POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

SUMÁRIO Objetivo

1. Conceitos e Definições

2. Âmbito da Política

3. Diretrizes Gerais

4. Classificação de Informações

5. Competências e Responsabilidades

6. Normas Adicionais

7. Tratamento de Dados

8. Penalidades

9. Considerações Finais

Anexo I – Normas Adicionais - NA

NA01 – Política de Controle de Acesso

NA02 – Política de Acesso a Internet

NA03 – Política de Uso de Equipamentos de Informática

NA04 – Política de uso de e-mail Corporativo

OBJETIVO

O objetivo é estabelecer diretrizes que permitam aos funcionários e colaboradores da Serra e Company seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e da proteção legal da instituição, preservando as informações no tocante a:

· **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

· **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

· **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Dessa forma, busca-se desenvolver um comportamento ético e profissional, para que todos possam utilizar da melhor forma as ferramentas de TI e as informações por elas geradas, ao mesmo tempo, busca-se reduzir ameaças através da adoção de medidas preventivas para evitar possíveis incidentes que tragam prejuízos à instituição.

1. Conceitos e Definições

Para os fins dessa Política, considera-se:

· **Acesso Não Autorizado** - Acesso indevido ou não previsto obtido, por quaisquer meios, procedimentos e a qualquer título, à revelia da política ou do controle de acesso vigentes, ou ainda decorrente de falhas ou imperfeições nos mecanismos de controle de acesso. Contrasta com acesso autorizado.

· **Acesso Lógico** – acesso a redes de computadores, sistemas e estações de trabalho por meio de autenticação;

· **Acesso Remoto** – ingresso, por meio de uma rede, aos dados de um computador fisicamente distante da máquina do usuário;

· **Ameaça** – conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

· **Análise/avaliação de riscos -** processo completo de análise e avaliação de riscos;

· **Ativo** - qualquer bem, tangível ou intangível, que tenha valor para a organização;

· **Ativo da Informação** – os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

· **Auditoria** – verificação e avaliação dos sistemas e procedimentos internos com o objetivo de reduzir fraudes, erros, práticas ineficientes ou ineficazes;

· **Autenticação** – é o ato de confirmar que algo ou alguém é autêntico, ou seja, uma garantia de que qualquer alegação de ou sobre um objeto é verdadeira;

· **Autenticidade** – propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

· **Banco de Dados (ou Base de Dados)** – é um sistema de armazenamento de dados, ou seja, um conjunto de registros que tem como objetivo organizar e guardar as informações;

· **Bloqueio de acesso** – processo que tem por finalidade suspender temporariamente o acesso;

· **Classificação da informação** - atribuição, pela empresa competente, de grau de sigilo dado à informação, documento, material, área ou instalação;

· **Colaborador** – servidores, empregados, contratados por tempo determinado, estagiários e prestadores de serviços que exercem atividades no âmbito da Secretaria de Administração.

· **Confidencialidade** – propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, empresa ou entidade não autorizadas;

· **Contingência** - descrição de medidas a serem tomadas por uma empresa, incluindo a ativação de processos manuais, para fazer com que seus processos vitais voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada que possa gerar maiores prejuízos à corporação;

· **Controle de Acesso** - conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

· **Cópia de Segurança (Backup)** – copiar dados em um meio separado do original, de forma a protegê-los de qualquer eventualidade. Essencial para dados importantes;

· **Correio Eletrônico** - é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação;

· **Credenciais ou contas de acesso** - permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário e senha;

· **Criptografia** – é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta");

· **Dado** – representação de uma informação, instrução, ou conceito, de modo que possa ser armazenado e processado por um computador;

· **Disponibilidade** - propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

· **Download** - (Baixar) copiar arquivos de um servidor (site) na internet para um computador pessoal;

· **Gestão de Continuidade de Negócios** - Processo de gestão global que identifica os potenciais ameaças para uma organização e os impactos nas operações da instituição que essas ameaças, se concretizando, poderiam causar, e fornecendo e mantendo um nível aceitável de serviço face a rupturas e desafios à operação normal do dia-a-dia;

· **Gestão de Risco** – conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

· **Gestão de Segurança da Informação e Comunicações** - conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

· **Gestor da Informação** - pessoa responsável pela administração de informações geradas em seu processo de trabalho e/ou sistemas de informação relacionados às suas atividades;

· **Gestor de Segurança da Informação e das Comunicações** – é responsável pelas ações de segurança da informação e comunicações no âmbito da empresa.

