valor para a Empresa, incluindo, mas não se limitando a, dados financeiros, dados de clientes, dados de funcionários, propriedade intelectual e segredos comerciais.

**Sistema de Informação:** qualquer hardware, software, rede ou outro recurso que seja utilizado para processar, armazenar ou transmitir informações.