· **Hardware** – É a parte física do computador, conjunto de componentes eletrônicos, circuitos integrados e periféricos, como a máquina em si, placas, impressora, teclado e outros;

· **Incidente de Segurança** - é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

· **Informação** - dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

· **Informação sigilosa** - informação submetida temporariamente à restrição de acesso em razão de sua imprescindibilidade para a segurança da empesa, e aquelas abrangidas pelas demais hipóteses legais de sigilo;

· **Integridade** – propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

· **Internet** – rede mundial de computadores;

· **Intranet –** rede de computadores privada que faz uso dos mesmos protocolos da Internet. Pode ser entendida como rede interna de alguma instituição em que geralmente o acesso ao seu conteúdo é restrito;

· **Log** - é o termo utilizado para descrever o processo de registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para reestabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento passo a passo. Um arquivo de log pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais;

· **Logon** - Procedimento de identificação e autenticação do usuário nos Recursos de Tecnologia da Informação. É pessoal e intransferível;

· **Norma** - Documento interno que regulamenta formal e administrativamente, de maneira geral ou específica, aspectos ou diretrizes expressas na PSI, no todo ou em parte da instituição. As normas mapeiam a PSI na organização técnico-administrativa da instituição, estabelecendo regras para a sua implementação.

· **Peer-to-peer (P2P)** – (Ponto a ponto) permite conectar o computador de um usuário a outro, para compartilhar ou transferir dados, como MP3, jogos, vídeos, imagens, entre outros;

· **Perfil de acesso** - conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

· **Política de Segurança da Informação (PSI)** – documento aprovado pela autoridade responsável pelo órgão, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação na instituição;

· **Protocolo** - convenção ou padrão que controla e possibilita uma conexão, comunicação, transferência de dados entre dois sistemas computacionais. Método padrão que permite a comunicação entre processos, conjunto de regras e procedimentos para emitir e receber dados numa rede;

· **Proxy** - é um serviço intermediário entre as estações de trabalho de uma rede e a Internet. O servidor de rede proxy serve para compartilhar a conexão com a Internet, melhorar o desempenho do acesso, bloquear acesso a determinadas páginas;

· **Recursos Computacionais** - recursos que processam, armazenam e/ou transmitem informações, tais como aplicações, sistemas de informação, estações de trabalho, notebooks, servidores de rede, equipamentos de conectividade e infraestrutura;

· **Rede Corporativa** - conjunto de todas as redes locais sob a gestão da empresa ou instituição;

· **Rede Pública** – rede de acesso a todos;

· **Responsabilidade** - Obrigações e deveres decorrentes da legislação vigente, ofício, cargo, função ou por força de contrato, na proteção dos ativos de informação de qualquer natureza.

· **Senha ou Credencial de Acesso** - Credencial que concede, de maneira prevista, o direito de acesso, físico ou lógico, a determinado ativo de informação de qualquer natureza, ou local que o abrigue. Uma senha ou credencial fraca é toda aquela que não obedece aos critérios e requisitos mínimos de qualidade vigentes.

· **Servidor de Rede** - recurso de TI com a finalidade de disponibilizar ou gerenciar serviços ou sistemas informáticos;

· **Software** - são todos os programas existentes em um computador, como sistema operacional, aplicativos, entre outros;

· **Site** - Conjunto de páginas virtuais dinâmicas ou estáticas, que tem como principal objetivo fazer a divulgação da instituição;

· **Streaming** - transferência de dados (normalmente áudio e vídeo) em fluxo contínuo por meio da Internet;

· **Termo de Responsabilidade** - termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

· **Tratamento de Incidentes de Segurança em Redes Computacionais** - serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

· **Usuário** – funcionários e colaboradores, clientes que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de uma empresa , formalizada por meio da assinatura do Termo de Responsabilidade;

· **VLAN (Virtual Local Area Network ou Virtual LAN)** – (Rede Local Virtual) é um agrupamento lógico de estações, serviços e dispositivos de rede que não estão restritos a um segmento físico de uma rede local;

· **VPN (Virtual Private Network)** – (Rede Privada Virtual) é uma rede de dados privada que faz uso das infraestruturas públicas de telecomunicações, preservando a privacidade, logo é a extensão de uma rede privada que engloba conexões com redes compartilhadas ou públicas. Com uma VPN pode-se enviar dados entre dois computadores através de uma rede compartilhada ou pública de uma maneira que emula uma conexão ponto a ponto privada;

· **Vulnerabilidade** - conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação;

· **Wireless (rede sem fio)** - rede que permite a conexão entre computadores e outros dispositivos através da transmissão e recepção de sinais de rádio.

2. Âmbito da Política

2.1. As diretrizes aqui estabelecidas deverão ser seguidas por todos os funcionários e colaboradores que exercem atividades no âmbito da empresa que foi lhe dada o direito ao acesso aos dados da informação em qualquer meio ou suporte.

2.2. Esta política dá ciência a funcionário e colaborador de que os ambientes, sistemas, computadores e redes da empresa são monitorados e gravados conforme previsto nas leis brasileiras.

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

3. Diretrizes Gerais

3.1. Todos os mecanismos de proteção utilizados para a segurança da informação devem ser mantidos para preservar a continuidade do negócio;

3.2. Toda informação gerada pelos colaboradores, utilizando integralmente ou parcialmente recursos da Serra e Company.;

3.3. Ameaças e riscos devem ser reavaliados periodicamente para garantir que a organização esteja efetivamente protegida.

3.4. O acesso às informações, produzidas ou recebidas pela área de TI, deve ser limitado às atribuições necessárias ao desempenho das respectivas atividades dos usuários internos e externos;

3.5. Os processos de aquisição ou contratação de bens e serviços de tecnologia da informação, a qualquer título, devem refletir a PSI e seus documentos acessórios;

3.6. Os equipamentos de informática e comunicação, sistemas e informações deverão ser utilizados para a realização das atividades profissionais.

3.7. Esta política de Segurança da Informação pode ser revisada periodicamente e eventualmente revista sempre que eventos ou fatos relevantes ocorram;

3.8. Os funcionários e colaboradores devem evitar a circulação das informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito “mesa limpa”, ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

4. Classificação da Informação

4.1. É de responsabilidade do Gerente/Supervisor de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com a tabela abaixo:

· **Pública -** É toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e público em geral.

· **Interna** - É toda informação que só pode ser acessada por funcionários da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.

· **Confidencial** - É toda informação que pode ser acessada por usuários da organização e por parceiros da organização. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro.

· **Restrita** - É toda informação que pode ser acessada somente por usuários da organização explicitamente indicado por seus diretores ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

5. Competências e Responsabilidades

5.1. Gerencia de TI: − Tem a função de assegurar que a implementação dos controles de segurança da informação tenha um alto nível de segurança e permite controle em toda a organização − Apoiar a Política e manter compromisso com sua continuidade e resultados.

5.2. Gerência de Tecnologia da Informação

– Promover cultura de segurança da informação e comunicações;

− Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

− Propor recursos necessários às ações de segurança da informação e comunicações;

− Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

− Propor Normas Adicionais e Procedimentos de Segurança da Informação e das Comunicações;

− Planejar e coordenar a execução dos programas, planos, projetos e ações de segurança da informação;

− Apurar os incidentes de segurança críticos e encaminhar os fatos apurados para aplicação das penalidades previstas;

− Supervisionar, analisar e avaliar a efetividade dos processos, procedimentos, sistemas e dispositivos de segurança da informação;

− Identificar controles físicos, administrativos e tecnológicos para mitigação do risco;

− Recepcionar, organizar, armazenar e tratar adequadamente as informações de eventos e incidentes de segurança, determinando aos respectivos gestores as ações corretivas ou de contingência em cada caso;

5.3. Cabe aos Funcionários e Colaboradores:

− Cumprir com todas as diretrizes e normas estabelecidas por esta política;

− Estar sempre atualizado e ciente das políticas, normas e procedimentos vigentes da empresa Serra e Company;

− Não divulgar, compartilhar, transmitir ou deixar-se conhecer informações a pessoas que não tenham nível de autorização suficiente;

− Não conduzir, transportar, enviar, transmitir, compartilhar ou deixar que dados e informações alcancem ambiente ou destinatário fora das dependências da empresa sem autorização formal dos Diretores.

5.4. Cabe ao Departamento de Recurso Humano

− Informar ao setor de tecnologia da informação todos os desligamentos, afastamentos, retornos e modificações no quadro funcional da empresa.

5.5. Cabe à Diretoria

- Prestar assessoramento de natureza jurídica, supervisionar e coordenar as atividades de natureza jurídica, inclusive aquelas relacionadas com a elaboração de atos normativos.

5.6. A Serra e Company deverá prestar apoio de natureza jurídica, na análise do não cumprimento pelos funcionários e colaborador das normas estabelecidas para a utilização da rede da instituição.

7. Tratamento da Informação

Diretrizes específicas e procedimentos próprios de tratamento da informação corporativa deverão ser fixados em norma complementar, considerando as seguintes diretrizes gerais:

A. Documentos imprescindíveis para as atividades dos usuários da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores, não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

B. Arquivos pessoais e/ou não pertinentes às atividades institucionais da SERRA E COMPANY (fotos, músicas, vídeos, etc..) não deverão ser copiados ou movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificados, os arquivos poderão ser excluídos definitivamente sem necessidade de comunicação prévia ao usuário.

Tratamento de Incidentes em Redes Computacionais é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências”.

A ocorrência de incidentes de segurança em redes de computadores da SERRA E COMPANY deverá ser comunicada ao DPO – Data Protection Officer, conforme procedimentos a serem definidos com vistas a permitir que sejam dadas soluções integradas, bem como a geração de estatísticas.

No tratamento de incidentes em redes computacionais, a Equipe Técnica de Segurança da Informação, responsável pelo tratamento e resposta ao incidente, deverá considerar, no mínimo, as seguintes diretrizes:

A. Todos os incidentes notificados ou detectados deverão ser registrados, com a finalidade de assegurar registro histórico das atividades desenvolvidas.

B. O tratamento da informação deverá ser realizado de forma a viabilizar e assegurar disponibilidade, integridade, confidencialidade e autenticidade da informação, observada a legislação em vigor, naquilo que diz respeito ao estabelecimento de graus de sigilo.

C. Durante o gerenciamento de incidentes de segurança em redes de computadores, havendo indícios de ilícitos criminais, o Gestor de Segurança da Informação ou membros da Equipe Técnica de Segurança da Informação tem como dever, sem prejuízo de suas demais atribuições, acionar as autoridades policiais competentes para a adoção dos procedimentos legais julgados necessários, observar os procedimentos para preservação das evidências, exigindo consulta às orientações sobre cadeia de custódia, e priorizar a continuidade dos serviços do SERRA E COMPANY.

8. Penalidades

A SERRA E COMPANY, ao gerir e monitorar seus ativos de informação, pretende garantir a integridade destes, juntamente com suas informações e recursos. O descumprimento ou inobservância de quaisquer regras ou diretrizes definidas nesse instrumento e em suas normas complementares constituem falta grave, às quais a SERRA E COMPANY responderá com a aplicação de todas as medidas administrativas, cíveis e judiciais cabíveis.

Toda tentativa de alteração dos parâmetros de segurança, por qualquer usuário, sem o devido credenciamento e a autorização para tal, será considerada

inadequada e os riscos relacionados serão informados ao usuário e ao respectivo gestor.

O uso de qualquer recurso em inobservância das normas vigentes ou para prática de atividades ilícitas poderá acarretar ações administrativas e penalidades decorrentes de processos administrativo, civil e criminal, em que a instituição cooperará ativamente com as autoridades competentes.

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a SERRA E COMPANY e/ou terceiros.

Portanto, o usuário vinculado a tais dispositivos identificadores será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal), sendo que o uso dos dispositivos e/ou senhas de identificação de outra pessoa viola as regras de segurança e poderá resultar na aplicação de medidas administrativas, cíveis e judiciais cabíveis.

9. Considerações Finais

9.1. Os casos omissos e dúvidas serão submetidos à Gerência de Tecnologia da Informação.

10. Normas Adicionais

10.1. O detalhamento da Política de Segurança da Informação está segmentado nas seguintes Normas Adicionais:

10.1.1. NA 01 - Política de Controle de Acesso;

10.1.2. NA 02 - Política de Acesso a Internet;

10.1.3. NA 03 - Política de uso de Equipamentos de Informática;

10.1.4. NA 04 – Política para uso do e-mail corporativo.

ANEXO I

NORMAS ADICIONAIS

NA 01 – Política de Controle de Acesso

1. Objetivo

Estabelecer critérios para a disponibilização e administração do acesso aos serviços de tecnologia de informação da Serra e Company, bem como estabelecer critérios relativos às senhas das respectivas contas.

2. Diretrizes Gerais

2.1. A conta de acesso é o instrumento para identificação do usuário na rede dos funcionários e colaboradores e caracteriza-se por ser de uso individual e intransferível e sua divulgação é vedada sob qualquer hipótese;

2.2. Todo cadastramento de conta de acesso à rede da Serra e Company deve ser efetuado mediante solicitação via e-mail da chefia imediata a Gerência de tecnologia da informação.

2.3. Qualquer utilização, por meio da identificação e da senha de acesso, é de responsabilidade do usuário aos quais as informações estão vinculadas;

2.4. Todas as senhas, de usuários comuns, para autenticação na rede da Serra e Company devem seguir os seguintes critérios mínimos:

· Toda senha deve ser constituída de, no mínimo, 8 caracteres sendo obrigatório o uso de caracteres alfanuméricos (letras e números);

· A senha não poderá conter parte do nome do usuário, por exemplo: se o usuário se chama Jose da Silva, sua senha não pode conter partes do nome como "1221jose" ou "1212silv";

· A data de expiração da senha deve ser de no máximo 90 dias, caso não seja alterada, esta será bloqueada;

· Será obrigatória a troca de senha ao efetuar o primeiro acesso;

· Não será permitida a repetição das 5 últimas senhas já utilizadas;

2.5. A base de dados de senhas deve ser armazenada com criptografia;

2.6. O acesso aos serviços de tecnologia de informação da Serra e Company deve ser disponibilizado aos colaboradores que oficialmente executem atividade vinculada à atuação a empresa Serra e Company;

2.7. O processo de aprovação do acesso deve ser iniciado pelo superior do usuário e os privilégios garantidos continuarão em efeito até que o usuário mude suas atividades ou deixe a empresa. Se um desses dois eventos ocorrer, a chefia deverá notificar imediatamente ao Departamento de TI.

2.8. Qualquer anormalidade percebida pelo usuário quanto ao privilégio de seu acesso aos recursos de tecnologia da informação deve ser imediatamente comunicada a Gerência de Tecnologia da Informação;

2.9. As contas com privilégio de administração de rede devem ser utilizadas somente para execução das atividades correspondentes à administração do ambiente conforme as responsabilidades atribuídas. As variáveis necessárias para acesso e administração devem ser de conhecimento restrito aos administradores dos equipamentos de rede.

2.10. Em caso de comprometimento comprovado da segurança do ambiente de TI por algum evento não previsto, todas as senhas de acesso deverão ser modificadas.

3. Acesso Remoto

3.1. O acesso remoto aos serviços corporativos somente deve ser disponibilizado aos colaboradores que, oficialmente, executem atividades vinculadas à empresa Serra e Company, desde que solicitado pela gerência responsável pela informação.

3.2. A liberação de acesso remoto só será efetivada após avaliação e aprovação pela Gerência de Tecnologia da Informação, para que se evitem ameaças à integridade e sigilo das informações contidas na rede;

3.3. As Conexões remotas à rede da Serra e Company devem ocorrer da seguinte maneira:

I. Utilização de autenticação;

II. As senhas e as informações que trafegam entre a estação remota e a rede da SC devem estar criptografadas;

III. É vedada a utilização do acesso remoto para fins não relacionados às atividades da instituição.

3.4. O serviço de acesso remoto deve ser cancelado sob as seguintes condições:

I. Finalização do período solicitado ou termino do Contrato;

II. Perda da necessidade de utilização do serviço;

III. Transferência do usuário para outras unidades;

IV. Identificação de vulnerabilidade, risco ou uso indevido.

4. Acesso a Base de Dados;

4.1. O acesso a base de dados Serra e Company dar-se-á por meio de senha de uso pessoal e intransferível, vedada sua divulgação;

4.2. É vedado ao usuário o acesso a base de dados Serra e Company, para pesquisa de dados corporativo com o objetivo de:

I. Compartilhar sem autorização da chefia imediata, no todo ou em parte, as informações contidas na base de dados corporativos;

4.3. É de responsabilidade do usuário que possui acesso as bases de dados da Serra e Company:

I. Manter em sigilo sua senha de acesso as bases de dados da Serra e Company;

II. Fechar o aplicativo de acesso a base de dados toda vez que se ausentar, evitando o acesso indevido;

4.4. Do acesso a base de dados Serra e Company:

4.4.1. Deverá ser firmado termo de responsabilidade, pelo órgão solicitante, sobre as informações disponibilizadas.

4.4.2. A responsabilidade da guarda dos dados obtidos através de integrações entre sistemas deverá ser do órgão solicitante.

5. Controle de Acesso Físico

5.1. Os controles de acesso físico visam restringir o acesso aos equipamentos de tecnologia da informação;

5.2. O acesso ao Datacenter somente poderá ser feito por pessoas autorizadas;

5.3. O acesso de visitantes ou terceiros ao Datacenter somente poderá ser realizado com acompanhamento de um colaborador da área de tecnologia de informação da SC;

NC 02 - Política de Acesso à Internet

1. Objetivo

Estabelecer critérios para administração e utilização de acesso aos serviços de Internet no âmbito da Serra e Company.

Diretrizes Gerais

2.1. O acesso à Internet deve restringir-se à esfera profissional com conteúdo relacionado às atividades desempenhadas pela empresa;

2.2. Cada usuário é responsável pelas ações e acessos realizados por meio da sua Conta de Acesso;

2.3. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, 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 desta Política de Segurança da Informação;

2.4. Toda alteração de nível de acesso somente será realizada mediante solicitação formal, pela chefia imediata do usuário, contendo a devida justificativa, que será avaliada pela Gerencia de Tecnologia da Informação - GTI, podendo esta solicitação ser negada em caso de risco ou vulnerabilidade a segurança e a integridade da rede da Serra e Company;

2.5. É vedado acessar páginas de conteúdo considerado ofensivo, ilegal ou impróprio, tais como:

a. Pornografia, pedofilia, preconceitos, vandalismo, entre outros;

b. Acessar ou obter na Internet arquivos que apresentem vulnerabilidade de segurança ou possam comprometer, de alguma forma, a segurança e a integridade da rede da Serra e Company;

c. Uso recreativo da internet em horário de expediente;

d. Uso de proxy anônimo; e. Acesso a rádio e TV em tempo real, exceto os canais corporativos em horário de expediente;

f. Acesso a jogos;

g. Acesso a outros conteúdos notadamente fora do contexto do trabalho desenvolvido;

h. Envio a destino externo de qualquer software licenciado à SC ou dados de sua propriedade ou de seus usuários, salvo expressa e fundada autorização do responsável pela sua guarda;

i. Contorno ou tentativa de contorno às políticas de bloqueios automaticamente aplicadas pelas ferramentas sistêmicas da SC;

j. Utilização de softwares de compartilhamento de conteúdo na modalidade peer-to-peer (P2P);

2.6. Caso a empresa julgue necessário, haverá bloqueios de acesso a arquivos e sites não autorizados que comprometam o uso de banda da rede, o desempenho e

produtividade das atividades do colaborador, bem como, que exponham a rede a riscos de segurança;

2.7. É proibido utilizar os recursos da SC para fazer o download ou distribuição de software ou dados não legalizados;

2.8. Haverá auditoria dos sites acessados por usuário para verificação da adequação à política vigente;

2.9. Comprovada a utilização irregular, o usuário envolvido poderá ter o seu acesso à Internet bloqueado, sendo comunicado o fato à chefia imediata, podendo incorrer em processo administrativo disciplinar e nas sanções legalmente previstas, assegurados o contraditório e a ampla defesa.

NC 03 – Política de Uso de Equipamentos de Informática

1. Objetivo

Estabelecer critérios na utilização dos equipamentos de informática na empresa.

2. Diretrizes Gerais

2.1. Os recursos computacionais somente devem ser utilizados para a execução de atividades de interesse da empresa;

2.2. Cada estação de trabalho possui controle de IP (Protocol Internet), os quais permitem que ela seja identificada na rede. Sendo assim, tudo que for executado na estação de trabalho será de responsabilidade do usuário. Por isso, sempre que ausentar do ambiente de trabalho tenha certeza que efetuou o logof ou bloqueou a estação de trabalho;

2.3. Não é permitido gravar nas estações de trabalho e na Rede da SC, MP3, filmes, fotos e software com direitos autorais ou qualquer outro tipo que possa ser considerado pirataria;

2.4. Todos os dados relativos às atividades da empresa devem ser mantidos no servidor de rede, onde existe sistema de backup diário e confiável;

2.5. Os arquivos gravados em diretórios temporários (pastas públicas) podem ser acessos por todos os usuários que utilizarem a rede local, portanto não garante sua integridade, podendo ser alterados ou excluídos sem prévio aviso e por qualquer usuário;

2.6. Não será feito cópia de segurança dos arquivos criados no computador local dos funcionários e colaboradores. O próprio usuário deve fazer cópia de segurança dos arquivos locais e verificar o que pode ser eliminado, evitando acumulo de dados desnecessários;

2.7. É proibida a abertura de computadores para qualquer tipo de reparo, caso seja necessário o reparo deverá ocorrer pela Gerência de Tecnologia da Informação;

2.8. Quanto à utilização de equipamentos de informática particulares (celulares, notebooks, tablets e/ou qualquer dispositivos móveis que venham acessar a rede sem fio ou rede estruturada) o colaborador deverá comunicar a chefia imediata, que solicitará sua liberação de acesso através da Gerência de Tecnologia da Informação;

2.9. Em caso de eventos no ambiente da empresa, tais como, seminários e cursos, etc, deverá ser solicitado à Gerência de Tecnologia da Informação – GTI;

2.10. Em caso de dano, inutilização ou extravio do equipamento o colaborador deverá comunicar imediatamente à Gerência de Tecnologia da Informação que deverá adotar as providências cabíveis;

2.11. Em caso de furto ou roubo, providenciar Boletim de Ocorrência junto à Polícia Civil e entregá-lo na Gerência de Tecnologia da Informação, que deverá adotar as providências cabíveis;

2.12. É obrigatória a vinculação dos componentes (gabinete, monitor, teclado e mouse), conforme nºs de ativos, impedindo a sua utilização para outro usuário que não assina o Termo de Responsabilidade;

2.13. É proibida a colocação de adesivos com imãs nos equipamentos;

2.14. É dever do colaborador zelar pela integridade do equipamento estritamente como instrumento de trabalho, juntamente com os acessórios que foram utilizados;

2.15. É de inteira responsabilidade dos funcionários e colaboradores ao receber o Termo de Responsabilidade, verificar as informações nele contidas como o nº. Ativo Fixo, série, além dos seus dados pessoais, matrícula e unidade de trabalho;

2.16. Não é permitido alterar as configurações de rede e da BIOS das máquinas, bem como, efetuar qualquer modificação que possa causar algum problema futuro;

2.17. Não é permitido retirar ou transportar qualquer equipamento de informática da SC sem autorização prévia da Gerência de Tecnologia da Informação;

2.18. Fica proibida a utilização, sem devido consentimento, da utilização de equipamentos de informática por pessoas sem vínculo com a empresa;

2.19. É vedado retirar e/ou danificar placas identificadoras de patrimônio, travas e lacres de segurança dos equipamentos de informática;

2.20. Não é permitido conectar e/ou configurar equipamento à rede, sem a prévia liberação da Gerência de Tecnologia da Informação;

2.21. O antivírus deve estar atualizado e com a autoproteção ativa na estação de trabalho;

2.22. O usuário deve obrigatoriamente executar o antivírus nos dispositivos removíveis antes de sua abertura quando inseridos na estação de trabalho.

3. Política de Backup e Restauração de Arquivos

3.1. Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente em horários em que não há nenhum ou pouco acesso de usuários ou processos aos sistemas de informática e arquivos.

3.2. Backups Incrementais Arquivos (Incremental diários) serão realizados de segunda à quinta-feira, realizados a partir das 20:00h., com um mês de retenção;

3.3. Os Backups completos Arquivos (completo semanais) são realizadas as sextas feiras de cada semana, realizados a partir das 20:00h., com um mês de retenção;

3.4. Os Backups completos da Maquinas Virtuais (full semanais) serão realizados na primeira sexta-feira da semana, realizados a partir das 20:00h., com uma semana de retenção;

3.5. A restauração de Arquivos só será possível em dados nos quais foram gerados backup no dia anterior;

3.6. Restauração de arquivo terá um prazo Máximo de 30 dias, não sendo possível recuperar arquivos mais antigos que esse período;

3.7. Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros;

3.8. As mídias de backup em HD devem ser acondicionadas em local seco, climatizado, seguro e distantes o máximo possível do Datacenter;

3.9. Mídias que apresentam erros devem primeiramente ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas.

4. Política de uso de impressoras

4.1. Todas as impressões deverão ser executas nas suas respectivas gerências;

4.2. Não é permitido imprimir documentos que não estejam dentro das atividades de trabalho;

4.3. Não é permitido deixar impressões erradas na mesa das impressoras;

4.4. Os colaboradores podem utilizar “senha segura” para a segurança e proteção de seus documentos;

4.5. Os documentos deverão preferencialmente ser impressos frente e verso, para economia de papel.

NC 04 – Política de Uso de E-mail Corporativo

1. Objetivo

Estabelecer critérios para disponibilização do serviço de correio eletrônico corporativo da Serra e Company aos usuários.

2. Diretrizes Gerais

2.1. O serviço de correio tem como finalidade o envio e o recebimento eletrônico de mensagens e documentos relacionados com as funções institucionais da Secretaria de Administração;

2.2. São usuários do serviço de correio eletrônico corporativo, os funcionários e colaboradores que executem atividade vinculada à atuação institucional da SC;

2.3. A concessão de contas de correio eletrônico depende de pedido da chefia imediata;

2.4. Poderá ser solicitada a criação de listas de distribuição, restritas aos seus respectivos âmbitos de atuação;

2.5. É vedado o acesso ao conteúdo das mensagens tramitadas por meio do serviço de correio eletrônico corporativo, salvo nas hipóteses previstas em lei;

2.6. O acesso ao serviço de correio eletrônico dar-se-á por meio de senha de uso pessoal e intransferível, vedada sua divulgação;

2.7. É vedado ao usuário o uso do serviço de correio eletrônico corporativo com o objetivo de:

I. Praticar crimes e infrações de qualquer natureza;

II. Executar ações nocivas contra outros recursos computacionais da SC ou de redes externas;

III. Distribuir material obsceno, pornográfico, ofensivo, preconceituoso, discriminatório, ou de qualquer forma contrário à lei e aos bons costumes;

V. Disseminar anúncios publicitários, mensagens de entretenimento e mensagens do tipo “corrente”, vírus ou qualquer outro tipo de programa de computador que não seja destinado ao desempenho de suas funções ou que possam ser considerados nocivos ao ambiente de rede da SC;

VI. Enviar arquivos de áudio, vídeo ou animações, salvo os que tenham relação com as funções institucionais desempenhadas pela SC;

VII. Divulgar, no todo ou em parte, os endereços eletrônicos corporativos constantes do catálogo de endereços do serviço;

VIII. Executar outras atividades lesivas, tendentes a comprometer a intimidade de usuários, a segurança e a disponibilidade do sistema, ou a imagem institucional. É de responsabilidade do usuário do correio eletrônico:

III. Manter em sigilo sua senha de acesso ao correio eletrônico;

IV. Fechar o aplicativo de correio (cliente) toda vez que se ausentar, evitando o acesso indevido;

V. Comunicar imediatamente a Gerência de Tecnologia da Informação, preferencialmente através do endereço usinf@SC.pe.gov.br, do recebimento de mensagens com vírus ou que venham a trazer algum tipo de dano aos sistemas de informática;

VI. Efetuar a manutenção de sua caixa postal, evitando ultrapassar o limite de armazenamento e garantindo o seu funcionamento contínuo.

· É de responsabilidade da Gerência de Tecnologia da Informação:

I. Criar e manter cadastro dos usuários, das caixas postais e das listas de distribuição;

II. Cancelar os acessos ao serviço de correio eletrônico dos usuários que se desvincularem da empresa;

III. Propor a divulgação de orientação sobre o uso correto do correio eletrônico;

IV. Fiscalizar a utilização do serviço de correio eletrônico, observados os critérios estabelecidos nesta norma;

V. Desenvolver demais ações que garantam a operacionalização desta norma.